ICAO

Doc 9859

Emniyet Yönetimi El Kitabı

Dördüncü Baskı, 2018

Genel Sekreterin yetkisi dahilinde onaylanmış ve yayınlanmıştır.

ULUSLARARASI SİVİL HAVACILIK TEŞKİLATI

ICAO

Doc 9859

Emniyet Yönetimi El Kitabı

Dördüncü Baskı, 2018

Genel Sekreterin yetkisi dahilinde onaylanmış ve yayınlanmıştır

ULUSLARARASI SİVİL HAVACILIK TEŞKİLATI

ULUSLARARASI SİVİL HAVACILIK TEŞKİLATI tarafından
İngilizce, Arapça, Çince, Fransızca, Rusça ve İspanyolca
baskılar halinde ayrı olarak yayınlanmıştır

999 Robert-Bourassa Boulevard, Montréal, Quebec, Kanada H3C 5H7

Sipariş bilgileri ve satış acentelerin ile kitapçılara ilişkin tam liste
için www.icao.int adresinde bulunan ICAO İnternet sitesini ziyaret
ediniz.

Birinci baskı, 2006
Üçüncü baskı, 2013
Dördüncü baskı, 2018

Doc 9859, *Emniyet Yönetimi El Kitabı*
Sipariş Numarası: 9859
ISBN 978-92-9258-552-5

ÖNSÖZ

Emniyet Yönetimi El Kitabının (SMM) bu dördüncü baskısı, 2013 yılının Mayıs ayında yayınlanan üçüncü baskıyı tümüyle yürürlükten kaldırarak söz konusu baskının yerini almaktadır. Bu baskının geliştirilmesine, söz konusu tadil ile getirilen değişikliklerin ele alınması ve son revizyondan itibaren kazanılan bilginin ve deneyimin yansıtılması için, Annex 19'a 1 sayılı Revizyonun kabulü sonrasında başlanmıştır.

Emniyet yönetimi uygulayarak geniş bir yelpazeye yayılan havacılık topluluğunun ihtiyaçlarına ve 2015 yılında gerçekleştirilen ikinci Üst Düzey Emniyet Konferansından ileri gelen tavsiyeye işaret etmek üzere, Emniyet Yönetimi El Kitabına (SMM) tamamlayıcı nitelikte olmak ve en iyi uygulamaların paylaşımına yönelik bir bilgi havuzu olarak hizmet etmek üzere Emniyet Yönetimi Uygulama (SMI) web sitesi (www.icao.int/SMI) oluşturulmuştur. Söz konusu web sitesinde, uygulamalı örnekler, araçlar ve destekleyici eğitici materyal süreklilik esasına dayalı olarak toplanacak, gözden geçirilecek ve ilan edilecektir.

Bu baskı, etkin Devlet emniyet programlarının (SSP) uygulanmasında Devletlere destek vermeyi amaçlamaktadır. Hizmet sağlayıcıları tarafından Annex 19 hükümlerine uygun olarak emniyet yönetimi sistemlerinin (SMS) uygulanmasının sağlanması buna dahildir. Emniyet yönetimi ilkeleriyle tutarlı olabilmek için, aşırı derecede kural koyucu olmaktan kasıtlı olarak sakınarak her bir Standart ve Tavsiye Edilen Uygulamanın (SARP) amaçlanan sonucuna odaklanmak üzere birbiriyle uyumlu çalışmalar yapılmıştır. Emniyet yönetiminin her bir organizasyon tarafından kendine özgü ortama uygun olacak şekilde uyarlanmasına önem verilmiştir.

Not 1.— Bu el kitabında, "organizasyon" terimi, gerek Devletlere gerek hizmet sağlayıcılarına atıfta bulunmak üzere kullanılmaktadır.

Not 2.— Bu el kitabında, "hizmet sağlayıcısı" terimi, söz konusu terimin, uluslararası genel havacılık işletmelerinin hariç tutulduğu, 3. Bölüm kapsamında yer alan ziyadesiyle spesifik bir organizasyonlar listesine atıfta bulunmak üzere kullanıldığı Annex 19'un aksine, ister zorunlu ister gönüllü esasta olsun, SMS uygulayan herhangi bir havacılık sektörü organizasyonuna atıfta bulunmak üzere kullanılmaktadır.

Dördüncü baskı, okuyucu tarafından emniyet yönetiminin dereceli olarak anlaşılmasını sağlayan dokuz bölüme ayrılmıştır. Bu bölümler, aşağıdaki üç tema kapsamında gruplandırılabilir:

1) *Emniyet yönetimi ana esasları* – Emniyet yönetimini destekleyen temel prensiplerin okuyucu tarafından anlaşılmasına yönelik 1. ila 3. Bölüm.

2) *Emniyet istihbaratının oluşturulması* – Ana esaslara dayalı olarak geliştirilmiş 4. ila 7. Bölüm. Bu bölümler, kaynakların en etkin ve verimli kullanımına ilişkin olanlar da dahil olmak üzere, veriye dayalı kararlar almak üzere herhangi bir organizasyonun liderliği tarafından kullanılabilen, eyleme geçirilebilir iç görülerin oluşturulmasına yönelik olarak emniyet verilerinin ve emniyet bilgilerinin desteklenmesine ilişkin olarak birbirleriyle ilişkili başlıktan oluşmaktadır.

3) *Emniyet yönetimi uygulaması* – 8. ve 9. Bölüm kapsamında, önceki bölümlerden elde edilen kavramların Devlet ve hizmet sağlayıcısı seviyesinde emniyet yönetiminin kurumsallaştırılması için nasıl uygulanması gerektiği açıklanmaktadır.

Bu el kitabında, Annex 19 kapsamı dışında yer alan, sektöre özgü emniyet yönetimi Standart ve Tavsiye Edilen Uygulamaların (SARP'ler) (örneğin, uçuş veri analizi programları) desteklenmesine yönelik kılavuzluğa yer verilmemektedir. *Hava Aracı Kaza ve Olay Soruşturması* adlı Annex 13'e uygun olarak bağımsız Devlet kaza ve olay soruşturmalarının yürütülmesine yönelik kılavuzluk, *Hava Aracı Kaza ve Olay Soruşturması El Kitabı* kapsamında yer almaktadır.

ICAO, katkılarından dolayı, Emniyet Yönetimi Heyeti (SMP) ile Emniyet Bilgileri Koruma Uygulama Grubu'na (SIP IG) ve bu el kitabına destek, tavsiye ve girdi sağlayan diğer uzman gruplara ve münferit uzmanlara teşekkürü borç bilir. Söz konusu içerik iki yılın üzerinde bir süre boyunca oluşturulmuş ve akabinde, bu el kitabının geniş bir topluluk için emniyet yönetimine yönelik kapsayıcı bir kılavuz materyal olmasının beklenildiği göz önünde bulundurularak uzman topluluğunun yorumlarını toplamak ve dikkate almak üzere, görevdaşların kapsamlı gözden geçirmesine sunulmuştur.

Bilhassa uygulanmasına ve kullanışlılığına ilişkin olmak üzere, bu el kitabına ilişkin olarak tüm Devletlerden, emniyet gözetimi denetim heyetlerinden ve ICAO teknik işbirliği alanındaki heyetlerden gelecek yorumlar takdir ile karşılanacaktır. Müteakip baskıların hazırlanmasında bu yorumlar dikkate alınacaktır. Yorumlar aşağıdaki adrese iletilmelidir:

Genel Sekreter
Uluslararası Sivil Havacılık Teşkilatı
999 Robert-Bourassa Boulevard
Montréal, Quebec
Kanada, H3C 5H7

İÇİNDEKİLER

Sayfa

SÖZLÜKÇE

TANIMLAR

Aşağıdaki terimler, bu el kitabında kullanıldıklarında aşağıda belirtilen anlamlara sahip olacaklardır.

Not.— Herhangi bir terimin yanında yıldız işareti olduğunda, söz konusu terim daha önceden Annex'lerde ve Hava Seyrüsefer Hizmetlerine İlişkin Usuller (PANS) kapsamında tanımlanmıştır.

Kabul edilebilir emniyet performansı seviyesi (ALoSP). Söz konusu Devletin Devlet emniyet programında tanımlanarak emniyet performansı hedefleri ve emniyet performansı göstergeleri bakımından ifade edilerek herhangi bir Devletteki sivil havacılık sistemi için ulaşılmak üzere Devlet otoriteleri tarafından kabul edilen emniyet performansı seviyesi.

Sorumlu yetkili. Hizmet sağlayıcısının Emniyet Yönetimi Sisteminin (SMS) etkin ve verimli performansından sorumlu olan, belirlenebilir tek kişi.

Değişim yönetimi. Herhangi bir organizasyonun bünyesindeki değişikliklerin, bu tür değişikliklerin uygulanması öncesinde, belirlenen tehlikelere ve risk hafifletme stratejilerine etki edebilecek olan değişiklikler göz önünde bulundurulacak şekilde yönetilmesine yönelik şekli süreç.

Savunmalar. Herhangi bir tehlikenin gerçekleşmesini veya istenmeyen sonuca dönüşmesini önlemek üzere uygulanan spesifik hafifletici tedbirler, önleyici kontroller veya kurtarma tedbirleri.

Hatalar. Herhangi bir operasyon personeli tarafından gerçekleştirilen, organizasyonun veya söz konusu operasyon personelinin niyetinden veya beklentisinden farklılığa yol açan herhangi bir eylem veya eylemsizlik.

****Tehlike.*** Herhangi bir hava aracı olayına veya kazasına sebebiyet verme veya katkıda bulunma potansiyeline sahip olan herhangi bir durum veya obje.

Risk hafifletme. Herhangi bir tehlikenin öngörülen sonucunun ciddiyetinin ve/veya ihtimalinin düşürülmesine yönelik olarak savunmaların, önleyici kontrollerin veya kurtarma tedbirlerinin dahil edilme süreci.

Emniyet. Hava araçlarının işletilmesine ilişkin veya hava araçlarının işletilmesinin doğrudan yararına olan havacılık faaliyetleriyle ilişkili risklerin azaltıldığı ve kabul edilebilir bir seviyede kontrol altına alındığı durum.

****Emniyet verileri.*** Havacılıkla ilgili çeşitli kaynaklardan toplanan, emniyeti muhafaza etmek veya iyileştirmek üzere kullanılan, tanımlanmış gerçekler dizisi veya emniyet değerleri dizisi.

Not.— Söz konusu emniyet verileri, aşağıdakiler de dahil olmak, ancak bunlarla sınırlı kalmamak üzere, ileriye etkili veya tepkisel nitelikteki emniyet ile ilgili faaliyetlerden toplanır:

a) kaza veya olay soruşturmaları;

b) emniyet raporlaması;

c) sürekli uçuşa elverişlilik raporlaması;

d) operasyonel performans izlemesi;

e) incelemeler, denetimler, teftişler veya

f) emniyet etütleri ve gözden geçirmeleri.

***Emniyet bilgileri.** Emniyet yönetimi amaçları için faydalı hale getirilmek üzere belirli bir bağlamda işlenen, düzenlenen veya analiz edilen emniyet verileri.

***Emniyet yönetimi sistemi (SMS).** Gerekli organizasyon yapıları, mesuliyet, sorumluluklar, politikalar ve prosedürler de dahil olmak üzere, emniyetin yönetilmesine yönelik sistematik bir yaklaşım.

***Emniyet amacı.** Devlet emniyet programı veya hizmet sağlayıcısının emniyet yönetimi sistemi tarafından ulaşılacak emniyet başarısına veya arzu edilen sonuca ilişkin kısa, üst seviye bir açıklama.

Not.— Emniyet amaçları, organizasyonun başlıca emniyet risklerinden oluşturulur ve daha sonraki emniyet performansı göstergelerinin ve hedeflerinin oluşturulması sırasında göz önünde bulundurulmalıdır.

***Emniyet gözetimi.** Herhangi bir Devlet tarafından, herhangi bir havacılık faaliyetini icra eden kişiler ve organizasyonlar tarafından emniyet ile ilgili ulusal kanunlara ve düzenlemelere riayet edildiğinden emin olmak üzere icra edilen görev.

***Emniyet performansı.** Herhangi bir Devletin veya hizmet sağlayıcısının, söz konusu Devletin veya hizmet sağlayıcısının emniyet performansı hedefleri ve emniyet performansı göstergeleriyle tanımlanan emniyet başarısı.

***Emniyet performansı göstergesi.** Emniyet performansının izlenmesi ve değerlendirilmesi için kullanılan, veri tabanlı bir parametre.

***Emniyet performansı hedefi.** Devletin veya hizmet sağlayıcısının, emniyet amaçlarıyla uygun olan belirli bir süre genelinde herhangi bir emniyet performansı göstergesine yönelik olarak planlanan veya amaçlanan hedefi.

***Emniyet riski.** Herhangi bir tehlikenin sonuçlarının veya akıbetinin tahmin edilen ihtimali ve ciddiyeti.

***Devlet emniyet programı (SSP).** Emniyetin iyileştirilmesine yönelik bir dizi entegre düzenlemeler ve faaliyetler.

***Gözetim.** Devlet tarafından havacılık lisansı, sertifikası, yetkilendirmesi veya onayı sahipleri tarafından belirlenmiş gereklilikleri karşılamaya devam edildiğinin ve söz konusu Devlet tarafından öngörülen yetkinlik ve emniyet seviyesinde görev yapıldığının incelemeler ve denetimler vasıtasıyla proaktif olarak doğrulandığı Devlet faaliyetleri.

***Sistem.** Birbiriyle ilişkili ve birbirine bağımlı unsurlardan ve bileşenlerden ve herhangi bir spesifik faaliyetin yürütülmesi veya herhangi bir problemin çözüme kavuşturulması için oluşturulan ilgili politikalardan, prosedürlerden ve uygulamalardan oluşan organize ve bir amaca yönelik yapı.

***Tetikleyici.** Gerekli görülen herhangi bir eylemin (örneğin, herhangi bir değerlendirme, düzeltme veya iyileştirici faaliyet) başlatılmasına hizmet eden belirli bir emniyet performansı göstergesine ilişkin belirlenmiş seviye veya kriter değeri.

KISALTMALAR VE AKRONİMLER

ADREP	Kaza/olay verileri raporlaması
AIA	Kaza soruşturma otoritesi
ALoSP	Kabul edilebilir emniyet performansı seviyesi
AOC	Hava işletme ruhsatı
ATS	Hava trafik hizmeti (hizmetleri)
CAA	Sivil havacılık otoritesi
CVR	Kokpit ses kayıt cihazı
D3M	Veriye dayalı karar alma
Doc	Doküman
ERP	Acil müdahale planı
FDA	Uçuş verileri analizi
FDR	Uçuş verileri kayıt cihazı
FMS	Finansal yönetim sistemi
FRMS	Yorgunluk riski yönetim sistemleri
GASP	Global Havacılık Emniyeti Planı
ICAO	Uluslararası Sivil Havacılık Teşkilatı
iSTARS	Entegre Emniyet Trendi Analiz ve Raporlama Sistemi
LOSA	Hat operasyonları emniyet denetimi
OHSMS	İş sağlığı ve güvenliği yönetimi sistemi OSHE İş güvenliği, sağlık ve çevre
PIRG	Planlama ve uygulama bölgesel grubu
QMS	Kalite yönetim sistemi
RASG	Bölgesel havacılık emniyeti grubu
RSOO	Bölgesel emniyet gözetimi organizasyonu
SAG	Emniyet eylem grubu
SARP'ler	Standartlar ve Tavsiye Edilen Uygulamalar
SD	Standart sapma
SDCPS	Emniyet verileri toplama ve işleme sistemi
SeMS	Güvenlik yönetimi sistemi
SMM	Emniyet yönetimi el kitabı
SMP	Emniyet Yönetimi Heyeti
SMS	Emniyet yönetimi sistemi (sistemleri)
SPI	Emniyet performansı göstergesi
SPT	Emniyet performansı hedefi
SRB	Emniyet gözden geçirme kurulu
SRBS	Emniyet riskine dayalı gözetim
SRM	Emniyet riski yönetimi
SSO	Devlet emniyet gözetimi
SSP	Devlet emniyet programı
STDEVP	Popülasyon standart sapması
TNA	Eğitim ihtiyaçları analizi
USOAP	Evrensel Emniyet Gözetimi Denetim Programı

YAYINLAR

(Bu el kitabında atıfta bulunulan yayınlar)

Bu el kitabında aşağıdaki dokümanlara atıfta bulunulmaktadır ve söz konusu dokümanlar ilave kılavuz materyal sunabilecektir.

ICAO DOKÜMANLARI

Uluslararası Sivil Havacılık Sözleşmesi Annex'leri

Annex 1 — *Personel Lisanslandırma*

Annex 6 — *Hava Araçlarının Operasyonu*
Kısım I — *Uluslararası Ticari Hava Taşımacılığı — Uçaklar*
Kısım II — *Uluslararası Genel Havacılık — Uçaklar*

Annex 8 — *Hava Araçlarının Uçuşa Elverişliliği*

Annex 13 — *Hava Aracı Kaza ve Olay Soruşturması*

Annex 14 — *Havaalanları*
Cilt I — *Havaalanı Tasarımı ve İşletimi*

Annex 18 — *Tehlikeli Maddelerin Hava Yoluyla Emniyetli Taşınması*

Annex 19 — *Emniyet Yönetimi*

PANS

Hava Seyrüsefer Hizmetlerine İlişkin Usuller (PANS — Havaalanları (Doc 9981)

Hava Seyrüsefer Hizmetlerine ilişkin Usuller — Hava Trafik Yönetimi (PANS-ATM) (Doc 4444)

El Kitapları

Havalimanı Hizmetleri El Kitabı (Doc 9137), Kısım 3 — *Yaban Hayatının*

Kontrolü ve Azaltılması Hava Trafik Hizmetleri Planlama El Kitabı (Doc 9426)

Uçuşa Elverişlilik El Kitabı (Doc 9760)

Havacılık Güvenliği El Kitabı (Doc 8973 — Hizmete Özel)

Global Havacılık Emniyeti Planı (GASP) (Doc 10004)

Hava Aracı Kaza ve Olay Soruşturması El Kitabı (Doc 9756)

Kısım I — *Organizasyon ve Planlama*
Kısım II — *Prosedürler ve Kontrol Listeleri*
Kısım III — *Soruşturma*
Kısım IV — *Raporlama*

Yorgunluk Yönetimi Yaklaşımlarının Gözetimine ilişkin El Kitabı (Doc 9966)

Lazer Yayıcı Cihazlara ve Uçuş Emniyetine ilişkin El Kitabı (Doc 9815)

Uzaktan Kumanda Edilen Pilotsuz Hava Aracı Sistemlerine ilişkin El Kitabı (RPAS) (Doc 10019)

Sivil Havacılık Emniyet Denetçilerinin Yetkinliklerine ilişkin El Kitabı (Doc 10070)

ICAO Kuş Çarpması Bilgilendirme Sistemine ilişkin El Kitabı (IBIS) (Doc 9332)

Emniyet Bilgilerinin Korunmasına ilişkin El Kitabı (Doc 10053)
Kısım I — *Kaza ve Olay Soruşturma Kayıtlarının Korunması*

Emniyet Gözetimi El Kitabı (Doc 9734)
Kısım A — *Devlet Emniyet Gözetim Sisteminin Oluşturulması ve Yönetimi*
Kısım B — *Bölgesel Emniyet Gözetimi Organizasyonunun Oluşturulması ve Yönetimi Tehlikeli*

Maddelerin Hava Yoluyla Emniyetli Taşınmasına Yönelik Teknik Talimatlar (Doc 9284)

Bölüm 1. GİRİŞ

1.1 EMNİYET YÖNETİMİ NEDİR?

1.1.1 Emniyet yönetimi, havacılık kazalarıyla ve olaylarıyla sonuçlanmaları öncesinde emniyet risklerinin proaktif bir şekilde hafifletilmesini amaçlamaktadır. Emniyet yönetiminin uygulanmasıyla, Devletler, emniyet faaliyetlerini daha disiplinli, bütünleyici ve odaklanmış bir şekilde yönetebilirler. Emniyetli operasyonlara yönelik katkısını ve rolünü tam olarak kavramak, ilgili Devletin ve havacılık sektörünün emniyet risklerinin ele alınmasına yönelik tedbirlere öncelik vermesine ve kaynaklarını havacılık emniyetinin optimal yararına daha etkin bir şekilde yönetmesine imkan verir.

1.1.2 Herhangi bir Devletin emniyet yönetimi faaliyetlerinin etkinliği, Devlet emniyet programı (SSP) vasıtasıyla ve hizmet sağlayıcılarına yönelik emniyet yönetimi sistemleri (SMS'ler) vasıtasıyla resmi ve kurumsallaşmış bir şekilde yürütüldüğünde güçlendirilir. Herhangi bir Devletin, hizmet sağlayıcılarına yönelik Emniyet Yönetimi Sistemleri (SMS'ler) ile birleştirilmiş emniyet programı kapsamında, emniyet riskleri sistematik bir şekilde ele alınır, her bir hizmet sağlayıcısının emniyet performansı iyileştirilir ve söz konusu Devletin emniyet performansı bir bütün halinde geliştirilir.

1.1.3 Devlet Emniyet Programı (SSP), her bir Devlet tarafından, söz konusu Devletin havacılık emniyeti performansının yönetilmesine yardımcı olunmasına yönelik yapılandırılmış bir yaklaşım olarak oluşturulur ve sürdürülür. Mevcut havacılık emniyeti kaydına uyum bazlı geleneksel yaklaşımla erişilir ve buna Devlet Emniyet Programının (SSP) temeli olarak muamele edilmeye devam edilmelidir. Böylelikle, Devletler tarafından etkin emniyet gözetimi sistemlerinin uygulandığından emin olunmalıdır. Devlet Emniyet Programı (SSP) hakkında daha fazla bilgiye 8. Bölüm kapsamında ulaşılabilir.

1.1.4 Devletler tarafından, tehlikeleri tanımlamak, verileri toplamak ve analiz etmek ve emniyet risklerini süreklilik esasına dayalı olarak değerlendirmek ve yönetmek suretiyle, emniyet performansının sürekli olarak iyileştirilmesi için, Annex 19 - *Emniyet Yönetimi* kapsamında belirlendiği şekilde, kendi yetkisi dahilindeki hizmet sağlayıcıları tarafından bir Emniyet Yönetim Sisteminin (SMS) oluşturulması ve sürdürülmesi gerekli görülecektir (Emniyet Yönetimi Sistemi uygulanabilirliğine ilişkin detaylar için bakınız madde 1.2). Emniyet Yönetimi Sisteminin uygulanmasına ilişkin daha fazla bilgiye 9. Bölüm kapsamında ulaşılabilir.

1.1.5 ICAO *Global Havacılık Emniyeti Planı* (GASP, Doc 10004) amaçları kapsamında Devletler tarafından sağlam ve sürdürülebilir emniyet gözetimi sistemlerinin yerleştirilmesi ve bu sistemlerin artan bir şekilde, emniyet performansının yönetilmesine yönelik daha gelişmiş araçlara dönüştürülmesi öngörülmektedir. Bu amaçlar, Devletler tarafından Devlet Emniyet Programlarının (SSP'ler) ve hizmet sağlayıcıları tarafından Emniyet Yönetim Sistemlerinin (SMS'ler) uygulanmasına yönelik ICAO gereklilikleri ile aynı doğrultudadır.

1.1.6 Sadece herhangi bir Devletin uyumlu olup olmamasına yoğunlaşılmasından ziyade, arzu edilen sonuca ulaşılmasına odaklanmakta olduğundan dolayı emniyete yönelik bu performansa dayalı yaklaşım sayesinde iyileştirmelere fırsat verir. Bununla birlikte, belirtilen sonuçlara ulaşmak, Devletlere ilişkin olarak ise her bir hizmet sağlayıcısının yaklaşımını değerlendirmek üzere, havacılık sektörü tarafında uygun yöntemlerin oluşturulması için gayret gerektirmekte olması sebebiyle, emniyet performansı yaklaşımının uygulanmasının ortak çalışmaya dayalı olduğunu kayda almak önem arz etmektedir.

1.1.7 EMNİYET YÖNETİMİNİN FAYDALARI

Emniyet yönetiminin uygulanmasının pek çok faydası mevcut olup, bu faydalardan bazıları şunlardır:

a) *Güçlendirilmiş emniyet kültürü* – Herhangi bir organizasyonun emniyet kültürü, yönetimin taahhüdünü görünür hale getirmek ve personeli emniyet riskinin yönetimine faal bir şekilde dahil etmek suretiyle güçlendirilebilir. Emniyet, yönetim tarafından faal bir şekilde bir öncelik olarak kabul edildiğinde, personel tarafından da genel olarak iyi bir şekilde algılanır ve normal operasyonların bir parçası haline gelir.

b) *Emniyetin güvence altına alınmasına yönelik belgelenmiş, süreç bazlı yaklaşım* – Personel tarafından idrak edilebilen ve başkalarına kolaylıkla anlatılabilen, emniyetli operasyonlara ulaşılmasına yönelik açık ve belgelenmiş bir yaklaşım oluşturur. İlaveten, temel performansın açık bir şekilde tanımlanması, bu sayede söz konusu organizasyon tarafından değişikliği uygulamak için gerekli kaynakların optimize edilmesine yardımcı olarak emniyet programı/sistemi sürekli olarak iyileştirilirken kontrollü değişikliklere imkan verir.

c) *Emniyet ile ilgili arayüzlerin ve ilişkilerin daha iyi anlaşılması* – Emniyet yönetimi arayüzlerini belgelendirme ve tanımlama süreci, uçtan uca sürecin daha iyi bir şekilde anlaşılmasına ve arttırılmış etkinliklere yönelik imkanların ortaya konmasına yol açarak süreç içi ilişkilerin söz konusu organizasyon tarafından anlaşılmasına fayda edebilir.

d) *Emniyet tehlikelerinin erken tespitinin geliştirilmesi* – Söz konusu Devletin/hizmet sağlayıcısının, tehlikelerin proaktif bir şekilde belirlenmesi ve emniyet risklerinin yönetilmesiyle kazaları ve olayları engelleyebilecek olan, ortaya çıkan emniyet sorunlarını tespit etme becerisini geliştirir.

e) *Emniyet verilerine dayalı karar alma* – Söz konusu Devletin/hizmet sağlayıcısının, emniyet analizi amacıyla emniyet verilerini elde etme becerisini geliştirir. Hangi soruların yanıtlanması gerektiğinin tespit edilmesine yönelik bir miktar stratejik düşünceyle, sonuçta oluşan emniyet bilgileri, karar vericilere, daha bilgiye dayalı, geçerli kararların alınmasında neredeyse gerçek zamanlı olarak yardımcı olabilir. Kaynakların daha fazla ilgi veya ihtiyaç gerektiren alanlara tahsis edilmesi, bu karar almanın önemli bir yönünü teşkil etmektedir.

f) *Geliştirilmiş emniyet iletişimi* – Organizasyon ve sektör genelinde ortak bir emniyet dili ortaya koyar. Organizasyonun emniyet hedeflerine ve başarılarına yönelik ortak bir anlayışın oluşturulmasında ortak emniyet dili temel etkendir. Ortak emniyet dili, özellikle, söz konusu organizasyonun emniyet amaçları ve emniyet performansı göstergeleri (SPI'ler) ile emniyetin yönlendirilmesine ve özendirilmesine imkan veren emniyet performansı hedeflerine (SPT'ler) yönelik takdir sağlar. Personel, organizasyonun performansının ve tanımlanan emniyet amaçlarına ulaşılmasına yönelik olarak gerçekleştirilen ilerlemenin yanı sıra bunların söz konusu organizasyonun başarısına nasıl katkı sağladığının daha fazla bilincinde olacaktır. Ortak emniyet dili, birden fazla havacılık işletmesine sahip olan hizmet sağlayıcıları tarafından organizasyonel kuruluşlardan emniyet bilgilerinin bir araya getirilmesine imkan verir. Havacılık sistemi genelindeki arayüzlerin yönetiminin desteklenmesi gerekir.

g) *Emniyetin bir öncelik olduğuna dair kanıt* – Organizasyon dahilinde ve haricinde olmak üzere, havacılık toplumu nezdinde artan güvene yol açarak emniyetin yönetim tarafından nasıl desteklendiğini ve olanaklı kılındığını, emniyet risklerinin nasıl tanımlandığını ve yönetildiğini ve emniyet performansının sürekli olarak nasıl iyileştirildiğini ortaya koyar. Ayrıca, yüksek kalibreli personelin artarak cezbedilmesine ve elde tutulmasına imkan verebilecek şekilde, personel tarafından söz konusu organizasyonun emniyet performansına güvenle bakılması sonucunu doğurur. Ayrıca, Devletler ve bölgesel emniyet gözetimi organizasyonları (RSOO'lar) tarafından hizmet sağlayıcıların emniyet performansına yönelik güven oluşturulmasına imkan verir.

h) *Olası finansal tasarruflar* – Bir takım hizmet sağlayıcıları tarafından, Emniyet Yönetimi Sistemi (SMS) sonuçlarına dayalı olarak sigorta primlerine ilişkin indirime ve/veya iş kazası sigortası primlerinde tenzilata hak kazanılmasına imkan verebilir.

i) *Arttırılmış etkinlikler* – Mevcut süreçlerdeki ve sistemlerdeki etkisizlikleri teşhir etmek suretiyle operasyonların maliyetindeki olası indirim. Diğer dahili veya harici yönetim sistemleriyle entegrasyon da ilave maliyet tasarrufları sağlayabilir.

j) *Maliyetten kurtulma*– Tehlikelerin proaktif bir şekilde tanımlanması ve emniyet riski yönetimi (SRM) ile kazalar ve olaylar sebebiyle altına girilen maliyetlerden kurtulunabilir. Bu gibi hallerde, doğrudan maliyetler yaralanmaları, mal zararını, ekipman onarımlarını ve tarife/program gecikmelerini içerebilir. Dolaylı maliyetler, yasal işlemleri, iş kaybını ve itibarın zarar görmesini, fazlalık yedek parçaları, araçları ve eğitimi, artan sigorta primlerini, personel verimliliğinin kaybını, ekipman kurtarmasını ve temizliğini, kısa vadeli ikame ekipmanlara sebebiyet veren ekipman kullanımı kaybını ve dahili soruşturmaları içerebilir.

1.2 EMNİYET YÖNETİMİNİN UYGULANABİLİRLİĞİ

Devlet emniyet yönetimi sorumlulukları Annex 19 Bölüm 3 kapsamında ortaya konmakta olup, Standart ve Tavsiye Edilen Uygulamalarda belirlenmiş hizmet sağlayıcıları tarafından Emniyet Yönetimi Sisteminin (SMS) uygulanmasının gerekli olduğuna yer verilmektedir. Hizmet sağlayıcıları tarafından Emniyet Yönetimi Sistemlerinin (SMS'ler) uygulanmasına ilişkin hükümlere Annex 19'un 2. Eki ve 4. Bölüm kapsamında ulaşılabilir.

1.2.1 Emniyet Yönetimi Sistemi (SMS) uygulanabilirliği

1.2.1.1 Annex 19'un 1 sayılı Revizyonuna ilişkin olarak Emniyet Yönetimi Sisteminin (SMS) uygulanabilirliğinin tespitine yönelik değerlendirme bir dizi kritere dayandırılmıştır. Uygulanabilirliğin diğer havacılık organizasyonlarını kapsayacak şekilde genişletilmesine yönelik ihtiyacın yeniden değerlendirilmesi için ICAO ile Emniyet Yönetimi Paneli (SMP) tarafından periyodik olarak aynı kriterlerin kullanılması beklenmektedir.

Toplam sistem emniyeti yaklaşımı

1.2.1.2 Toplam sistem emniyeti yaklaşımında havacılık sektörünün tümü bir sistem olarak değerlendirilir. Tüm hizmet sağlayıcıları ve bunların emniyetin yönetilmesine yönelik sistemleri alt sistemler olarak değerlendirilir. Bu sayede, Devletler tarafından etkileşimlerin ve tüm sistem genelinde sebebin ve sonucun değerlendirilmesine imkan verilir. Tüm emniyet sistemlerini aynı yolla oluşturmak genelde olanaksız veya elverişsizdir. Bu sebeple, farklı etkileşen sistemler arasında arayüzlerin en iyi ne şekilde yönetilmesi gerektiği Devletler ve hizmet sağlayıcıları için temel sorunu teşkil etmektedir.

1.2.1.3 Emniyet Yönetimi Sisteminin (SMS) uygulanabilirliği gözden geçirilirken, Annex 19 kapsamında daha önceden Emniyet Yönetimi Sistemi (SMS) gerekliliğine sahip olan hizmet sağlayıcıları ile herhangi bir havacılık faaliyetini yürüten diğer organizasyonlar arasındaki bağ değerlendirilmiştir. Emniyet Yönetimi Sisteminin (SMS) uygulanması, emniyet boşlukları veya çakışmaları riskini azaltmalı, azaltılmış birlikte işlerlikle emniyet riskini arttırmamalıdır.

Alt yükleniciye vermenin sonuçları

1.2.1.4 Emniyet Riski Yönetiminin (SRM) hizmet sağlayıcıları genelinde etkin olması için, boşluklar veya çakışmalar olmadan, tehlikelerin tanımlanmasına ve sistem dahilindeki tüm hizmetler zinciri için ilişkili emniyet risklerinin yönetilmesine yönelik sorumlulukların açık bir şekilde tanımlanması önem arz etmektedir. Emniyet Yönetimi Sistemi (SMS) gerekliliğine sahip olan herhangi bir hizmet sağlayıcısı tarafından Emniyet Yönetimi Sistemine (SMS) tabi olmayan herhangi bir organizasyon ile sözleşme yapıldığı hallerde, söz konusu yüklenici tarafından potansiyel olarak getirilen tehlikeler ve emniyet riskleri söz konusu hizmet sağlayıcısının Emniyet Yönetimi Sistemi (SMS) kapsamında ele alınır. Bu sayede, yüklenicisinin (yüklenicilerinin) faaliyetleri ile tetiklenen emniyet riskleri hakkında bilgi sahibi olmalarını sağlamak üzere, söz konusu hizmet sağlayıcısına ilave Emniyet Riski Yönetimi (SRM) sorumlulukları getirilir. Emniyet Riski Yönetimi (SRM) hakkında daha fazla bilgi için bakınız Bölüm 2.

Emniyet riskinin düzenlemelerle kontrolü

1.2.1.5 Devletler tarafından, mevcut mevzuat ve düzenlemeler kapsamında, söz konusu faaliyet tarafından öngörülen tehlikelerin etkin bir şekilde ele alınıp alınmadığı değerlendirilmelidir. Mevcut gereklilikler kapsamında yeterli emniyet riski hafifletmesinin sağlanması ve Annex 19 kapsamında geçerli olmayan organizasyonlar için Emniyet Yönetimi Sistemi (SMS) gerekliliğinin öngörülmesinin esaslı emniyet faydası getirmemesi söz konusu olabilir.

1.2.2 İsteğe bağlı Emniyet Yönetimi Sistemi (SMS) uygulanabilirliğinin genişletilmesi

1.2.2.1 Yukarıda belirtilmekte olan uygulanabilirlik kriterleri, Emniyet Yönetimi Sisteminin (SMS) Annex 19 kapsamında tanımlanmakta olanın ötesine genişletilmesi veya gönüllü uygulamanın teşvik edilmesi değerlendirilirken Devletlere yönelik kılavuz materyal olarak da hizmet edebilir. İsteğe bağlı Emniyet Yönetimi Sistemi (SMS) uygulanabilirliğinin uygulanması dikkatlice değerlendirilmelidir. Emniyet Yönetimi Sistemi (SMS) uygulanabilirliğinin sektörlere veya hizmet sağlayıcılarına genişletilmesine yönelik kararda, söz konusu Devlette tanımlanan emniyet riskleri göz önünde bulundurulmalı ve böyle bir kararın verilmesi halinde, Devlet Emniyet Programı (SSP) kapsamında Emniyet Yönetimi Sistemi (SMS) uygulaması takip edilmelidir. Emniyet Yönetimi Sisteminin (SMS) öngörülmesi öncesinde, Devletler tarafından;

a) emniyet performansındaki arzu edilen gelişmeye ulaşılması için herhangi bir başka uygulanabilir opsiyonun olup olmadığının ve

b) söz konusu Devlet ve sanayi sektörü için Emniyet Yönetimi Sisteminin (SMS) uygulanması ve takibi için yeterli kaynakların mevcut olup olmadığının değerlendirilmesi talep edilir. Bilhassa, kadro oluşturma üzerindeki olası etkinin ve gerekli becerilerin ve bilginin elde edilmesinde ve entegre edilmesinde karşılaşılacak olası zorlukların dikkate alınması gerekir.

1.2.2.2 Her bir Devlet tarafından kendi endüstrisi genelindeki kabul edilebilir emniyet performansı seviyesi (ALoSP) dikkate alınmalı ve söz konusu Devletin emniyet amaçlarına ulaşması en muhtemel olan bir Emniyet Yönetimi Sistemi (SMS) uygulanabilirlik planı tesis edilmelidir. Uygulanan Emniyet Yönetimi (SMS) uygulanabilirlik planının, söz konusu Devletin kabul edilebilir emniyet performansı seviyesi (ALoSP) ile sürekli olarak uyuşarak gelişmesi muhtemeldir.

1.2.3 Emniyet yönetimi sorumluluğu

Annex 19 kapsamındaki hiçbir hükümde, havacılık hizmeti sağlayıcısının veya işleticinin sorumluluklarının Devlete devredilmesi amaçlanmamaktadır. Devletler, kendi sistemleri dahilinde emniyeti yönetmek üzere bir çok araca sahiptirler. Kendi Devlet Emniyet Programı (SSP) kapsamında, her bir Devlet tarafından, güncel ICAO Annex'lerinin kapsamına girmeyebilecek havacılık faaliyetlerinin veya yeni veya yeni geliştirilen faaliyetlerin gözetimine yönelik en iyi opsiyonlar göz önünde bulundurulmalıdır.

1.2.4 Devlete ait olan veya askeri hizmet sağlayıcıları için uygulanabilirlik

1.2.4.1 Bazı Devletlerde, hizmet sağlayıcısı görevi Devletin kamu veya askeri hizmetleri tarafından sağlanmaktadır. Bazı sivil hizmet sağlayıcıları tarafından askeriyeye sözleşmeli olarak hizmetler sunulmakta ve bazı askeri kuruluşlar tarafından sivil hizmet sağlanmaktadır. Düzenlemeye bakılmaksızın, söz konusu Devletteki sivil hizmete yönelik hizmet sağlayıcısı tarafından, söz konusu organizasyonun kendine has mahiyetine bakılmaksızın Annex 19 Emniyet Yönetimi Sistemi (SMS) gereklilikleri de dahil olmak üzere, tüm geçerli ICAO Standart ve Tavsiye Edilen Uygulamalar (SARP'ler) ele alınmalıdır. Söz konusu Devletin veya hizmet sağlayıcısının sistem tanımında bu organizasyonların görevleri ile birbirleri ile olan ilişkisi dikkate alınmalıdır. İster sivil, ister askeri olsun, söz konusu hizmet sağlayıcısının sorumlu yöneticisi, düzenlemeleri ve emniyet risklerinin nasıl yönetildiğini açıklayabilmelidir. Basitçe ifade etmek gerekirse, hizmet sağlayıcıları tarafından emniyet, organizasyonel düzenlemelere bakılmaksızın yönetilmelidir.

1.2.4.2 Söz konusu Devletin hizmet sağlayıcısı olarak faaliyet gösterdiği hallerde, söz konusu Devletin hizmet sağlayıcısı olarak görevleri ile söz konusu Devletin düzenleyici otoritesinin görevleri arasında açık bir ayrım olmalıdır. Bu ayrım, çıkar çatışmalarının önlenmesine yönelik olarak Devlet otoritesi ile hizmet sağlayıcısı personeline ilişkin görevlerin ve sorumlulukların açık bir şekilde tanımlanmış olmasıyla sağlanır.

1.2.5 Havacılık emniyeti karşısında iş güvenliği, sağlık ve çevre

İş güvenliği, sağlık ve çevre (İGSÇ) (ayrıca iş sağlığı ve güvenliği (İSG) veya işyeri sağlığı ve güvenliği (İYSG) olarak da anılmaktadır), kişilerin iş başında oldukları sıradaki güvenliği, sağlığı ve refahı ile ilgili olan bir alandır. Havacılık emniyeti yönetimi ile İGSÇ sistemleri arasındaki başlıca fark amaçtır. Bir çok Devlette, işverenler, çalışanlarının sağlığına ve güvenliğine yönelik makul özen göstermekle yasal olarak yükümlüdürler. İGSÇ programları, emniyetli ve sağlıklı bir çalışma ortamını teşvik ederek işverenlerin yasal ve etik yükümlülüklerini karşılamayı amaçlamaktadır. Bu konular normalde, havacılık konularını ele alan devlet organından farklı olan bir devlet organı bünyesinde ele alınır. Bu itibarla, Annex 19, Bölüm 2, *Uygulanabilirlik* kapsamında özel olarak "hava araçlarının emniyetli işletilmesine ilişkin veya hava araçlarının emniyetli işletilmesini doğrudan destekler nitelikteki emniyet yönetimi görevlerine" odaklanılmaktadır.

1.3 EMNİYET YÖNETİMİNİN UYGULANMASI

1.3.1 Etkin emniyet yönetimi uygulamasına ulaşılması için sağlam bir zeminin kurulması elzemdir. Devlet Emniyet Programı (SSP) veya Emniyet Yönetimi Sistemi (SMS) gerekliliklerinin uygulanmasında aşağıdaki yönlerin ilk adımlar olarak ele alınması gerekmektedir:

a) *Üst yönetim taahhüdü*: Tüm Devlet havacılık kurumlarının üst yönetimi tarafından etkin emniyet yönetimi uygulamasının taahhüt edilmesi elzemdir.

b) *Kuralcı gerekliliklere uyum*: Devletler tarafından, kalifiye teknik personel de dahil olmak üzere, söz konusu Devlette havacılık faaliyetleri icra eden kişilerin ve organizasyonların lisanslandırılmasına, sertifikasyonuna, yetkilendirilmesine ve onaylanmasına yönelik olarak olgunlaşmış bir emniyet gözetim sisteminin uygulanması sağlanmalıdır. Hizmet sağlayıcıları tarafından, yerleşmiş kuralcı gerekliliklere sürekli uyumun sağlanmasına yönelik olarak uygulanan süreçlere sahip olunması sağlanmalıdır.

c) *Yürütme düzeni*: Devletler tarafından, taraflarca farklılıkların ve önemsiz ihlallerin yönetilmesine ve çözüme kavuşturulmasına imkan veren bir yürütme politikası ve çerçeveler tesis edilmelidir.

d) *Emniyet bilgilerinin korunması*: Emniyet verilerinin ve emniyet bilgilerinin sürekli elverişliliğini sağlamak üzere Devletler tarafından koruyucu bir yasal çerçevenin uygulanması elzemdir.

1.3.2 Sistem tanımı

Sistem tanımı, söz konusu organizasyonun (Devlet veya hizmet sağlayıcısı) kendi emniyet sistemi kapsamında yer alan emniyet riski değerlendirmesi ve tehlike tanımlaması için değerlendirilmesi gereken süreçlerinin, faaliyetlerinin ve arayüzlerin bir özetidir. Söz konusu organizasyonun görev yaptığı ve çeşitli kuruluşların ve otoritelerin dahil olduğu havacılık sistemini tanımlar. Söz konusu organizasyonun bünyesindeki arayüzlerin yanı sıra, hizmetlerin emniyetli bir şekilde sunulmasına katkı sağlayan harici organizasyonlar ile olan arayüzleri içerir. Sistem tanımı, Devlet Emniyet Programının (SSP)/Emniyet Yönetim Sisteminin (SMS) uygulanmasına yönelik bir başlangıç noktası sunar. Devletlere ve hizmet sağlayıcılarına yönelik sistem tanımı hakkında daha fazla bilgiye, sırasıyla, 8. ve 9. Bölümlerde ulaşılabilir.

1.3.3 Arayüzler

1.3.3.1 Devletler ve hizmet sağlayıcıları tarafından emniyet yönetiminin uygulanması değerlendirildiğinde, birbirleriyle arayüze sahip olan kuruluşlar tarafından tetiklenen emniyet risklerinin göz önünde bulundurulması önem arz etmektedir. Arayüzler dahili (örneğin, işletme ve bakım veya finans, insan kaynakları veya hukuk müşavirliği departmanları arasında) veya harici (örneğin, diğer Devlet, hizmet sağlayıcıları veya anlaşmalı hizmetler) nitelikte olabilir. Devletler ve hizmet sağlayıcıları, arayüzler belirlendiğinde ve yönetildiğinde, ilgili emniyet risklerinin üzerinde daha fazla kontrole sahiptirler. Arayüzler, sistem tanımı kapsamında tanımlanırlar.

Arayüz emniyet etkisi değerlendirmesi

1.3.3.2 Herhangi bir Devlet veya hizmet sağlayıcısı tarafından arayüzlerinin belirlenmesi sonrasında, söz konusu organizasyonun mevcut emniyet riski değerlendirmesi süreçleri kullanılarak her bir arayüz tarafından teşkil edilen emniyet riski değerlendirilir (detaylar için bakınız Bölüm 2). Belirlenen emniyet risklerine dayalı olarak, söz konusu Devlet veya hizmet sağlayıcısı tarafından uygun bir emniyet riski kontrol stratejisinin tespit edilmesi için diğer organizasyonlarla çalışılması değerlendirilebilecektir. İşbirliği çerçevesinde çalışan organizasyonlar tarafından, ilgili emniyet riskleri değerlendirilerek ve karşılıklı olarak uygun kontroller tespit edilerek daha fazla arayüz tehlikesi belirlenebilecektir. Emniyet riski algısının organizasyonlar arasında farklılık gösterebilecek olmasına bağlı olarak ortak çalışma ziyadesiyle makbuldür.

1.3.3.3 Dahil olan her bir organizasyonun kendi organizasyonuna tesir eden tehlikelerin belirlenmesinden ve belirlenen tehlikelerin yönetilmesinden sorumlu olduğunun kabulü de önem arz etmektedir. Söz konusu arayüzün kritikliği her bir organizasyon için farklılık gösterebilecektir. Her bir organizasyon tarafından makul çerçevede farklı emniyet riski sınıflandırmaları uygulanabilecek ve (emniyet performansı, kaynaklar, zaman bakımından) farklı emniyet riski önceliklerine sahip olunabilecektir.

Arayüzlerin izlenmesi ve yönetimi

1.3.3.4 Devletler ve hizmet sağlayıcıları, hizmetlerin emniyetli bir şekilde sunulmasını sağlamak üzere kendi arayüzlerinin sürekli olarak izlenmesinden ve yönetilmesinden sorumludurlar. Birbirleriyle arayüz bağlantısına sahip olan organizasyonlar arasında, açık bir şekilde tanımlanmış izleme ve yönetim sorumluluklarının yer aldığı resmi anlaşmaların tesis edilmesi, Emniyet Riski Yönetiminin (SRM) arayüzlenmesine yönelik etkin bir yaklaşım teşkil etmektedir. Tüm arayüz emniyet sorunlarının, emniyet raporlarının ve öğrenilen derslerin yanı sıra emniyet risklerinin belgelenmesi ve birbirleriyle arayüz bağlantısına sahip olan organizasyonlar arasında paylaşılması açık bir anlayışa imkan verecektir. Paylaşım, her bir organizasyonun emniyet etkinliğini iyileştirebilecek olan bilgi transferine ve çalışma uygulamalarına imkan verir.

1.3.4 Uygulamanın planlanması

1.3.4.1 Devlet Emniyet Programının (SSP)/Emniyet Yönetimi Sisteminin (SMS) uygulanmasına başlanmadan önce boşluk analizinin gerçekleştirilmesi, söz konusu organizasyona, mevcut organizasyon yapıları ve süreçleri ile etkin Devlet Emniyet Programı (SSP) veya Emniyet Yönetimi Sistemi (SMS) işleyişi için gerekli olanlar arasındaki boşluğu belirleme imkanı verecektir. Devlet Emniyet Programı (SSP) için, Devlet Emniyet Programının (SSP) temeli olarak değerlendirilen Evrensel Emniyet Gözetimi Denetim Programı (USOAP) protokol sorularının gözden geçirilmesine yer verilmesi önemlidir.

1.3.4.2 Devlet Emniyet Programı (SSP) veya Emniyet Yönetimi Sistemi (SMS) uygulama planı, adından da anlaşılabileceği üzere, Devlet Emniyet Programı (SSP) veya Emniyet Yönetimi Sistemi (SMS) uygulamasına yönelik bir plandır. Gerekli kaynaklara, görevlere ve süreçlere ve önemli görevlerin ve sorumlulukların gösterge niteliğindeki zamanlamasına ve sıralandırılmasına ilişkin açık bir tanım sunar. Devletler ve hizmet sağlayıcıları için emniyet yönetiminin uygulanması hakkında daha fazla bilgiye, sırasıyla 8. ve 9. Bölümlerde ulaşılabilir.

Olgunluk değerlendirmesi

1.3.4.3 Devlet Emniyet Programının (SSP) veya Emniyet Yönetimi Sisteminin (SMS) ana bileşenlerinin ve unsurlarının uygulanmasının hemen sonrasında, ne denli etkin çalışmakta olduğunu takip etmek üzere periyodik değerlendirmeler gerçekleştirilmelidir. Sistem olgunlaştıkça, söz konusu organizasyon tarafından, sistemin amaçlandığı şekilde çalıştığına ve belirlenen emniyet amaçlarına ve hedeflerine ulaşılmasında etkin olduğuna dair güvence arayışında olunmalıdır. Emniyet yönetiminin olgunlaşması zaman alır ve amaç, söz konusu organizasyonun emniyet performansının muhafaza edilmesi veya sürekli olarak iyileştirilmesi olmalıdır.

1.3.5 Boyut ve karmaşıklık hususları

1.3.5.1 Her bir Devlet ve her bir hizmet sağlayıcısı farklıdır. Devlet Emniyet Programları (SSP'ler) ve Emniyet Yönetimi Sistemleri (SMS'ler), her bir Devletin veya hizmet sağlayıcısının kendine özgü ihtiyaçlarını karşılayacak şekilde uygun hale getirilmek üzere tasarlanır. Devlet Emniyet Programının (SSP)/Emniyet Yönetimi Sistemlerinin (SMS) tüm bileşenleri ve tüm unsurları birbirleriyle bağlantılı ve birbirine bağımlı ve etkin bir şekilde işlemek üzere gereklidir. Devlet Emniyet Programı (SSP) ve Emniyet Yönetimi Sistemi (SMS) gerekliliklerinin sadece kuralcı bir şekilde uygulanmamaları önemlidir. Geleneksel kuralcı gereklilikler, performansa dayalı bir yaklaşımla tamamlanmalıdır.

1.3.5.2 Program/sistem, her bir organizasyon için gereksiz külfet olmaksızın arzu edilen sonuçları sunmak üzere tasarlanır. İyi bir şekilde uygulanan Devlet Emniyet Programının (SSP) ve Emniyet Yönetimi Sisteminin (SMS) amacı, söz konusu organizasyonun mevcut sistemlerini ve süreçlerini tamamlamak ve iyileştirmektir. Etkin emniyet yönetimine, her bir gerekliliğin söz konusu organizasyonun kültürüne ve çalışma ortamına uygun olan yollarla ele alınması sağlanarak dikkatli planlama ve uygulamayla ulaşılır. Devletler ve hizmet sağlayıcıları için Devlet Emniyet Programının (SSP)/Emniyet Yönetimi Sisteminin (SMS) uygulanmasında nelerin göz önünde bulundurulması gerektiği hakkında daha fazla bilgiye, sırasıyla, 8. ve 9. Bölüm kapsamında ulaşılabilir.

1.3.6 Temel unsurların entegre edilmesi

Tüm sistemlerin, kişiler, süreçler ve teknolojiden oluşan üç temel unsurdan oluştuğunun unutulmaması önem arz etmektedir. Bu husus, emniyet yönetimi için de geçerlidir. Farklı süreçler, faaliyetler ve görevler tesis ederken veya sürdürürken tüm Devletler ve hizmet sağlayıcıları tarafından, her bir gerekliliğin amacının ve en önemlisi, söz konusu organizasyonun emniyet amaçlarını karşılamak için bunların birlikte nasıl çalışacaklarının göz önünde bulundurulmuş olduğundan emin olunmalıdır. Emniyet yönetiminin bu unsurlarının her biri ve karşılıklı ilişkiler bu el kitabının tümünde ele alınacaktır.

1.4 ENTEGRE RİSK YÖNETİMİ

1.4.1 Havacılık sistemi, bir bütün olarak finans, çevre, emniyet ve güvenlik gibi bir çok ve farklı işlevsel sistemlerden oluşur. Bunlardan son ikisi, daha büyükçe havacılık sisteminin başlıca operasyonel alanlarını teşkil eder. Kavramlar olarak tümünün çeşitli büyüklüklerde sonuçlara sahip olan olaylar riskiyle ilgili olmaları sebebiyle önemli özellikleri paylaşırlar. Bununla birlikte, amaca ilişkin önemli unsur bakımından farklılık gösterirler. Güvenlik, herhangi bir sistemin performansını aksatmaya yönelik kötü niyetli, kasti eylemlere ilişkindir. Emniyet, ilgili sistemlerin performansında, faktörlerin kombinasyonunun kasıtsız sonuçlarının sebebiyet verdiği olumsuz etkiye odaklanır.

1.4.2 Operasyonel bağlamda, tüm işlevsel sistemler tarafından, olumsuz sonuçların azaltılmasına yönelik olarak uygun bir şekilde yönetilmesi gereken bir takım riskler üretilir. Geleneksel olarak, her bir sistem tarafından, her bir sistemin ayrı özelliklerinin ele alınmasına yönelik olarak tasarlanan sektöre özgü risk yönetimi çerçeveleri ve uygulamaları geliştirilmiştir. Bu risk yönetimi uygulamalarının çoğu, genellikle kasıtsız sonuçların yönetilmesi olarak anılan, sistem içi sonuçların kapsamlı analizini içerir. Başka bir yön de sisteme özgü risk yönetim süreçlerinden kaynaklanan sistemlerarası sonuçlardır. Bu husus, tek bir belirli sektörün etkin risk yönetimi stratejisinin havacılığın başka bir operasyonel sektörü üzerinde olumsuz etkiye sahip olabilmesine ilişkindir. Havacılıkta, en çok vurgulanan sistemlerarası bağımlılık emniyet/güvenlik ikilemidir. Etkin güvenlik tedbirleri emniyet üzerinde, emniyet de etkin güvenlik tedbirleri üzerinde olumsuz etkilere sahip olabilir. Emniyet ve güvenlik alanları dayanak amaç unsuru bakımından farklılık gösterebilmekle birlikte, (kişilerin ve varlıkların korunmasına yönelik ortak amaçta birleşirler (siber tehditlerin ve risklerin ele alınması için havacılık emniyeti ve güvenliği alanları genelinde koordinasyonun gerekli olması gibi). Bazı hallerde, söz konusu alanlardan birinin içsel riskinin yönetilmesi diğer alana, aşağıdaki örneklerdeki gibi öngörülemeyen yollarla etki edebilecektir:

a) güvenlik riskleri sebebiyle gerekli kılınan güçlendirilmiş kokpit kapıları herhangi bir uçağın işletiminde emniyet sonuçlarına sahip olabilecektir;

b) kabinde kişisel elektronik cihazların taşınmasına yönelik kısıtlamalar, arttırılmış emniyet riskine sebebiyet vererek güvenlik riskinin kabinden kargo kompartımanına geçmesini sağlayabilecektir ve

c) çatışma bölgeleri üzerinde uçuş gerçekleştirilmesini önlemek üzere gerçekleştirilen rota değişiklikleri emniyet problemi teşkil eden sıkışık hava koridorlarıyla sonuçlanabilecektir.

1.4.3 Havacılıktaki başarılı risk yönetiminde, dahil olan tüm işlevsel sistemler de dahil olmak üzere, sistemde genel olarak risk azaltımı amaçlanmalıdır. Bu süreç, tüm sistemin uygun kuruluşun en üst seviyesinde (Devlet, bölgesel organizasyonlar, hizmet sağlayıcıları) analitik olarak değerlendirilmesini gerektirir. İşlevsel sistem ihtiyaçlarının ve karşılıklı bağımlılığın değerlendirilmesine ve entegrasyonuna entegre risk yönetimi (IRM) adı verilir. Entegre Risk Yönetimi (IRM), söz konusu organizasyonun genel risk azaltımına odaklanır. Buna, gerek içsel risklerin gerekse de sektöre özgü risk yönetimi süreçlerinin etkinliğinin ve etkisinin kantitatif ve kalitatif analiziyle ulaşılır. Entegre Risk Yönetiminde (IRM), risk yönetimi süreçlerinin risk azaltımına yönelik tek bir amaçla koordine edilmesine, uyumlaştırılmasına ve optimize edilmesine yönelik sistem geneline yayılan bir sorumluluk mevcuttur. Entegre Risk Yönetimi (IRM), işlevsel sistemlerin kendine özgü risk yönetimlerinin yerini alamaz ve bu yönetimlere ilave görevler ve sorumluluklar verme amacı taşımaz. Entegre Risk Yönetimi (IRM), sektöre özgü risk yönetiminin uzmanlığının desteklenmesine ve sosyal bakımdan kabul edilebilir bir seviyede en yüksek sistem performansı seviyesine ulaşmak için bütünsel geri bildirim sağlanmasına yönelik ayrı bir üst seviye kavramdır. Bu el kitabının kapsamı dahilinde olan emniyet riski yönetimi hakkında daha fazla bilgiye (Devletler için) 2. ve 8. Bölüm ve (hizmet sağlayıcıları için) 9. Bölüm kapsamında ulaşılabilir.

Not.— Söz konusu Devlet dahilindeki hükümetin yapısı ve sorumluluk alanları her bir alanın gözetimine etki edebilecektir. Örneğin, havacılık emniyetinden sivil havacılık otoritesinin (CAA) sorumlu olması, çevresel gözetimden ise çevre koruma kurumunun sorumlu olması. Her bir gözetim kuruluşu farklı gerekliliklere ve metodolojilere sahip olabilecektir.

Bölüm 2

EMNİYET YÖNETİMİ ANA ESASLARI

2.1 EMNİYET KAVRAMI VE GELİŞİMİ

2.1.1 Bu bölümde, temel emniyet yönetimi kavramlarına ve uygulamalarına ilişkin genel bilgiler verilmektedir. Sonraki bölümlerde yer alan emniyet yönetimine ilişkin detaylara odaklanılması öncesinde bu ana esasların idrak edilmesi önem arz etmektedir.

2.1.2 Havacılık bağlamında, emniyet, "hava araçlarının işletilmesine ilişkin veya hava araçlarının işletilmesinin doğrudan yararına olan havacılık faaliyetleriyle ilişkili risklerin azaltıldığı ve kabul edilebilir bir seviyede kontrol altına alındığı durum"dur.

2.1.3 Havacılık emniyeti dinamiktir. Yeni emniyet tehlikeleri ve riskleri sürekli olarak ortaya çıkar ve bu tehlikelerin ve risklerin hafifletilmesi gerekir. Emniyet riskleri uygun bir kontrol seviyesinde tutulduğu sürece, havacılık kadar açık ve dinamik bir sistem de emniyetli halde tutulabilir. Kabul edilebilir emniyet performansının genellikle yerel ve uluslararası normlar ve kültür ile tanımlandığını ve bunlardan etkilendiğini dikkate almak önemlidir.

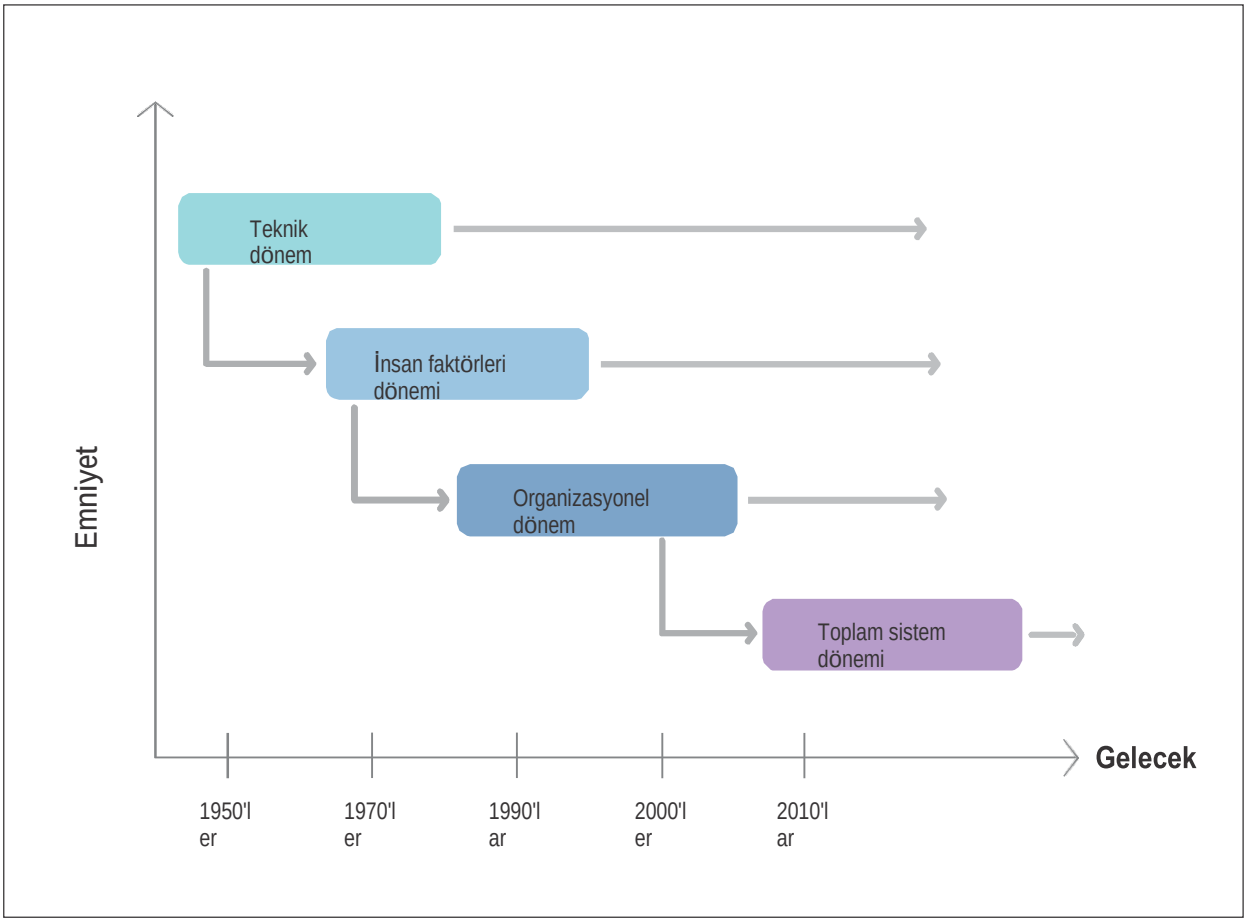
2.1.4 Havacılık emniyetindeki ilerleme, genel hatlarıyla faaliyet dönemleri doğrultusunda olan dört yaklaşımla açıklanabilir. Söz konusu yaklaşımlar aşağıda sıralanmakta ve Şekil 2-1 kapsamında resmedilmektedir.

a) *Teknik* — 1900'lerin başından 1960'ların sonlarına kadar, havacılık, tanımlanan emniyet eksikliklerinin başlangıçta teknik etkenler ve teknolojik arızalarla ilgili olduğu bir toplu taşıma şekli olarak ortaya çıkmıştır. Bu sebeple, emniyet çalışmalarının odak noktası, teknik etkenlerin (örneğin hava araçları) soruşturulması ve iyileştirilmesi olmuştur. 1950'li yıllara gelindiğinde, teknolojik gelişmeler sonucunda kazaların meydana gelme oranında kademli bir düşüş başlamış ve emniyet süreçleri de düzenlemelere uyumu ve gözetimi kapsayacak şekilde genişletilmiştir.

b) *İnsan faktörleri* — 1970'lerin başlarında, havacılık kazalarının sıklığı, büyük teknolojik ilerlemelere ve emniyet düzenlemelerindeki gelişmelere bağlı olarak belirgin bir düşüş göstermiştir. Havacılık, çok daha güvenli bir taşıma şekli haline gelmiş ve emniyet çalışmalarının odak noktası, "insan/makine arayüzü" de dahil olmak üzere, insan faktörlerini kapsayacak şekilde geliştirilmiştir. Hataların hafifletilmesine yönelik olarak yapılan kaynak yatırımına rağmen, insan faktörleri, kazaların tekrarlanmasında tekrar eden bir etken olarak anılmaya devam etmiştir. İnsan faktörleri, operasyonel ve organizasyonel bağlam tümüyle dikkate alınmadan kişiye odaklanma eğiliminde olmuştur. Kişilerin, davranışa etki edebilecek birden fazla etkeni içeren karmaşık bir ortamda faaliyet gösterdiklerinin kabulü ancak 1990'ların başlarında olmuştur.

c) *Organizasyonel* — 1990'ların ortaları sırasında, emniyet, sistematik bir perspektiften görülmeye ve organizasyonel etkenlerin yanı sıra, insan faktörleri ile teknik etkenleri kapsamaya başlamıştır. "Organizasyonel kaza" kavramı ortaya çıkarılmıştır. Bu perspektifte, organizasyon kültürü ve politikaları gibi hususların emniyet riski kontrollerinin etkinliği üzerindeki etkisi dikkate alınmıştır. İlaveten, reaktif ve proaktif metodolojilerin kullanıldığı rutin emniyet verileri toplama ve analizi, organizasyonlar tarafından bilinen emniyet risklerinin izlenmesine ve yeni çıkan emniyet trendlerinin tespit edilmesine imkan vermiştir. Bu gelişmeler, güncel emniyet yönetimi yaklaşımına yol açan öğrenmeyi ve temeli ortaya çıkarmıştır.

d) *Toplam sistem* — 21. yüzyılın başından itibaren, bir çok Devlet ve hizmet sağlayıcısı tarafından geçmişteki emniyet yaklaşımlarına sahip çıkılmış ve daha yüksek düzeyde bir emniyet olgunluğu geliştirilmiştir. Söz konusu Devletler ve hizmet sağlayıcıları tarafından Devlet Emniyet Programı (SSP) veya Emniyet Yönetimi Sistemleri (SMS'ler) uygulanmaya başlanmıştır ve emniyet faydalarının meyveleri toplanmaktadır. Bununla birlikte, toplam havacılık sistemine yönelik daha geniş bağlama minimal düzeyde itibar edilerek, emniyet sistemleri bugüne kadar ağırlıklı olarak münferit emniyet performansına ve yerel kontrole odaklanmıştır. Bu odaklanma, havacılık sisteminin karmaşıklığının ve havacılık emniyetinde tümü bir role sahip olan farklı organizasyonların giderek tanınmasına yol açmıştır. Organizasyonlar arasındaki arayüzlerin olumsuz sonuçlara katkıda bulunduğunu gösteren bir çok kaza ve olay örneği mevcuttur.



Şekil 2-1. Emniyetin gelişimi

2.1.5 Emniyetin istikrarlı, yoğunlaşan gelişimi, Devletleri ve hizmet sağlayıcılarını, sistemin bileşenleri olan kişiler, süreçler ve teknolojiler arasındaki etkileşimlere ve arayüzlere ciddi ehemmiyetin verildiği bir noktaya getirmiştir. Bu da kişilerin sistemde oynadıkları rolün daha fazla takdir görmesini sağlamıştır. Emniyet, hizmet sağlayıcıları arasındaki ve hizmet sağlayıcıları ile Devletler arasındaki işbirliğinden fayda görür. Bu perspektif, hizmet sağlayıcıları arasında birden fazla ortak çalışmaya dayalı girişimi ve emniyet sorunları ele alınırken ortak çalışmanın getirdiği faydaların takdirini teşvik etmiştir. ICAO Pist Emniyeti Programı iyi bir örnektir.

2.1.6 Ortak çalışmaya dayalı toplam sistemin gelişmesi için, organizasyonlar (Devletler de dahil olmak üzere) arasındaki arayüzlerin ve etkileşimlerin iyi bir şekilde idrak edilmesi ve yönetilmesi gerekir. Toplam havacılık sistemi yaklaşımının Devlet Emniyet Programlarının (SSP) geliştirilmesinde oynayabileceği rolü Devletler de kabul etmeye başlamışlardır. Örneğin, toplam havacılık sistemi yaklaşımı, birden fazla havacılık faaliyetlerinin ötesine geçen emniyet risklerinin yönetilmesine yardımcı olur.

2.2 SİSTEMDEKİ BİREYLER

221 Kişilerin emniyete yönelik sorumlulukları hakkında ne şekilde düşündükleri ve iş yerindeki görevlerinin ifasında başkaları ile nasıl etkileşim kurdukları, organizasyonlarının emniyet performansına belirgin bir şekilde etki eder. Emniyetin yönetilmesinde, kişiler tarafından organizasyonel emniyete, gerek pozitif gerek negatif olmak üzere, nasıl katkıda bulunduğu ele alınmalıdır. İnsan faktörleri, kişilerin dünya ile etkileşim kurdukları yolların, kabiliyetlerinin ve sınırlarının anlaşılması ve kişilerin iş yapma yollarını geliştirmek üzere beşeri faaliyete etki edilmesi ile ilgilidir. Sonuç olarak, insan faktörlerinin göz önünde bulundurulması, emniyet yönetiminin, riskleri anlamak, tanımlamak ve hafifletmek ve bireyler tarafından organizasyonel emniyete yönelik katkıları optimize etmek için gerekli olan ayrılmaz bir parçasıdır.

222 Emniyet yönetimi süreçlerinde insan faktörlerinin göz önünde bulundurulduğu kilit yollar şunlardır:

a) üst yönetim tarafından, insan performansını optimize eden ve personeli, söz konusu organizasyonun emniyet yönetimi süreçlerine faal bir şekilde katılmaya ve bu süreçlere katkıda bulunmaya teşvik eden bir çalışma ortamının oluşturulmasına yönelik taahhütte bulunulması;

b) ortak anlayışı ve beklentileri sağlamak üzere personelin emniyet yönetimine ilişkin sorumluluklarının açıklığa kavuşturulması;

c) personele, söz konusu organizasyon tarafından aşağıdaki türden bilgilerin temin edilmesi:

1) organizasyonel süreçlere ve prosedürlere ilişkin olarak beklenen davranışları tanımlayan;

2) münferit davranışlara karşılık olarak söz konusu organizasyon tarafından hangi tedbirlerin alınacağını tanımlayan;

d) insan kaynakları seviyelerinin operasyonel taleplerin karşılanması için yeterli kişinin mevcut olmasını sağlayacak şekilde izlenmesi ve ayarlanması;

e) emniyet raporlamasını teşvik etmek üzere politikaların, süreçlerin ve prosedürlerin tesis edilmesi;

f) ilişkili organizasyonel ve operasyonel etkenlere özellikle dikkat gösterilerek, değişken insan performansına ve insan sınırlarına ilişkin risklerin göz önünde bulundurulmasına imkan vermek üzere emniyet verilerinin ve emniyet bilgilerinin analiz edilmesi;

g) aşağıdaki amaçlarla, açık, öz ve işletilir politikaların, süreçlerin ve prosedürlerin oluşturulması:

1) insan performansının optimize edilmesi;

2) yanlışlıkla yapılan hataların önlenmesi;

3) değişken insan performansının istenmeyen sonuçlarının azaltılması; bunların etkinliğinin normal operasyonlar sırasında sürekli olarak izlenmesi;

h) normal operasyonların sürekli izlenmesi, süreçlerin ve prosedürlerin takip edilip edilmediğinin ve takip edilmediğinde, sebebin tespiti için soruşturmaların yürütülüp yürütülmediğinin değerlendirilmesini kapsar;

i) emniyet soruşturmaları, çoğu durumda kişilerin işin yapılması için ellerinden geleni yaptığına dair anlayışla, katkıda bulunan insan faktörlerinin değerlendirilmesini, sadece davranışları değil, aynı zamanda bu davranışların sebeplerinin (bağlam) incelenmesini içerir;

j) değişim yönetim süreci, kişilerin sistemdeki gitgide gelişen görevlerinin ve rollerinin göz önünde bulundurulmasını içerir;

k) görevlerini ifa etmeye yetkin olmalarını sağlamak üzere personel eğitime tabi tutulur, eğitimin etkinliği gözden geçirilir ve eğitim programları, değişen ihtiyaçları karşılayacak şekilde uyarlanır.

223 Emniyet yönetiminin etkinliği ağırlıklı olarak üst yönetim tarafından, insan performansını optimize eden ve personeli, söz konusu organizasyonun emniyet yönetimi süreçlerine faal bir şekilde katılmaya ve bu süreçlere katkıda bulunmaya teşvik eden bir çalışma ortamının oluşturulmasına yönelik taahhütte bulunma derecesine bağlıdır.

224 Söz konusu organizasyon tarafından insan performansına etki edilme yolunun ele alınması için, etkin emniyet yönetimi uygulamak üzere üst düzey destek mevcut olmalıdır. Bu destek, doğru çalışma ortamının ve insan faktörlerine işaret edecek doğru emniyet kültürünün oluşturulmasına yönelik yönetim taahhüdünü kapsar. Bu sayede, söz konusu organizasyondaki herkesin tutum ve davranışlarına etki edilecektir. Emniyet kültürü hakkında daha fazla bilgiye 3. Bölüm kapsamında ulaşılabilir.

225 Emniyet performansına ilişkin olarak insan faktörlerinin değerlendirilmesini desteklemek üzere bir dizi model oluşturulmuştur. Farklı sistem bileşenlerinin insanlar üzerindeki etkisini ve etkileşimini tasvir etmek için SHELL Modeli iyi bilinen, faydalı ve insan faktörlerinin Emniyet Riski Yönetiminin (SRM) entegre bir parçası olarak değerlendirilmesi gerektiğini vurgulayan bir modeldir.

226 İnsan (modelin merkezinde olmak üzere) ve işyeri bileşenleri arasındaki ilişki Şekil 2-2'de tasvir edilmektedir. SHELL Modeli dört uydu bileşen içerir:

a) Yazılım (S): prosedürler, eğitim, destek, vb.;

b) Donanım (H): makineler ve ekipmanlar;

c) Ortam (E): L-H-S sisteminin geri kalanının işlemesi gereken çalışma ortamı ve

d) İnsanlar (Liveware) (L): işyerindeki diğer kişiler.

Şekil 2-2. SHELL Modeli

2.2.7 *İnsanlar (Liveware*). Söz konusu modelin kritik odak noktası, operasyonların ön saflarındaki kişilerdir ve bu kişiler, modelin merkezinde resmedilmektedir. Bununla birlikte, bu unsur, modeldeki tüm boyutlar arasında en az öngörülebilir ve dahili (açıklık, yorgunluk, motivasyon, vb.) ve harici (sıcaklık, ışık, gürültü, vb.) etkilenimlerin etkilerine en duyarlı olandır. Yeni koşullara dikkat çekici derecede uyabilmelerine karşın, kişiler, performansta kayda değer değişimlere tabidirler. Kişiler, donanımlarla aynı derecede standart hale getirilemez; dolayısıyla, bu yapının uçları basit ve düz değildir. İnsan performansını tehlikeye atabilecek gerilimlerin önlenmesi için çeşitli SHELL yapıları ile merkezi Liveware yapısı arasındaki arayüzlerdeki düzensizliklerin etkilerinin anlaşılması gerekmektedir. Modüllerin sivriltilmiş uçları, her bir modülün eksik eşleşmesini temsil etmektedir. Bu husus, havacılık sisteminin çeşitli bileşenleri arasındaki aşağıdaki arayüzlerin görselleştirilmesinde fayda sağlamaktadır:

a) *Liveware (İnsanlar)-Donanım (L-H).* L-H arayüzü, insan ve ekipmanın, makinelerin ve tesislerin fiziksel özellikleri arasındaki ilişkiye işaret etmektedir. Burada, ekipmanların personel tarafından kullanılmasının ergonomisi, emniyet bilgilerinin nasıl gösterildiği ve anahtarların ve çalıştırma kollarının nasıl etiketlendiği ve kullanım bakımından mantıklı ve sezgisel olacak şekilde nasıl kullanıldığı değerlendirilmektedir.

b) *Liveware (İnsanlar) - Yazılım (L-S)*. L-S arayüzü, düzenlemeler, el kitapları, kontrol listeleri, yayınlar, süreçler ve prosedürler ve bilgisayar yazılımları gibi, işyerinde bulunan destekleyici sistemler ile insanlar arasındaki ilişkidir. Tecrübenin güncelliği, tutarlılık, format ve sunum, kelime hazinesi, açıklık ve sembollerin kullanımı gibi hususları kapsar. L-S kapsamında süreçler ve prosedürler ve bunların takip ve anlaşılma bakımından ne kadar basit oldukları değerlendirilir.

c) *Liveware (İnsanlar)-Liveware (İnsanlar) (L-L)*. L-L arayüzü, çalışma ortamındaki insanların arasındaki ilişki ve etkileşimdir. Bu etkileşimlerin bazıları organizasyon dahilinde (iş arkadaşları, amirler, yöneticiler), bir çoğu ise farklı rollere sahip olan farklı organizasyonlardan olan kişilerin arasındadır (hava trafik kontrolleri ile pilotlar, pilotlar ile teknisyenler, vb.) İnsan performansının tespit edilmesinde iletişim ile kişilerarası becerilerin yanı sıra, grup dinamiklerinin önemi göz önünde bulundurulur. Ekip kaynak yönetiminin ilerlemesi ve ekip kaynak yönetiminin hava trafik hizmetlerine (ATS) ve bakım operasyonlarına genişletilmesi, organizasyonlar tarafından hataların yönetiminde ekip performansının dikkate alınmasına imkan vermiştir. Personel/yönetim ilişkileri ve organizasyon kültürü de bu arayüzün kapsamı dahilindedir.

d) *Liveware (İnsanlar)-Ortam (L-E)*. Bu arayüz, insan ile fiziki ortam arasındaki ilişkiyi kapsar. Sıcaklık, ortam ışığı, gürültü, titreşim ve hava kalitesi gibi hususları içerir. Hava durumu, altyapı ve bölge gibi harici çevresel etkenleri de dikkate alır.

2.3 KAZALARDAKİ NEDEN- SONUÇ İLİŞKİSİ

2.3.1 Profesör James Reason tarafından geliştirilen ve havacılık endüstrisinde iyi bilinen "İsviçre Peyniri" (veya Reason) Modeli, kazaların birden fazla savunmanın ardışık ihlallerini içerdiğini tasvir etmektedir. Bu ihlaller, ekipman arızaları veya operasyonel hatalar gibi bir dizi etkinleştirici faktör tarafından tetiklenebilmektedir. İsviçre Peyniri Modelinde, havacılık gibi karmaşık sistemlerin, savunma katmanlarıyla ("bariyerler" olarak da bilinir) fazlasıyla savunulduğu ileri sürülmektedir. Tek nokta kırılması nadiren sonuca bağlıdır. Emniyet savunmalarındaki ihlaller, etkileri veya zarar verme potansiyeli belirli çalışma koşulları (gizli koşullar olarak bilinir) ile etkinleştirilinceye değin uykuda kalabilecek olan, söz konusu organizasyonun üst seviyelerinde alınan kararların sonuçların geciktirilmiş bir sonucu olabilir. Bu gibi spesifik koşullar altında, operasyonel seviyedeki insan kaynaklı kırılmalar (veya "aktif kırılmalar), emniyet savunmasının son katmanını ihlal edecek şekilde hareket eder. Reason Modelinde, tüm kazalarda aktif kırılmaların ve gizli koşulların bir kombinasyonunun yer aldığı ileri sürülür.

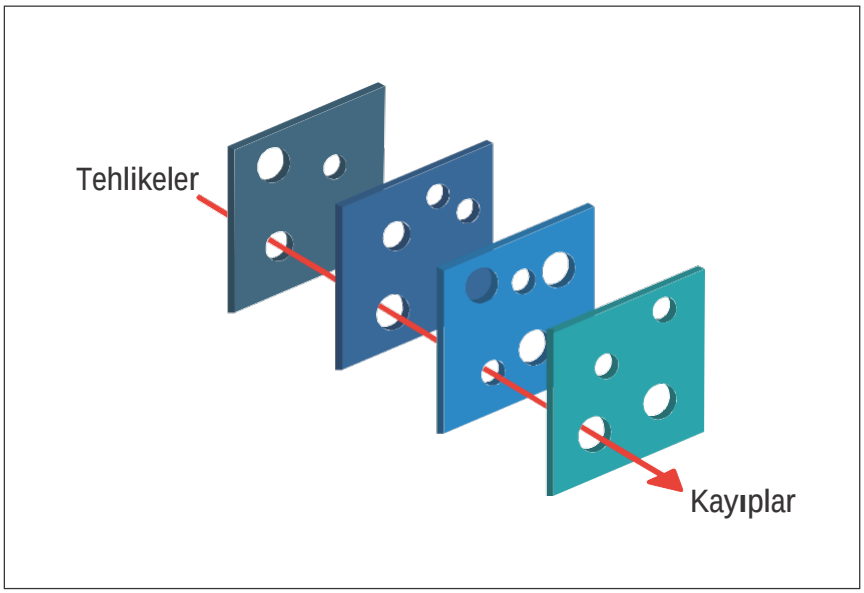
2.3.2 Aktif kırılmalar, hatalar ve kural ihlalleri de dahil olmak üzere, ani olumsuz etkiye sahip olan eylemler veya eylemsizliklerdir. Bunlara geçmiş tecrübelerden edinilmiş bilgilerle, emniyetsiz eylemler olarak bakılır. Aktif kırılmalar, ön saflardaki personel (pilotlar, hava trafik kontrolörleri, hava aracı bakım teknisyenleri, vb.) ile ilişkilidir ve zararlı sonuçlara yol açabilirler.

2.3.3 Gizli koşullar, zarar verici herhangi bir sonucun çok ötesinde sistemde mevcut olabilirler. Gizli koşulların sonuçları, uzun bir süre boyunca uykuda kalmaya devam edebilir. Başlangıçta, bu gizli koşullar zararlı olarak algılanmaz, ancak belirli koşullar altında, operasyonel seviye savunmaları ihlal edildiğinde açık hale gelebilir. Olaydan zaman ve yer bakımından çok uzakta kalan kişiler tarafından bu koşullar yaratılabilir. Sistemdeki gizli koşullar, emniyet kültürü, ekipman tercihleri veya prosedür tasarımı, çelişen organizasyon hedefleri, kusurlu organizasyonel sistemler veya yönetim kararları tarafından oluşturulan koşulları kapsayabilir.

2.3.4 Kişilerden kaynaklanan aktif kırılmaları minimize etmek amacıyla, yerel çalışmalardan ziyade sistem genelini esas alarak bu gizli koşulları tanımlamakla "organizasyonel kaza" paradigması bu hususta yardım sağlar. Burada önemli olan, gizli koşulların, oluşturulduklarında, iyi niyete sahip olmuş olmalarıdır. Organizasyonel karar alıcılar tarafından genellikle sonu olan kaynaklar ve potansiyel olarak çelişen öncelikler ve maliyetler dengelenir. Karar alıcılar tarafından büyük çaplı organizasyonlarda günlük esasa dayalı olarak alınan kararlar, belirli koşullarda, istemsiz bir şekilde zarar verici bir sonuca yol açabilmektedir.

2.3.5 Şekil 2-3'de, İsviçre Peyniri Modelinin, kazalardaki neden-sonuç ilişkisindeki organizasyonel ve yönetimsel etkenlerin karşılıklı etkileşiminin idrak edilmesine nasıl yardımcı olduğu tasvir edilmektedir. Organizasyonun tüm seviyelerindeki kararlardaki veya insan performansındaki değişimler karşısında koruma sağlamak amacıyla havacılık sisteminde birden fazla koruyucu katman oluşturulur. Bununla birlikte, her bir tabaka genel olarak, "İsviçre Peyniri"nin dilimlerindeki deliklerle resmedilen zayıflıklara sahiptir. Kimi zaman, söz konusu zayıflıkların tümü, tüm savunma bariyerlerine nüfuz eden ve felaket niteliğinde sonuca sebebiyet verebilecek olan bir ihlale yol açarak sıralanır (hizalaştırılan deliklerle temsil edilmektedir). İsviçre Peyniri Modeli, gizli koşulların sistemde nasıl daimi olarak mevcut olduğunu ve yerel tetikleme etkenleriyle nasıl açığa çıkabildiğini gösterir.

2.3.6 Savunmalardan bazılarının veya ihlallerin, arayüz bağlantısına sahip olan herhangi bir organizasyon tarafından tesir görebileceğini fark etmek önemlidir. Bu sebeple, hizmet sağlayıcıları tarafından bu arayüzlerin değerlendirilmesi ve yönetilmesi hayati önem arz etmektedir.



Şekil 2-3. Kazalarda neden-sonuç ilişkisi kavramı

2.3.7 Emniyet yönetimine yönelik "İsviçre Peyniri" uygulamaları

2.3.7.1 "İsviçre Peyniri" Modeli, söz konusu durumun açığa çıkmasına imkan vermiş olabilecek organizasyonel koşullarda herhangi bir kazaya veya belirlenmiş tehlikeye müdahil olan kişiler görmezden gelinerek gerek Devletler gerek hizmet sağlayıcıları tarafından bir analiz rehberi olarak kullanılabilir. Emniyet Riski Yönetiminde, emniyet gözetiminde, iç denetimde, değişim yönetiminde ve emniyet soruşturmasında uygulanabilir. Her bir durumda, söz konusu model, söz konusu organizasyonun savunmalarından hangilerinin etkin olduğunun, hangilerinin ihlal edilebildiğinin veya ihlal edilmiş olduğunun ve sistemin ilave savunmalardan nerelerde fayda görebileceğinin değerlendirilmesi için kullanılabilir. Belirlenmesi sonrasında, savunmalardaki zayıflıklar gelecekteki kazalar ve olaylar karşısında güçlendirilebilir.

2.3.7.2 Uygulamada, söz konusu olay, Şekil 2-3'ün yorumlanmasında gösterilen ok (tehlikelerden kayıplara doğru olmak üzere) istikametinde savunmaları ihlal edecektir. Duruma ilişkin değerlendirmeler ise, bu kez kayıplardan tehlikeye doğru olmak üzere, karşı yönde yürütülecektir. Gerçek havacılık kazalarında genellikle ilave bir karmaşıklık derecesi yer alacaktır. Devletlere ve hizmet sağlayıcılarına, kazaların nasıl ve neden oluştuğunun idrak edilmesinde yardımcı olabilecek daha fazla komplike model mevcuttur.

2.3.8 Pratik kopma

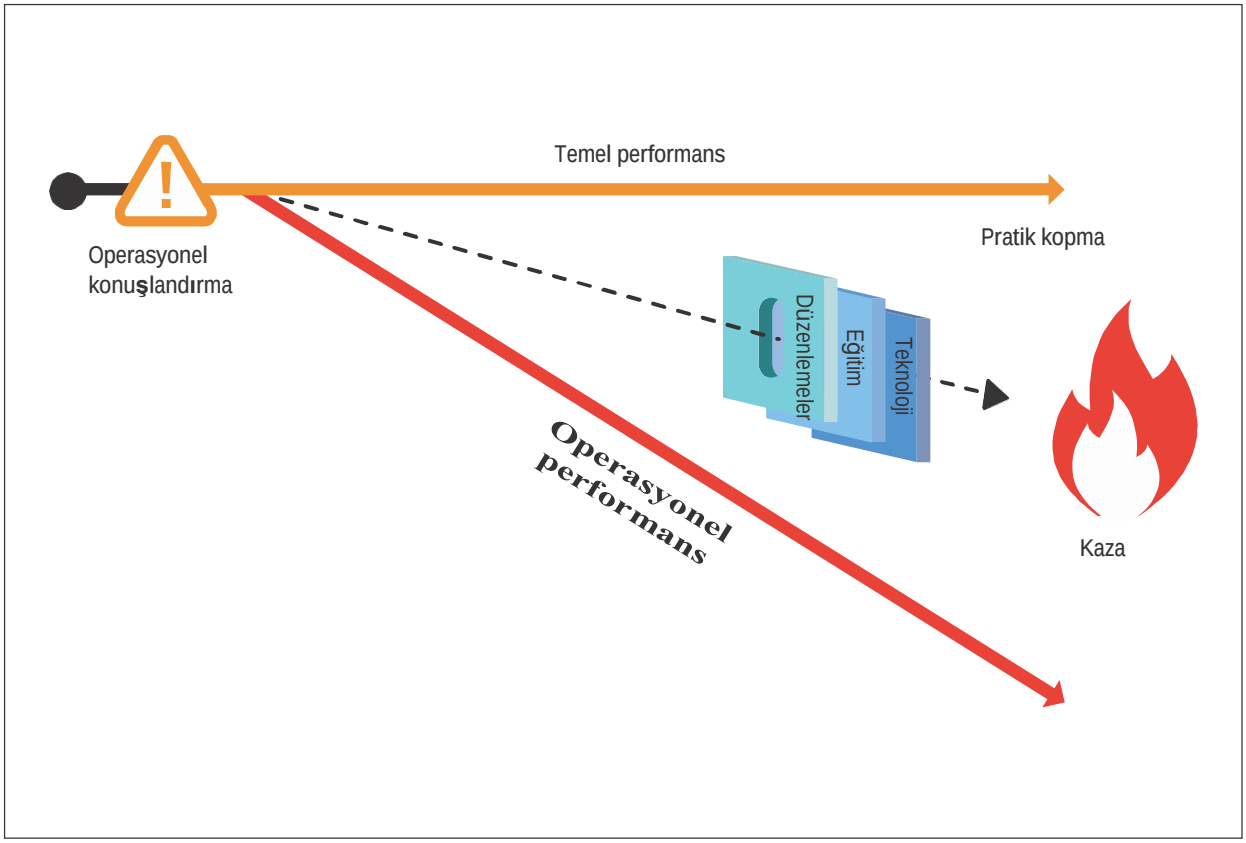
2.3.8.1 Scott A. Snook'un pratik kopma teorisi, herhangi bir sistemin performansının başlangıçtaki tasarımından nasıl "koptuğunu" anlamak üzere kullanılmaktadır. Görevler, prosedürler ve ekipmanlar genellikle, başlangıçta, neredeyse her şeyin önceden görülebileceğine ve kontrol edilebileceğine dair zımni bir varsayımla ve her şeyin beklendiği gibi çalıştığı ideal koşullarda teorik bir ortamda tasarlanır ve planlanır. Bu husus genel olarak aşağıdaki üç ana varsayıma dayalıdır:

a) sistem üretim hedeflerine ulaşmak için ihtiyaç duyulan teknolojinin mevcut olması;

b) personelin, söz konusu teknolojiyi amaçlandığı şekilde hakkıyla kullanmak üzere eğitilmesi, buna yetkin ve bu konuda motive olması ve

c) politika ve prosedürler tarafından sistemin ve insan davranışının dikte edilecek olması.

Şekil 2-4'de gösterilen operasyonel konuşlandırmanın başlangıcından itibaren grafik olarak düz bir çizgi olarak sunulabilen temel (veya ideal) sistem performansının altında bu varsayımlar yatar.



Şekil 2-4. Pratik kopma kavramı

2.3.8.2 Operasyonel olarak konuşlandırılması sonrasında, söz konusu sistemin, çoğu zaman temel performansı (turuncu çizgi) takip ederek ideal olarak tasarlandığı şekilde çalışması gerekir. Gerçekte, operasyonel performans, karmaşık, sürekli değişen ve genellikle zahmetli ortamdaki gerçek hayat operasyonlarının sonucu olarak varsayılan temel performanstan genellikle farklılık gösterir. Buradaki kopmanın günlük uygulamanın bir sonucu olması sebebiyle "pratik kopma" olarak anılır. "Kopma" terimi bu bağlamda, dış etkilenimler sebebiyle amaçlanan yoldan aşamalı olarak ayrılmak anlamında kullanılır.

2.3.8.3 Snook, tasarımının ne kadar dikkatli ve iyi bir şekilde düşünülmüş olmasına bakılmaksızın, pratik kopmanın tüm sistemlerde kaçınılmaz olduğunu iddia etmektedir. Pratik kopmanın bazı sebepleri şunlardır:

a) öngörüldüğü gibi işlemeyen teknoloji;

b) belirli çalışma koşullarında planlandığı gibi yürütülemeyen prosedürler;

c) ilave bileşenler de dahil olmak üzere, sistemdeki değişiklikler;

d) diğer sistemler ile etkileşimler;

e) emniyet kültürü;

f) kaynakların yeterliliği (veya yetersizliği) (örneğin, destek ekipmanları);

g) operasyonların geliştirilmesi için başarılardan ve başarısızlıklardan ders alınması ve benzeri.

2.3.8.4 Gerçekte, yerel uyarlamalar (veya geçici çözümler) ve kişisel stratejiler uygulayarak kişiler, söz konusu sistemin eksikliklerine karşın, sistemin genel olarak günlük esasta çalışmasını sağlayacaklardır. Bu geçici çözümler, mevcut emniyet riski kontrollerinin ve savunmalarının korunmasını baypas edebilecektir.

2.3.8.5 Denetimler, gözlemler ve Emniyet Performansı Göstergelerinin (SPI'ler) izlenmesi gibi emniyet güvence faaliyetleri, "pratikte kopan" faaliyetlerin açığa çıkarılmasına yardımcı olabilir. Söz konusu kopmanın neden oluştuğunu tespit etmek için emniyet bilgilerinin analiz edilmesi, emniyet risklerinin hafifletilmesine yardımcı olur. Pratik kopma, operasyonel konuşlandırmanın ne kadar başlangıcında belirlenirse, söz konusu organizasyon tarafından müdahale bulunulması o kadar kolay olur. Devletlere ve hizmet sağlayıcılarına yönelik emniyet güvencesi hakkında daha fazla bilgiye, sırasıyla, 8. ve 9. Bölüm kapsamında ulaşılabilir.

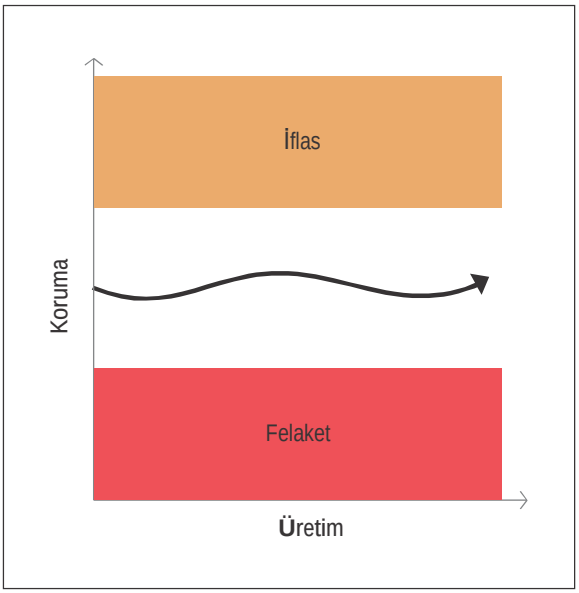
2.4 YÖNETİM İKİLEMİ

2.4.1 Hizmet sunumu ile iştigal eden her organizasyonda üretim/karlılık ve emniyet riskleri birbirleriyle bağlantılıdır. Organizasyonlar tarafından işe devam edebilmek için çıktıyı kabul edilebilir emniyet riskleriyle (ve emniyet riski kontrollerinin uygulanmasına dahil olan maliyetlerle) dengeleyerek karlılık sürdürülmelidir. Tipik emniyet riski kontrolleri, teknolojiyi, eğitimi, süreçleri ve prosedürleri kapsar. Devletler için de emniyet riski kontrolleri benzer niteliktedir, diğer bir deyişle, personelin eğitimi, teknolojinin uygun kullanımı, etkin gözetim ve gözetimi destekleyen dahili süreçler ve prosedürler. Emniyet riski kontrollerinin uygulanmasının, para, zaman, kaynaklar gibi bir bedeli vardır ve emniyet riski kontrollerinin amacı genel olarak üretim performansını değil, emniyet performansını iyileştirmektir. Bununla birlikte, "korumada"ki bazı yatırımlar da kazaları ve olayları ve bu sayede ilişkili maliyetleri azaltarak "üretimi" iyileştirebilir.

2.4.2 Emniyet alanı, emniyet riski kontrolleri vasıtasıyla öngörülen emniyet koruması sürdürülürken organizasyon tarafından istenen üretimin/karlılığın dengelendiği alana yönelik bir metafordur. Örneğin, herhangi bir hizmet sağlayıcısı tarafından yeni ekipman yatırımında bulunulmak istenebilir. Söz konusu yeni ekipman eş zamanlı olarak gerekli verimlilik iyileştirmelerinin yan sıra iyileştirilmiş güvenilirlik ve emniyet performansı sunabilir. Bu tür karar alma, gerek söz konusu organizasyonun elde edeceği faydaların gerekse de dahil olan emniyet risklerinin değerlendirilmesini içerir. Emniyet riski kontrollerine haddinden fazla kaynak tahsis edilmesi, söz konusu faaliyetin kar getirmez, böylelikle de söz konusu organizasyonun yaşama kabiliyetini tehlike atar hale gelmesine yol açabilir.

2.4.3 Diğer taraftan, koruma pahasına üretim için haddinden fazla kaynak tahsis edilmesi, söz konusu ürün veya hizmet üzerinde herhangi bir etkiye sahip olabilir ve sonuç itibariyle herhangi bir kazaya yol açabilir. Bu sebeple, kaynakların dengelenmemiş tahsisatının mevcut olduğuna veya oluşmakta olduğuna dair erken uyarı veren bir emniyet sınırının tanımlanması elzemdir. Organizasyonlar, iflasa çok yaklaştıklarını fark etmek için finansal yönetim sistemlerini kullanır ve emniyet performanslarını izlemek için emniyet yönetimi tarafından kullanılan aynı mantığı ve araçları tatbik ederler. Bu sayede, söz konusu organizasyonun emniyet alanı dahilinde emniyetli ve karlı bir şekilde faaliyet göstermesine imkan verilir. Organizasyonun emniyet alanının sınırları Şekil 2-5 kapsamında tasvir edilmektedir. Emniyet risklerinin ve harici etkilenimlerin zamanla değişmesine bağlı olarak emniyet alanının organizasyonlar tarafından sürekli olarak izlenmesi ve yönetilmesi gerekir.

2.4.4 Karlılığı ve emniyeti (veya üretimi ve korumayı) dengeleme ihtiyacı, hizmet sağlayıcılarının perspektifinden rahatlıkla anlaşılan ve kabul edilen bir gereklilik haline gelmiştir. Sertifikasyonu ve gözetimi içeren Devlet koruma işlevleri için gerekli olan kaynakları dengeleme gerekliliği göz önünde bulundurulduğunda, bu denge, emniyetin Devlet tarafından yönetimi için de eşit ölçüde geçerlidir.



Şekil 2-5. Emniyet alanı kavramı

2.5 EMNİYET RİSKİ YÖNETİMİ

Emniyet Riski Yönetimi (SRM), emniyet yönetiminin kilit bir bileşenidir ve tehlike tanımlamayı, emniyet riski değerlendirmesini, emniyet riskinin hafifletilmesinin ve risk kabulünü içerir. Havacılık sisteminin sürekli olarak değişmesi, yeni tehlikelerin ortaya çıkabilmesi ve bazı tehlikelerin ve ilişkili emniyet risklerinin zamanla değişebilmesi sebebiyle, Emniyet Riski Yönetimi (SRM) süreklilik arz eden bir faaliyettir. İlaveten, başkaca tedbirin gerekli olup olmadığını tespit etmek için, uygulanan emniyet riski hafifletme stratejilerinin etkinliği izlenmelidir.

2.5.1 Tehlikelere giriş

2.5.1.1 Havacılıkta, tehlike, sistem veya sistemin ortamı dahilinde bir veya başka bir şekilde mevcut olan, uykudaki zarar potansiyeli olarak değerlendirilebilir. Bu zarar potansiyeli, doğal koşul (örneğin, bölge) veya teknik durum (örneğin, pist işaretlemeleri) gibi farklı şekillerde ortaya çıkabilir.

2.5.1.2 Tehlikeler, havacılık faaliyetlerinin kaçınılmaz bir parçasıdır, ancak tehlikelerin ortaya çıkması ve olası olumsuz sonuçlar, söz konusu tehlikenin herhangi bir emniyetsiz koşula yol açma potansiyelini içermeyi amaçlayan hafifletme stratejileri ile ele alınabilir. Havacılık, kontrol edildikleri sürece tehlikelerle birlikte var olabilir. Tehlike tanımlama, Emniyet Riski Yönetimi (SRM) sürecindeki birinci adımdır. Emniyet riski değerlendirmesinin önünde gelir ve tehlikelerin ve ilgili sonuçlarının açık bir şekilde kavranmasını gerektirir.

2.5.2 Tehlikelerin ve sonuçlarının kavranması

2.5.2.1 Tehlike tanımlama, hava araçlarının veya havacılık emniyeti ile ilgili ekipmanların, ürünlerin ve hizmetlerin emniyetsiz bir şekilde kullanılmasına sebebiyet verebilecek veya katkıda bulunabilecek olan koşullara veya nesnelere odaklanır (doğrudan havacılık emniyetine ilişkin olan tehlikelerin diğer genel/endüstriyel tehlikelerden ayırt edilmesine ilişkin rehberlik müteakip maddelerde ele alınmaktadır).

2.5.2.2 Mesela, on beş knotluk bir rüzgar düşünün. On beş knotluk rüzgarın tehlikeli bir koşul olması gerekmez. Gerçekte, doğrudan pist üzerine gelen on beş knotluk rüzgar uçağın kalkış ve iniş performansını iyileştirir. Fakat, on beş knotluk rüzgarın pist boyunca esmesi halinde, operasyonlar için tehlikeli olabilecek olan bir yan rüzgar koşulu oluşur. Bunun sebebi ise uçağın instabil olmasına katkıda bulunma potansiyelidir. Kontroldeki azalma, yanal pist ihlali gibi bir olaya sebebiyet verebilecektir.

2.5.2.3 Tehlikeleri akıbetleri ile karşılaştırmak insanlarda yaygın görülen bir durumdur. Akıbet, herhangi bir tehlike tarafından tetiklenebilen sonuçtur. Örneğin, pist ihlali (zamanında duramama) kontamine pist tehlikesine ilişkin olası akıbettir. Öncelikle tehlikeyi açık bir şekilde tanımlayarak olası akıbetler kolaylıkla tanımlanabilir.

2.5.2.4 Yukarıdaki yan rüzgar örneğinde, yanal kontrolün kaybedilerek pist ihlalinin oluşması söz konusu tehlikenin ani bir sonucudur. Nihai akıbet ise bir kaza olabilir. Tehlikenin zarar verme potansiyeli bir veya daha fazla akıbetle gerçekleşebilir. Emniyet riski değerlendirmelerinde tüm olası akıbetlerin belirlenmesi önemlidir. En uçtaki akıbet olan insan hayatının kaybının, hava aracı kazaları, artan uçuş ekibi iş yükü veya yolcu rahatsızlığı gibi daha düşük akıbetleri içerenlerden ayırt edilmesi gerekir. Akıbetlerin tanımlanması risk değerlendirmesine ve kaynakların önceliklendirilmesi ve tahsisi yoluyla müteakip hafifletmelerin geliştirilmesine ve uygulanmasına bilgi sağlayacaktır. Detaylı ve kapsamlı tehlike tanımlaması, emniyet risklerinin daha tutarlı bir şekilde değerlendirilmesini beraberinde getirecektir.

Tehlike tanımlama ve önceliklendirme

2.5.2.5 Tehlikeler, organizasyonun tüm seviyelerinde mevcuttur ve raporlama sistemleri, incelemeler, denetimler, beyin fırtınası oturumları ve uzman değerlendirmesi de dahil olmak üzere, bir çok kaynak vasıtasıyla tespit edilebilir. Amaç, kazalara, olaylara veya emniyet ile ilgili diğer hadiselere yol açmaları öncesinde tehlikeleri proaktif bir şekilde tanımlamaktır. Proaktif tehlike tanımlamaya ilişkin en önemli mekanizma, gönüllü emniyet raporlaması sistemidir. Gönüllü emniyet raporlaması sistemlerine ilişkin ilave rehberliğe 5. Bölüm kapsamında ulaşılabilir. Bu tür raporlama sistemleri vasıtasıyla toplanan bilgiler, rutin yerinde incelemeler veya organizasyonel denetimler sırasında kayda alınan bulgular veya gözlemlerle tamamlanabilir.

2.5.2.6 Tehlikeler ayrıca, iç ve dış soruşturma raporlarının gözden geçirilmesi veya incelenmesi sırasında da tanımlanabilir. Kaza veya olay soruşturma raporlarının gözden geçirilmesi sırasında tehlikelerin dikkate alınması, söz konusu kuruluşun tehlike tanımlama sisteminin geliştirilmesine yönelik iyi bir yoldur. Söz konusu organizasyonun emniyet kültürü henüz etkin gönüllü emniyet raporlamasını destekleyecek kadar olgun olmadığında veya sınırlı olaylara veya raporlara sahip olan küçük çaplı organizasyonlarda bu husus özellikle önem arz etmektedir. ICAO, ticaret birlikleri veya diğer uluslararası kuruluşlar gibi dış kaynaklar, operasyonlar ve faaliyetler ile bağlantılı spesifik tehlikeler için önemli bir kaynaktır.

2.5.2.7 Tehlike tanımlama kapsamında ayrıca, söz konusu organizasyonun dışında üretilen tehlikeler ile ağır hava koşulları veya volkanik kül gibi, söz konusu organizasyonun doğrudan kontrolü dışında olan tehlikeler de göz önünde bulundurulabilir. Yeni gelişen emniyet risklerine ilişkin tehlikeler de organizasyonlar tarafından sonuçta ortaya çıkabilecek durumlara yönelik olarak hazırlık yapılmasına yönelik önemli bir yoldur.

2.5.2.8 Tehlikeler tanımlanırken aşağıdakilerin göz önünde bulundurulması gerekir:

a) sistem tanımı;

b) ekipman ve görev tasarımı da dahil olmak üzere tasarım faktörleri;

c) insan performansı sınırları (örneğin, fizyolojik, psikolojik, fiziki ve bilişsel);

d) dokümantasyon ve kontrol listeleri ile bunların gerçek çalışma koşullarında doğrulanması da dahil olmak üzere, prosedürler ve çalışma uygulamaları;

e) iletişim araçları, terminoloji ve dil de dahil olmak üzere, iletişim etkenleri;

f) personelin işe alınmasına, eğitimine ve elde tutulmasına, üretim ve emniyet hedeflerinin uyumluluğuna, kaynakların tahsisatına, çalışma baskılarına ve kurumsal emniyet kültürüne ilişkin olanlar gibi organizasyonel etkenler;

g) çalışma ortamına ilişkin etkenler (örneğin, hava durumu, ortam gürültüsü ve titreşim, sıcaklık ve aydınlatma);

h) düzenlemelerin uygulanabilirliği ve yürütülebilirliği ile ekipmanların, personelin ve prosedürlerin sertifikasyonu da dahil olmak üzere, düzenleyici gözetim etkenleri;

i) pratik kopmayı, operasyonel sapmaları veya ürün güvenilirliğinin bozulmasını tespit eden performans izleme sistemleri;

j) insan-makine arayüz etkenleri ve

k) diğer organizasyonlar ile olan Devlet Emniyet Programı (SSP)/Emniyet Yönetimi Sistemi (SMS) arayüzlerine ilişkin etkenler.

İş güvenliği, sağlık ve çevre tehlikeleri

2.5.2.9 Havacılık emniyetinin yanı sıra İGSÇ'ye de eşzamanlı olarak etki eden birleşik tehlikeler ile ilişkili emniyet riskleri, sırasıyla, ayrı ayrı havacılık ve İGSÇ akıbetlerini ele alacak ayrı (paralel) risk hafifletme süreçleriyle yönetilebilir. Alternatif olarak, birleşik tehlikeleri ele almak için entegre bir havacılık ve İGSÇ risk hafifletme sistemi kullanılabilir. Havalimanı transit kapısında herhangi bir uçağın yaşadığı yıldırım çarpması birleşik tehlikeye örnek verilebilir. Bu tehlike, İGSÇ denetçisi tarafından bir "işyeri tehlikesi" (yer personeli/işyeri emniyeti) olarak addedilebilir. Havacılık emniyeti denetçisi için ise, bu aynı zamanda hava araçlarına ve yolcu emniyetine zarar verme riskine sahip olan bir havacılık tehlikesidir. Daima aynı olmamaları sebebiyle, bu tür birleşik tehlikelerin İGSÇ ve havacılık emniyeti akıbetlerinin birlikte dikkate alınması önemlidir. İGSÇ ve havacılık emniyeti akıbetlerine yönelik koruyucu kontrollerin amacı ve odak noktası farklılık gösterebilir.

Tehlike tanımlama metodolojileri

2.5.2.10 Tehlikelerin tanımlanması için aşağıdaki iki ana metodoloji mevcuttur:

a) *Reaktif*. Bu metodoloji, geçmişteki sonuçların ve olayların analizini içerir. Tehlikeler, emniyet olaylarının soruşturulmasıyla tanımlanır. Olaylar ve kazalar sistem eksikliklerinin işaretidir ve bu sebeple, söz konusu olaya hangi tehlikenin (tehlikelerin) katkıda bulunduğunu tespit etmek üzere kullanılabilirler.

b) *Proaktif*. Bu metodoloji, daha düşük akıbetli olaylara veya süreç performansına ilişkin emniyet verilerinin toplanmasını ve tehlikenin herhangi bir kazaya veya olaya sebebiyet verip vermeyeceğini tespit etmek üzere emniyet bilgilerinin veya olay sıklığının analiz edilmesini içerir. Proaktif tehlike tanımlamaya yönelik emniyet bilgileri ağırlıklı olarak uçuş verileri analiz (FDA) programlarından, emniyet raporlaması sistemlerinden ve emniyet güvence işlevinden elde edilir.

2.5.2.11 Tehlikeler ayrıca, olumsuz trendleri tanımlayan ve gelişen tehlikeler hakkında tahminler üreten emniyet verileri analizi yoluyla da tanımlanabilir.

Dış organizasyonlarla olan Emniyet Yönetimi Sistemi (SMS) arayüzlerine ilişkin tehlikeler

2.5.2.12 Organizasyonlar tarafından kendi emniyet yönetimi arayüzlerine ilişkin tehlikeler de tanımlanmalıdır. Bu tanımlama, mümkün olduğunda, arayüz bağlantısına sahip olunan organizasyonlarla ortak bir uygulama olarak yürütülmelidir. Tehlike tanımlama kapsamında, çalışma ortamı ile söz konusu hizmetin emniyetli bir şekilde sunulmasına veya ürünün elverişliliğine, işlevselliğine veya performansına katkıda bulunabilecek olan çeşitli organizasyonel kabiliyetler (insanlar, süreçler, teknolojiler) dikkate alınmalıdır.

2.5.2.13 Örnek olarak, herhangi bir uçağın hizmete dönüşü tümü söz konusu uçakta ve söz konusu uçağın etrafında çalışan birçok organizasyonu ve operasyon personelini içerir. Operasyon personeli, ekipmanları ve hizmete dönüş faaliyetinin koordinasyonu arasındaki arayüzlere ilişkin tehlikelerin olması muhtemeldir.

2.5.3 Emniyet riski olasılığı

2.5.3.1 Emniyet riski olasılığı, herhangi bir emniyet akıbetinin veya sonucunun ortaya çıkma ihtimalidir. Tüm olası akıbetler göz önünde bulundurulabilecek şekilde geniş bir dizi senaryonun öngörülmesi önemlidir. Olasılığın tespit edilmesinde aşağıdaki sorular yardımcı olabilir:

a) Değerlendirme kapsamında olana benzer olaylar geçmişte görülmüş mü yoksa bu istisnai bir olay mı?

b) Aynı türden başka hangi ekipmanlar veya komponentler benzer sorunlara sahip olabilir?

c) Söz konusu prosedürleri takip eden veya bunlara tabi olan personelin sayısı nedir?

d) Değerlendirme kapsamında olan tehlikenin riski nedir? Örneğin, söz konusu ekipman veya faaliyet operasyonun yüzde kaçında kullanılmaktadır?

2.5.3.2 Bu sorulara temel teşkil edebilecek etkenlerin göz önünde bulundurulması, herhangi bir öngörülebilir senaryo kapsamında tehlike akıbetlerinin olasılığının değerlendirilmesinde yardım sağlayacaktır.

2.5.3.3 Herhangi bir makul kişi tarafından aynı koşullar altında söz konusu türden olayın ortaya çıkmasının beklenmesi halinde olayın öngörülebilir olduğu değerlendirilir. Olası veya teorik olarak mümkün olan her tehlikenin tanımlanması mümkün değildir. Bu sebeple, tehlike tanımlama kapsamında uygun detay seviyesinin tespit edilmesi için sağduyu gereklidir. Ürünlerine veya hizmetlerine ilişkin belirgin ve makul çerçevede öngörülebilir tehlikeleri tanımlarken, hizmet sağlayıcıları tarafından gerekli özen gösterilmelidir.

Not.— Ürün tasarımına ilişkin olarak "öngörülebilir" teriminin amacı, söz konusu ürünün uçuşa elverişlilik düzenlemeleri, politikası ve kılavuz materyal kapsamındaki kullanımıyla tutarlı olmaktır.

2.5.3.4 Tablo 1 kapsamında, tipik emniyet riski olasılığı sınıflandırma tablosu sunulmaktadır. Bu tablo, emniyetsiz olaya veya koşula ilişkin olasılığı, her bir kategoriye ilişkin açıklamayı ve her bir kategoriye bir değer verilmesini belirtmek üzere beş kategori içerir. Bu örnekte kalitatif terimler kullanılır; daha tutarlı bir değerlendirme sağlamak için kantitatif terimler tanımlanabilir. Bu husus, uygun emniyet verilerinin elverişliliğine ve söz konusu organizasyonun ve operasyonun karmaşıklığına bağlı olacaktır.

Tablo 1. Emniyet riski olasılığı tablosu

İhtimal	*Anlam*	*Değer*
Sık	Bir çok kez meydana gelmesi muhtemeldir (sıklıkla meydana gelmiştir)	5
Zaman zaman	Zaman zaman meydana gelmesi muhtemeldir (seyrek olarak meydana gelmiştir)	4
Uzak ihtimal	Meydana gelmesi muhtemel değil, ancak mümkündür (nadiren meydana gelmiştir)	3
İhtimal dışı	Meydana gelmesi fazlasıyla ihtimal dışıdır (meydana geldiği bilinmemektedir)	2
Aşırı ihtimal dışı	Olayın meydana geleceği neredeyse tasavvur dahi edilemez.	1

Not.— Bu sadece örnektir. Detay seviyesi ve tabloların ve matrislerin karmaşıklığı her bir organizasyonun belirli ihtiyaçlarına ve karmaşıklıklarına uyarlanmalıdır. Organizasyonların kalitatif ve kantitatif kriterler içerebileceği de dikkate alınmalıdır.

2.5.4 Emniyet riski şiddeti

2.5.4.1 Olasılık değerlendirmesinin tamamlanması sonrasında, bir sonraki adım, söz konusu tehlikeye ilişkin olası akıbetleri dikkate alarak şiddetin değerlendirilmesidir. Emniyet riski şiddeti, tanımlanan tehlikenin akıbeti veya sonucu olarak ortaya çıkması makul çerçevede beklenebilecek zarar ölçüsü olarak tanımlanmaktadır. Şiddet sınıflandırmasında aşağıdakiler göz önünde bulundurulmalıdır:

a) aşağıdakiler neticesinde ortaya çıkabilecek ölümler veya ciddi yaralanma:

   1) hava aracının içerisinde olunması;

   2) hava aracından ayrılmış hale gelen parçalar da dahil olmak üzere, hava aracının herhangi bir parçası ile doğrudan temasta olunması veya

   3) jet blasta doğrudan maruz kalınması ve

b) hasar:

   1) hava aracının maruz kaldığı, aşağıdaki türden hasar veya yapısal arıza:

      i) hava aracının yapısal mukavemetine, performansına veya uçuş karakteristiklerine olumsuz bir şekilde etki eden;

      ii) etkilenen komponentin normalde büyük çaplı onarımını veya ikame edilmesini gerektirebilecek olan;

   2) ATS veya havaalanı ekipmanlarının maruz kaldığı, aşağıdaki türden hasar:

      i) hava aracı ayrımının yönetimine olumsuz bir şekilde etki eden veya

      ii) iniş kabiliyetine olumsuz bir şekilde etki eden.

2.5.4.2 Şiddet değerlendirmesinde, en kötü öngörülebilir durum göz önünde bulundurularak, herhangi bir tehlikeye ilişkin olası tüm akıbetler dikkate alınmalıdır. Tablo 2'de, tipik bir emniyet riski şiddeti tablosu sunulmaktadır. Bu tabloda, şiddetin seviyesini, her bir kategorinin açıklanmasını ve her bir kategoriye bir değer tayin edilmesini göstermek üzere beş kategori yer almaktadır. Emniyet riski olasılığı tablosu gibi bu tablo da sadece bir örnektir.

Tablo 2. Örnek emniyet riski şiddeti tablosu

Şiddet	*Anlam*	*Değer*
Katastrofik (Yıkıcı)	• Hava aracının / ekipmanın tahrip olması • Birden fazla ölüm	A
Tehlikeli	• Operasyon personeli tarafından görevlerinin tutarlı veya eksiksiz bir şekilde icra edilmesi için itimat edilemeyecek şekilde emniyet sınırlarında büyük ölçüde azalma, fiziki sıkıntı veya iş gücü olması • Ciddi yaralanma • Büyük çaplı ekipman hasarı	B
Önemli	• Emniyet sınırlarında belirgin ölçüde azalma, iş yükündeki artış neticesinde veya verimliliklerini zayıflatan koşullar neticesinde operasyon personelinin olumsuz çalışma koşulları ile başa çıkma becerisindeki azalma • Ciddi olay • Kişilerin yaralanması	C
Önemsiz	• Rahatsızlık • İşletme sınırlamaları • Acil durum prosedürlerinin kullanımı • Küçük çaplı olay	D
Göz ardı edilebilir	• Akıbetlerin az sayıda olması	E

2.5.5 Emniyet riski tolere edilebilirliği

2.5.5.1 Olasılık ve şiddet notlarının sonuçları birleştirilerek emniyet riski endeks notu oluşturulur. Yukarıdaki örnekte, bu not, alfanümerik bir göstergedir. İlgili şiddet/olasılık kombinasyonları, Tablo 3'deki emniyet riski değerlendirme matrisinde sunulmaktadır. Emniyet riski değerlendirme matrisi, emniyet riski tolere edilebilirliğini tespit etmek için kullanılır. Örneğin, (4B) emniyet riski endeksiyle sonuçlanarak emniyet riski olasılığının Zaman Zaman (4) olarak değerlendirilmiş olduğu, emniyet riski şiddetinin ise Tehlikeli (B) olarak değerlendirilmiş olduğu bir durum düşünün.

Tablo 3. Örnek emniyet riski matrisi

Emniyet Riski		*Şiddet*				
Olasılık		*Katastrofik (Yıkıcı) A*	*Tehlikeli B*	*Önemli C*	*Önemsiz D*	*Göz Ardı Edilebilir E*
Sık	5	5A	5B	5C	5D	5E
Zaman zaman	4	4A	4B	4C	4D	4E
Uzak ihtimal	3	3A	3B	3C	3D	3E
İhtimal dışı	2	2A	2B	2C	2D	2E
Aşırı ihtimal dışı	1	1A	1B	1C	1D	1E

Not.— Emniyet riski tolere edilebilirliğinin tespit edilmesinde, tehlike tanımlama için kullanılan verilerin kalitesi ve güvenilirliği ile emniyet riski olasılığı göz önünde bulundurulmalıdır.

2.5.5.2 Emniyet riski değerlendirme matrisinden elde edilen endeks, bunun akabinde, belirli organizasyon için tolere edilebilirlik kriterlerini anlatımsal şekilde açıklayan emniyet riski tolere edilebilirliği tablosuna çıkarılmalıdır. Tablo 4'de, emniyet riski tolere edilebilirlik tablosuna ilişkin bir örnek sunulmaktadır. Yukarıdaki örneği kullanarak, 4B olarak değerlendirilen emniyet riskine ilişkin kriter "tolere edilemez" kategorisine tekabül etmektedir. Bu durumda, akıbetin emniyet riski endeksi kabul edilemezdir. Bu sebeple, söz konusu organizasyon tarafından aşağıdakilerin düşürülmesi için risk kontrol tedbiri alınmalıdır:

a) söz konusu organizasyonun belirli riske maruz kalması, başka bir deyişle, riskin olasılık bileşeninin kabul edilebilir bir seviyeye indirilmesi;

b) tehlikeye ilişkin akıbetlerin şiddeti, başka bir deyişle, riskin şiddet bileşeninin kabul edilebilir bir seviyeye indirilmesi veya

c) söz konusu risk kabul edilebilir bir seviyede yönetilecek şekilde şiddet ve olasılık.

2.5.5.3 Emniyet riskleri, kavramsal olarak kabul edilebilir, tolere edilebilir veya tolere edilmez olarak değerlendirilir. Başlangıçta tolere edilemez alanına tekabül eder olarak değerlendirilen emniyet riskleri hiçbir koşulda kabul edilemezdir. Tehlikelerin akıbetlerinin olasılığı ve/veya şiddeti, hafifletme eylemini gerektirecek veya faaliyetleri durduracak kadar büyüktür ve söz konusu tehlikenin zarar verme potansiyeli emniyet bakımından böylesi bir tehdit arz etmektedir.

Tablo 4. Emniyet riski tolere edilebilirliği örneği

Emniyet Riski Endeksi Aralığı	*Emniyet Riski Açıklaması*	*Tavsiye Edilen Tedbir*
5A, 5B, 5C, 4A, 4B, 3A	TOLERE EDİLEMEZ	Söz konusu riski hafifletmek için derhal tedbir alın veya söz konusu faaliyeti durdurun. Emniyet riski endeksini tolere edilebilire geri çekmek için ilave veya geliştirilmiş koruyucu kontrollerin uygulandığından emin olmak üzere öncelik emniyet riski hafifletmesi gerçekleştirin.
5D, 5E, 4C, 4D, 4E, 3B, 3C, 3D, 2A, 2B, 2C, 1A	TOLERE EDİLEBİLİR	Emniyet riski hafifletmesine dayalı olarak tolere edilebilir. Söz konusu riskin kabulü için yönetim kararı gerektirebilir.
3E, 2D, 2E, 1B, 1C, 1D, 1E	KABUL EDİLEBİLİR	Olduğu gibi kabul edilebilir. Herhangi bir başka emniyet riski hafifletmesine gerek bulunmaz.

2.5.6 İnsan faktörleri ile ilgili risklerin değerlendirilmesi

2.5.6.1 Kişilerin, aşağıdaki yollarla, emniyet risklerinin gerek kaynağı gerek çözümü olabilmesine bağlı olarak insan faktörlerinin değerlendirilmesi Emniyet Riski Yönetiminde özellikle önemlidir:

a) insan sınırlarına bağlı olarak değişken performansla herhangi bir kazaya veya olaya katkıda bulunulması;

b) herhangi bir tehlikeli durumun tahmin edilmesi veya böyle bir durumun önlenmesi için uygun tedbirlerin alınması ve

c) problemlerin çözüme kavuşturulması, karar alınması ve riskleri hafifletecek tedbirlerin alınması.

2.5.6.2 Bu sebeple, risklerin tanımlanmasına, değerlendirilmesine ve hafifletilmesine uygun insan faktörleri uzmanlığının dahil edilmesi önem arz etmektedir.

2.5.6.3 Emniyet Riski Yönetimi (SRM), insanlara ilişkin olanlar da dahil olmak üzere, emniyet riskinin tüm yönlerinin ele alınmasını gerektirir. İnsan performansıyla ilişkili risklerin değerlendirilmesi, aşağıdaki sebeplerden dolayı, teknoloji ve çevre ile ilişkili risk faktörlerinden daha karmaşıktır:

a) söz konusu kişiye dahili ve harici bakımından etkileşen geniş bir dizi etki ile insan performansının ziyadesiyle değişken olması. Bu etkiler arasındaki etkileşimin etkilerinden bir çoğunun tahmin edilmesinin zor veya imkansız olması ve

b) değişken insan performansının akıbetlerinin icra edilen göreve ve bağlama göre farklılık gösterecek olması.

2.5.6.4 Bu husus, söz konusu riskin olasılığının ve şiddetinin nasıl tespit ettiğini karmaşık hale getirmektedir. Dolayısıyla, insan faktörleri uzmanlığı, emniyet risklerinin tanımlanmasında ve değerlendirilmesinde değere sahiptir. (Emniyet Yönetimi Sistemi (SMS) süreçleri kullanılarak yorgunluğun yönetilmesi, *Yorgunluk Yönetimi Yaklaşımlarının Gözetimine ilişkin El Kitabı* (Doc 9966) kapsamında ele alınmaktadır).

2.5.7 Emniyet riski hafifletme stratejileri

2.5.7.1 Emniyet riski hafifletmesi genel olarak emniyet riski kontrolü olarak anılır. Emniyet riskleri, uygun emniyet riski kontrollerinin uygulanmasıyla emniyet riskinin hafifletilmesi suretiyle kabul edilebilir bir seviyede yönetilmelidir. Bunun, zamana, maliyete ve emniyet riskinin azaltılmasına veya giderilmesine yönelik tedbir alınmasının zorluğu karşısında dengelenmesi gerekir. Olası akıbetlerin şiddetini azaltarak, olayın ihtimalini düşürerek veya söz konusu emniyet riskine maruz kalma halini azaltarak emniyet riskinin seviyesi düşürülebilir. İhtimalin düşürülmesi şiddetin düşürülmesinden daha kolay ve daha yaygındır.

2.5.7.2 Emniyet riski hafifletmeleri, genellikle çalışma prosedürlerinde, ekipmanlarda veya altyapıda değişikliklere yol açan tedbirlerdir. Emniyet riski hafifletme stratejileri üç kategoriye ayrılır:

a) *Önleme*: Emniyet riskinin söz konusu faaliyete devam edilmesinin getirdiği faydaları aşması sebebiyle söz konusu operasyonun veya faaliyet iptal edilmesi veya önlenmesi ve bu sayede emniyet riskinin tümüyle giderilmesi.

b) *Azaltma*: Söz konusu operasyonun veya faaliyetin sıklığının azaltılması veya emniyet riskinin akıbetlerinin büyüklüğünü düşürmek için tedbir alınması.

c) *Ayırma*: Emniyet riskinin akıbetlerinin etkilerinin izole edilmesi veya bu etkilere karşı koruma sağlamak üzere fazlalık oluşturulması için tedbir alınması.

2.5.7.3 İnsanlar tarafından hafifletici veya düzeltici eylemlerin uygulanmasının veya bunlara katkı sağlanmasının gerekli olması sebebiyle, insan faktörlerinin değerlendirilmesi etkin hafifletmelerin tanımlanmasının ayrılmaz bir parçasıdır. Örneğin, hafifletmeler, süreçlerin veya prosedürlerin kullanımını içerebilir. Bunları "gerçek dünya" durumlarında kullanacak olanlardan ve/veya insan faktörleri uzmanlığına sahip olan kişilerden girdi olmadan, oluşturulan süreçler veya prosedürler, bu süreçlerin veya prosedürlerin amacına uygun olmayabilir ve istenmeyen akıbetlere yol açabilir. Ayrıca, insan performansı değişkenliğinin ele alınmasına yönelik hata yakalama stratejileri oluşturularak insan performansı sınırlarının emniyet riski hafifletmesi kapsamında göz önünde bulundurulması gerekir. Netice itibariyle, bu önemli insan faktörleri perspektifi daha kapsamlı ve etkin hafifletmelerle sonuçlanır.

2.5.7.4 Risk hafifletme stratejisi, yukarıda tanımlanan yaklaşımlardan birini içerebilir veya birden fazla yaklaşımı kapsayabilir. Optimal çözümü bulmak için her türlü olası kontrol tedbirlerinin göz önünde bulundurulması önemlidir. Karar alınması öncesinde her bir alternatif stratejinin etkinliği değerlendirilmelidir. Önerilen her bir emniyet riski hafifletmesi alternatifinin aşağıdaki perspektiflerden incelenmesi gerekir:

a) *Etkinlik*. Alternatifler tarafından emniyet risklerinin azaltılma veya giderilme derecesi. Etkinlik, emniyet risklerini azaltabilen veya giderebilen teknik, eğitimsel ve düzenleyici savunmalar bakımından tespit edilebilir.

b) *Maliyet/fayda*. Hafifletmenin algılanan faydalarının maliyetlerden daha ağır basma derecesi.

c) *Kullanışlılık*. Hafifletmenin uygulanabildiği derece ve mevcut teknoloji, finansal ve idari kaynaklar, mevzuat, siyasi irade, operasyonel gerçekler vb. bakımından bunun ne kadar uygun olduğu.

d) *Kabul Edilebilirlik*. Söz konusu alternatifin, söz konusu alternatifi uygulaması beklenecek kişiler için kabul edilebilir olma derecesi.

e) *Yürütülebilirlik*. Yeni kurallara, düzenlemelere veya çalışma prosedürlerine uyumun takip edilebilme derecesi.

f) *Devamlılık*. Söz konusu hafifletmenin sürdürülebilir ve etkin olma derecesi.

g) *Artık emniyet riskleri*. İlk hafifletmenin uygulanması sonrasında gelen ve ilave emniyet riski kontrol tedbirlerini gerektirebilecek olan emniyet riski derecesi.

h) *İstenmeyen akıbetler*. Herhangi bir hafifletme alternatifinin uygulanmasıyla ilişkili yeni tehlikelerin ve ilgili emniyet risklerinin tanıtılması.

i) *Zaman.* Emniyet riski hafifletme alternatifinin uygulanması için gereken zaman.

2.5.7.5 Düzeltici faaliyet kapsamında mevcut savunmalar ile bunların kabul edilebilir emniyet riski seviyesine ulaşma yeterliliği (yetersizliği) göz önünde bulundurulmalıdır. Bu işlem, söz konusu düzeltici faaliyetten tesir görmüş olabilecek olan önceki emniyet riski değerlendirmelerinin gözden geçirilmesine yol açabilir. Emniyet riski hafifletmelerinin ve kontrollerinin, etkin olduklarından emin olmak üzere doğrulanması/denetlenmesi gerekecektir. Hafifletmelerin etkinliğinin izlenmesine yönelik bir diğer yol da Emniyet Performansı Göstergelerinin (SPI'ler) kullanılmasıdır. Emniyet performansı yönetimi ve Emniyet Performansı Göstergeleri (SPI'ler) hakkında daha fazla için bakınız Bölüm 4.

2.5.8 Emniyet riski yönetimi dokümantasyonu

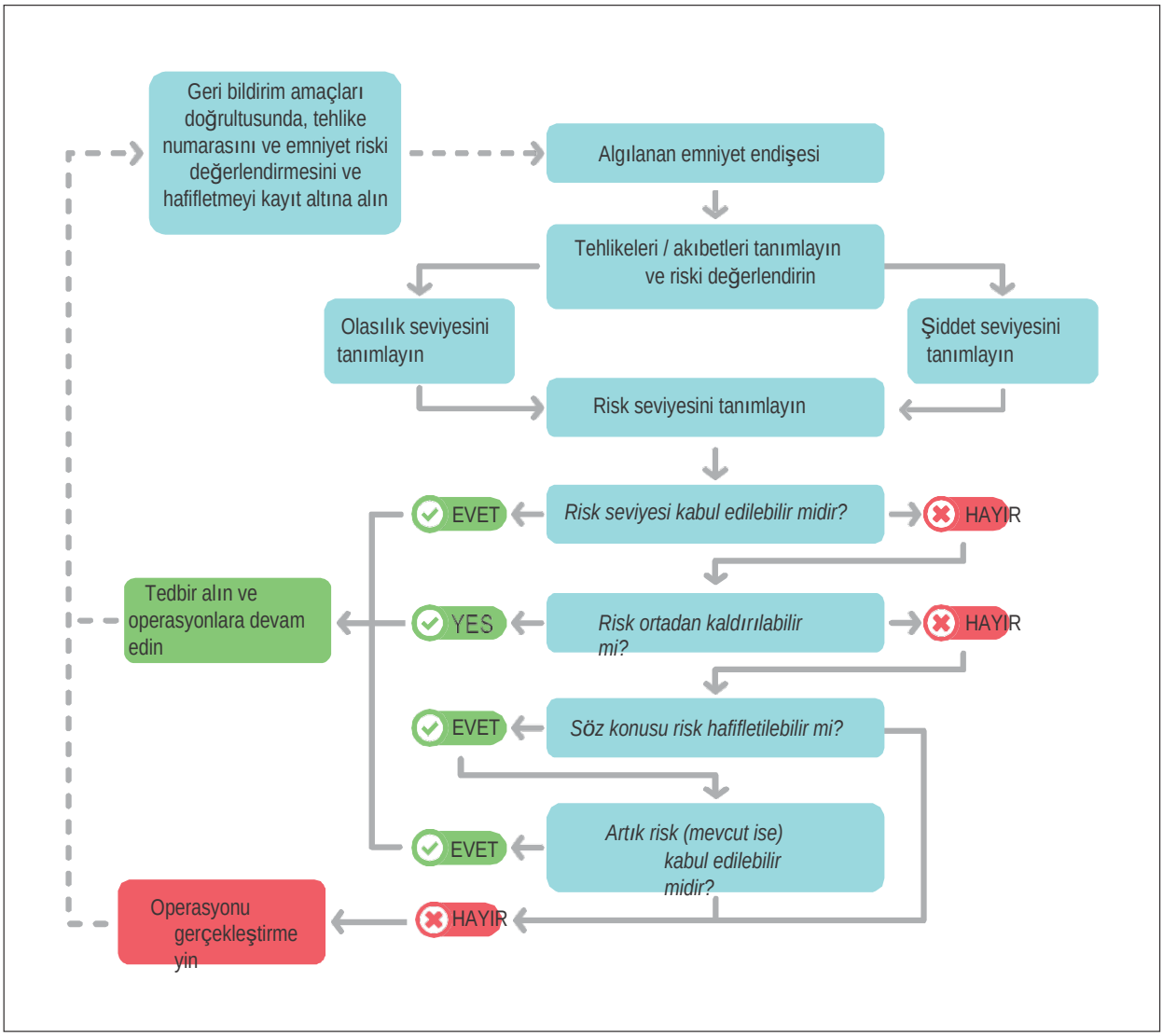
2.5.8.1 Olasılık ve şiddet değerlendirmesine dayanak teşkil eden varsayımlar, alınan kararlar ve alınan emniyet riski hafifletme tedbirleri de dahil olmak üzere, emniyet riski yönetimi faaliyetlerinin belgelenmesi gerekir. Bu belgeleme bir hesaplama çizelgesi veya tablo ile yapılabilir. Bazı organizasyonlar tarafından, büyük miktarlarda emniyet verilerinin ve emniyet bilgilerinin saklanabildiği ve analiz edilebildiği veritabanı veya başka yazılımlar kullanılabilir.

2.5.8.2 Tanımlanan tehlikelerinin bir sicilinin tutulması, söz konusu organizasyon tarafından söz konusu organizasyona ait bilinen tehlikelerin izinin kaybedilmesi ihtimalini en aza indirir. Söz konusu tehlikenin daha önceden kayda alınıp alınmadığını ve söz konusu tehlikeyi hafifletmek için hangi tedbirin (tedbirlerin) alınmış olduğunu görmek üzere, tehlikeler, tanımlandıklarında, söz konusu sicildeki bilinen tehlikeler ile karşılaştırılabilir. Tehlike sicilleri genellikle tablo formatında olup, tipik olarak şunları içerir: söz konusu tehlike, olası akıbetler, ilişkili risklere ilişkin değerlendirme, tanımlama tarihi, tehlike kategorisi, kısa açıklama, ne zaman veya nerede geçerli olduğu, tehlikenin kimin tarafından tanımlandığı ve riskleri hafifletmek için hangi tedbirin uygulanmış olduğu.

2.5.8.3 Organizasyonel emniyet karar alıcıları tarafından alınan kararların tekrarlanabilirliğini ve gerekçelendirilmesini iyileştirmek için emniyet riski karar alma araçları ve süreçleri kullanılabilir. Aşağıdaki Şekil 2.6'da emniyet riski karar yardımcısı örneği verilmektedir.

2.5.9 Maliyet - fayda analizi

Maliyet-fayda veya maliyet etkinliği analizi normalde emniyet riski hafifletme faaliyetleri sırasında uygulanır. Bu işlem yaygın olarak düzenleyici etki analizi veya proje yönetimi süreçlerinde olduğu gibi işletme yönetimi ile ilişkilidir. Bununla birlikte, emniyet riski değerlendirmesinin belirgin finansal etkiye sahip olabileceği durumlar söz konusu olabilir. Bu gibi durumlarda, emniyet riski değerlendirmesini destekleyecek tamamlayıcı bir maliyet-fayda analizi veya maliyet etkinlik süreci gerekebilir. Bu sayede, maliyet etkinliği analizinin veya tavsiye edilen emniyet riski kontrol tedbirlerinin gerekçelendirilmesinin, ilişkili finansal yansımalarla göz önünde bulundurulmasına imkan verilecektir.



Şekil 2-6. Emniyet riski yönetimi karar yardımcısı

Bölüm 3

EMNİYET KÜLTÜRÜ

3.1 GİRİŞ

3.1.1 Emniyet kültürü, havacılık sisteminde insanlara sahip olunmasının doğal sonucudur. Emniyet kültürü, "kişilerin, onları izleyen hiç kimse yokken emniyete ve riske ilişkin olarak nasıl hareket ettikleri" olarak tanımlanmıştır. Herhangi bir organizasyonun bünyesinde yönetim ve çalışanlar tarafından emniyetin nasıl algılandığının, değer gördüğünün ve önceliklendirildiğinin ve kişilere ve gruplara ilişkin olarak nasıl yansıtıldığının ifade edilmesidir:

a) kişilerin ve grupların söz konusu organizasyon ve söz konusu organizasyonun faaliyetleri tarafından karşı karşıya kalınan risklerin ve bilinen tehlikelerin bilincinde olması;

b) sürekli olarak emniyetin muhafaza edilmesine ve iyileştirilmesine yönelik olarak davranılması;

c) emniyetli operasyonlar için gerekli olan kaynaklara erişilebilmesi;

d) emniyet sorunları ile karşı karşıya kalındığında istekli ve uyum sağlayabilir olunması;

e) emniyet sorunlarının iletilmesi hususunda istekli olunması ve

f) emniyet ile ilgili davranışların söz konusu organizasyon genelinde devamlı olarak değerlendirilmesi.

3.1.2 Annex 19 kapsamında, Devlet Emniyet Programı (SSP)/Emniyet Yönetimi Sistemi (SMS) vasıtasıyla etkin emniyet yönetimi uygulanmasını desteklemek amacıyla gerek Devletler gerek hizmet sağlayıcıları tarafından pozitif bir emniyet kültürünün teşvik edilmesi öngörülmektedir. Bu bölümde, pozitif emniyet kültürüne ilişkin kılavuz bilgiler sunulmaktadır.

3.2 EMNİYET KÜLTÜRÜ VE EMNİYET YÖNETİMİ

3.2.1 Farkında olsun veya olmasın, organizasyonlar, grup seviyesindeki tutumları ve davranışları yansıtan bir dizi farklı "emniyet kültürüne" sahip olurlar. Hiçbir organizasyon diğeriyle aynı değildir ve aynı organizasyonun bünyesinde dahi farklı gruplar emniyet hakkında düşünülmesine, emniyet hakkında konuşulmasına veya emniyet sorunlarına yönelik hareket edilmesinde çeşitli yollara sahip olabilir. Bu farklılık, farklı faaliyetler için uygun olabilir.

3.2.2 Emniyet değerlerinin yönetim ve personel tarafından uygulamalara nasıl dönüştürüldüğü, Devlet Emniyet Programının (SSP) ve Emniyet Yönetimi Sisteminin (SMS) kilit unsurlarının nasıl tesis ve muhafaza edildiğine doğrudan etki eder. Sonuç olarak, emniyet kültürü, emniyet performansı üzerinde doğrudan etkiye sahiptir. Kişinin, emniyetin geçici çözümlerden, kestirmeden gitmelerden veya emniyetsiz kararlarda veya yargılarda bulunmaktan çok da önemli olmadığına inanması, özellikle risk düşük olarak algılandığında ve herhangi bir açık akıbet veya tehlike söz konusu olmadığında sonucu teşkil edebilir. Bu sebeple, herhangi bir organizasyonun emniyet kültürü, söz konusu organizasyon tarafından Devlet Emniyet Programının (SSP) veya Emniyet Yönetimi Sisteminin (SMS) nasıl geliştiğine ve nasıl etkin hale geldiğine belirgin bir şekilde etki eder. Emniyet kültürü, tartışmaya açık olmak üzere, emniyetin yönetilmesi üzerindeki tek başına en önemli tesirdir. Herhangi bir organizasyon tarafından tüm emniyet yönetimi gerekliliklerinin tesis edilmiş olması, ancak söz konusu organizasyonun pozitif emniyet kültürüne sahip olmaması halinde, söz konusu organizasyonun beklenenden daha düşük performans göstermesi muhtemeldir.

3.2.3 Organizasyon pozitif emniyet kültürüne sahip olduğunda ve bu kültür üst ve orta düzey yönetim tarafından fark edilir bir şekilde desteklendiğinde, ön saflardaki personel, organizasyonun emniyet amaçlarına ulaşılmasına yönelik ortak sorumluluk anlayışına sahip olma eğiliminde olur. Etkin emniyet yönetimi aynı zamanda, yönetimin desteğinin görülürlüğünü artırarak ve emniyet riskinin yönetilmesine personelin faal bir şekilde katılımını iyileştirerek giderek artan pozitif bir emniyet kültürüne ulaşılmasına yönelik çalışmaları destekler.

3.2.4 Pozitif emniyet kültürü, personel ile yönetim arasında yüksek düzeyde güvene ve saygıya dayalıdır. Yönetimin kararları ve eylemleri veya eylemsizlikleri ile kolaylıkla zarar görebilecek olan pozitif emniyet kültürünün oluşturulması için zaman ve gayret gerekir. Sürekli gayret ve takviyeye ihtiyaç vardır. Liderlik tarafından faal bir şekilde onaylayan emniyetli uygulamalar, işlerin normal yapılma şekli haline gelir. Bütünüyle uygulanan ve etkin bir Devlet Emniyet Programı (SSP)/Emniyet Yönetimi Sistemi (SMS) ve pozitif emniyet kültürü ideal durumu teşkil eder. Bu nedenle, organizasyonların emniyet kültürü genellikle, Devlet Emniyet Programlarının (SSP)/Emniyet Yönetimi Sistemlerinin (SMS) olgunluğun bir yansıması olarak görülür. Etkin emniyet yönetimi pozitif emniyet kültürünü, pozitif emniyet kültürü de etkin emniyet yönetimini güçlendirir.

3.2.5 Emniyet kültürü ve emniyet kültürünün emniyet raporlaması üzerindeki etkisi

3.2.5.1 Devlet Emniyet Programları (SSP'ler) ve Emniyet Yönetimi Programları (SMS'ler), personel tarafından tanımlanan emniyet sorunları da dahil olmak üzere, mevcut ve olası emniyet eksikliklerine ve tehlikelere işaret etmek için gerekli olan emniyet verileri ve emniyet bilgileri ile sürdürülür. Herhangi bir raporlama sisteminin başarısı tümüyle, organizasyonlardan ve kişilerden gelen kesintisiz bilgi akışına ve organizasyonlara ve kişilere yapılan geri bildirime bağlıdır. Bilgilerin sürekli olarak elverişliliğini sağlamak için emniyet verilerinin, emniyet bilgilerinin ve ilgili kaynakların korunması elzemdir. Örneğin, gönüllü emniyet raporlaması sistemlerinde, bu husus, gizli olan ve emniyetin muhafaza edilmesi veya iyileştirilmesi haricindeki amaçlarla kullanılmayan bir sistem vasıtasıyla gerçeğe dönüştürülebilir. Faydaları iki kat daha fazladır. Personel, genellikle, emniyet tehlikelerine en yakın olandır ve bu sebeple, gönüllü raporlama sistemi, personele, bu tehlikeleri faal bir şekilde tanımlama ve işe yarar çözümler önerme imkanı verir. Aynı zamanda, düzenleyici kurum veya yönetim tarafından önemli emniyet bilgileri toplanabilir ve söz konusu bilgileri rapor eden organizasyonlar veya operasyon personeli ile güven inşa edilebilir. Emniyet verilerinin ve emniyet bilgilerinin korunması hakkında daha fazla bilgi için bakınız Bölüm 7.

3.2.5.2 Organizasyonların veya kişilerin deneyimlerini ve hatalarını rapor etmeye istekli olup olmamaları, ağırlıklı olarak, raporlama ile ilişkili dezavantajlara ve algılanan faydalara bağlıdır. Emniyet raporlama sistemleri anonim veya gizli olabilir. Genel olarak herhangi bir anonim raporlama sisteminde, rapor edenler kimliklerini bildirmezler. Bu durumda, söz konusu raporun içeriğine veya geri bildirim sağlanabilmesine ilişkin daha fazla açıklama imkanı bulunmaz. Gizli raporlama sisteminde, rapor edenler hakkındaki tanımlayıcı bilgiler sadece tayin edilen saklayıcı tarafından bilinir. Emniyet sorunlarını rapor eden kişilerin ve organizasyonların adil ve tutarlı bir şekilde korunması ve muamele görmesi halinde, söz konusu kişiler ve organizasyonlar tarafından bu tür bilgilerin ifşa edilmesi ve ilişkili emniyet riskinin (risklerinin) etkin bir şekilde yönetilmesi için düzenleyici kurum veya yönetim ile çalışması daha olasıdır.

3.2.5.3 Devletler tarafından, emniyet verilerinin, emniyet bilgilerinin ve ilgili kaynakların korunması için Annex 19 kapsamında ortaya konan hükümlere riayet edilmesine yönelik kanunların çıkarılması beklenir. Gönüllü raporlama sistemi durumunda, gizliliğin sağlanması ve raporlama sisteminin emniyet koruması kanunlarına uygun olarak işletilmesi gerekir. Ayrıca, organizasyonların, herkesin erişimine açık olan ve herkes tarafından geniş ölçüde anlaşılan uygun bir disiplin politikasına sahip olmaları gerekir. Disiplin politikası kapsamında, hangi davranışların kabul edilemez olarak değerlendirildiği ve söz konusu organizasyon tarafından bu gibi hallerde nasıl tepki verileceği açık bir şekilde belirtilmelidir. Disiplin politikasının adil, makul ve istikrarlı bir şekilde uygulanması gerekir. Son olarak, organizasyonlar ve kişiler tarafından deneyimlerinin ve hatalarının, çalışma arkadaşları veya işverenleri tarafından yargılanmayacakları veya haksızca muamele tabi tutulmayacakları bir ortamda rapor edilmesi daha olasıdır.

3.2.5.4 Genel olarak, organizasyonlar ve kişiler, emniyetin yararına raporlama yapılırken destek göreceklerine inanmalıdırlar. Organizasyonel hatalar ve kişisel hatalar ile yanlışlıklar buna dahildir. Gizli raporlardaki artış ile anonim raporlardaki düşüş genel olarak söz konusu organizasyonun pozitif emniyet kültürüne doğru ilerlemesine dair bir işarettir.

3.2.6 Emniyet kültürü ve kültürel çeşitlilik

3.2.6.1 Ulusal kültür, bireyin toplum içerisindeki rolü, otoritenin dağıtılma şekli ve kaynaklara, sorumluluklara, ahlaka, amaçlara ve hukuk sistemlerine ilişkin ulusal öncelikler de dahil olmak üzere, belirli ulusların karakteristik özelliklerini farklılaştırır.

3.2.6.2 Emniyet yönetimi perspektifinden bakıldığında, ulusal kültür, organizasyonel kültüre etki eder ve düzenleyici otorite personeli ile sektör personeli arasındaki ilişki ve emniyet bilgilerinin korunma derecesi de dahil olmak üzere, düzenleyici uygulama politikalarının mahiyetinin ve kapsamının belirlenmesinde büyük bir rol oynar. Bunlar, sırasıyla, kişilerin emniyet sorunlarını rapor etme istekliliğine etki eder.

3.2.6.3 Günümüzde çoğu organizasyon tarafından, uyruklarına, etnik kökenlerine, dinlerine ve/veya cinsiyetlerine göre tanımlanabilecek olan birden fazla kültürel geri plandan kişiler istihdam edilmektedir. Havacılık operasyonları ve emniyeti, her bir kendi mesleki kültürüne sahip olan farklı meslek grupları arasındaki etkin etkileşime dayalıdır. Dolayısıyla, organizasyonun emniyet kültürü de iş gücünün üyelerinin kültürel geri planlarının çeşitliliğinden belirgin bir şekilde etkilenebilir.

3.2.6.4 Havacılık sistemi dahilinde emniyetin yönetilmesi bu sebeple, kültürel olarak farklı personel ile etkileşimi ve bu personelin yönetimini gerektirir. Bununla birlikte, emniyet yönetimi uygularken yöneticilerin kültürel çeşitliliğe sahip olan iş gücünü verimli ekipler halinde biçimlendirebilmeleri gerekir. Farklı kültürel yorumlamalardan kaynaklanabilecek emniyet riski algılarındaki farklılıkların giderilmesi ve iletişim, liderlik stilleri ve amirler ile astlar arasındaki etkileşim gibi diğer emniyet ile ilgili yönlerin geliştirilmesi kilit öneme sahiptir. Başarı derecesi, yönetimin, emniyete yönelik ortak bir anlayışı teşvik etme becerisine ve etkinliğinde her bir bireyin rolüne dayalı olacaktır. Bireylerin kültürel geri planına bakılmaksızın, etkin emniyet yönetimi, söz konusu organizasyondaki herkes tarafından "izleyen kimse yokken dahi" emniyete ve riske ilişkin olarak nasıl davranmalarının beklendiğine dair anlayışa sahip olunacak şekilde, paylaşımlı bir emniyet kültürüne dayalıdır.

3.2.7 Emniyet kültürü ve organizasyonel değişim

Emniyet yönetimi, organizasyonlar tarafından organizasyonel ve operasyonel değişimlere ilişkin emniyet risklerinin yönetilmesini gerektirir. İş yüküne ilişkin personel kaygıları, iş güvenliği ve eğitime erişim, organizasyonlardaki belirgin değişim ile ilişkilidir ve emniyet kültürü üzerinde olumsuz bir etkiye sahip olabilir. Personelin, değişimin gelişimine dahil olduklarını hissetme ve süreçteki rollerini kavrama derecesi de emniyet kültürüne tesir edecektir.

3.3 POZİTİF EMNİYET KÜLTÜRÜNÜN OLUŞTURULMASI

3.3.1 Pozitif emniyet kültürü aşağıdaki özelliklere sahiptir:

a) yöneticilerin ve çalışanların, ayrı ayrı ve birlikte olmak üzere, emniyeti destekleyen kararları ve tedbirleri almayı istemeleri;

b) kişilerin ve grupların davranışlarının ve süreçlerin sürekli olarak kritiğini yapmaları ve ortam değiştikçe değişime ve iyileşmeye yönelik fırsatlar arayarak başkalarının yaptığı kritiği hoş karşılamaları;

c) yönetimin ve personelin, söz konusu organizasyon ve söz konusu organizasyonun faaliyetleri tarafından karşı karşıya kalınan tehlikelere ve risklere ve risklerin yönetilme ihtiyacına yönelik olarak ortak bir bilinci paylaşmaları;

d) kişilerin, emniyetin iş yapma biçimlerinin bir parçası olduğuna dair ortak bir düşünceye göre hareket etmeleri ve kararlar almaları;

e) kişiler tarafından emniyet hakkında bilgilendirilmeye ve başkalarını bilgilendirmeye değer verilmesi;

f) kişilerin, çalışma arkadaşlarına ve yöneticilerine deneyimleri hakkındaki bilgileri açması ve gelecekte işlerin nasıl yapıldığını iyileştirmek için hataların ve yanlışlıkların raporlanmasının teşvik edilmesi.

3.3.2 Yönetim ve çalışanlar tarafından gerçekleştirilen eylemler, emniyet kültürünün daha pozitif hale getirilmesine yardımcı olabilir. Tablo 5 kapsamında, herhangi bir organizasyonda pozitif emniyet kültürüne imkan veren veya vermeyen yönetim ve çalışan eylemleri türlerine ilişkin örnekler sunulmaktadır. Organizasyonlar tarafından, pozitif emniyet kültürünün teşvik edilmesi ve pozitif emniyet kültürüne ulaşılması için imkan verenlerin sunulmasına ve imkan vermeyenlerin ortadan kaldırılmasına odaklanılmalıdır.

Tablo 5. Pozitif emniyet kültürüne imkan verecek veya vermeyecek olan eylemlere ilişkin örnekler

Unsur	*Genel Açıklama*	*İmkan Veren Eylemler*	*İmkan Vermeyen Eylemler*
Emniyet taahhüdü			
Emniyet taahhüdü, söz konusu organizasyondaki üst yönetim tarafından emniyete yönelik pozitif tutuma sahip olunma ve emniyetin öneminin fark edilmesi derecesini yansıtır. Üst yönetim tarafından yüksek düzeyde emniyete ulaşılması ve bu emniyet düzeyinin muhafaza edilmesi gerçekten taahhüt edilmeli ve çalışanlara da bu yönde motivasyon ve yöntemler sağlanmalıdır.		• Yönetim, emniyet kültürünü yönlendirir ve sadece konuşarak değil, aynı zamanda rol modeller olarak hareket ederek çalışanlarını emniyete özen göstermek üzere faal bir şekilde motive etmektedir. • Yönetim tarafından bir dizi emniyet ile ilgili görevlere (örneğin eğitim) yönelik kaynaklar temin edilir. • Sürekli emniyet yönetimi gözetimi ve yönetişim tesis edilir.	• Yönetim tarafından faal bir şekilde, karın, maliyet azaltmanın ve verimliliğin önce geldiği faal bir şekilde gösterilmektedir. • Emniyetin iyileştirilmesine yönelik yatırımlar genellikle düzenlemeler tarafından gerekli görüldüğünde veya kazalar sonrasında yapılır. • Emniyet yönetimine ilişkin olarak gözetim veya yönetişim tesis edilmez.
Adapte Olabilirlik			
Adapte olabilirlik, çalışanların ve yönetimin geçmişteki deneyimlerden ders almaya istekli olma ve organizasyon dahilindeki emniyet seviyesinin iyileştirilmesi amacıyla gerekli tedbirleri alabilme derecesini yansıtır.		• Emniyet sorunları ele alınırken çalışan girdisi faal bir şekilde teşvik edilir. • Tüm olaylar ve denetim bulguları soruşturmaya tabi tutulur ve buna dayalı olarak hareket edilir. • Organizasyonel süreçler ve prosedürler emniyet etkisi bakımından sorgulanır (yüksek derecede öz eleştiri).	• Tüm seviyelerdeki çalışanlardan emniyet problemlerine yönelik olarak çalışan girdisi aranmaz. • Tedbirler genellikle sadece kazalar sonrasında veya düzenlemeler tarafından gerekli görüldüğünde alınır. • Herhangi bir kaza ortaya çıkmadığı sürece organizasyonel süreçlerin ve prosedürlerin yeterli olduğu değerlendirilir (kayıtsızlık veya öz eleştiri eksikliği)

Unsur	*Genel Açıklama*	*İmkan Veren Eylemler*	*İmkan Vermeyen Eylemler*
		• Emniyete yönelik açık proaktif bir yaklaşım sergilenir ve izlenir.	• Söz konusu kuruluş, herhangi bir kaza ortaya çıktığında dahi kendini sorgulamaya isteksizdir. • Emniyete yönelik reaktif bir yaklaşım sergilenir ve izlenir.
Farkındalık			
Farkındalık, çalışanların ve yönetimin söz konusu organizasyon ve söz konusu organizasyonun faaliyetleri tarafından karşı karşıya kalınan havacılık risklerinin farkında olma derecesini yansıtır. Devlet perspektifinden bakıldığında, personel, kendi faaliyetleri ve gözetim altında tuttukları organizasyonlar tarafından tetiklenen emniyet risklerinin farkındadır. Çalışanlar ve yönetim tarafından emniyet sorunlarına ilişkin olarak daima yüksek düzeyde ihtiyat muhafaza edilmelidir.		• Tehlike tanımlamaya ilişkin etkin bir yol tesis edilmiştir. • Soruşturmalar, kök nedenin belirlenmesini amaçlamaktadır. • Söz konusu organizasyon, önemli emniyet iyileştirmelerinden haberdardır ve kendisini gerektiği şekilde buna göre adapte eder. • Söz konusu organizasyon sistematik olarak emniyet iyileştirmelerinin amaçlandığı gibi uygulanıp uygulanmadığını ve çalışıp çalışmadığını değerlendirmektedir. • Söz konusu organizasyonun uygun mensupları kendi eylemlerinden ve şirket operasyonlarından / faaliyetlerinden kaynaklanan emniyet risklerinin tümüyle farkındadır.	• Tehlike tanımlamaya ilişkin hiçbir gayret sarf edilmemektedir. • Soruşturmalar, kök nedeni araştırmaktan ziyade ilk geçerli sebepte sona ermektedir. • Söz konusu organizasyon, önemli emniyet iyileştirmelerinden haberdar değildir. • Söz konusu organizasyon tarafından emniyet iyileştirmelerinin gereğince uygulanıp uygulanmadığı değerlendirilmemektedir. • Uygun olduğu hallerde, söz konusu organizasyonun uygun mensupları kendi eylemlerinden ve şirket operasyonlarından / faaliyetlerinden kaynaklanan emniyet risklerinin farkında değildir. • Emniyet verileri toplanmakta, ancak analiz edilmemekte ve bunlara dayalı olarak hareket edilmemektedir.
Emniyete ilişkin davranış			
Emniyete ilişkin davranış, söz konusu organizasyonun her bir seviyesi tarafından emniyet seviyesinin muhafaza edilmesi ve iyileştirilmesi bakımından hareket etme derecesini yansıtır. Emniyetin önemi ve emniyetin muhafaza edilmesi için uygulanması gereken süreçler ve prosedürler bilinmelidir.		• Çalışanlar emniyetli bir şekilde hareket etmek için ve rol modeller olarak hareket ederek kendilerini motive etmektedirler. • Emniyetli davranışa yönelik olarak sürekli izleme uygulanmaktadır.	• Çalışanlar, kendi çıkarları veya başka çıkarlar için kasti emniyetsiz davranış dolayısıyla cezalandırılmamaktadır.

Unsur	*Genel Açıklama*	*İmkan Veren Eylemler*	*İmkan Vermeyen Eylemler*
		• Yönetim ve iş arkadaşları tarafından kasıtlı emniyetsiz davranışa tolere edilmemektedir. • Çalışma koşulları havacılık emniyetini daima desteklemektedir.	• Çalışma koşulları, havacılık emniyeti bakımından zararlı davranışa ve geçici çözümlere yol açmaktadır. • Söz konusu organizasyonun ürünleri veya hizmetleri dahilinde havacılık emniyeti izlemesi uygulanmamaktadır. • Havacılık emniyetinin yararına olan yapıcı eleştiri hoş karşılanmamaktadır.
Bilgilendirme			
Bilgilendirme, söz konusu organizasyon dahilindeki tüm gerekli kişilere bilgilerin dağıtılma derecesini yansıtır. Çalışanların havacılık emniyeti kaygılarını rapor etmelerine imkan verilmeli ve çalışanlar bu yönde cesaretlendirilmeli ve raporlarına ilişkin geri bildirim almalıdırlar. Havacılık emniyetine ilişkin iş bilgilerinin, tehlikeli havacılık sistemi durumlarına ve sonuçlarına yol açabilecek iletişim eksikliklerinin önlenmesi amacıyla doğru insanlara anlamlı olarak iletilmesi gerekmektedir. Söz konusu Devlet, havacılık emniyeti ile ilgili bilgileri tüm hizmet sağlayıcıları ile paylaşmaya açıktır.		• Açık ve adil bir emniyet raporlaması ortamı mevcuttur. • Emniyetli operasyonlara veya kararların alınmasına imkan verebilmek amacıyla, çalışanlara emniyet ile ilgili bilgiler zamanında sunulmaktadır. • Emniyet ile ilgili bilgilerin anlaşılıp anlaşılmadığı ve bunlara dayalı olarak hareket edilip edilmediği yönetim ve amirler tarafından düzenli olarak kontrol edilmektedir. • Havacılık emniyetine ilişkin bilgi aktarımı ve eğitim faal bir şekilde uygulanmaktadır (örneğin, öğrenilen derslerin paylaşılması)	• Suçlayıcı bir emniyet raporlaması ortamı açıktadır. • Emniyet ile ilgili bilgiler alıkoyulmaktadır. • Emniyet iletişimi, etkinliği bakımından izlenmemektedir. • Bilgi aktarımı ve eğitim sağlanmamaktadır.

Unsur	*Genel Açıklama*	*İmkan Veren Eylemler*	*İmkan Vermeyen Eylemler*
Güven			
Çalışanların emniyete yönelik katkısı, eğitimleri ve deneyimleri ile örtüşen eylemlerinin veya kusurlarının cezalandırılmayacağı, güveni destekleyen bir raporlama ortamında zenginleşir. İşe yarar bir yaklaşım kapsamında bir akla yatkınlık testi uygulanmalı; başka bir deyişle, aynı düzeyde deneyime ve eğitime sahip olan bir kişi tarafından aynı şeyin yapılabilmesinin makul olup olmadığı test edilmelidir. Böyle bir ortam, etkin ve verimli emniyet raporlaması bakımından esastır. Etkin emniyet raporlaması sistemleri, Devletler ve hizmet sağlayıcıları tarafından mevcut ve olası emniyet eksikliklerine ve tehlikelerine işaret edilmesi için gerekli olan ilgili verilere ve bilgilere erişilecek şekilde, kişilerin kendi hatalarını ve deneyimlerini rapor etmeye istekli olmalarının sağlanmasına yardımcı olur. Bu sistemler, kişilerin emniyet verilerinin ve emniyet bilgilerinin sadece emniyetin iyileştirilmesi için kullanılacağından emin olabildikleri bir ortam yaratır.		• Tüm çalışanlarca bilinen, kabul edilebilir ile kabul edilemez davranış arasında bir ayrım vardır. • Hadiselere (kazalar ve olaylar da dahil) yönelik soruşturmalarda kişinin yanı sıra organizasyonel etkenler de göz önünde bulundurulmaktadır. • İyi havacılık emniyeti performansı fark edilmekte ve düzenli esasta ödüllendirilmektedir. • Çalışanlar ve operasyon personeli arasında, dahil oldukları olayların rapor edilmesi yönünde isteklilik mevcuttur.	• Kabul edilebilir ve kabul edilemez davranış arasında herhangi bir belirlenebilir ayrım mevcut değildir. • Çalışanlar, insan hatalarından dolayı sistematik ve katı bir şekilde cezalandırılmaktadır. • Kaza ve olay soruşturmaları sadece bireysel etkenlere odaklanmaktadır. • İyi emniyet performansı ve emniyetli davranış kanıksanmaktadır.

3.3.3 Emniyet kültürünün izlenmesi

3.3.3.1 Emniyet kültürü birçok etkiye tabidir ve organizasyonlar tarafından aşağıdaki amaçlarla kendi emniyet kültürlerinin değerlendirilmesi seçilebilir:

a) kişilerin söz konusu organizasyon hakkında ne hissettiklerini ve emniyetin ne denli önemli algılandığını anlamak;

b) güçlü ve zayıf yönleri belirlemek;

c) herhangi bir organizasyon dahilindeki çeşitli gruplar (alt kültürler) arasındaki farklılıkları tanımlamak ve

d) zamanla değişimleri incelemek (örneğin, herhangi bir kaza, üst yönetimdeki herhangi bir değişiklik veya değiştirilmiş sektörel ilişkiler düzenlemesi sonrasındaki belirgin organizasyonel değişikliklere karşılık olarak).

3.3.3.2 Genellikle aşağıdakilerle kombinasyon halinde olmak üzere, emniyet kültürü olgunluğunu değerlendirmek için kullanılan bir dizi araç mevcuttur:

a) anketler;

b) mülakatlar ve odak grupları;

c) gözlemler ve

d) doküman gözden geçirmeleri.

3.3.3.3 Emniyet kültürü olgunluğunun değerlendirilmesi, yönetim tarafından arzu edilen emniyet davranışlarını teşvik edecek eylemlere yol açarak değerli içgörü sağlayabilir. Bu tür değerlendirmelerde bir öznellik derecesinin olduğu ve bunların sadece belirli bir anda dahil olan kişilerin görüşlerini ve algılarını yansıtabileceği dikkate alınmalıdır. Ayrıca, emniyet kültürünün notlandırılması, söz konusu organizasyonun, emniyet kültürünü anlamak ve iyileştirmek için birlikte çalışmaktan ziyade, "doğru" nota ulaşmaya çalışmak için kasıtsız olarak teşvik edilmesiyle istenmeyen sonuçlara sahip olabilir.

Bölüm 4

EMNİYET PERFORMANSI YÖNETİMİ

4.1 GİRİŞ

4.1.1 Emniyet performansı yönetimi, Devlet Emniyet Programlarının (SSP'ler) ve Emniyet Yönetimi Sistemlerinin (SMS'ler) merkezindedir. Layığıyla uygulandığında, organizasyona, faaliyetlerinin ve süreçlerinin söz konusu organizasyonun emniyet amaçlarına ulaşılmasında etkin bir şekilde çalışıp çalışmadığının tespit edilmesine yönelik yöntemler sağlar. Buna, emniyet performansını izlemek ve ölçmek için kullanılan emniyet performansı göstergelerinin (SPI'ler) tanımlanmasıyla ulaşılabilir. Emniyet Performansı Göstergelerinin (SPI'ler) tanımlanmasıyla, elde edilen bilgiler, üst yönetimin, söz konusu organizasyon tarafından emniyet hedeflerine ulaşılmasını sağlamak üzere emniyet risklerinin daha fazla hafifletilmesi için tedbirlerin gerekli olup olmadığının tespit edilmesi de dahil olmak üzere, mevcut durumun ve destek karar almanın farkında olmasını sağlayacaktır.

4.1.2 Genel emniyet performansı yönetimi süreci ve bu sürecin, sırasıyla 5. ve 6. Bölümlerde ele alınan emniyet verilerini toplama ve işleme sistemleri (SDCPS) ve emniyet analizi ile nasıl bağlantılı olduğu aşağıdaki Şekil 4-1'de gösterilmektedir. Emniyetin teşvik edilmesi ile olan bağlantı, bu bilgilerin organizasyon genelinde aktarılmasının önemini vurgulamak amacıyla gösterilmektedir. Devlet Emniyet Planının (SSP) Emniyet Yönetimi Sisteminin (SMS) önemli bir bileşeni olan ve gerekli değerin genellikle verilmediği emniyetin teşvik edilmesi hakkında daha fazla bilgiye sırasıyla 8. ve 9. Bölümlerde ulaşılabilir.

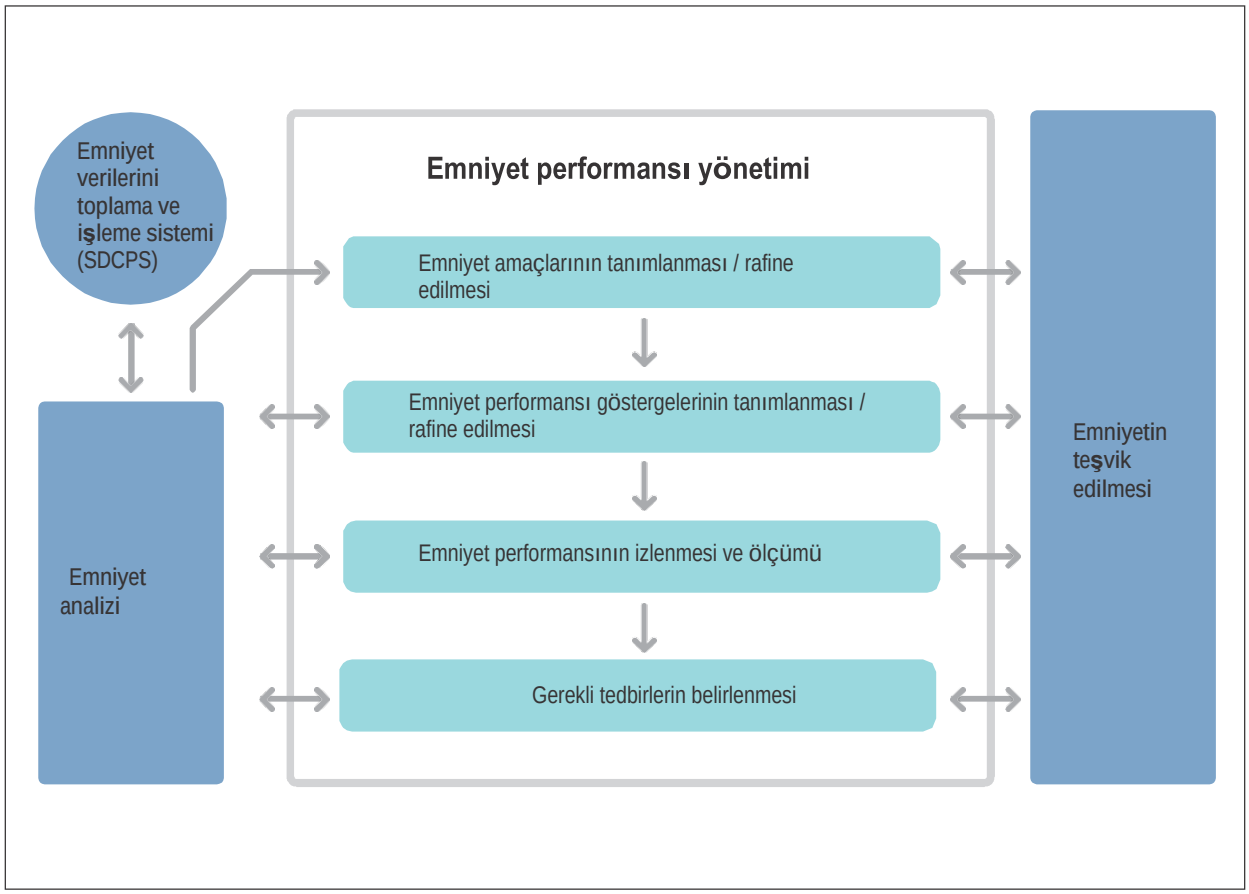
4.1.3 Emniyet performansı yönetimi, söz konusu organizasyona emniyet yönetimine ilişkin dört önemli sorunun sorulmasında ve cevaplanmasında yardımcı olur:

a) Söz konusu organizasyonun başlıca emniyet riskleri nelerdir? *Havacılık kaza ve olay verilerinin gözden geçirilmesinin yanı sıra yükselen risklerin saptanmasına ve tanımlanmasına yönelik kestirimci analizden elde edilen.*

b) Söz konusu organizasyon emniyet bakımından neye ulaşmak istemektedir ve ele alınması gereken başlıca emniyet riskleri nelerdir? *Söz konusu organizasyonun emniyet amaçları.*

c) Söz konusu organizasyon, emniyet amaçlarına yönelik ilerleme kaydedip kaydetmediğini nasıl bilecektir? *Emniyet Performansı Göstergeleri (SPI'ler), Emniyet Performansı Hedefleri (SPT'ler) ve uygulanması halinde, emniyet tetikleyicileri vasıtasıyla.*

d) Bilgiye dayalı emniyet kararlarının verilmesi için hangi emniyet verilerine ve emniyet bilgilerine ihtiyaç duyulmaktadır? Söz konusu organizasyonun kaynaklarının tahsis edilmesi de dahil olmak üzere. *Gitgide gelişen bir emniyet verilerini toplama ve işleme sistemi (SDCPS) ve emniyet verileri analizi vasıtasıyla.*



Şekil 4-1. Emniyet Performansı Yönetimi Süreci

4.1.4 Emniyet performansı yönetim sistemi aynı zamanda kabul edilebilir emniyet performansı seviyesi (ALoSP) oluşturmak için de kullanılabilir. Kabul edilebilir emniyet performansı seviyesinin oluşturulması hakkında daha fazla bilgiye 8. Bölümde ulaşılabilir.

4.1.5 Devletler ve hizmet sağlayıcıları arasındaki ilişki

4.1.5.1 Emniyet performansı tekniklerinin kullanımında ve uygulamasında Devletler ve hizmet sağlayıcıları arasında benzerlikler bulunmaktadır. Bu bölümdeki rehberlik hem Devletler hem de hizmet sağlayıcıları için oluşturulmuş olsa da bu bölümde bir takım farklılıklar saptanmıştır.

4.1.5.2 Devlet emniyet performansının geliştirilmesi, söz konusu Devlet tarafından emniyetin yönetilmesinde en önemli yönler olarak değerlendirilen yönlere odaklanmalıdır. Devlet için, etkili bir şekilde uygulanan Devlet Emniyet Programı (SSP), söz konusu Devletin hizmet sağlayıcılarının emniyet performansını, söz konusu Devletin gözetim kabiliyetini ve kılavuz ilkelerin belirlenmesiyle hizmet sağlayıcılarına sunulan desteği içermesi gereken, emniyet performansının yönetilmesine yönelik bir karar alma aracı olarak kullanılır. Devletler tarafından aşağıdaki hususlardaki becerilerinin ölçülmesi göz ardı edilmemelidir:

a) emniyet gözetimi sistemlerinin muhafaza edilmesi;

b) spesifik emniyet tedbirlerinin uygulanması ve emniyet inisiyatiflerinin uygulamaya koyulması ve

c) etkin halde kalmalarını sağlamak üzere mevcut emniyet riski kontrollerinin uyarlanması.

4.1.5.3 Hizmet sağlayıcıları için, emniyet performansı yönetiminin birincil amacı, emniyet risklerinin ne kadar iyi yönetildiğinin izlenmesi ve ölçülmesidir. Bu amaca, emniyet riski kontrollerinin uygulanması ve kaynakların tahsisi de dahil olmak üzere, emniyetin yönetimine ilişkin kararların alınması için kullanılacak bilgileri üreten bir Emniyet Yönetimi Sisteminin (SMS) etkili bir şekilde uygulanmasıyla ulaşılır.

4.1.5.4 Emniyet yönetiminin başarısı, söz konusu Devlet ile söz konusu Devletin hizmet sağlayıcıları arasındaki bağlılığa bağlıdır. Bilhassa kabul edilebilir emniyet performansı seviyesinin (ALoSP) belirlenmesine yönelik olmak üzere, hizmet sağlayıcıları tarafından izlenebilecek ve ardından söz konusu Devlet ile paylaşılabilecek uygun Emniyet Performansı Göstergelerini (SPI'ler) belirleyen Devlette faydalar olabilecektir. Hizmet sağlayıcılarından alınan bilgiler, havacılık endüstrisinin emniyet performansının ve söz konusu Devletin hizmet sağlayıcılarına etkin gözetim ve destek sunma becerisinin değerlendirilmesinde söz konusu Devlete yardım sağlayacaktır. Bununla birlikte, hizmet sağlayıcıları, kendi Emniyet Performansı Göstergelerinin (SPI'ler) kendilerinin operasyonel bağlamına, performans geçmişine ve beklentilerine uygun olmasını sağlamalıdırlar.

4.1.6 Emniyet performansı yönetimi ve arayüzleri

4.1.6.1 Devletler ve hizmet sağlayıcıları tarafından emniyet yönetiminin uygulanması değerlendirildiğinde, birbirleriyle arayüze sahip olan kuruluşlar tarafından tetiklenen emniyet risklerinin göz önünde bulundurulması önem arz etmektedir. Arayüzler dahili (örneğin, işletme ve bakım veya finans, insan kaynakları veya hukuk müşavirliği departmanları arasında) veya harici (örneğin, diğer Devlet, hizmet sağlayıcıları veya anlaşmalı hizmetler) nitelikte olabilir. Arayüz noktalarındaki tehlikeler ve ilgili riskler, emniyet olaylarına en çok katkıda bulunan unsurlar arasında yer almaktadır. Devletler ve hizmet sağlayıcıları, arayüzleri belirlenip yönetildiğinde arayüz ile ilgili riskler üzerinde daha fazla kontrole sahiptirler. Arayüzler, söz konusu organizasyonun sistem tanımında tanımlanmalıdır.

4.1.6.2 Devletler ve hizmet sağlayıcıları, emniyetli sonuçları sağlamak için arayüzlerinin sürekli olarak izlenmesinden ve yönetilmesinden sorumludurlar. Her bir arayüz tarafından teşkil edilen emniyet riski, ideal olarak, arayüz bağlantısına sahip olan kuruluşlar tarafından ortaklaşa olarak değerlendirilmelidir. Emniyet risklerine ve bunların tolere edilebilirliğine yönelik algının arayüz bağlantısına sahip olan organizasyonlar arasında değişkenlik arz edebilecek olması sebebiyle, işbirliği ziyadesiyle makbuldür. Emniyet Performansı Göstergelerinin (SPI'ler) belirlenmesi ve izlenmesi yoluyla arayüz riski yönetiminin paylaşılması, bilgisizlik veya potansiyel olarak tek taraflı risk yönetimi yerine emniyet risklerine yönelik karşılıklı bilinci teşvik eder. Aynı zamanda, her iki organizasyonun emniyet etkinliğini iyileştirebilecek bilgi transferine ve çalışma uygulamalarına yönelik bir fırsat yaratır.

4.1.6.3 Bu sebeple, riskleri ve hafifletme tedbirleri izlemek ve ölçmek için Emniyet Performansı Göstergeleri (SPI'ler) kararlaştırılmalı ve belirlenmelidir. Arayüz bağlantısına sahip olan organizasyonlar arasındaki, açık bir şekilde tanımlanmış izleme ve yönetim sorumluluklarının yer aldığı resmi bir arayüz yönetimi sözleşmesi etkin bir yaklaşıma ilişkin örnektir.

4.2 EMNİYET AMAÇLARI

4.2.1 Emniyet amaçları, emniyet başarılarına veya ulaşılacak arzu edilen sonuçlara yönelik kısa ve öz, üst seviye beyanlardır. Emniyet amaçları, söz konusu organizasyonun faaliyetlerini yönlendirir ve bu sebeple, söz konusu organizasyonun üst seviye emniyet taahhüdünü ortaya koyan emniyet politikası ile tutarlı olmalıdır. Aynı zamanda emniyet önceliklerinin personele ve havacılık topluluğuna bir bütün olarak bildirilmesi bakımından yarar sağlar. Emniyet amaçlarının belirlenmesi, emniyet performansı yönetimi sürecine yönelik stratejik yönlendirme sağlar ve emniyet ile ilgili karar almaya yönelik olarak sağlam bir temele imkan verir. Emniyet performansının yönetimi, politikalarda veya süreçlerde değişiklikler yapılırken veya emniyet performansının iyileştirilmesi amacıyla söz konusu organizasyonun kaynakları tahsis edilirken göz önünde bulundurulması gereken birincil husustur.

4.2.2 Emniyet amaçları aşağıdaki türlerden olabilir:

a) *süreç odaklı*: operasyon personelinden beklenen emniyetli davranışlar veya söz konusu organizasyon tarafından emniyet riskinin yönetilmesi için uygulanan tedbirlerin gerçekleştirilmesi bakımından belirtilir veya

b) *sonuç odaklı*: kazaların veya operasyonel kayıpların çevrelenmesine yönelik tedbirleri ve trendleri kapsar.

4.2.3 Emniyet amaçları takımında, Emniyet Performansı Göstergeleri (SPI'ler) ve Emniyet Performansı Hedefleri (SPT'ler) için yeterli kapsama ve yönlendirme sağlamak için gerek süreç odaklı gerek sonuç odaklı amaçların bir harmanı yer almalıdır. Emniyet amaçlarının ve beraberindeki Emniyet Performansı Göstergelerinin (SPI'ler) ve Emniyet Performansı Hedeflerinin (SPT'ler) organizasyon tarafından emniyet performansının muhafaza edilip edilmediğinin veya iyileştirilip iyileştirilmediğinin kanıtlanmasına imkan veren bir paket oluşturmalı kaydıyla, emniyet amaçlarının tek başlarına spesifik, ölçülebilir, ulaşılabilir, ilgili ve zamanında (SMART (George T. Doran, 1981) olması gerekmez.

Tablo 6. Emniyet amaçlarına ilişkin örnekler

Emniyet amaçlarına ilişkin örnekler		
süreç odaklı	Devlet veya hizmet sağlayıcısı	Emniyet raporlaması seviyelerinin arttırılması.
sonuç odaklı	hizmet sağlayıcısı	Olumsuz apron emniyeti olayları oranının düşürülmesi. (yüksek seviye) veya Olumsuz apron emniyeti olaylarının yıllık sayısının bir önceki yıla göre azaltılması.
sonuç odaklı	Devlet	X sektöründeki emniyet olaylarının yıllık sayısının düşürülmesi.

4.2.4 Organizasyonlar aynı zamanda, emniyet amaçlarını taktiksel veya operasyonel seviyede belirlemeyi veya emniyet amaçlarını spesifik projelere, ürünlere ve süreçlere uygulamayı da seçebilirler. Herhangi bir emniyet amacı aynı zamanda benzer anlama sahip olan diğer terimlerin (örneğin, gaye veya hedef) kullanılmasıyla da ifade edilebilir.

4.3 EMNİYET PERFORMANSI GÖSTERGELERİ VE EMNİYET PERFORMANSI HEDEFLERİ

4.3.1 Emniyet performansı göstergeleri türleri

Kalitatif ve kantitatif göstergeler

4.3.1.1 Emniyet Performansı Göstergeleri (SPI'ler), üst yönetime, söz konusu organizasyonun emniyet amacına ulaşmasının muhtemel olup olmadığının bilinmesinde yardımcı olmak üzere kullanılırlar ve kalitatif veya kantitatif olabilirler. Kantitatif göstergeler, nitelikten ziyade niceliğe göre ölçüme ilişkindir, kalitatif göstergeler ise tanımlayıcıdır ve niteliğe göre ölçüdür.

Daha kolay bir şeklide sayılmaları ve karşılaştırılmaları sebebiyle, kantitatif göstergeler kalitatif göstergeler karşısında tercih edilir. Gösterge seçimi, nicelik bakımından ölçülebilen güvenilir verilerin elverişliliğine bağlıdır. Gerekli verilerin, karşılaştırılabilir, genelleştirilebilir veriler (kantitatif) yoksa emniyet durumunun tanımlayıcı bir görünümü (kalitatif) şeklinde mi olması gerekir? İster kalitatif ister kantitatif olsun her bir seçenek farklı Emniyet Performansı Göstergeleri (SPI'ler) türlerini içerir ve dikkatli bir Emniyet Performansı Göstergesi (SPI) seçimi süreci gerektirir. Bir çok durumda yaklaşımların kombinasyonu faydalıdır ve tek bir yaklaşımın benimsenmesinden doğabilecek problemlerin bir çoğunu çözüme kavuşturabilir. Hizmet sağlayıcılarının Emniyet Yönetimi Sisteminin (SMS) belirli bir sektördeki olgunluğu Devlet için, emniyet kültürünün değerlendirilmesi ise hizmet sağlayıcısı için kalitatif gösterge örneğidir.

4.3.1.2 Kantitatif göstergeler sayı olarak (x adet ihlal) veya oran olarak (n hareketi başına x adet ihlal) ifade edilebilir. Bazı hallerde, sayısal ifade yeterli olacaktır. Bununla birlikte, sadece sayıların kullanılması, faaliyet seviyesinde dalgalanma olması halinde gerçek emniyet durumunun çarpıtılmış olarak ifade edilmesine yol açabilecektir. Örneğin, hava trafik kontrol tarafından Temmuz ayında üç, Ağustos ayında altı irtifa sapmasının kayıt altına alınması halinde, emniyet performansındaki belirgin kötüleşmeye yönelik büyük kaygı söz konusu olabilecektir. Öte yandan, Ağustos ayında, Temmuz ayında gerçekleşen hareketler ikiye katlanmıştır ki bu da hareket başına irtifa sapmalarının veya oranın artmamış, düşmüş olduğu anlamına gelmektedir. Bu husus, detaylı inceleme seviyesini değiştirilebilir veya değiştirmeyebilir, ancak veriye dayalı emniyet karar alma süreci bakımından hayati olabilecek başka bir değerli bilgi sunar.

4.3.1.3 Bu sebeple, uygun olduğu hallerde, faaliyet seviyesine bakılmaksızın performans seviyesinin ölçülmesi için Emniyet Performansı Göstergelerinin (SPI'ler) nisbi oran bakımından yansıtılması gerekir. Bu sayede, söz konusu faaliyet ister artsın ister düşsün, performansın normalleştirilmiş ölçümüne imkan verilir. Başka bir örnek olarak, herhangi bir Emniyet Performansı Göstergesi (SPI) pist ihlallerinin sayısını ölçebilir. Fakat, izlenen dönemde daha az sayıda kalkış olması halinde sonuç yanıltıcı olabilecektir. Hareket sayısına göre pist ihlali sayısı daha tutarlı ve değerli bir performans ölçümü olabilecektir; örneğin, 1000 hareket başına x adet ihlal.

Gecikmeli ve öncü göstergeler

4.3.1.4 Devletler ve hizmet sağlayıcıları tarafından Emniyet Performansı Göstergelerini (SPI'ler) sınıflandırmak için kullanılan en yaygın iki kategori gecikmeli ve öncüdür. Gecikmeli Emniyet Performansı Göstergeleri (SPI'ler), daha önceden ortaya çıkan olayları ölçerler. Bunlara aynı zamanda "sonuca dayalı Emniyet Performansı Göstergeleri (SPI'ler)" olarak da anılır ve (her zaman olmamakla birlikte) normalde söz konusu organizasyonun kaçınmayı amaçladığı olumsuz sonuçlardır. Öncü Emniyet Performansı Göstergeleri (SPI'ler), emniyetin iyileştirilmesi veya muhafaza edilmesi için uygulanmakta olan süreçleri ve girdileri ölçerler. Bu göstergeler, herhangi bir spesifik sonuca yol açma veya katkıda bulunma potansiyeline sahip olan koşulları izlemeleri ve ölçmeleri sebebiyle aynı zamanda "faaliyet veya süreç Emniyet Performansı Göstergeleri (SPI'ler)" olarak da bilinirler.

4.3.1.5 Gecikmeli Emniyet Performansı Göstergeleri (SPI'ler), organizasyona, geçmişte neyin gerçekleştiğinin anlaşılmasında yardımcı olurlar ve uzun vadeli eğilim belirleme bakımından faydalıdırlar. Üst seviye gösterge olarak veya "hava aracı tipine göre kaza türleri" veya "bölgeye göre spesifik olay türleri" gibi spesifik olay türlerinin göstergesi olarak kullanılabilirler. Emniyet sonuçlarını ölçmelerine bağlı olarak gecikmeli Emniyet Performansı Göstergeleri (SPI'ler), emniyet hafifletmelerinin etkinliğini ölçebilirler. Sistemin genel emniyet performansının doğrulanmasında etkindirler. Örneğin, "apron işaretlemelerinin yeniden tasarımını izleyen araçlar arasındaki hareket başına aprondaki çarpışmaların sayısının" izlenmesi, (başka hiçbir şeyin değişmediği varsayılarak) yeni işaretlemelerin etkinliğine yönelik ölçüme imkan verir. Çarpışmalardaki azalma, apron sisteminin genel emniyet performansındaki, söz konusu sistemdeki değişikliğe atfedilebilir nitelikte bir iyileşmeyi doğrular.

4.3.1.6 Sistemde var olan ve ele alınması gereken koşulları belirlemek için gecikmeli Emniyet Performansı Göstergelerindeki (SPI'ler) trendler analiz edilebilir. Önceki örnek kullanılarak, hareket sayısına göre aprondaki çarpışmalardaki artan trend, hafifletme olarak standart altı apron işaretlemelerinin belirlenmesine sebebiyet veren unsur olabilecektir.

4.3.1.7 Gecikmeli Emniyet Performansı Göstergeleri (SPI'ler) iki türe ayrılır:

a) *düşük ihtimal/yüksek önem derecesi*: kazalar veya ciddi olaylar gibi sonuçlar. Yüksek öneme sahip sonuçların düşük sıklığı, (sektör segmenti seviyesinde veya bölgesel seviyede olmak üzere) verilerin birleştirilmesinin daha anlamlı analizlerle sonuçlanabileceği anlamına gelir. "Kuş çarpması sebebiyle hava aracı ve/veya motor hasarı" bu tür gecikmeli Emniyet Performansı Göstergesine (SPI) örnek olabilir.

b) *yüksek ihtimal/düşük önem derecesi*: kendilerini mutlaka ciddi bir kazada veya olayda göstermemiş olan sonuçlar; bunlara bazı hallerde öncül göstergeler de denir. Yüksek ihtimal/düşük önem derecesine yönelik Emniyet Performansı Göstergeleri (SPI'ler) ağırlıklı olarak spesifik emniyet sorunlarının izlenmesi ve mevcut emniyet riski hafifletmelerinin etkinliğinin ölçülmesi için kullanılır. Gerçek kuş çarpması miktarından ziyade kuş faaliyeti seviyesini gösteren "kuş radarı tespitleri" bu türden öncül Emniyet Performansı Göstergesine (SPI) örnek olabilir.

4.3.1.8 Havacılık emniyeti tedbirleri, "düşük ihtimal/yüksek önem derecesine sahip" sonuçları yansıtan Emniyet Performansı Göstergelerine (SPI'ler) karşı tarih boyunca önyargılı olmuştur. Kazaların ve olayların yüksek profile sahip olaylar olmaları ve sayılmalarının kolay olması sebebiyle bu husus anlaşılabilirdir. Bununla birlikte, emniyet performansı yönetimi perspektifinden bakıldığında, kazalara ve ciddi olaylara güvenilir bir emniyet performansı göstergesi olarak haddinden fazla itimat edilmesinde çekinceler vardır. Örneğin, kazalar ve ciddi olaylar seyrektir (yılda sadece tek bir kaza olabilir veya hiç olmayabilir) veya trendlerin belirlenmesine yönelik olarak istatistiksel analiz yapılmasını zorlaştırır. Bu, söz konusu sistemin mutlaka güvenli olduğunu göstermez. Bu tür verilere itimat edilmesinin akıbeti, aslında tehlikeli bir şekilde kazaya yakın iken, organizasyonun veya sistemin emniyet performansının etkin olduğuna dair potansiyel olarak yanlış bir güven hissidir.

4.3.1.9 Öncü göstergeler, emniyetin iyileştirilmesi veya muhafaza edilmesi için uygulanmakta olan süreçlere ve girdilere odaklanan tedbirlerdir. Bu göstergeler, herhangi bir spesifik sonuç haline gelme veya herhangi bir spesifik sonuca katkıda bulunma potansiyeline sahip olan koşulları izlemeleri ve ölçmeleri sebebiyle aynı zamanda "faaliyet veya süreç Emniyet Performansı Göstergeleri (SPI'ler)" olarak da bilinirler.

4.3.1.10 Proaktif emniyet performansı yönetimine yönelik olarak organizasyonel kabiliyetlerin gelişimine destek veren Emniyet Performansı Göstergeleri (SPI'ler), "emniyet eğitimini vaktinde başarılı bir şekilde tamamlayan personel yüzdesi" veya "kuş korkutma faaliyetlerinin sıklığı" gibi unsurları içerir.

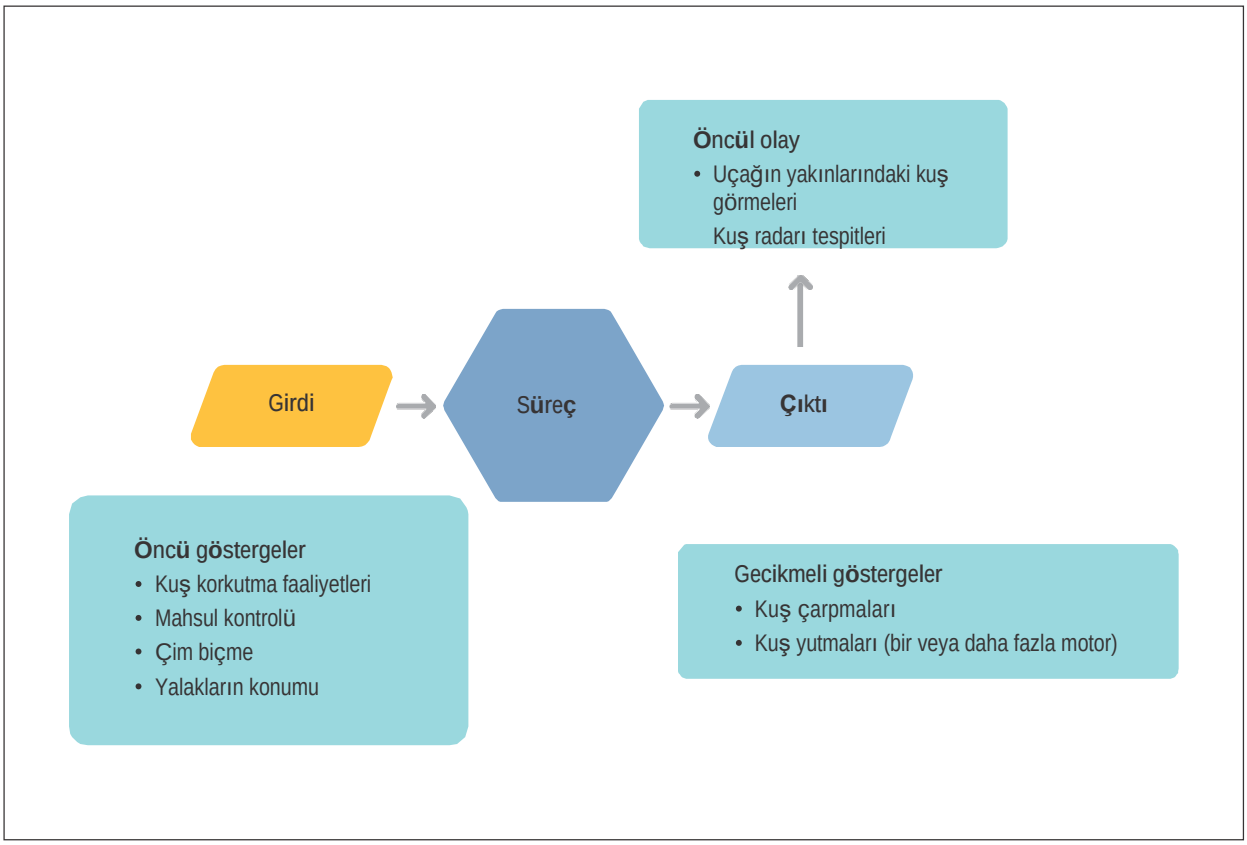
4.3.1.11 Öncü Emniyet Performansı Göstergeleri (SPI'ler) aynı zamanda, söz konusu organizasyonu, çalışma ortamındaki değişiklikler de dahil olmak üzere, operasyonlarda değişikliklerle nasıl başa çıkıldığı hakkında bilgilendirebilir. Odak noktası, değişiklik sonucundaki zayıflıkların ve kırılganlıkların tahmin edilmesi veya herhangi bir değişiklik sonrasında performansın izlenmesi olacaktır. "X prosedürünü uygulayan iş sahası yüzdesi", operasyonlardaki herhangi bir değişikliğin izlenmesine yönelik Emniyet Performansı Göstergesine (SPI) örnektir.

4.3.1.12 Emniyet performansının daha tutarlı ve yararlı bir şekilde gösterilmesi için, hem "düşük ihtimal/yüksek önem derecesine sahip" olayları hem de "yüksek ihtimal/düşük önem derecesine sahip" olayları ölçen gecikmeli Emniyet Performansı Göstergeleri (SPI'ler), öncü Emniyet Performansı Göstergeleri (SPI'ler) ile birleştirilmelidir. Organizasyonun emniyet performansına dair daha kapsamlı ve gerçekçi bir resim sunan öncü ve gecikmeli göstergeler kavramı Şekil 4-2'de açıklanmaktadır.

4.3.2 Emniyet Performansı Göstergelerinin (SPI'ler) seçilmesi ve tanımlanması

4.3.2.1 Emniyet Performansı Göstergeleri (SPI'ler), organizasyona, emniyete ilişkin olarak önceden nerede olduğu, halihazırda nerede olduğu ve nereye yöneldiği bakımından, emniyet performansına ilişkin bir görünüm sunan parametrelerdir. Bu resim, söz konusu organizasyonun veriye dayalı emniyet kararlarının dayalı olarak alındığı sağlam ve savunulabilir bir temel işlevi görür. Bu kararlar, sırasıyla, söz konusu organizasyonun emniyet performansına olumlu yönde etki eder. Bu sebeple, Emniyet Performansı Göstergelerinin (SPI'ler) belirlenmesi gerçekçi, ilgili ve basitliğe veya karmaşıklığa bakılmaksızın, emniyet amaçlarıyla bağlantılı olmalıdır.

4.3.2.2 Emniyet Performansı Göstergelerinin (SPI'ler) başlangıçtaki seçiminin, yakalanması kolay ve/veya uygun olan olayları veya süreçleri (kolaylıkla mevcut olabilecek olan emniyet verileri) temsil eden parametrelerin izlenmesi ve ölçümüyle sınırlı olması muhtemeldir. İdeal olarak, Emniyet Performansı Göstergeleri (SPI'ler) ulaşılması kolay olanlardan ziyade, emniyet performansının önemli göstergeleri olan parametrelere odaklanmalıdır.



Şekil 4-2. Öncü karşısında Gecikmeli gösterge kavramı aşamaları

4.3.2.3 Emniyet Performansı Göstergeleri (SPI'ler):

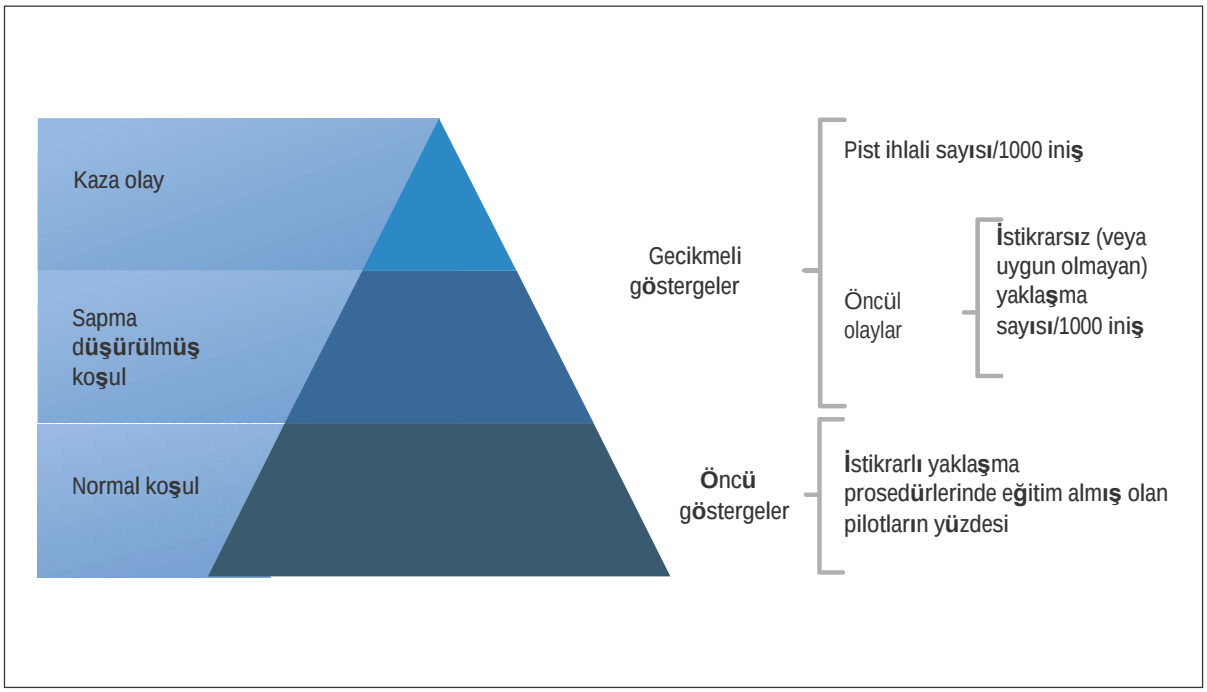
a) göstermeyi amaçladıkları emniyet amacı ile ilgili olmalı;

b) mevcut verilere ve güvenilir ölçüme dayalı olarak seçilmeli veya geliştirilmeli;

c) uygun bir şekilde spesifik ve ölçülebilir olmalı ve

d) ihtimaller ve söz konusu organizasyonun kısıtları göz önünde bulundurularak gerçekçi olmalıdır.

4.3.2.4 Emniyet performansının açık bir şekilde gösterilmesini sağlamak için genellikle Emniyet Performansı Göstergelerinin (SPI'ler) bir kombinasyonu gereklidir. Gecikmeli ve öncü Emniyet Performansı Göstergeleri (SPI'ler) arasında açık bir bağlantı olmalıdır. İdeal olarak gecikmeli Emniyet Performansı Göstergeleri (SPI'ler), öncü Emniyet Performansı Göstergeleri (SPI'ler) tespit edilmeden önce tanımlanmalıdır. Daha ciddi bir olay veya koşul (gecikmeli Emniyet Performansı Göstergesi (SPI)) ile bağlantılı olan öncül Emniyet Performansı Göstergesinin (SPI) tanımlanması ikisi arasında açık bir korelasyonun olmasını sağlar. Gecikmeli veya öncü, Emniyet Performansı Göstergelerinin (SPI'ler) tümü eşit ölçüde geçerli ve değerlidir. Şekil 4-3'de bu bağlantıların bir örneği yer almaktadır.



Şekil 4-3. Gecikmeli ve öncü göstergeler arasındaki bağlantı

4.3.2.5 Organizasyonun emniyet amaçları ile ilgili olan Emniyet Performansı Göstergelerinin (SPI'ler) seçilmesi önemlidir. İyi bir şekilde tanımlanmış ve hizalanmış Emniyet Performansı Göstergelerine (SPI'ler) sahip olunması, emniyet amaçlarına ulaşılması yönünde kaydedilen ilerlemeyi gösterecek olan Emniyet Performansı Hedeflerinin (SPT'ler) belirlenmesini kolaylaştıracaktır. Bu sayede, organizasyon tarafından kaynakların, planlanan emniyet performansına ulaşmak için ne zaman ve nasıl hareket edilmesi gerektiğini ve tam olarak neyin gerekli olduğunu bilerek en büyük emniyet etkisine yönelik olarak tahsis edilmesine imkan verilir. Örneğin, herhangi bir Devlet, "pist ihlali sayısının üç yıl içerisinde yüzde elli oranında azaltılmasına" ilişkin bir emniyet amacına ve "tüm havaalanları genelinde milyon kalkış başına pist ihlali sayısına" ilişkin iyi hizalanmış ilişkili bir Emniyet Performansı Göstergesine (SPI) sahiptir. İzleme başladığında ihlal sayısının başlangıçta düşmesi, ancak on iki ay sonrasında tekrar yukarı çıkmaya başlaması halinde, söz konusu Devlet, kaynakları, Emniyet Performansı Göstergelerine (SPI'ler) göre, emniyet amacına kolaylıkla ulaşıldığı alandan istenmeyen trendin azaltılması için pist ihlallerinin düşürülmesine yönelik olarak yeniden tahsis etmeyi seçebilecektir.

Emniyet Performansı Göstergelerinin (SPI'ler) tanımlanması

4.3.2.6 Her bir Emniyet Performansı Göstergesinin (SPI) içeriğinde aşağıdakiler yer almalıdır:

a) söz konusu Emniyet Performansı Göstergesi (SPI) tarafından neyin ölçüldüğüne ilişkin açıklama;

b) söz konusu Emniyet Performansı Göstergesinin (SPI) amacı (neyin yönetilmesinin amaçlandığı ve kimin bilgilendirilmesinin amaçlandığı);

c) ölçü birimleri ve hesaplanmasına yönelik gereklilikler;

d) söz konusu Emniyet Performansı Göstergesinin (SPI) toplanmasından, doğrulanmasından, izlenmesinden, raporlanmasından ve buna dayalı olarak hareket edilmesinden kimin sorumlu olduğu (bu kişiler, söz konusu organizasyonun farklı kısımlarından çalışanlar olabilecektir);

e) verilerin nereden veya nasıl toplanması gerektiği ve

f) Emniyet Performansı Göstergesi (SPI) verilerinin raporlanmasının, toplanmasının, izlenmesinin ve analiz edilmesinin sıklığı.

Emniyet Performansı Göstergeleri (SPI'ler) ve emniyet raporlaması

4.3.2.7 Operasyonel uygulamalardaki değişiklikler, etkileri potansiyel rapor edenler tarafından tümüyle kabul edilinceye değin eksik raporlamaya yol açabilir. Bu durum "raporlama ön yargısı" olarak bilinir. Emniyet bilgilerinin ve ilgili kaynakların korunmasına ilişkin hükümlerdeki değişiklikler de fazladan raporlamaya yol açabilir. Her iki durumda da raporlama ön yargısı, Emniyet Performansı Göstergesi (SPI) için kullanılan verilerin amacını ve doğruluğunu çarpıtabilir. Sağduyulu bir şekilde kullanıldığında, emniyet raporlaması, emniyet performansının yönetimi için yine de değerli veriler sağlayabilir.

4.3.3 Emniyet performansı hedeflerinin belirlenmesi

4.3.3.1 Emniyet performansı hedefleri (SPT'ler), emniyet performansında arzu edilen kısa ve orta vadeli başarıları tanımlar. Bu hedefler, söz konusu organizasyonun emniyet amaçlarına ulaşılmasında doğru yolda olduğuna dair güven veren ve emniyet performansı yönetimi faaliyetlerinin etkinliğinin doğrulanmasına yönelik ölçülebilir bir yol sunan "kilometre taşları" işlevi görürler. Emniyet Performansı Hedefinin (SPT) belirlenmesinde, geçerli emniyet riski seviyesinin, emniyet riski tolere edilebilirliğinin yanı sıra belirli havacılık sektörünün emniyetine yönelik beklentiler gibi etkenler dikkate alınmalıdır. Emniyet Performansı Hedefleri (SPT'ler) ilişkili havacılık sektörü için gerçekçi bir şekilde neyin ulaşılabilir olduğunun ve geçmiş trend verileri mevcut olduğunda, belirli Emniyet Performansı Göstergesinin (SPI) geçmiş performansının değerlendirilmesi sonrasında belirlenmelidir.

4.3.3.2 Emniyet amaçlarının, birlikte çalışan Emniyet Performansı Göstergelerinin (SPI'ler) ve Emniyet Performansı Hedeflerinin (SPT'ler) kombinasyonunun SMART olması halinde, bu sayede söz konusu organizasyonun emniyet performansını daha etkin bir şekilde kanıtlamasına imkan verilir. Özellikle Emniyet Performansı Hedefleri (SPT'ler) olmak üzere, emniyet performansı yönetimin amaçlarına ulaşılmasına yönelik birden fazla yaklaşım mevcuttur. Bu yaklaşımlardan biri, hizalanmış Emniyet Performansı Göstergelerine (SPI'ler) sahip olan genel olarak yüksek seviyede emniyet amaçlarının oluşturulmasını ve ardından, temel emniyet performansının tesis edilmesi sonrasında makul iyileştirme seviyelerinin tanımlanmasını içerir. Bu iyileştirme seviyeleri, spesifik hedeflere (örneğin, yüzde düşüşü) veya pozitif trende ulaşılmasına dayalı olabilir. Emniyet amaçları SMART olduğunda kullanılabilecek bir diğer yaklaşım ise, emniyet amaçlarına ulaşılmasında emniyet hedeflerinin kilometre taşları işlevini görmesini sağlamaktır. Bu yaklaşımların her ikisi de geçerlidir ve emniyet performansının kanıtlanmasında organizasyon tarafından etkin bulunan başka yaklaşımlar da olabilir. Spesifik koşullara uygun olarak farklı yaklaşımlar kombinasyon halinde kullanılabilir.

Yüksek seviye emniyet amaçlarına sahip hedeflerin belirlenmesi

4.3.3.3 Hedefler, yüksek seviye emniyet amaçlarının üst yönetim tarafından kabul edilmesiyle oluşturulur. Organizasyon tarafından, bunun akabinde, kararlaştırılan emniyet amacına (amaçlarına) yönelik emniyet performansı iyileştirmesini gösterecek olan uygun Emniyet Performansı Göstergeleri (SPI'ler) belirlenir. Söz konusu Emniyet Performansı Göstergeleri (SPI'ler), mevcut veri kaynakları kullanılarak ölçülecek olmakla birlikte, ilave verilerin toplanmasını da gerektirebilecektir. Organizasyon tarafından, bunun ardından, Emniyet Performansı Göstergeleri (SPI'ler) toplanmaya, analiz edilmeye ve sunulmaya başlanır. Organizasyonun emniyet performansına ve emniyet amaçlarına doğru yöneldiğine veya emniyet amaçlarından uzaklaştığına yönelik genel görünümü ortaya koyacak olan trendler ortaya çıkmaya başlar. Bu noktada, söz konusu organizasyon tarafından her bir Emniyet Performansı Göstergesine (SPI) ilişkin makul ve erişilebilir Emniyet Performansı Hedefleri (SPT'ler) belirlenebilir.

SMART emniyet amaçlarına sahip hedeflerin belirlenmesi

4.3.3.4 Emniyet amaçları iletilmesi zor olabilir ve ulaşılması zorlu görülebilir; emniyet amaçlarının daha küçük somut emniyet hedeflerine bölünmesiyle bu amaçların hayata geçirilmesinin yönetilmesi daha kolay olur. Bu yolla, hedefler, strateji ile günlük operasyonlar arasında kritik bir bağlantı oluşturur. Organizasyonlar tarafından, emniyet performansını yönlendiren kilit alanlar belirlenmeli ve bunların ölçülmesine yönelik bir yol tesis edilmelidir. Temel emniyet performansını belirleyerek organizasyonun mevcut emniyet performansının ne olduğu hakkında bir fikre sahip olması sonrasında, söz konusu organizasyon tarafından, ulaşma amacında olunması gerekenler hakkında Devletteki herkese açık bir anlayış vermek için Emniyet Performansı Hedeflerinin (SPT'ler) belirlenmesine başlanabilir. Söz konusu organizasyon tarafından, performans hedeflerinin belirlenmesini desteklemek için karşılaştırma da kullanılabilir. Bu, toplumdaki diğerlerinin nasıl yaptıklarının anlaşılması amacıyla performanslarını ölçmekte olan benzer organizasyonlardan performans bilgilerinin kullanılmasını içerir.

4.3.3.5 Şekil 4-4'de, emniyet amaçları, Emniyet Performansı Göstergeleri (SPI'ler) ve Emniyet Performansı Hedefleri (SPT'ler) arasındaki ilişkiye ilişkin bir örnek açıklanmaktadır. Bu örnekte, söz konusu organizasyon tarafından 2018 yılında milyon hareket başına 100 pist ihlali kayda alınmıştır. Bu rakamın çok fazla olduğu tespit edilmiş ve 2022 itibariyle pist ihlali sayısının yüzde elli oranında azaltılmasına yönelik bir amaç belirlenmiştir. Bu hedefleri karşılamak için spesifik hedeflenmiş tedbirler ve ilişkili zaman çizelgeleri tanımlanmıştır. İlerlemesini izlemek, ölçmek ve rapor etmek üzere, söz konusu organizasyon tarafından Emniyet Performansı Göstergesi (SPI) olarak "yılda milyon hareket başına PİST ihlali" seçilmiştir. Söz konusu organizasyon, emniyet amacıyla hizalı spesifik hedeflerin belirlenmesi halinde ilerlemenin daha çabuk ve etkili olacağının bilincindedir. Dolayısıyla, söz konusu organizasyon tarafından, raporlama dönemi (dört yıl) genelinde yıl başına 12.5'lik bir ortalama azaltıma denk gelen bir emniyet hedefi koyulmuştur. Grafiksel açıklamada gösterildiği gibi, söz konusu ilerlemenin ilk yıllarda daha fazla olması ancak sonraki yıllarda bundan daha düşük olması beklenmektedir. Bu durum, söz konusu amaca yönelik kavisli öngörü ile gösterilmektedir. Şekil 4-4'de;

a) SMART emniyet amacı, "2022 itibariyle PİST ihlallerinde yüzde 50 azaltım"'dır;

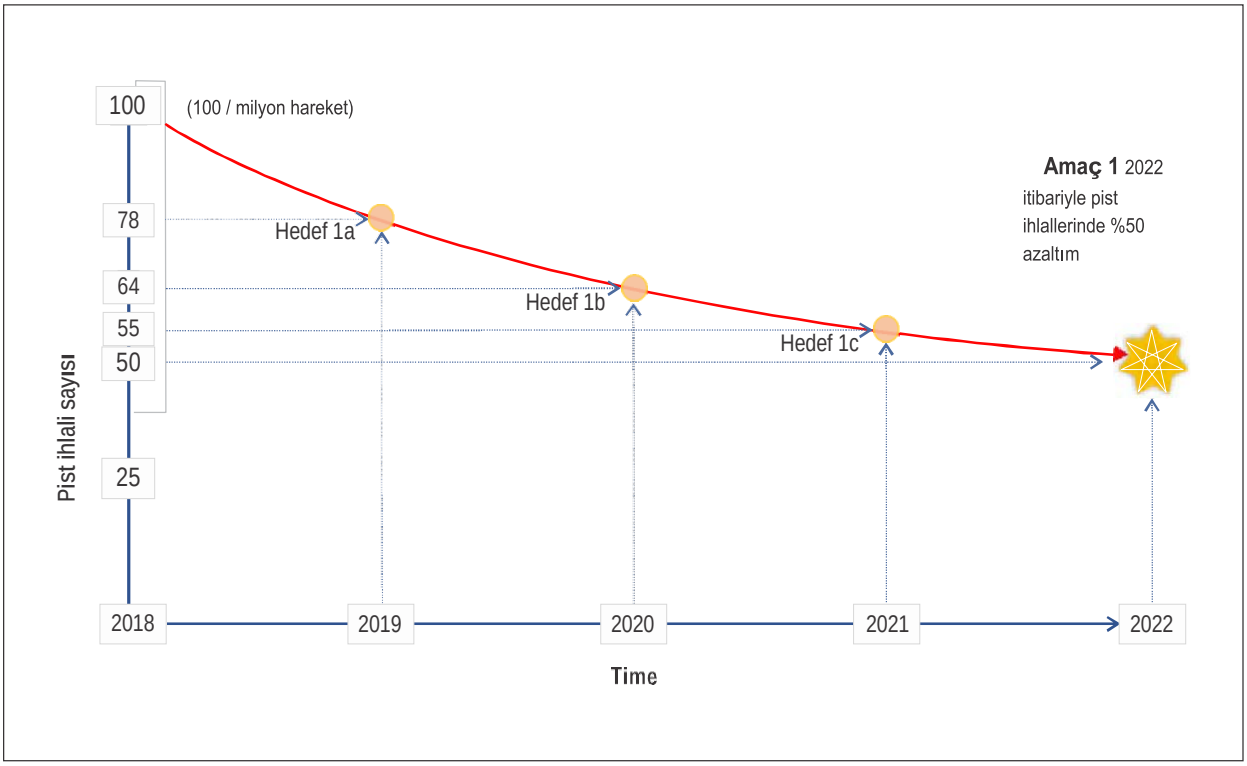
b) seçilen Emniyet Performansı Göstergesi (SPI), "yılda milyon hareket başına pist ihlali sayısı"dır ve

c) bu amaca ilişkin emniyet hedefleri, SMART emniyet amacına ulaşılmasına yönelik kilometre taşlarını temsil etmekte ve 2022'ye kadar her yıl yüzde ~12 azaltıma tekabül etmektedir;

   1) 1a Emniyet Performansı Göstergesi (SPT) "2019 yılında milyon hareket başına 78 pist ihlalinin altı"dır;

   2) 1b Emniyet Performansı Göstergesi (SPT) "2020 yılında milyon hareket başına 64 pist ihlalinin altı"dır;

   3) 1c Emniyet Performansı Göstergesi (SPT) "2021 yılında milyon hareket başına 55 pist ihlalinin altı"dır;



Şekil 4-4. SMART emniyet amalarına sahip Emniyet Performansı Hedefleri (SPT'ler) Örneği

Emniyet Performansı Göstergesi (SPI) ve Emniyet Performansı Hedefi (SPT) seçiminde dikkate alınması gereken ilave hususlar

4.3.3.6 Emniyet Performansı Göstergelerinin (SPI'ler) ve Emniyet Performansı Hedeflerinin (SPT'ler) seçiminde aşağıdakiler dikkate alınmalıdır:

a) *İş yükü yönetimi.* Çalışılabilir miktarda Emniyet Performansı Göstergesinin (SPI) oluşturulması, personel tarafından iş yükünün izlenmesinin ve raporlanmasının yönetilmesine yardımcı olabilir. Emniyet Performansı Göstergelerinin (SPI'ler) karmaşıklığı veya gerekli verilerin elverişliliği için de aynı durum geçerlidir. Neyin yapılabilir olduğunun kararlaştırılması ve ardından Emniyet Performansı Göstergelerinin (SPI'ler) bu esasa dayalı olarak önceliklendirilmesi daha iyidir. Herhangi bir Emniyet Performansı Göstergesinin (SPI) artık emniyet performansı hakkında bilgi vermemesi veya herhangi bir Emniyet Performansı Göstergesine (SPI) daha düşük öncelik verilmesi halinde, daha faydalı veya daha yüksek önceliğe sahip olan bir göstergeden yana son vermeyi dikkate alın.

b) *Emniyet Performansı Göstergelerinin (SPI'ler) optimal yayılması*. Emniyet Performansı Göstergelerinin (SPI'ler) odak alanlarını kapsayan kombinasyonu, söz konusu organizasyonun genel emniyet performansına yönelik bir içgörünün kazanılmasına yardımcı olacak ve veriye dayalı karar almaya imkan verecektir.

c) *Emniyet Performansı Göstergelerinin (SPI'ler) Anlaşılırlığı* Emniyet Performansı Göstergesi (SPI) seçerken, neyin ne kadar sık ölçüldüğü açık olmalıdır. Açık tanımlara sahip olan Emniyet Performansı Göstergeleri (SPI'ler), sonuçların anlaşılmasına yardımcı olur, yanlış yorumlamayı önler ve zamanla anlamlı kıyaslamalara imkan verir.

d) *Arzu edilen davranışın teşvik edilmesi*. Emniyet Performansı Hedefleri (SPT'ler) davranışları değiştirebilir ve arzu edilen sonuçlara katkı sağlayabilir. Bu husus özellikle, söz konusu hedefe ulaşılmasının yönetim ücretlendirmesi gibi organizasyonel ödüllerle bağlantılı olması halinde ilgilidir. Emniyet Performansı Hedefleri (SPT'ler), özellikle savunulabilir kararlarla ve emniyet performansının iyileştirilmesiyle sonuçlanan olumlu organizasyonel ve bireysel davranışları desteklemelidir. Emniyet Performansı Göstergelerini (SPI'ler) ve Emniyet Performansı Hedeflerini (SPT'ler) seçerken potansiyel istenmeyen davranışların göz önünde bulundurulması eşit ölçüde önemlidir.

e) *Değerli tedbirlerin seçilmesi*. Sadece ölçülmesi kolay olanların değil, faydalı Emniyet Performansı Göstergelerinin (SPI'ler) seçilmesi zorunludur. Karar almayı, emniyet performansı yönetimini ve söz konusu organizasyonun emniyet amaçlarına ulaşılmasını iyileştirmek üzere yönlendirenler olmak üzere, en faydalı emniyet parametrelerinin neler olduğuna dair karar organizasyona bırakılmalıdır.

f) *Emniyet Performansı Hedeflerine (SPT'ler) Ulaşılması*. Bu, bilhassa önem arz eden bir husustur ve arzu edilen emniyet davranışları ile bağlantılıdır. Kararlaştırılan Emniyet Performansı Hedefine (SPT) ulaşılması daima emniyet performansı iyileştirmesini göstermez. Organizasyon tarafından sadece Emniyet Performansı Hedeflerinin (SPT'ler) karşılanması ile gerçek, kanıtlanabilir organizasyonel emniyet performansı iyileştirmesi arasında ayrım yapılmalıdır. Organizasyon tarafından, başkalarından ayrı olarak Emniyet Performansı Hedefine (SPT) bakmaktan ziyade, söz konusu hedefe ulaşılan bağlamın dikkate alınması zorunludur. Münferit Emniyet Performansı Hedefine (SPT) ulaşılmasından ziyade, emniyet performansında genel iyileşmenin kabulü, arzu edilen organizasyonel davranışları destekleyecek ve Emniyet Riski Yönetiminin (SRM) ve emniyet güvencesinin tam kalbinde yatan emniyet bilgileri alışverişini teşvik edecektir. Bu sayede, Devlet ile hizmet sağlayıcısı arasındaki ilişki ile bunların emniyet verilerini ve fikirlerini paylaşmaya istekliliği arttırılacaktır.

Emniyet Performansı Hedeflerinin (SPT'ler) belirlenmesine yönelik uyarılar

4.3.3.7 Herhangi bir hedefin tespit edilmesine yönelik olarak kullanılmaktan ziyade trendlerin izlenmesi için daha iyi olan bir takım Emniyet Performansı Göstergelerinin (SPI'ler) olabilecek olmasına bağlı olarak Emniyet Performansı Hedeflerinin (SPT'ler) tanımlanması daima gerekli veya uygun değildir. Emniyet raporlaması, herhangi bir hedefe sahip olunmasının (söz konusu hedefin herhangi bir sayıyı aşmaması gerekmesi halinde) kişileri raporlama yapmaktan veya (söz konusu hedefin belirli bir sayıya ulaşılması yönünde olması halinde) sıradan konuları raporlamaktan caydırmasına örnek teşkil etmektedir. Aynı zamanda, bunların tespit edilmesinin zor olabilecek olmasına bağlı olarak mutlak bir hedefin tanımlanmasından ziyade sürekli olarak emniyet performansının iyileştirilmesinin (başka bir deyişle, olayların sayısının düşürülmesinin) hedeflenmesine yönelik bir istikamet yönünün tanımlanması için kullanılması daha iyi olan Emniyet Performansı Göstergeleri (SPI'ler) de söz konusu olabilir. Uygun Emniyet Performansı Hedeflerinin (SPT'le) kararlaştırılmasında aşağıdakilerin dikkate alınması gerekir:

a) İstenmeyen davranışlara sevk; başarı göstergesi olarak sayılara ulaşılmasına çok fazla odaklanmaları halinde, yöneticiler veya organizasyonlar tarafından emniyet performansındaki amaçlanan iyileştirmeye ulaşılamayabilir.

b) Operasyonel hedefler; Emniyet Performansı Hedefleri (SPT'ler) dengesi olmadan (zamanında kalkışlar, genel giderlerin indirilmesi gibi) operasyonel hedeflere ulaşılmasına çok fazla odaklanılması, emniyet performansının iyileştirmeyerek "operasyonel hedeflere ulaşılmasına" yol açabilir.

c) Nitelikten ziyade niceliğe odaklanılması; personeli veya departmanları hedefi karşılamaya teşvik edebilir, ancak hedefe ulaşılması kötü ürün veya hizmet ortaya koyabilir.

d) Üst limit inovasyonu; amaçlanmamasına rağmen, herhangi bir hedefe ulaşılması gevşemeye ve başka iyileştirmeye ihtiyaç duyulmamasına ve rehavetin yerleşmesine yol açabilir.

e) Organizasyonel çatışma; birlikte çalışmaya çalışılmasına odaklanılmasından ziyade kimin sorumlu olduğuna dair tartışmalarına bağlı olarak hedefler departmanlar ve organizasyonlar arasında çatışmalar oluşturabilir.

4.3.4 Emniyet Performansı Ölçümü

Emniyet performansı ölçümüne doğru bir şekilde ulaşılması, emniyet amaçlarına ulaşılmasının en iyi nasıl ölçüleceğine karar verilmesini içerir. Bu husus, Devletten Devlete ve hizmet sağlayıcısından hizmet sağlayıcısına farklılık gösterecektir. Organizasyonların, emniyet amaçlarına yönelik emniyet iyileştirmesini neyin tetiklediğine dair stratejik farkındalıklarını oluşturmaya zaman ayırmaları gerekir.

4.3.5 Emniyet Performansı Göstergelerinin (SPI'ler) ve Emniyet Performansı Hedeflerinin (SPT'ler) Kullanımı

Emniyet Performansı Göstergeleri (SPI'ler) ve Emniyet Performansı Hedefleri (SPT'ler), emniyet performansının kanıtlanmasına yönelik olarak farklı yollarla kullanılabilir. Organizasyonlar tarafından çeşitli ölçüm araçlarının ve yaklaşımlarının kendilerine özgü koşullara ve ölçülen şeyin mahiyetine bağlı olarak uyarlanması, seçilmesi ve uygulanması kritik öneme sahiptir. Örneğin, bazı hallerde, organizasyonlar tarafından tümü spesifik ilişkili olan Emniyet Performansı Hedeflerine (SPT'lere) sahip olan Emniyet Performansı Göstergeleri (SPI'ler) benimsenebilir. Başka bir durumda, spesifik hedef değerler olmadan Emniyet Performansı Göstergelerinde (SPI'ler) pozitif bir trende ulaşılmasına odaklanılması tercih edilebilir. Seçilen performans metrikleri paketinde genel olarak bu yaklaşımların bir kombinasyonu kullanılır.

4.4 EMNİYET PERFORMANSININ İZLENMESİ

4.4.1 Planlanan sonucu ortaya koyacaklarına inandıkları Emniyet Performansı Göstergelerine (SPI'ler) dayalı hedefleri saptadıklarında, organizasyonlar tarafından ortaya konacak sonucuna yönelik açık sorumluluk tayin edilerek paydaşlar tarafından takip sağlanmalıdır. Her bir havacılık otoritesi, sektör ve hizmet sağlayıcısı için Emniyet Performansı Hedeflerinin (SPT'ler) tanımlanması, açık hesap verme sorumluluğu tayin edilerek söz konusu Devlet için kabul edilebilir emniyet performansı seviyesine (ALoSP) ulaşılmasını destekler.

4.4.2 Kaydedilen ilerlemenin beklendiği gibi olmaması halinde hangi değişikliklere ihtiyaç duyulduğunun belirlenmesi ve organizasyonun emniyet amaçlarını karşılama taahhüdünün güçlendirilmesi için söz konusu organizasyonun emniyet performansının izlenmesine ve ölçülmesine yönelik mekanizmalar oluşturulmalıdır.

4.4.3 Temel emniyet performansı

Organizasyonun emniyet amaçlarına yönelik ilerlemeyi nasıl planladığının kavranması, söz konusu organizasyonun emniyete ilişkin olarak nerede olduğunu bilmesini gerektirir. Organizasyonun emniyet performansı yapısının (emniyet amaçları, göstergeler, hedefler, tetikleyiciler) oluşturulması ve çalışır halde olması sonrasında, bir izleme süresiyle söz konusu organizasyonun temel emniyet performansının öğrenilmesi mümkündür. Temel emniyet performansı, ilerlemenin ölçülebileceği referans noktası olan, emniyet performansı ölçümü sürecinin başlangıcındaki emniyet performansıdır. Şekil 4-3 ve 4-4 kapsamında kullanılan örnekte, belirli emniyet amacına ilişkin temel emniyet performansı "(2018) yılı sırasında milyon hareket başına 100 pist ihlali" olmuştur. Bu sağlam temelden doğru ve anlamlı yansımalar ve hedefler kayıt altına alınabilir.

4.4.4 Emniyet Performansı Göstergelerinin (SPI'ler) ve Emniyet Performansı Hedeflerinin (SPT'ler) Geliştirilmesi

4.4.4.1 Emniyet amaçlarına yönelik kaydedilen ilerlemenin takip edilmesi ve hedeflerin gerçekçi ve ulaşılabilir olmasının sağlanması için ihtiyaç duyulan bilgileri sunup sunmadıklarını tespit etmek için Emniyet Performansı Göstergelerinin (SPI'ler) ve ilişkili Emniyet Performansı Hedeflerinin (SPT'ler) gözden geçirilmesi gerekecektir.

4.4.4.2 Emniyet performansı yönetimi, süreklilik arz eden bir faaliyettir. Emniyet riskleri ve/veya verilerin elverişliliği zamanla değişir. Başlangıçtaki Emniyet Performansı Göstergeleri (SPI'ler), emniyet bilgilerine yönelik sınırlı kaynaklar kullanılarak geliştirilebilir. Sonrasında, daha fazla raporlama kanalı oluşturulabilir, daha fazla emniyet verileri elverişli olabilir ve söz konusu organizasyonun emniyet analizi kabiliyetlerinin olgunlaşması muhtemel olur. Organizasyonlar için başlangıçta basit (daha geniş) Emniyet Performansı Göstergelerinin (SPI'ler) oluşturulması uygun olabilir. Daha fazla veri ve emniyet yönetimi kabiliyeti topladıkça, arzu edilen emniyet amaçlarıyla daha fazla uyumlu hale getirilmek üzere Emniyet Performansı Göstergelerinin (SPI'ler) ve Emniyet Performansı Hedeflerinin (SPT'ler) kapsamının geliştirilmesi değerlendirilebilir.

Küçük, karmaşık olmayan organizasyonlar tarafından, Emniyet Performansı Göstergelerinin (SPI'ler) ve Emniyet Performansı Hedeflerinin (SPT'ler) geliştirilmesi veya çoğu havacılık sistemi için geçerli olan genel (ancak spesifik) göstergeler seçilebilir. Genel göstergelere ilişkin bazı örnekler şunlardır:

a) Ekipmanların yapısal hasar görmesini içeren olaylar;

b) neredeyse kazanın ortaya çıktığı koşullara işaret eden olaylar;

c) operasyon personelinin veya havacılık topluluğunun üyelerinin ölümcül veya ciddi bir şekilde yaralandığı olaylar;

d) operasyon personelinin inkapasite veya görevlerini emniyetli bir şekilde ifa edemez hale geldiği olaylar;

e) gönüllü olay raporlarının oranı ve

f) zorunlu olay raporlarının oranı.

4.4.4.3 Daha büyük ve karmaşık organizasyonlar tarafından daha geniş ve/veya derin bir yelpazede Emniyet Performansı Göstergelerinin (SPI'ler) ve Emniyet Performansı Hedeflerinin (SPT'ler) oluşturulması ve faaliyete özgü olanlarla yukarıda listelenenler gibi genel göstergelerin entegre edilmesi seçilebilir. Örneğin, büyük çaplı havayollarına hizmet sunan ve karmaşık bir hava sahasında bulunan büyük bir havalimanında, operasyonun spesifik yönlerini temsil eden daha derin kapsama sahip olan Emniyet Performansı Göstergelerine (SPI'ler) sahip olan genel nitelikteki bir takım Emniyet Performansı Göstergelerinin (SPI'ler) birleştirilmesi değerlendirilebilecektir. Bunların izlenmesi daha fazla çaba gerektirecek olmakla birlikte üstün emniyet sonuçları ortaya koyması muhtemeldir. Emniyet Performansı Göstergelerinin (SPI'ler) ve Emniyet Performansı Hedeflerinin (SPT'ler) nispi karmaşıklığı ile söz konusu Devletin veya hizmet sağlayıcısının operasyonlarının karmaşıklığı arasında açık bir korelasyon mevcuttur. Bu nispi karmaşıklık söz konusu gösterge ve hedef setinde yansıtılmalıdır. Emniyet performansı yönetiminin tesis edilmesinden sorumlu olanlar bunun bilincinde olmalıdır.

4.4.4.4 Organizasyon tarafından seçilen Emniyet Performansı Göstergeleri (SPI'ler) ve Emniyet Performansı Hedefleri (SPT'ler) seti, organizasyonel emniyet performansının yansımaları olarak sürekli anlam taşıdıklarından emin olunmak için periyodik olarak gözden geçirilmelidir. Emniyet Performansı Göstergelerinin (SPI'ler) ve Emniyet Performansı Hedeflerinin (SPT'ler) devam ettirilmesine, sonlandırılmasına veya değiştirilmesine ilişkin bazı nedenler şunları içerir:

a) Emniyet Performansı Göstergelerinin (SPI'ler) sürekli olarak aynı değeri (yüzde sıfır veya yüzde 100 gibi) bildirmesi; bu Emniyet Performansı Göstergelerinin (SPI'ler) üst yönetimin karar alma sürecine anlamlı girdi sağlamasının muhtemel olmaması;

b) Benzer davranışa sahip olan ve böylelikle tekrar olarak değerlendirilen Emniyet Performansı Göstergeleri (SPI'ler);

c) herhangi bir programın veya hedeflenen iyileştirmenin uygulamaya konmasının ölçülmesine yönelik olarak uygulanan Emniyet Performansı Göstergesine (SPI) yönelik Emniyet Performansı Hedefinin (SPT) karşılanması;

d) başka bir emniyet kaygısının izlenmek ve ölçülmek için daha yüksek öncelik haline gelmesi;

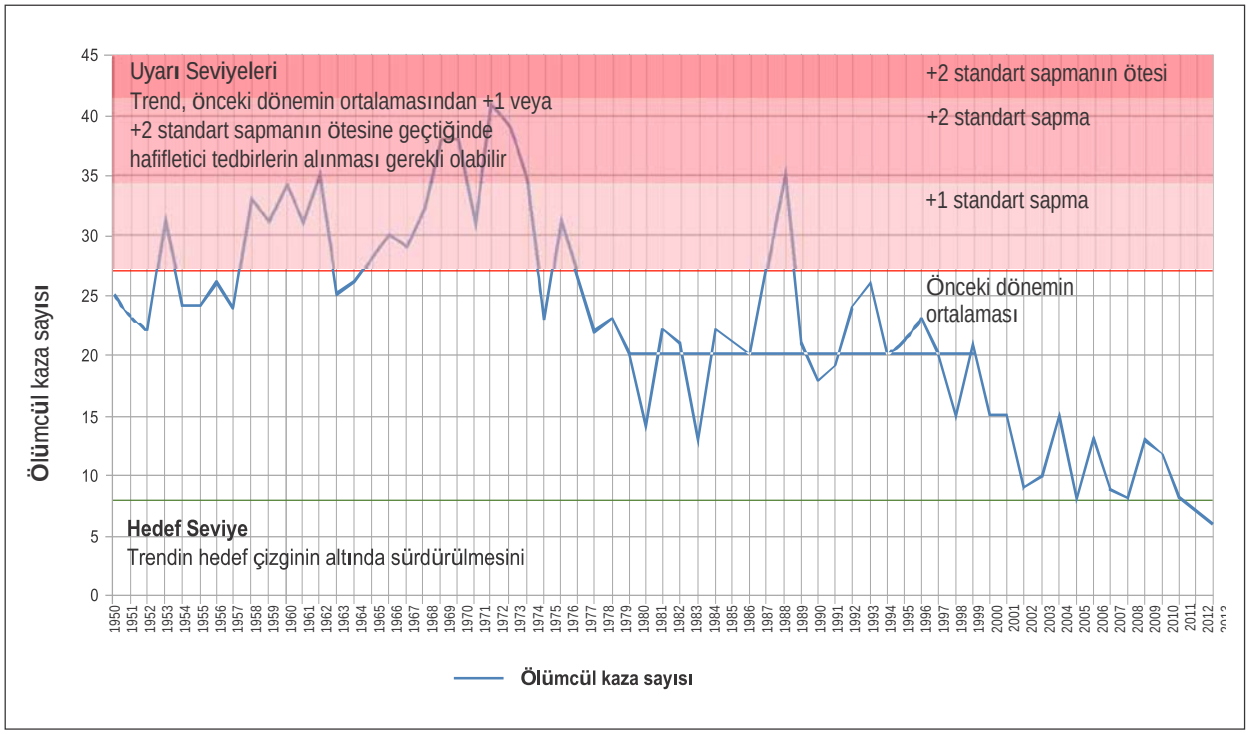
e) herhangi bir Emniyet Performansı Göstergesinin (SPI) detaylarının daraltılması suretiyle (başka bir deyişle, "sinyali" açıklığa kavuşturmak için "gürültünün" azaltılması) belirli bir emniyet kaygısının daha iyi anlaşılması ve

f) emniyet amaçlarının değişmiş olması ve sonuç olarak Emniyet Performansı Göstergelerinin (SPI'ler) ilgili olmaya devam için güncellenmesinin gerekmesi.

4.4.5 Emniyet tetikleyicileri

4.4.5.1 Tetikleyiciler kavramına yönelik kısa ve öz perspektif, organizasyon tarafından emniyet performansının yönetilmesi bağlamında tetikleyicilerin sahip olduğu nihai role yardımcı olunmasında yerindedir.

4.4.5.2 Tetikleyici, belirli bir göstergeye ilişkin değerlendirmeyi, kararı, düzeltmeyi veya iyileştirici faaliyeti tetiklemeye (başlatmaya) yarayan, belirlenmiş seviye veya kriterler değeridir. Popülasyon standart sapma (STDEVP) prensibinin kullanımı, Emniyet Performansı Hedeflerine (SPT'ler) yönelik limit dışı tetikleyici kriterlerin belirlenmesine yönelik bir yöntemdir. Bu yöntemde, belirli bir emniyet göstergesinin önceki geçmişe ait veri göstergelerine dayalı standart sağma (SD) değeri elde edilir. Standart Sapma (SD) değeri ile geçmişe ait veri setinin ortalama (vasati) değeri, bir sonraki izleme dönemine ilişkin temel tetikleyici değeri teşkil eder. Standart Sapma (SD) prensibi (temel bir istatistiksel işlev), değişkenliği (veri göstergesi dalgalanmaları) de dahil olmak üzere, belirli göstergenin (veri seti) geçmişteki gerçek performansına dayalı tetikleyici seviye kriterlerini belirler. Daha değişken bir geçmişe ait veri seti genellikle, bir sonraki izleme dönemine ilişkin daha yüksek (daha verimli) bir tetikleyici seviye değeri ile sonuçlanacaktır. Tetikleyiciler, karar alıcılar tarafından bilgiye dayalı emniyet kararlarının alınmasına imkan veren ve bu sayede emniyet performansını iyileştiren erken uyarılar sunarlar. Aşağıdaki Şekil 4-5'te, standart sapmalara (SD'ler) dayalı tetikleyici seviyelere ilişkin bir örnek gösterilmektedir. Bu örnekte, trend bir önceki dönemin ortalamasından +1 Standart Sapmanın (SD) veya +2 Standart Sapmanın (SD) ötesine geçtiğinde veriye dayalı kararların ve emniyet hafifletme tedbirlerinin alınması gerekebilir. Genellikle, tetikleyici seviyeler (bu durumda +1 Standart Sapma (SD), +2 Standart Sapma (SD) veya +2 Standart Sapmanın (SD) ötesi), karar yönetimi seviyeleri ve tedbirin ivediliği ile uyumlu olur.



Şekil 4-5. Emniyet tetikleyicileri (uyarı) seviyelerinin temsiline ilişkin örnek

4.4.5.3 Emniyet Performansı Hedeflerinin (SPT'ler) ve tetikleme ayarlarının (kullanılması halinde) tanımlanması sonrasında, ilgili performans durumları için ilişkili Emniyet Performansı Göstergesi (SPI) takip edilebilir. Belirli bir izleme dönemi için genel Emniyet Performansı Hedefine (SPT) ve tam Emniyet Performansı Göstergeleri (SPI'ler) paketinin tetikleme performansının sonucuna ilişkin konsolide bir özet derlenebilir ve/veya birleştirilebilir. Her bir Emniyet Performansı Hedefi (SPT) başarısı ve ihlal edilmeyen her bir tetikleyici seviye için kalitatif değerler (yeterli/yetersiz) tayin edilebilir. Alternatif olarak, söz konusu Emniyet Performansı Göstergeleri (SPI'ler) paketinin genel performansının kantitatif ölçümünün sağlanması için sayısal değerler (puanlar) kullanılabilir.

4.4.5.4 Tetikleyici değerlerin, belirli bir göstergeye ilişkin değerlendirmeyi, kararı, düzeltmeyi veya iyileştirici faaliyeti tetiklemeye (başlatmaya) yaradığı dikkate alınmalıdır. Tetiklenen Emniyet Performansı Göstergesinin (SPI) mutlaka yıkıcı olması veya başarısızlık göstergesi olması gerekmez. Sadece, söz konusu faaliyetin önceden belirlenen limitin ötesine geçtiğine dair bir işarettir. Tetikleyicinin amacı, koşullara bağlı olarak iyileştirici tedbir alıp almaması gereken karar alıcıların dikkatini çekmektir.

4.4.6 Tetikleyicilere ilişkin uyarılar

4.4.6.1 Güvenilir tetikleyici seviyelerin saptanmasında zorluklar mevcuttur. Tetikleyiciler ve ilişkili seviyeleri en iyi, bol miktarda emniyet verileri ve emniyet verileri yönetimi kabiliyetleri olduğunda işler. Bu husus, söz konusu organizasyon üzerinde ilave iş yükü öngörebilir. Tetikleyici kavramı tamamen teknik sistemlerin (örneğin uçak motoru izlemesi) Emniyet Riski Yönetimi (SRM) için tasarlanmıştır ve bu sistemler için en uygundur. Bu durumda, büyük miktarlardaki kantitatif veriler doğru tetikleyicilerin ve tetikleme seviyelerinin saptanmasını destekler. Tetikleyiciler kavramı, tartışmaya açık olmak üzere, sosyo-teknik sistemlerin Emniyet Riski Yönetimi (SRM) ile daha az ilgilidir. Sosyo-teknik sistemler, sistemin hizmet sunumuna veya üretim amaçlarına ulaşmak üzere kişilerin faal bir şekilde süreçlerle ve teknolojilerle etkileşim halinde olduğu sistemlerdir. Gerek Devlet Emniyet Programı (SSP) gerek Emniyet Yönetimi Sistemi (SMS) sosyo-teknik sistemlerdir. Kişiler konuya dahil olduğunda güvenilir tedbirlere yönelik sınırlamaların söz konusu olması sebebiyle, sosyo-teknik sistemlerde daha az güvenilir ve anlamlı tetikleyiciler kullanılır.

4.4.6.2 Bu sebepten dolayı, tetikleyicilerin anlamı olması için daha esnek bir yaklaşıma ihtiyaç duyulur. Annex 19 kapsamında, Devletler veya hizmet sağlayıcıları tarafından her bir Emniyet Performansı Göstergesi (SPI) için tetikleme seviyelerinin tanımlanması gerekli görülmemektedir. Bununla birlikte, organizasyonlar için herhangi bir Emniyet Performansı Göstergesine (SPI) yönelik verilerinin çok spesifik olduğu, yeterli veri göstergelerinin olduğu ve söz konusu verilerin yeterli şekilde güvenilir olduğu faydalar mevcuttur.

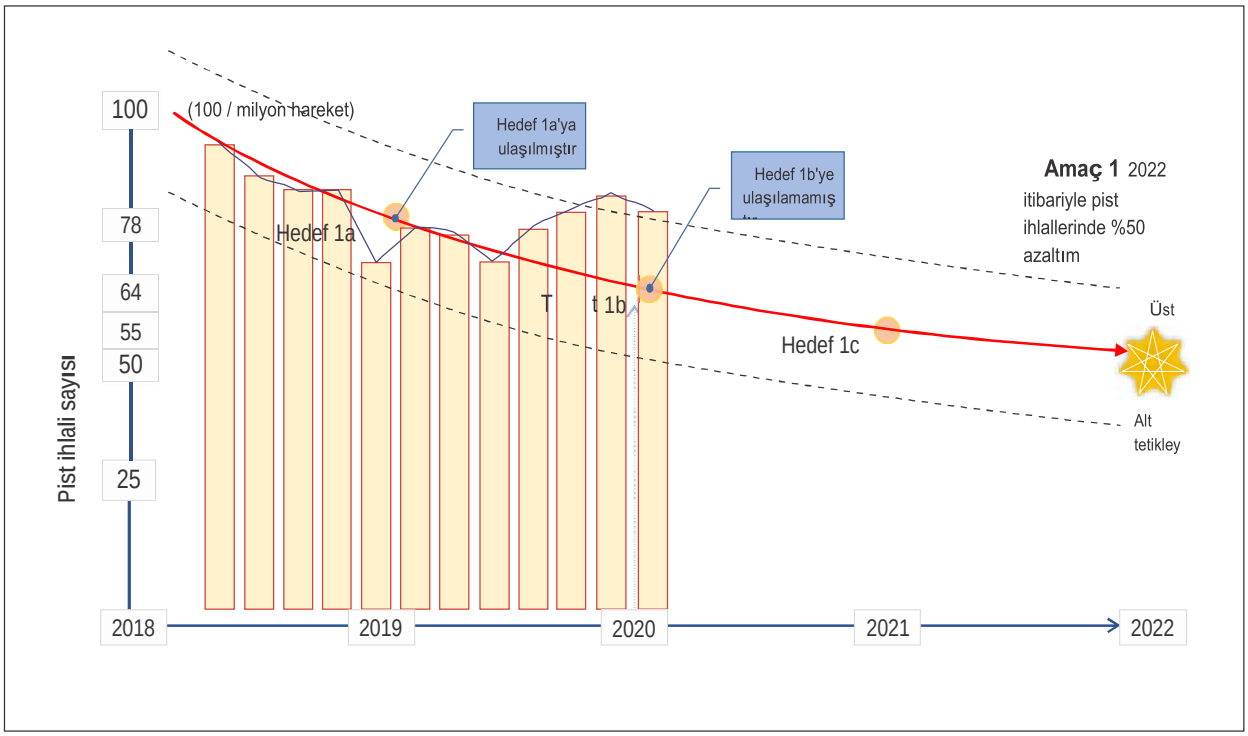
4.4.6.3 Aşağıdaki Şekil 4-6'da "2022 itibariyle pist ihlallerinde yüzde 50 azaltım" adlı bir önceki örneğin genişletilmesi yer almaktadır. Bu senaryoda 2020 yılına gelinmiştir. Söz konusu organizasyon tarafından emniyet verileri toplanmakta (Emniyet Performansı Göstergesi (SPI)-"Milyon hareket/yıl başına hiçbir pist ihlali yoktur") ve örnekleri düşürmek için paydaşlarla birlikte çalışılmaktadır. 2019 yılı için olan Emniyet Performansı Hedefine (SPT) (yılda milyon hareket başına <78 pist ihlali) ulaşılmıştır. Bununla birlikte, söz konusu Emniyet Performansı Göstergesi (SPI), 2020 yılına ilişkin Emniyet Performansı Hedefine (SPT) (yılda milyon hareket başına <64 pist ihlali) ulaşılmamasının yanı sıra, birbirini izleyen iki raporlama dönemindeki ihlal sayısının tetikleyiciyi aştığını göstermektedir. Karar alıcılar emniyet performansındaki kötüleşme dolayısıyla uyarılmışlardır ve başka tedbir almak üzere söz konusu verilere dayalı olarak karar almak durumundadırlar. Veriye dayalı kararlarının amacı, emniyet performansının kabul edilebilir bölgeye geri getirilmesi ve emniyet amacına ulaşılmaya yönelik ilerlenmesi olacaktır.

4.4.7 Gerekli tedbirlerin belirlenmesi

4.4.7.1 Tartışmaya açık olmak üzere, emniyet performansı yönetim yapısının oluşturulmasının en önemli sonucu, organizasyonun karar alıcılarına, güncel, güvenilir emniyet verilerine ve emniyet bilgilerine dayalı olarak kararlar alabilmelerine imkan verecek şekilde bilgilerin sunulmasıdır. Amaç daima, kararların emniyet politikasına uygun ve emniyet amaçlarına yönelik olarak alınabilmesi olmalıdır.

4.4.7.2 Emniyet performansı yönetimine ilişkin olarak, veriye dayalı karar alma, izlenen ve ölçülen Emniyet Performansı Göstergelerinin sonuçlarına veya diğer raporlarına ve emniyet verilerinin ve emniyet bilgilerinin analizine dayalı olarak etkin, tamamen bilgiye dayalı kararlar alınmasıdır. Bağlamı sunan bilgilerle birleştirilmiş geçerli ve ilgili emniyet verilerinin kullanılması, söz konusu organizasyona emniyet amaçlarıyla ve hedefleriyle uyumlu kararlar alınmasında destek verir. Bağlamsal bilgiler aynı zamanda diğer paydaş önceliklerini, verilerdeki bilinen eksiklikleri ve söz konusu karar ile ilişkili avantajların, dezavantajların, fırsatların, sınırlamaların ve risklerin değerlendirilmesi için tamamlayıcı nitelikteki diğer verileri de içerebilir. Bilgilere kolaylıkla ulaşılabilir ve yorumlanması kolay bir şekilde sahip olunması, karar alma sürecindeki ön yargının, tesirin ve insan hatasının hafifletilmesine yardımcı olur.

4.4.7.3 Veriye dayalı karar alma aynı zamanda, emniyet hedefleriyle yeniden sıraya koyulmasına yönelik olarak geçmişte alınan kararların değerlendirilmesini de destekler. Veriye dayalı karar alma hakkında daha fazla yönlendirme Bölüm 6 kapsamında yer almaktadır.



Şekil 4-6. Emniyet tetikleyicilerinin belirlenmesine ilişkin örnek

4.5 EMNİYET AMAÇLARININ GÜNCELLENMESİ

Emniyet performansı yönetimi "belirle ve unut" amaçlı olamaz. Emniyet performansı yönetimi dinamiktir ve her Devletin ve her hizmet sağlayıcısının işleyişinde merkezi noktadır ve aşağıdaki şekilde gözden geçirilmeli ve güncellenmelidir:

a) üst düzey emniyet kurulu tarafından belirlenen ve kararlaştırılan periyodik devreye uygun olarak rutin bir şekilde;

b) emniyet analizlerinden edinilen girdilere dayalı olarak (detaylar için bakınız Bölüm 6) ve

c) operasyon, en yüksek riskler veya çevredeki büyük çaplı değişikliklere cevaben.

Bölüm 5

EMNİYET VERİLERİNİ TOPLAMA VE İŞLEME SİSTEMLERİ

5.1 GİRİŞ

5.1.1 Emniyet verileri ile emniyet bilgileri arasındaki ayrım Annex 19 kapsamında yer alan tanımlarda yapılmaktadır. Emniyet verileri, herhangi bir gözlemin veya ölçümün sonucu olarak başlangıçta rapor edilen veya kayıt altına alınan verilerdir. Emniyetin yönetilmesi için faydalı hale getirilmesine yönelik belirli bir bağlamda işlendiğinde, düzenlendiğinde, entegre veya analiz edildiğinde emniyet bilgilerine dönüştürülür. Emniyet bilgileri, farklı anlamların çıkarılmasına yönelik farklı yollarla işlenmeye devam edebilir.

5.1.2 Emniyetin etkin yönetimi, emniyet verilerinin toplanmasının, analiz edilmesinin ve genel yönetim kabiliyetlerinin etkinliğine ziyadesiyle bağlıdır. Emniyet verilerine ve emniyet bilgilerine ilişkin sağlam bir temele sahip olunması, veriye dayalı karar almaya esas teşkil etmesi sebebiyle emniyet yönetimi için esastır. Trendleri saptamak, kararlar almak ve emniyet hedeflerine ve emniyet amaçlarına ilişkin emniyet performansını değerlendirmek ve risk değerlendirmesi yapmak için güvenilir emniyet verilerine ve emniyet bilgilerine ihtiyaç duyulur.

5.1.3 Annex 19 kapsamında, hizmet sağlayıcıları tarafından, emniyet verilerinin toplanmasına yönelik reaktif ve proaktif yöntemlerin bir kombinasyonuna dayalı olarak kendi faaliyetlerindeki tehlikelere ilişkin geri bildirimin toplanmasına, kayıt altına alınmasına, bu geri bildirime dayalı olarak hareket edilmesine ve bu geri bildirimin oluşturulmasına yönelik resmi bir sürecin oluşturulması ve muhafaza edilmesi öngörülmektedir.

5.1.4 Benzer şekilde, Annex 13 - *Hava Aracı Kaza ve Olay Soruşturması* Bölüm 8 kapsamında, gerçek veya olası emniyet eksikliklerinin etkin analizinin kolaylaştırılması ve gerekli önleyici tedbirlerin belirlenmesi için Devletler tarafından bir kaza ve olay veri tabanının oluşturulması ve muhafaza edilmesi öngörülmektedir.

5.1.5 Annex 19 kapsamında, emniyet performansı yönetimi faaliyetlerini desteklemek üzere emniyet verilerinin ve emniyet bilgilerinin elde edilmesi, saklanması, birleştirilmesi ve analizine imkan verilmesi için Devletler tarafından emniyet verilerini toplama ve işleme sistemlerinin (SDCPS) oluşturulması öngörülmektedir. Emniyet Verilerini Toplama ve İşleme Sistemleri (SDCPS), emniyet bilgilerinin ve kayıt altına alınan bilgilerin değişimine yönelik işleme ve raporlama sistemlerine, veri tabanlarına ve programlarına işaret etmek üzere kullanılan genel bir terimdir. "Emniyet veri tabanı" terimi, tek veya birden fazla veri tabanına işaret edebilir. Devlet Emniyet Programının (SSP) uygulanmasına yönelik sorumluluklara sahip olan devlet otoriteleri, emniyet sorumluluklarını desteklemek üzere Emniyet Verilerini Toplama ve İşleme Sistemlerine (SDCPS) erişim imkanına sahip olmalıdırlar.

5.1.6 Emniyet Verilerini Toplama ve İşleme Sistemleri (SDCPS) vasıtasıyla emniyet amaçlarını desteklemek üzere, hizmet sağlayıcıları tarafından da Emniyet Performansı Göstergelerine (SPI'ler) ve Emniyet Performansı Hedeflerine (SPT'ler) ilişkin olarak kendi emniyet performanslarının doğrulanmasına yönelik yolların oluşturulması ve muhafaza edilmesi öngörülmektedir. Bu yollar, emniyet verilerinin ve emniyet bilgilerinin toplanmasına yönelik reaktif ve proaktif yöntemlere dayalı olabilir.

5.1.7 Bu bölüm kapsamında sunulan rehberlik, toplanan emniyet verileri ve emniyet bilgileri tarafından etkin ve geçerli karar almanın sağlanmasının güvence altına alınması bakımından Devletler ve hizmet sağlayıcıları için eşit olarak geçerlidir.

5.1.8 Organizasyonlar, emniyet verilerini toplamaya ve saklamaya ehil personele ve emniyet verilerinin işlenmesi için ihtiyaç duyulan yetkinliklere sahip olduklarından emin olmalıdırlar. Bu genellikle, güçlü bilgi teknolojisi becerilerinin yanı sıra veri gerekliliklerine, veri standardizasyonuna, verilerin toplanmasına ve saklanmasına, veri yönetişimine ve analiz için ihtiyaç duyulabilecek olası sorgulara sahip olan kişileri gerektirir. İlaveten, söz konusu organizasyon tarafından her bir Emniyet Verilerini Toplama ve İşleme Sisteminin (SDCPS), Annex 19'un Ek 3'üne uygun olarak emniyet verilerine, emniyet bilgilerine ve ilgili kaynaklara koruma uygulayacak olan belirlenmiş saklayıcıya sahip olması sağlanmalıdır. Daha fazla detay Bölüm 7 kapsamında yer almaktadır.

5.2 EMNİYET VERİLERİNİN VE EMNİYET BİLGİLERİNİN TOPLANMASI

5.2.1 Havacılık sisteminin farklı seviyelerindeki amaçlar

5.2.1.1 Devletler tarafından emniyet verilerinin ve emniyet bilgilerinin toplanmasına yönelik raporlama sistemlerinin tesis edilmesini öngörerek ICAO tarafından 1970'lerden beri Annex'ler, Hava Seyrüsefer Hizmetlerine ilişkin Usuller (PANS) genelinde hükümler ortaya konulmaktadır. Özel olarak kazaların ve ciddi olayların raporlanmasına odaklanan Annex 13 istisna olmak üzere, bu hükümlerin çoğu sektöre özgü emniyet raporlaması sistemlerine ilişkindir. Annex 19 kapsamında yer alan zorunlu ve gönüllü emniyet raporlaması sistemlerine yönelik hükümler Annex 13'den kaynaklanmıştır.

5.2.1.2 Bir çok hizmet sağlayıcısı tarafından, zorunlu ve gönüllü emniyet raporlaması sistemlerinin yanı sıra otomatikleştirilmiş veri yakalama sistemleri de dahil olmak üzere, bol miktar emniyet verileri ve emniyet bilgileri toplanmıştır. Bu emniyet verileri ve emniyet bilgileri, hizmet sağlayıcıları tarafından tehlikelerin saptanmasına imkan vermekte ve hizmet sağlayıcısı seviyesindeki emniyet performansı yönetimi faaliyetlerini desteklemektedir. Özellikle tek bir hizmet sağlayıcısının görüşünün ötesinde olan tehlikelerin saptanması olmak üzere, emniyet bilgilerinin paylaşılmasının bir çok faydası mevcuttur. Emniyet bilgilerinin paylaşılmasına ve değişimine ilişkin bilgilere Bölüm 6 kapsamında ulaşılabilir.

5.2.1.3 Annex 19 kapsamında, havacılık sisteminin genelinde etkili olan tehlikelerin saptanmasını desteklemek üzere, emniyet verilerinin ve emniyet bilgilerinin elde edilmesine, saklanmasına, birleştirilmesine ve analizine imkan verilmesine yönelik olarak Devletler tarafından Emniyet Verilerini Toplama ve İşleme Sistemlerinin (SDCPS) oluşturulması öngörülmektedir. Bu, söz konusu verilerin sadece hizmet sağlayıcılarının emniyet performansının izlenmesi amacıyla görüntülenmesine erişim imkanına sahip olunmasından çok daha fazla anlama sahiptir. Ayrıca, analize imkan vermek üzere emniyet verilerinin elverişliliğinin sağlanması için emniyet verilerinin ve emniyet bilgilerinin toplanmasına yönelik raporlama sistemlerinin ve veri tabanlarının uygulamaya konması yeterli değildir. Devletler tarafından aynı zamanda, Emniyet Verilerini Toplama ve İşleme Sistemini (SDCPS) beslemek için, Annex 19'da belirtilen emniyet verilerinin ve emniyet bilgilerinin raporlanmasını ve hizmet sağlayıcılarından ve diğerlerinden toplanmasını sağlamak üzere kanunlar, düzenlemeler, süreçler ve prosedürler de uygulamaya konmalıdır. Bunun için, emniyet verilerinin ve emniyet bilgilerinin emniyetin muhafaza edilmesi veya iyileştirilmesi amacıyla kullanımını sağlamak için, Annex 19 Ek 3 uyarınca uygulanan korumalara sahip olunması gerekir. İlgili Devlet hesabına emniyet verilerini ve emniyet bilgilerini toplamak, saklamak ve analiz etmek için üçüncü taraflara yönelik düzenlemeler de uygulamaya koyulabilir. Emniyet verilerinin ve emniyet bilgilerinin korunmasına ilişkin bilgilere Bölüm 7 kapsamında ulaşılabilir.

5.2.1.4 Ayrıca, Devlet sınırlarını aşan tehlikelerin saptanmasını kolaylaştırmak ve emniyet risklerinin hafifletilmesine yönelik işbirliğine dayalı çalışmaları teşvik etmek için, emniyet verilerinin ve emniyet bilgilerinin bölgesel havacılık emniyeti grupları (RASG'ler) vasıtasıyla bölgesel seviyede toplanması, saklanması ve analiz edilmesi gerekir.

5.2.2 Nelerin toplanması gerektiğinin belirlenmesi

5.2.2.1 Her bir organizasyon, emniyet performansı yönetimi sürecini desteklemek ve emniyet kararları almak için kendisi tarafından hangi emniyet verilerinin ve emniyet bilgilerinin toplanması gerektiğini belirlemelidir. Emniyet verileri ve emniyet bilgileri gereklilikleri tepeden aşağı ve/veya alttan yukarı yaklaşım kullanılarak belirlenebilir. Seçilen yaklaşım, ulusal ve yerel koşullar ve öncelikler gibi farklı düşüncelerden veya Emniyet Performansı Göstergelerinin (SPI'ler) izlenmesini desteklemek üzere verileri sunma ihtiyacından tesir görebilir.

5.2.2.2 Emniyet verilerinin belirlenmesi ve toplanması, söz konusu organizasyonun emniyeti etkin bir şekilde yönetme ihtiyacı ile uyumlu olmalıdır. Bazı hallerde, söz konusu etkiyi (ihtimal ve önem düzeyini) daha iyi bir şekilde değerlendirmek için ilave emniyet verilerine yönelik ihtiyaç Emniyet Riski Yönetimi (SRM) sürecinde vurgulanacaktır. Eşit ölçüde, belirli bir sorunun daha kapsamlı bir şekilde kavranması veya Emniyet Performansı Göstergelerinin (SPI'ler) oluşturulmasının veya geliştirilmesinin kolaylaştırılması için ilave bilgilere yönelik ihtiyaç, emniyet performansı yönetimi sürecinde vurgulanabilir.

5.2.2.3 Emniyet verileri ve emniyet bilgileri toplanırken ve kullanılırken olası ön yargının göz önünde bulundurulması gerekir. Örneğin, gönüllü raporlarda kullanılan dil bazen duygusal veya herhangi bir kişinin, mutlaka söz konusu organizasyonun tümünün üstün yararına olmayabilecek olan amaçlarına ulaşılmasına yönelik olabilir. Bu durumlarda, söz konusu bilgilerin sağduyulu bir şekilde kullanılması gerekir.

5.2.2.4 Devletler ve hizmet sağlayıcıları tarafından, gerek dahili gerek harici, farklı kaynaklardan gelen emniyet verilerinin toplanmasına yönelik entegre bir yaklaşımın benimsenmesi değerlendirilmelidir. Entegrasyon, organizasyonlar tarafından emniyet risklerine ve söz konusu organizasyon tarafından emniyet amaçlarına ulaşılmasına dair daha tutarlı bir görüşe sahip olunmasına imkan verir. Başlangıçta ilgisiz görünen emniyet verilerinin ve emniyet bilgilerinin daha sonradan emniyet sorunlarının saptanması ve veriye dayalı karar almanın desteklenmesi bakımından kritik öneme sahip hale gelebilecek olması dikkat edilmesi gereken bir husustur.

5.2.2.5 Söz konusu organizasyon bünyesinde emniyetin etkin bir şekilde yönetilmesine neyin özellikle destek verdiği belirlenerek emniyet verilerinin ve emniyet bilgilerinin miktarının düzene koyulması tavsiye edilir. Toplanan emniyet verileri ve emniyet bilgileri, söz konusu sistemin performansına yönelik güvenilir ölçümü ve söz konusu organizasyonun faaliyetleri kapsamındaki bilinen risklerin yanı sıra yükselen risklerin değerlendirilmesini desteklemelidir. Gerekli görülen emniyet verileri ve emniyet bilgileri, organizasyonun faaliyetlerinin boyutundan ve karmaşıklığından tesir görecektir.

5.2.2.6 Çoğu durumda halihazırda mevcut olan tipik emniyet verilerine ve emniyet bilgilerine ilişkin örnekler Şekil 5-1'de sunulmaktadır. Tekrarı önlemek üzere, emniyet verilerinin raporlanmasına ve toplanmasına yönelik çalışmaları düzene koymak için departmanlar veya birimler arasında koordinasyon gereklidir.

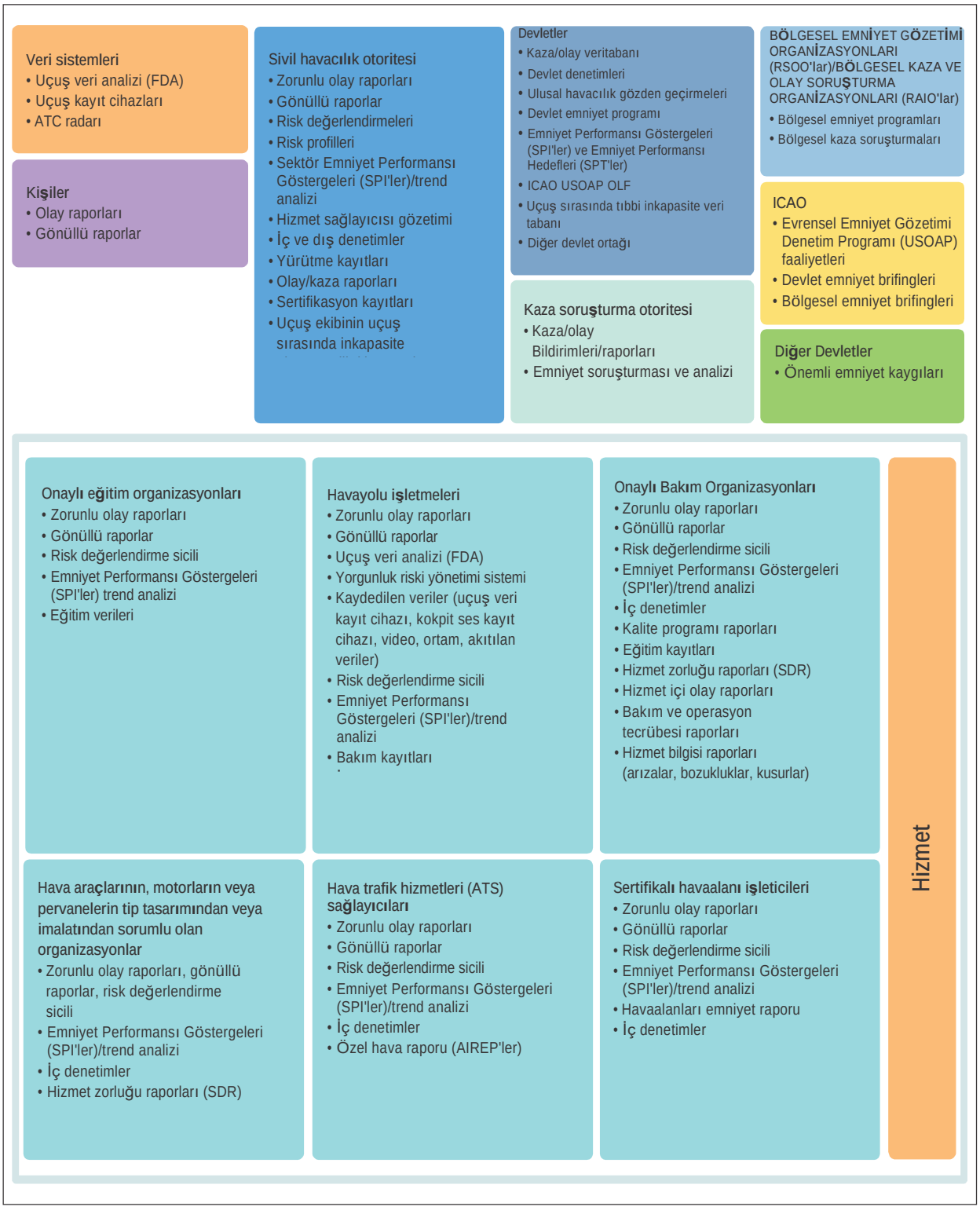
5.2.3 Kaza ve olay soruşturmaları

Annex 13 kapsamında, gerçek veya olası emniyet eksikliklerinin etkin analizinin kolaylaştırılması ve gerekli önleyici tedbirlerin belirlenmesi için Devletler tarafından bir kaza ve olay veri tabanının oluşturulması ve muhafaza edilmesi öngörülmektedir. Devlet Emniyet Programının (SSP) uygulanmasından sorumlu olan devlet otoriteleri, emniyet sorumluluklarını desteklemek üzere Devlet kaza ve olay veri tabanına erişim imkanına sahip olmalıdırlar. Önleyici faaliyetlerin dayandırılacağı ilave bilgiler, soruşturmaya tabi tutulan kazalara ve olaylara ilişkin Nihai Raporlarda yer alabilir.

5.2.4 Devlet otoriteleri veya havacılık hizmet sağlayıcıları tarafından yürütülen emniyet soruşturmaları

5.2.4.1 Annex 13'ün hükümlerine göre, Devletlerin, kendi topraklarında oluşan 2250 kg'un üzerinde azami kütleye sahip olan hava araçlarının kazalarını ve ciddi olaylarını soruşturmaları gerekmektedir. Bu soruşturmalar, söz konusu Devletin kaza soruşturma otoritesi (AIA) tarafından Annex 13'e uygun olarak yürütülür. Bu tür soruşturmaların yürütülmesi, karşılıklı düzenleme ve muvafakat ile başka bir Devlete veya herhangi bir bölgesel kaza ve olay soruşturma organizasyonuna (RAIO) delege edilebilir.

5.2.4.2 Annex 13 tarafından zorunlu kılınanlar dışındaki emniyet soruşturmaları, emniyet performansı yönetimini destekleyen faydalı emniyet bilgileri sunmaları sebebiyle teşvik edilir. Hizmet sağlayıcısı emniyet soruşturmaları hakkında ilave bilgilere Bölüm 9 kapsamında ulaşılabilir.



Şekil 5-1. Tipik emniyet verileri ve emniyet bilgileri kaynakları

5.2.5 Zorunlu emniyet raporlaması sistemleri

5.2.5.1 Annex 19 kapsamında, Devletler tarafından, olayların raporlanmasını içeren ancak bununla sınırlı olmayan, zorunlu emniyet raporlaması sisteminin tesis edilmesi öngörülmektedir. Devletler ve hizmet sağlayıcıları tarafından geliştirilen raporlama sistemlerinin, zorunlu raporlara erişilecek, zorunlu raporlar üretilecek ve sunulacak kadar mümkün olduğunca basit bir şekilde oluşturulması gerekir. Zorunlu emniyet raporlaması sistemlerinin amacı, neyin, nerede, ne zaman gerçekleştiği ve raporun kime hitaben olduğu da dahil olmak üzere, herhangi bir olay hakkındaki tüm değerli bilgileri elde etmek olmalıdır. İlaveten, zorunlu emniyet raporlaması sistemlerinin, kazalara katkıda bulunduğu bilinen, zamanında saptanması ve bildirilmesi değerli addedilen bir takım spesifik tehlikelerin (örneğin, rutin meteorolojik koşullar, volkanik etkinlik, vb.) yakalanmasına imkan vermeleri gerekir.

5.2.5.2 Zorunlu raporlama sisteminin (sistemlerinin) kapsamına bakılmaksızın, zorunlu olarak toplanan tüm raporların 7. Bölümde detayları verilen ilkeler uyarınca korunması tavsiye olunur.

5.2.5.3 Zorunlu olay raporlaması sistemleri, insan performansı yönünden daha fazla teknik bilgi (örneğin, donanım arızaları) toplama eğilimindedir. Daha geniş bir yelpazede emniyet raporlamasına yönelik ihtiyacın ele alınması için Devletler tarafından bir de gönüllü emniyet raporlaması sistemi uygulanmalıdır. Bu sistemin amacı, insan faktörleri ile ilgili yönler gibi daha fazla bilginin elde edilmesi ve havacılık emniyetinin geliştirilmesidir.

Kazaların ve olayların raporlanması

5.2.5.4 Kaza ve olay raporlaması, havacılıktaki her paydaşı ilgilendirir. Operasyon personeli tarafından kazaların ve belirli türden olayların mümkün olan en kısa süre içerisinde ve mevcut olan en hızlı yollarla söz konusu Devletin Kaza Soruşturma Otoritesine (AIA) raporlanması gerekmektedir. Ciddi olayların rapor edilmesi gerekmekte olup, ciddi olay olması muhtemel olan olaylara ilişkin örneklerin listesine Annex 13 Ek C kapsamında ulaşılabilir.

5.2.5.5 Herhangi bir olayın ciddi olay olarak sınıflandırılmasına gerek olup olmadığına karar verilirken aşağıdaki iki ana unsur değerlendirilmelidir:

a) Kazaya dair yüksek bir ihtimalin mevcut olduğuna işaret eden koşullar var mıydı?

b) Söz konusu kaza sadece tedbirliliğe bağlı olarak mı önlenmiştir?

5.2.6 Gönüllü emniyet raporlaması sistemleri

5.2.6.1 Zorunlu emniyet raporlaması sistemi tarafından elde edilmeyen emniyet verilerinin ve emniyet bilgilerinin toplanması için gönüllü emniyet raporlaması sistemleri tesis edilmelidir. Bu raporlar, tipik olay raporlamasının ötesine geçer. Gönüllü raporlar, uygun olmayan emniyet prosedürleri veya düzenlemeleri, insan hatası gibi, saklı koşulları açığa kavuşturma eğilimindedir. Gönüllü raporlama, tehlikelerin saptanmasına yönelik bir yoldur.

5.2.6.2 Gönüllü emniyet raporlaması sistemleri ve ilgili kaynaklar tarafından elde edilen emniyet verileri ve bunlardan elde edilen emniyet bilgileri için Devletler tarafından koruma sağlanmalıdır. Emniyet verilerine, emniyet bilgilerine ve ilgili kaynaklara korumanın nasıl uygulanacağına yönelik rehberlik için devletler ve hizmet sağlayıcıları tarafından 7. Bölümün referans alınması tavsiye olunur. Söz konusu korumanın uygun bir şekilde uygulanması, emniyet verilerinin ve emniyet bilgilerinin sürekli olarak elverişliliğini sağlayacaktır. Devletler tarafından ayrıca, gönüllü raporlamanın teşvik edilmesine yönelik yollar da değerlendirilmelidir.

5.2.7 Sektöre özgü emniyet raporlaması hükümleri

Emniyet raporlaması sistemlerine yönelik hükümler gelişmeye devam etmektedir. Spesifik emniyet kaygılarına ve yükselen havacılık faaliyetlerine işaret etmek üzere yakın geçmişte, yorgunluk ve uzaktan kumanda edilen pilotsuz hava aracı sistemleri (RPAS) gibi sektöre özgü yeni raporlama gereklilikleri ortaya konmuştur. Çeşitli Annex'ler, PANS ve dokümanlar kapsamında yer verilen sektöre özgü raporlama sistemlerine ilişkin bazı örnekler Tablo 7'de sunulmaktadır.

Tablo 7. Çeşitli Annex'ler, PANS ve dokümanlar kapsamındaki sektöre özgü raporlama sistemlerine ilişkin örnekler

Raporlama Sistemi	*Referans*	*Devlet / Hizmet Sağlayıcısı için*	*İlk kabul / onay yılı*
Hava Aracı Kaza ve olay soruşturması raporlaması	Annex 13 — *Hava Aracı Kaza ve Olay Soruşturması*	Devlet	1951
Hava trafik olayı raporlaması	PANS-ATM (Doc 4444), *Hava Seyrüsefer Hizmetlerine ilişkin Usuller - Hava Trafiği Yönetimi*	Devlet ve hizmet sağlayıcısı	1970
Tehlikeli madde kaza ve olay raporlaması	Annex 18 — *Tehlikeli Maddelerin Hava Yoluyla Emniyetli Taşınması*	Devlet	1981
Hizmet zorluğu raporlaması	Annex 8 — *Hava Araçlarının Uçuşa Elverişliliği*	Devlet	1982
Hava trafik olayı raporlaması	Doc 9426, *Hava Trafik Hizmetleri Planlaması El Kitabı*, Kısım 2	Hizmet sağlayıcısı	1984
Yabani hayvan/kuş çarpması raporlaması	Doc 9332, *ICAO Kuş Çarpması Bilgilendirme Sistemi (IBIS)*	Hizmet sağlayıcısı	1989
	Annex 14 — *Havaalanları*, Cilt I — *Havaalanı Tasarımı ve İşletimi*	Devlet ve hizmet sağlayıcısı	1990
	Doc 9137, *Havaalanı Hizmetleri El Kitabı*, Kısım 3 — *Yaban Hayatının Kontrolü ve Azaltılması*	Devlet ve hizmet sağlayıcısı	1991
Lazer yayımı raporlaması	Doc 9815, *Lazer Yayıcı Cihazlara ve Uçuş Emniyetine ilişkin El Kitabı*	Devlet	2003
Yorgunluk raporlaması	Annex 6 — *Hava Araçlarının İşletilmesi*, Kısım I — *Uluslararası Ticari Hava Taşımacılığı — Uçaklar*	Hizmet sağlayıcısı	2011
	Doc 9966, *Yorgunluk Yönetimi Yaklaşımlarının Gözetimine ilişkin El Kitabı*	Hizmet sağlayıcısı	2012
Hizmet zorluğu raporlaması	Doc 9760, *Uçuşa Elverişlilik El Kitabı*	Devlet	2014
Havaalanı emniyeti raporlaması	Doc 9981, *Hava Seyrüsefer Hizmetlerine ilişkin Usuller (PANS) - Havaalanları*	Hizmet sağlayıcısı	2014
Uzaktan kumanda edilen pilotsuz hava aracı sistemleri (RPAS)	Doc 10019, *Uzaktan Kumanda Edilen Pilotsuz Hava Aracı Sistemlerine ilişkin El Kitabı (RPAS)*	Hizmet sağlayıcısı	2015
Uçuş sırasındaki inkapasitasyon olayları ve tıbbi değerlendirme bulguları	Annex 1 — *Personel Lisanslandırma*	Devlet	2016
Tehlikeli madde kaza ve olay raporlaması	Doc 9284, *Tehlikeli Maddelerin Hava Yoluyla Emniyetli Taşınmasına Yönelik Teknik Talimatlar*	Devlet ve hizmet sağlayıcısı	2017

5.2.8 Kendiliğinden açıklamalı raporlama sistemleri

Hizmet sağlayıcısının, havacılık emniyeti eylem programı (ASAP) ve FDA programları (uçuş operasyonları kalite güvence (FOQA) programı, hat operasyonları emniyet denetimi (LOSA) ve normal operasyonlar emniyet araştırması (NOSS)) gibi otomatik veri yakalama da dahil olmak üzere, kendiliğinden açıklamalı raporlama sistemleri vasıtasıyla emniyet verilerinin toplanmasına yönelik sistemleri, sırasıyla, uçuş ekiplerinin veya hava trafik kontrolörlerinin doğrudan gözlemleri vasıtasıyla emniyet verilerini elde eden sistemlere örneklerdir. Bu sistemlerin tümü, sistem ve insan performansının başarılı bir şekilde kayıt altına alınmasına imkan verir. Kendiliğinden açıklamalı raporlama sistemleri tarafından elde edilen emniyet verilerinin ve emniyet bilgilerinin ve kaynaklarının korunması hakkındaki bilgiler için bakınız Bölüm 7.

5.2.9 İncelemelerin, denetimlerin veya araştırmaların sonuçları

İncelemeler, denetimler veya araştırmalar gibi, Devlet temsilcileri ile hizmet sağlayıcıları arasındaki etkileşimlerin sonuçları da emniyet verileri ve emniyet bilgileri havuzu için faydalı bir girdi olabilir. Bu etkileşimlerden elde edilen emniyet verileri ve emniyet bilgileri, gözetim programının kendisinin etkinliğine dair kanıt olarak kullanılabilir.

5.2.10 Emniyet verilerinin ve emniyet bilgilerinin optimal toplanması

Veriye dayalı karar almaya dayanak olarak kullanılan emniyet verilerinin ve emniyet bilgilerinin bir çoğu, söz konusu organizasyondan elde edilebilen rutin, günlük operasyonlardan ileri gelir. Organizasyon tarafından ilkin, emniyet verilerinin ve emniyet bilgilerinin hangi spesifik soruya cevabın amaçlandığı veya hangi problemin ele alınması gerektiği belirlenmelidir. Bu sayede, uygun kaynağın tespit edilmesi ve ihtiyaç duyulan veri veya bilgi miktarının açıklığa kavuşturulması mümkün olacaktır.

5.3 SINIFLANDIRMALAR

5.3.1 Emniyet verileri, ideal olarak, söz konusu verilerin anlamlı terimlerle elde edilebilmesi ve saklanabilmesi için sınıflandırmalar ve destekleyici tanımlar kullanılarak kategorize edilmelidir. Ortak sınıflandırmalar ve tanımlar, bilgi ve iletişim kalitesini arttırarak standart bir dil oluşturur. Havacılık topluluğunun emniyet sorunlarına odaklanma kapasitesi, ortak bir dilin paylaşılmasıyla geniş ölçüde iyileştirilir. Sınıflandırmalar, analize imkan verir ve bilgi paylaşımını ve değişimini kolaylaştırır. Bir takım sınıflandırma örnekleri şunlardır:

a) Hava aracı modeli: Söz konusu organizasyon tarafından işletilmek üzere sertifikalandırılmış tüm modelleri içeren bir veri tabanı oluşturulabilir.

b) Havalimanı: Söz konusu organizasyon tarafından havalimanlarının tanımlanması için ICAO veya Uluslararası Hava Taşımacılığı Birliği (IATA) kodları kullanılabilir.

c) Olay tipi: Organizasyonlar tarafından, olayları sınıflandırmak için ICAO veya diğer uluslararası kuruluşlar tarafından geliştirilen sınıflandırmalar kullanılabilir.

5.3.2 Sektörde yaygın olan bir dizi havacılık sınıflandırması mevcuttur. Bazı örnekler şunlardır:

a) ADREP: ICAO'nun kaza ve olay raporlaması sistemi kapsamında yer alan olay kategorisi sınıflandırması. Bu kategorilere ilişkin emniyet trendi analizine imkan veren ilgili değerlerin ve özelliklerin derlemesidir.

b) Ticari Havacılık Emniyet Ekibi (CAST)/Uluslararası Sivil Havacılık Teşkilatı (ICAO) Ortak Sınıflandırma Ekibi (CICTT): hava aracı kaza ve olay raporlaması sistemlerine yönelik ortak sınıflandırmaların ve tanımların geliştirilmesiyle görevlidir.

c) Emniyet Performansı Göstergeleri Görev Gücü (SPI-TF): bilgilerin toplanmasında ve analiz sonuçlarının karşılaştırılmasında birörnekliğin sağlanması için, Emniyet Yönetimi Sistemleri (SMS) kapsamında hizmet sağlayıcılarının Emniyet Performansı Göstergelerine (SPI'ler) yönelik global olarak uyumlaştırılmış metriklerin geliştirilmesiyle görevlidir.

5.3.3 Tablo 8'de sadece örnek amaçlı olmak üzere, CICTT'den bir sınıflandırma alıntısı sunulmaktadır.

Tablo 8. Tipik sınıflandırma örneği

Operasyon Tipi	*Faaliyet/altyapı/sistem*	*Değer*
Havaalanı, Hava Seyrüsefer Hizmet Sağlayıcısı, Hava Operasyonu, Bakım Organizasyonu, Tasarım ve İmalat Organizasyonu	Düzenleyici Otorite	Mevzuat ve/veya düzenleme eksikliği, yetersiz veya etkisiz mevzuat ve/veya düzenlemeler
		Kaza soruşturma kabiliyetinin olmaması veya etkisiz olması
		Yetersiz gözetim kabiliyeti
	Yönetim	Yönetimin taahhüdünün sınırlı olması veya mevcut olmaması – Yönetim tarafından söz konusu faaliyete yönelik desteğin sergilenmemesi
		Görevlere, mesuliyetlere ve sorumluluklara ilişkin tanımın mevcut olmaması veya eksik olması
		Personel de dahil olmak üzere, kaynak müsaitliğinin veya planlamasının sınırlı veya eksik olması
		Politikaların olmaması veya etkisiz olmaması
		Talimatlar da dahil olmak üzere, yanlış veya eksik prosedürler
		Yönetim ve işçi-işveren ilişkilerinin mevcut olmaması veya yönetimin ve işçi-işveren ilişkilerinin kötü olması
		Organizasyon yapısının olmaması veya etkisiz olması
		Organizasyonel emniyet kültürünün düşük olması
		Denetim prosedürlerinin olmaması veya etkisiz olması
		Kaynak tahsisatının olmaması veya sınırlı olması

5.3.4 Tehlike sınıflandırmaları özellikle önemlidir. Tehlikenin saptanması genellikle, risk yönetimi sürecindeki ilk adımdır. Yaygın olarak kabul gören bir dille başlanması, emniyet verilerini daha anlamlı, sınıflandırılması kolay ve işlenmesi basit yapar. Tehlike sınıflandırmasının yapısı genel ve özel bir bileşen içerebilir.

5.3.5 Genel bileşen, tanımlamaya, analize ve kodlamaya yardımcı olmak amacıyla tehlikenin mahiyetinin kullanıcılar tarafından belirlenmesine imkan verir. CICTT tarafından, tehlikeleri tehlike türü ailelerinde (Çevresel, Teknik, Organizasyonel ve İnsani) sınıflandıran üst seviye bir tehlike sınıflandırması geliştirilmiştir.

5.3.6 Özel bileşen ise tehlike tanımına ve bağlamına kesinlik getirir. Bu da daha detaylı risk yönetimi işlemesine imkan verir. Tehlike tanımlarını formüle ederken aşağıdaki kriterler faydalı olabilir. Herhangi bir tehlike adlandırılırken, söz konusu tehlike;

a) açık bir şekilde belirlenebilir olmalı;

b) arzu edilen (kontrollü) durumda açıklanmalı ve

c) kabul edilen isimler kullanılarak belirlenmelidir.

5.3.7 Veri tabanları arasında ortak sınıflandırmalar daima mevcut olmayabilir. Böyle bir durumda, denkliğe dayalı olarak emniyet verilerinin ve emniyet bilgilerinin standart hale getirilmesine imkan vermek için veri haritalaması kullanılmalıdır. Uçak tipi örneğinden yola çıkılırsa, verilerin haritalanması, herhangi bir veri tabanındaki "Boeing 787-8"in başka bir veri tabanında "788" ile eşdeğer olduğunu gösterebilir. Emniyet verilerinin ve emniyet bilgilerinin elde edilmesi sırasında detay seviyesinin farklılık gösterebilecek olmasına bağlı olarak bu, düz yönlü bir süreç olmayabilir. Bir çok Emniyet Verilerini Toplama ve İşleme Sistemi (SDCPS), veri haritalama külfetini kolaylaştırarak veri yakalamanın standart hale getirilmesine yardım sağlayacak şekilde konfigüre edilecektir.

5.4 EMNİYET VERİLERİNİN İŞLENMESİ

Emniyet verilerinin işlenmesi, şemalar, raporlar veya tablolar gibi faydalı şekillerde anlamlı emniyet bilgilerinin üretilmesi için emniyet verilerinin işleme tabi tutulması anlamına gelir. Emniyet verilerinin işlenmesine ilişkin olarak veri kalitesini, birleştirmeyi, tümleştirmeyi ve filtrelemeyi içeren bir dizi önemli husus mevcuttur.

5.4.1 Veri kalitesi

5.4.1.1 Veri kalitesi, temiz ve amaca uygun olan veriler ile ilgilidir. Veri kalitesi aşağıdaki yönleri kapsar:

a) temizlik;

b) ilgililik;

c) güncellik ve

d) tutarlılık ve doğruluk.

5.4.1.2 Veri temizleme, herhangi bir kayıt setinden, tablodan veya veri tabanından bozuk veya doğru olmayan kayıtların tespit edilme ve düzeltilme (veya çıkarılma) sürecidir ve söz konusu verilerin eksik, yanlış, tutarsız veya ilgisiz kısımlarının belirlenerek kirli veya ham verilerin değiştirilmesi, düzeltilmesi veya silinmesi anlamına gelmektedir.

5.4.1.3 İlgili veriler, söz konusu organizasyonun ihtiyaçlarını karşılayan ve en önemli sorunlarını yansıtan verilerdir. Verilerin ilgili olması, organizasyonlar tarafından kendi ihtiyaçlarına ve faaliyetlerine dayalı olarak değerlendirilmelidir.

5.4.1.4 Emniyet verilerinin ve emniyet bilgilerinin güncelliği, geçerliliğine ilişkin bir işlevdir. Kararlar için kullanılan veriler, neyin gerçekleştiğini mümkün olduğunca gerçek zamana yakın olarak yansıtmalıdır. Durumun değişkenliğine dayalı olarak genellikle muhakeme gereklidir. Örneğin, belirgin değişiklikler olmadan aynı güzergahta halen işletilmekte olan herhangi bir uçak tipine ilişkin olarak iki yıl önce toplanan veriler söz konusu durumun güncel bir yansımasını sunabilir. Oysa, artık hizmette olmayan herhangi bir uçak tipine ilişkin olarak bir hafta önce toplanan veriler şimdiki gerçeğin anlamlı, güncel bir yansımasını vermeyebilir.

5.4.1.5 Veri doğruluğu, doğru olan ve belirli senaryoyu tanımlandığı şekilde yansıtan değerlere işaret eder. Veri yanlışlığı yaygın olarak kullanıcılar tarafından yanlış değer girildiğinde veya yazım hatası yapıldığında ortaya çıkar. Bu sorunun üstesinden, becerikli ve eğitimli veri girişi personeline sahip olunarak veya uygulamada yazım denetimi gibi bileşenlere sahip olunarak gelinebilir. Veri değerleri zamanla yanlış hale gelebilir ve bu durum aynı zamanda "veri bozulması" olarak da bilinir. Doğru olmayan verilerin bir başka sebebi de taşımadır. Verilerin bir veri tabanından çıkarılarak dönüştürülmesine ve başka bir veri tabanına taşınmasına bağlı olarak veriler, özellikle söz konusu yazılımın sağlam olmaması halinde bir derecede değişikliğe uğrayabilir.

5.4.2 Emniyet verilerinin ve emniyet bilgilerinin birleştirilmesi

Veri birleştirmesi, emniyet verilerinin ve emniyet bilgilerinin toplanması ve organizasyonun Emniyet Verilerini Toplama ve İşleme Sisteminde (SDCPS) saklanması ve analiz için özet şekilde ifade edilmesidir. Emniyet verilerini ve emniyet bilgilerini birleştirmek, bu verilerin ve bilgilerin daha büyük bir veri seti ile sonuçlanarak birlikte toplanmasıdır. Emniyet Verilerini Toplama ve İşleme Sistemi (SDCPS) durumunda, münferit emniyet verileri kalemleri, hiçbir emniyet verisine diğeri karşısında öncelik tanınmadan bir veri tabanında birleştirilir. Konum, filo tipi veya meslek grubu gibi spesifik değişkenlere dayalı olarak belirli bir grup veya faaliyet türü hakkında bilgi edinilmesi yaygın bir birleştirme amacıdır. Veri birleştirme bazı hallerde, emniyet verilerinin ve emniyet bilgilerinin kaynaklarını korumak ve analizi desteklemek üzere uygun kimliksizleştirmenin sağlanması için yeterli verilere sahip olmayan birden fazla organizasyon veya bölge genelinde faydalı olabilir.

5.4.3 Veri tümleştirme

Veri tümleştirme, herhangi bir münferit emniyet verileri seti tarafından sağlananlardan daha uyumlu, bağlantılı ve faydalı emniyet verileri üretmek üzere birden fazla emniyet verileri setinin birleştirilmesi sürecidir. Azaltımı veya değiştirilmesi tarafından takip edilen emniyet verileri setinin entegrasyonu, söz konusu verilerin güvenilirliğini ve kullanılabilirliğini geliştirir. Bu sebeple, örneğin, havayolu işletmelerinin FDA sistemlerinden alınan veriler, ileriki işleme için daha faydalı bir veri seti elde etmek üzere meteorolojik veriler ve radar verileri ile birleştirilebilecektir.

5.4.4 Emniyet verilerinin ve emniyet bilgilerinin filtrelenmesi

Emniyet verilerinin filtrelenmesi, emniyet verisi setlerinin geliştirilmesine yönelik geniş bir dizi stratejiye veya çözüme işaret eder. Bu da veri setlerinin, tekrarlayan, ilgisiz veya hatta hassas nitelikte olabilen diğer verileri içermeksizin, karar alıcılar tarafından ihtiyaç duyulanlara basitçe geliştirilmesi anlamına gelir. Raporlar üretmek veya verileri, iletişimi kolaylaştıran yollarla sunmak için farklı türlerden veri filtreleri kullanılabilir.

5.5 EMNİYET VERİLERİNİN VE EMNİYET BİLGİLERİNİN YÖNETİMİ

5.5.1 Emniyet verilerinin ve emniyet bilgilerinin yönetimi, söz konusu organizasyon tarafından kullanılan emniyet verilerinin ve emniyet bilgilerinin genel bütünlüğünü, elverişliliğini, kullanılabilirliğini ve korunmasını sağlayan planların, politikaların, programların ve uygulamaların geliştirilmesi, yürütülmesi ve denetlenmesi olarak tanımlanabilir.

5.5.2 Gerekli işlevleri ele alan emniyet verileri ve emniyet bilgileri yönetimi, söz konusu organizasyonun emniyet verilerinin ve emniyet bilgilerinin amaçlandığı gibi toplanmasını, saklanmasını, analiz edilmesini, muhafaza edilmesini ve arşivlenmesini ve yönetilmesini, korunmasını ve paylaşılmasını sağlar. Özellikle aşağıdakileri tanımlaması gerekir:

a) hangi verilerin toplanacağı;

b) veri tanımları, sınıflandırma ve formatlar;

c) verilerin nasıl toplanacağı, diğer emniyet verileri ve emniyet bilgileri kaynaklarıyla nasıl harmanlanacağı ve entegre edileceği;

d) emniyet verilerinin ve emniyet bilgilerinin nasıl saklanacağı, arşivleneceği ve yedekleneceği; özellikle, veri tabanı yapısı ve herhangi bir BT sistemi halinde destekleyici altyapı;

e) emniyet verilerinin ve emniyet bilgilerinin nasıl kullanılacağı;

f) bilgilerin diğer taraflarla nasıl paylaşılacağı ve değişiminin yapılacağı;

g) emniyet verileri ve emniyet bilgileri türüne ve kaynağına özgü olmak üzere, emniyet verilerinin ve emniyet bilgilerinin nasıl korunacağı ve

h) niteliğin nasıl ölçüleceği ve muhafaza edileceği.

5.5.3 Emniyet bilgilerinin üretilmesine yönelik açık bir şekilde tanımlanmış süreçler olmadan, organizasyonlar tarafından, veriye dayalı kararların güvenle alındığı, savunulabilir, güvenilir ve tutarlı bilgilere ulaşılamaz.

5.5.4 Veri yönetişimi

Veri yönetişimi, organizasyonun veri yönetimi faaliyetlerini destekleyen süreçler ve prosedürler üzerindeki yetki, kontrol ve karar almadır. Emniyet verilerinin ve emniyet bilgilerinin nasıl toplandığını, analiz edildiğini, kullanıldığını, paylaşıldığını ve korunduğunu öngörür. Veri yönetişimi, veri yönetimi sisteminin (sistemlerinin) aşağıda tanımlanan bütünlüğe, elverişliliğe, kullanılabilirliğe ve korumaya ilişkin temel özellikler vasıtasıyla istenilen etkiye sahip olmasını sağlar.

Bütünlük — Veri bütünlüğü, kaynakların, bilgilerin ve içerilen olayların güvenilirliğine işaret eder. Bununla birlikte, veri bütünlüğü, kullanım süresi genelinde verilerin doğruluğunun ve tutarlılığının muhafaza edilmesini ve güvence altına alınmasını kapsar. Bu, verilerin saklanması, işlenmesi veya geri getirilmesi sırasında Emniyet Verilerini Toplama ve İşleme Sisteminin (SDCPS) tasarımı, uygulanması ve kullanımı bakımından kritik bir husustur.

Elverişlilik — Saklanan emniyet verilerini ve emniyet bilgilerini kullanmak veya paylaşmak üzere kimin izne sahip olduğu açık olmalıdır. Burada, veri/bilgi sahibi ile saklayıcı arasındaki anlaşma dikkate alınmalıdır. Verileri kullanmasına izin verilen kuruluşlar için, verilere nasıl erişileceği ve verilerin nasıl işleneceği açık olmalıdır. Saklama konumlarının bolluğu ve veri erişimi yöntemleri ve araçları da dahil olmak üzere, veri elverişliliğinin azami seviye çıkarılmasına yönelik çeşitli teknikler mevcuttur.

Kullanılabilirlik — Emniyet verilerine ve emniyet bilgilerine ilişkin getirilerin azami seviyeye çıkarılmasını teminen, kullanılabilirlik standartlarının da göz önünde bulundurulması önem arz eder. İnsanlar, alınmalarına bağlı olarak emniyet verileri ve emniyet bilgileri ile sürekli olarak etkileşimde bulunmakta ve ilişki kurmaktadırlar. Organizasyonlar tarafından, otomasyon uygulamalarının uygulanmasına bağlı olarak insan hatası en aza indirgenmelidir. Kullanılabilirliğini arttırabilen araçlar veri sözlüklerini ve üst veri havuzlarını içerir. İnsan etkileşiminin büyük veri uygulamalarına ve makine öğrenimi süreçlerine doğru gelişmesiyle, gelecekte emniyet verilerinin ve emniyet bilgilerinin yanlış hesaplanmasının en aza indirgenmesi için makinelere uygulanmasına bağlı olarak insan kullanılabilirliğinin daha iyi kavranması giderek daha önemli hale gelecektir.

Koruma — Devletler tarafından, emniyet verilerine, emniyet bilgilerine ve ilgili kaynaklara uygun koruma sağlandığından emin olunmalıdır. Daha fazla bilgi için bakınız Bölüm 7.

5.5.5 Üst veri yönetimi

5.5.5.1 Üst veri, diğer verileri tanımlayan ve diğer veriler hakkında bilgi veren bir veri seti, başka bir deyişle veri hakkında veri olarak tanımlanır. Üst veri standartlarının kullanılması, söz konusu veriye ilişkin ortak bir anlam veya tanım sunar. Sahipler ve kullanıcılar tarafından uygun kullanım ve yorumlama ile söz konusu verilerin analiz için kolaylıkla geri çekilmesini sağlar.

5.5.5.2 Organizasyonlar tarafından verilerinin, aşağıdakiler de dahil olmak, ancak bunlarla sınırlı kalmamak üzere, kendi özelliklerine dayalı olarak listelenmesi önemlidir:

a) söz konusu verilerin neler olduğu;

b) nereden geldiği (orijinal kaynak);

c) verileri kimin oluşturduğu;

d) verilerin ne zaman oluşturulduğu;

e) verilerin kimin tarafından kullanıldığı;

f) verilerin ne için kullanıldığı;

g) toplama sıklığı ve

h) işleme veya dönüştürme.

5.5.5.3 Üst veri, söz konusu verilerin neler olduğuna dair ortak anlayış sunar ve sahipleri ve kullanıcıları tarafından doğru kullanımı ve yorumlamayı sağlar. Bu aynı zamanda, programın sürekli iyileştirmelerine yol açan, veri toplamadaki hataları belirler.

Bölüm 6

EMNİYET ANALİZİ

6.1 GİRİŞ

6.1.1 Emniyet analizi; faydalı bilgileri ortaya çıkarmak, sonuçları ortaya koymak ve veriye dayalı karar almayı desteklemek amacıyla emniyet verilerini ve emniyet bilgilerini kontrol edecek, inceleyecek, açıklayacak, dönüştürecek, özetleyecek, değerlendirecek ve görselleştirecek istatistiksel veya diğer analitik tekniklerin uygulanması sürecidir. Analiz, eyleme geçirilebilir bilgileri istatistik, grafik, harita, pano ve sunum şeklinde oluşturmaları konusunda organizasyonlara yardımcı olur. Emniyet analizi, özellikle zengin emniyet verilerine sahip olan büyük ve/veya olgun organizasyonlar için değerlidir. Emniyet analizi; istatistiklerin, hesaplamaların ve operasyon araştırmasının aynı anda uygulanmasına dayanır. Emniyet analizinin sonucu, emniyet durumunu, karar alıcıların veriye dayalı emniyet kararları almasına imkan veren şekillerde ortaya koymalıdır.

6.1.2 Devletlerin, emniyet verilerini toplama ve işleme sisteminden (SDCPS) ve ilişkili emniyet veri tabanlarından alınan emniyet verilerini ve emniyet bilgilerini analiz edecek bir süreç tesis ederek idame ettirmeleri gerekmektedir. Emniyet verileri ve emniyet bilgileri analizinin Devlet düzeyindeki amaçlarından biri, aksi takdirde münferit hizmet sağlayıcılarının emniyet verileri analiz süreçleri ile tespit edilemeyebilecek sistemik ve önemli tehlikelerin tespit edilmesidir.

6.1.3 Emniyet analizi, söz konusu Devlet veya hizmet sağlayıcısı tarafından tesis edilmesi gerekebilecek yeni bir fonksiyon olabilir. Etkili emniyet analizinin gerçekleştirilmesi için ihtiyaç duyulan yetkinliklerin, geleneksel bir emniyet denetçisinin yetkinlik alanının dışında kalabileceği kayda alınmalıdır. Devletler ve hizmet sağlayıcıları, emniyet bilgilerinin analiz edilmesi için ihtiyaç duyulan vasıfları göz önünde bulundurmalı ve bu görevin, uygun eğitim sağlanarak, mevcut bir pozisyonun uzantısı mı olması gerektiğine yoksa yeni bir pozisyon tesis edilmesinin, görevin dış kaynak kullanımı yoluyla alınmasının veya bu yaklaşımların bir karışımından yararlanılmasının mı daha verimli olacağına karar vermelidir. Her Devletin veya hizmet sağlayıcısının planları ve koşulları, söz konusu kararı yönlendirecektir.

6.1.4 Mevcut yazılımın yanı sıra işletme ve karar alma politikaları ve süreçlerinin analizi, insan kaynakları ile ilgili olarak göz önünde bulundurulması gereken hususlarla paralel olmalıdır. Etkili olabilmesi için, emniyet analizinin söz konusu organizasyonun mevcut temel araçları, politikaları ve süreçleri ile entegre olması gerekmektedir. Birleştirildikten sonra, emniyet istihbaratının sürekli gelişimi sorunsuz şekilde gerçekleştirilmeli ve organizasyonun olağan işletme uygulamasının bir parçası haline getirilmelidir.

6.1.5 Emniyet verileri ve emniyet bilgileri analizi pek çok yolla gerçekleştirilebilmekte olup, bunlardan bazıları, diğerlerine kıyasla daha güçlü veriler ve analitik kabiliyetler gerektirmektedir. Emniyet verilerinin ve emniyet bilgilerinin analizi için uygun araçların kullanılması, verilerin, içinde yer alan mevcut ilişkileri, bağlantıları, modelleri ve trendleri ortaya çıkaran şekillerde incelenmesi suretiyle, genel durumun daha doğru bir şekilde anlaşılmasını sağlar.

6.1.6 Olgunlaşmış analiz kabiliyetine sahip olan organizasyonlar:

a) etkili emniyet metriklerini tesis edebilir;

b) emniyet bilgilerinin karar alıcılar tarafından kolay bir şekilde yorumlanmasına yönelik emniyet sunum kabiliyetlerini (örneğin: emniyet panosu) tesis edebilir;

c) belirli bir sektörün, organizasyonun, sistemin veya sürecin emniyet performansını izleyebilir;

d) emniyet trendlerini ve emniyet hedeflerini ön plana çıkarabilir;

e) emniyet tetikleyicilerine dayalı olarak, emniyet karar alıcılarını uyarabilir;

f) değişime neden olan faktörleri tespit edebilir;

g) çeşitli faktörler arasındaki veya içindeki bağlantıları veya "korelasyonları" tespit edebilir;

h) varsayımları test edebilir ve

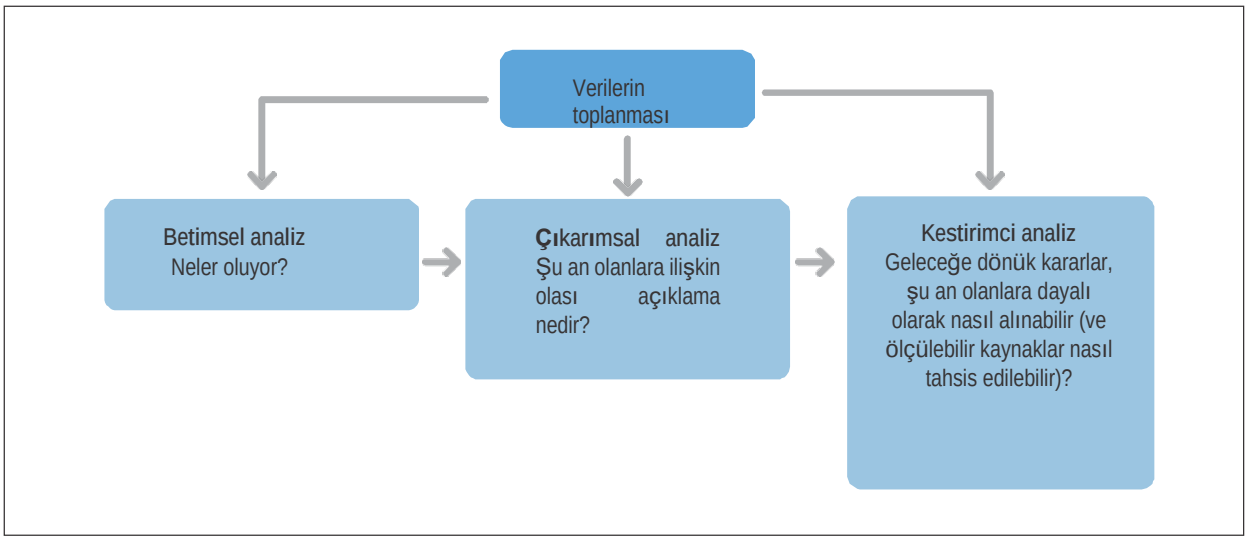
i) kestirimci modelleme kabiliyetleri geliştirebilir.

6.1.7 Organizasyonlar, emniyet analizlerine, yalnızca "emniyet verileri" değil, bir dizi uygun bilgi kaynağını dahil etmelidirler. Veri setine eklenebilecek faydalı konulara ilişkin örnekler: hava, arazi, trafik, toplumsal istatistikler, coğrafi özellikler vb. Daha geniş veri kaynaklara erişim sağlanması ve bunlardan yararlanılması, analistlerin ve emniyet karar alıcılarının, emniyet kararlarının alındığı daha büyük resmi görmelerini sağlayacaktır.

6.1.8 Bilhassa Devletler, havacılık sistemi genelinde etkili olan emniyet trendlerini ve tehlikelerini tespit eden bilgilerle özellikle ilgilenmelidir.

6.2 ANALİZ TÜRLERİ

Emniyet verilerinin ve emniyet bilgilerinin analizi, emniyet verilerinden sonuç çıkarılmasına yardımcı olmak amacıyla, karar alıcıların, bilgileri, diğer gruplar (başka bir ifadeyle; kontrol veya karşılaştırma grubu) ile karşılaştırmasına da imkân sağlar. Ortak yaklaşımlar; Şekil 6-1'de gösterildiği üzere, betimsel (betimleyen) analizi, çıkarımsal (çıkarım yapan) analizi ve kestirimci (öngörüde bulunan) analizi içermektedir.



Şekil 6-1. Bilinen istatistiksel analiz türleri

6.2.1 Betimsel analiz

6.2.1.1 Betimsel istatistikler, verilerin anlamlı ve faydalı olan yollarla betimlenmesi veya özetlenmesi amacıyla kullanılır. Verileri, modellerin verilerden elde edilebileceği ve çalışmaları, fırsatları ve zorlukları net bir şekilde tanımlamaya yardımcı olabilecekleri şekillerde betimlemeye, göstermeye veya özetlemeye yardım ederler. Betimsel teknikler, verilerle ilgili bilgi vermekle birlikte, kullanıcıların, analiz edilen verilerin ötesinde çıkarım yapmalarına veya verilerle ilgili hipotezlerle alakalı çıkarımlara ulaşabilmelerine izin vermez. Bunlar, verilerin betimlenmesi için kullanılan bir yoldur.

6.2.1.2 Betimsel istatistikler faydalıdır; çünkü başta çok büyük miktarda olanlar olmak üzere ham verileri yalnızca ortaya koyuyor olsaydık, verilerin bize ne gösterdiğini görselleştirmemiz zor olurdu. Betimsel istatistikler, kullanıcıların verileri daha mantıklı bir şekilde ortaya koymalarını ve görmelerini sağlar; bu da, verilerin daha basit şekilde yorumlanmasına imkân sağlar. Tablolar, matrisler, grafikler, şemalar ve hatta haritalar gibi araçlar, verilerin özetlenmesi amacıyla kullanılan araçlara ilişkin örneklerdir. Betimsel istatistikler; çeşitlilik, kuvartiller, minimum ve maksimum, frekans dağılımları, varyasyon ve standart sapma (SD) gibi değişkenlik ölçümlerinin yanı sıra ortalama, orta değer ve üst değer gibi merkezi eğilim ölçümlerini içermektedir. Bu özetler ya daha kapsamlı bir istatistiksel analiz kapsamında verilerin betimlenmesine ilişkin ilk dayanak olabilmekte ya da daha özel bir soruşturma için yeterli olabilmektedir.

6.2.2 Çıkarımsal analiz

Çıkarımsal (veya tümevarımsal) istatistikler, veri numunesinin temsil ettiği daha geniş popülasyon hakkında bilgi edinmek için verilerin kullanılmasını amaçlar. Bütün popülasyonun her bir unsurunu incelemek veya bütün popülasyona erişim sağlamak her zaman elverişli ya da mümkün değildir. Çıkarımsal istatistikler, mevcut verilerin kullanıcılarına, trendleri betimlemek için numunelerin alındığı popülasyon ile ilgili genellemelerde, çıkarımlarda ve hükümlerde bulunmasına imkân sağlayan tekniklerdir. Bunlar; farklılıkların veya benzerliklerin tespit edilmesi amacıyla parametrelerin tahmin edilmesine, istatistiksel hipotezlerin test edilmesine, aynı tedbire ilişkin iki grubun ortalama performansının karşılaştırılmasına ve değişkenler arasındaki olası korelasyonların ve ilişkilerin tespit edilmesine yönelik yöntemleri içermektedir.

6.2.3 Kestirimci analiz

Diğer analiz türleri de geçmiş ve güncel verilerden bilgi elde ederek bunları, trendleri ve davranış biçimlerini tahmin etmek amacıyla kullanan olasılık analizi veya kestirimci analizi içermektedir. Verilerde ortaya çıkarılan biçimler, ortaya çıkan risklerin ve fırsatların tespit edilmesine yardımcı olur. İlginin söz konusu olduğu bilinmeyen olaylar genellikle geleceğe dönüktür; ancak kestirimci analiz, geçmişte, mevcut durumda veya gelecekteki bilinmeyen her tür olay için uygulanabilir. Kestirimci analizin özü, geçmiş olaylardan kaynaklanan farklılıklar arasındaki ilişkilerin bulunarak, bilinmeyen sonucu tahmin etmek amacıyla kullanılmasına dayanır. Bazı sistemler, kullanıcıların, farklı sonuçlara sahip olan farklı risk veya fırsat senaryolarını modellemelerine imkân sağlar. Bu, karar alıcıların farklı bilinmeyen durumlar karşısında alabilecekleri kararları değerlendirmelerini ve en yüksek risklerin ya da en iyi fırsatların mevcut olduğu alanlara sınırlı kaynaklarını nasıl etkili bir şekilde tahsis edebileceklerini değerlendirmelerini sağlar.

6.2.4 Birleşik analiz

6.2.4.1 Farklı istatistiksel analiz türleri birbirine bağlıdır ve genellikle birlikte uygulanır. Örneğin; bir veri seti ile ilgili olarak çıkarım yapmak amacıyla kullanılan ana araç çıkarımsal teknik iken, betimsel istatistikler de genellikle kullanılarak ortaya konmaktadır. Çıkarımsal istatistiklerin çıktıları, genellikle, kestirimci analize ilişkin esas olarak kullanılmaktadır.

6.2.4.2 Emniyet analizine, aşağıdaki amaçlarla analitik teknikler uygulanabilir:

a) havacılık emniyetinin sürekli iyileştirilmesine zarar verecek tehlikelere ve unsurlara ilişkin katkı sağlayıcı faktörlerin ve nedenlerin tespit edilmesi;

b) emniyet kontrollerinin etkinliğinin iyileştirilmesine ve arttırılmasına ilişkin alanların incelenmesi;

c) emniyet performansı ve trendlerinin sürekli izlenmesine destek sağlanması.

6.3 ANALİZ SONUÇLARININ RAPORLANMASI

6.3.1 Emniyet veri analizinin sonuçları, yüksek emniyet riskine sahip alanları ön plana çıkararak karar alıcılara ve yöneticilere aşağıdaki hususların yerine getirilmesinde yardımcı olabilir:

a) derhal düzeltici eylemlerin uygulanması;

b) emniyet riskine dayalı gözetimin uygulanması;

c) emniyet politikasının veya emniyet amaçlarının tanımlanması veya rafine edilmesi;

d) emniyet performans göstergelerinin (SPI'ların) tanımlanması veya rafine edilmesi;

e) emniyet performansı hedeflerinin (SPT'lerin) tanımlanması veya rafine edilmesi;

f) emniyet performans göstergesi (SPI) tetikleyicilerinin belirlenmesi;

g) emniyetin teşvik edilmesi ve

h) daha ayrıntılı emniyet risk değerlendirmesinin gerçekleştirilmesi.

6.3.2 Emniyet analizin sonuçları, havacılık emniyeti paydaşlarına, kolayca anlaşılabilecek bir şekilde sunulmalıdır. Sonuçlar; organizasyonun karar alıcıları, harici hizmet sağlayıcıları, Sivil Havacılık Otoriteleri (CAA'lar) ve diğer Devletler gibi kitleler göz önünde bulundurularak sunulmalıdır. Emniyet analizi sonuçları, birkaç şekilde sunulabilecek olup, örneklerden bazıları aşağıda yer almaktadır:

a) Yakın emniyet uyarıları: felaket niteliğinde olabilecek ve acil eylem gerektiren olası sonuçlara neden olabilecek emniyet tehlikelerinin diğer Devletlere veya hizmet sağlayıcılarına bildirilmesi.

b) Emniyet analizi raporları: genellikle analiz bulgularına müdahil olan belirsizlik derecesi ve kaynağı ile ilgili net bir açıklaması olan kantitatif ve kalitatif bilgileri ortaya koyar. Bu raporlar, ilgili emniyet tavsiyelerini de içerebilir.

c) Emniyet konferansları: Devletlerin ve hizmet sağlayıcılarının, işbirliğine dayalı çalışmaları teşvik edebilecek emniyet bilgilerini ve emniyet analizi sonuçlarını paylaşmalarına yöneliktir.

6.3.3 Tavsiyelerin, söz konusu organizasyon bünyesindeki karar alıcılar tarafından göz önünde bulundurulması gereken eylem planlarına, kararlara ve önceliklere dönüştürülmesine ve mümkün olması halinde, analiz sonuçları ile ilgili olarak kimin, neyi, ne zamana kadar yapması gerektiğinin genel hatlarıyla belirtilmesine yardımcı olur.

6.3.4 Şemalar, grafikler, görseller ve panolar gibi görselleştirme araçları, veri analizi sonuçlarının ortaya konmasına yönelik basit ancak etkili yöntemlerdir. Görsel veri analizi raporlarına ilişkin birkaç örnek, ICAO'nun https://icao.int/safety/iSTARSadresi üzerinden ulaşılabilen Entegre Emniyet Trendi Analiz ve Raporlama Sistemi'nde (iSTARS) yer almaktadır.

6.3.5 Emniyet panoları

6.3.5.1 Organizasyonun emniyet performansı kanıtlanabilir olmalı ve tüm ilgili taraflara, emniyetin etkin bir şekilde yönetildiğini açık bir şekilde ifade etmelidir. Bunu kanıtlamaya yönelik yaklaşımlardan biri; üst düzey yöneticilerin, yöneticilerin ve emniyet profesyonellerinin organizasyonun emniyet performansını hızlı ve kolay bir şekilde incelemelerine imkân sağlayan görsel bir sunum olan "emniyet panosu"dur.

6.3.5.2 Panolar, organizasyonun emniyet performansı göstergelerini (SPI'lar) ve emniyet performansı hedeflerini (SPT'ler) gerçek zamanlı göstermelerinin yanı sıra, belirli tehlikelerin kategorisine, nedenine ve önem derecesine ilişkin bilgileri de içerebilir. Tercihe bağlı olarak; pano üzerinde sunulan bilgiler, organizasyonun çeşitli düzeylerde karar almasını desteklemek için gereken bilgileri gösterecek şekilde uyarlanabilir. Tetikleyicilerin kullanımı, belirli bir göstergeye ilişkin olarak ele alınması gereken herhangi bir konunun olup olmadığını ön plana çıkaracak temel görsellerin sağlanması bakımından yararlıdır. Analistler ve karar alıcılar, metrikleri daha derinlemesine araştırmalarına imkân sağlayan bir özelliğin yanı sıra, panoyu, kendilerinin en üst seviyedeki göstergelerini gösterecek şekilde konfigüre edebilmeyi isteyeceklerdir.

6.3.5.3 Etkili yönetim ve karar alma için gereken verilerin toplanması ve analiz edilmesi, süreklilik arz eden bir süreçtir. Veri analizinin sonuçları, organizasyonun hayata geçirmesi gereken eylemleri ve kararları desteklemek için, daha fazla ve daha nitelikli verilerin toplanarak analiz edilmesi gerektiğini ortaya çıkarabilir. Şekil 6-2, analiz sonuçlarının raporlanmasının, veri toplanmasına yönelik ilave gereklilikleri nasıl ortaya koyabildiğini göstermektedir.

6.4 EMNİYET BİLGİLERİNİN PAYLAŞILMASI VE DEĞİŞİMİ

Emniyet bilgileri paylaşıldığında veya değişimi yapıldığında, emniyet daha da geliştirilebilir. Küresel, Devlet ve organizasyon düzeylerindeki emniyet sorunlarına tutarlı, veri odaklı ve şeffaf bir şekilde müdahalede bulunmasını sağlar. Emniyet bilgilerinin paylaşılması, söz konusu bilgilerin verilmesine atıfta bulunurken, emniyet bilgilerinin değişimi, söz konusu bilgilerin verilip alınmasına atıfta bulunmaktadır.

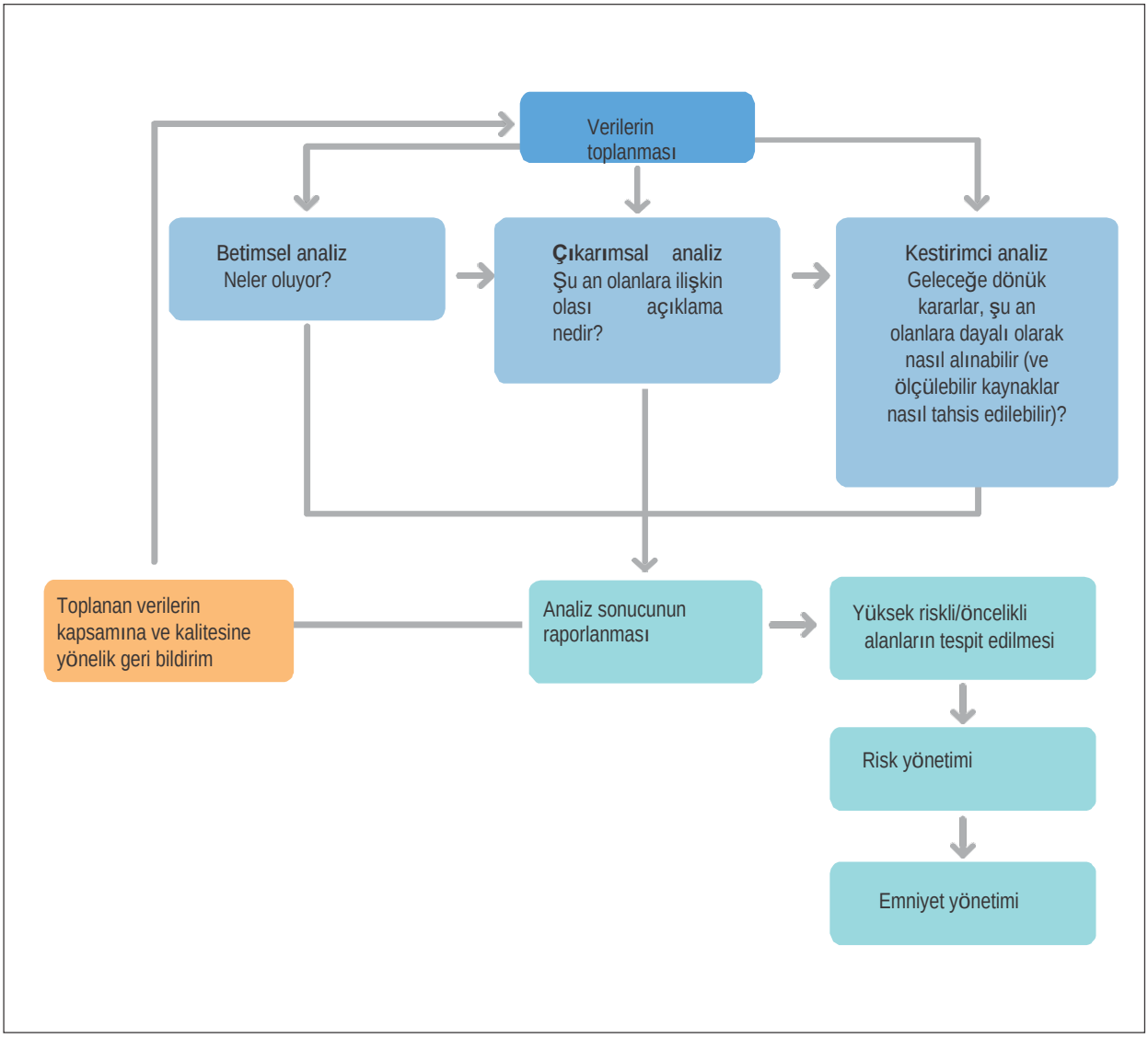
6.4.1 Devlet içi paylaşım

6.4.1.1 Devletler, havacılık sisteminin kullanıcıları arasında emniyet bilgilerinin paylaşılmasına ve değişimine yönelik ağların tesis edilmesini teşvik etmeli ve kendi ulusal hukukları kapsamında aksi belirtilmediği sürece, emniyet bilgilerinin paylaşılmasını ve değişimini kolaylaştırmalıdır. Devletlere ve hizmet sağlayıcılarına yönelik emniyet bilgilerine ilişkin rehberlik, sırasıyla 8. ve 9. Bölüm kapsamında yer almaktadır.

6.4.1.2 Koruma seviyesi ile emniyet bilgilerinin Devlet otoriteleri ve hizmet sağlayıcıları arasında paylaşılacağı ve değişiminin yapılacağı şartlar ulusal kanunlar ile uyum içerisinde olmalıdır. Emniyet verilerinin ve emniyet bilgilerinin koruma seviyesine ilişkin ayrıntılı bilgiler 7. Bölüm kapsamında yer almaktadır.

6.4.2 Devletlerarası paylaşım

Emniyet verilerini toplama ve işleme sistemi (SDCPS) içerisinde yer alan bilgilerin analizi sonucunda, başka bir Devletin ilgisini çekebilecek emniyet sorunlarının tespit edilmesi halinde Devletler, emniyet bilgilerini mümkün olan en kısa süre içerisinde diğer Devletler ile paylaşmalıdırlar. Devletler, emniyet bilgilerini, Bölgesel Havacılık Emniyeti Grubu (RASG) içerisinde paylaşma konusunda da teşvik edilmektedir. Devletler; emniyet bilgilerini paylaşmadan önce, koruma seviyesinin ve emniyet bilgilerinin paylaşılacağı şartların Annex 19'un Ek 3'üne uygun olmasını sağlamalıdırlar. Ayrıntılı rehberlik 7. Bölüm kapsamında yer almaktadır.



Şekil 6-2. Emniyet yönetimi ile D3M entegrasyonu

6.5 VERİYE DAYALI KARAR ALMA

6.5.1 Emniyet analizinin ve emniyet raporlamasının temel amacı, karar alıcılara, ortaya konulan verilere dayalı olarak karar almalarını sağlayan emniyet durumuna ilişkin resmi göstermektir. Bu, aynı zamanda, karar almaya ilişkin süreç odaklı bir yaklaşım olan veriye dayalı karar alma (DDDM veya D3M olarak da anılmaktadır) olarak da bilinmektedir.

6.5.2 Pek çok havacılık olayı, en azından kısmen, kötü yönetim kararlarından kaynaklanmakta olup para, iş gücü ve kaynak israfı ile sonuçlanabilmektedir. Emniyet karar alıcılarının hedefi, kısa vadede kötü sonuçları en aza indirmek, uzun vadede ise organizasyonun emniyet amaçlarının elde edilmesine katkıda bulunmaktır.

6.5.3 İyi kararlar alınması kolay değildir. Kararlar genellikle tüm ilgili faktörler göz önünde bulundurulamadan alınmaktadır. Karar alıcılar, aynı zamanda, bilinçli olsun veya olmasın, alınan kararları etkileyen önyargılarla karşı karşıya kalmaktadır.

6.5.4 D3M'nin amacı, muhakkak "mükemmel" veya "olması gereken" kararın alınmasından ziyade, kısa vadeli amaca (gerçek kararın alındığı konu hakkında) ulaşan iyi bir karar almak ve uzun vadeli amacın (organizasyonun iyileştirilen emniyet performansı) elde edilmesine yönelik işler gerçekleştirmektir. İyi kararlar aşağıdaki kriterleri karşılamaktadır:

a) *Şeffaf*: Havacılık camiası, karar almak için kullanılan süreç de dahil olmak üzere, bir kararı etkileyen faktörlerin tamamını bilmelidir.

b) *Hesap Verebilir*: Karar alıcı, kararı ve ilişkili sonuçları "sahiplenir". Açıklık ve şeffaflık, beraberinde hesap verebilirliği de getirmektedir – Görev ve sorumlulukların ayrıntılı bir şekilde tanımlandığı ve yeni karar ile ilişkili beklentilerin net bir şekilde ana hatlarıyla belirtildiği durumlarda bir kararın arkasına saklanmak kolay değildir.

c) *Adil ve tarafsız*: Karar alıcı, karar ile ilgisi olmayan hususlardan (örneğin: maddi kazanç veya kişisel ilişkiler) etkilenmez.

d) *Gerekçeli ve savunulabilir*: Karara ilişkin girdiler ve izlenen süreç göz önünde bulundurulduğunda, kararın makul olduğu gösterilebilir.

e) *Tekrarlanabilir*: Karar alıcının elinde bulunan bilgilerin aynıları göz önünde bulundurularak ve aynı süreç kullanılarak, başka bir şahıs da aynı sonuca varmış olurdu.

f) *Uygulanabilir*: Karar yeterince açıktır ve bu açıklık, belirsizlikleri en aza indirir.

g) *Pragmatik*: İnsanlar, duyguları olan canlılar olduklarından duyguların mevcut olmadığı bir karar muhtemel değildir. Ancak, kişinin kendi menfaatine yarayan duygusal önyargılar ortadan kaldırılabilir. Zorlu kararlarla karşı karşıya kalındığında sorulması gereken soru şudur: Karar kime hizmet ediyor?

6.5.5 Veriye dayalı karar almanın avantajları

6.5.5.1 D3M; karar alıcıların, emniyet politikası ve amaçları ile uyumlu olan ve değişim yönetimi, emniyet risk değerlendirmeleri vb. ile ilgili çeşitli hususları ele alan, istenen emniyet sonuçlarına odaklanmalarına imkân sağlar. D3M, aşağıdaki hususlara ilişkin kararlar konusunda yardımcı olur:

a) organizasyonu etkileyebilecek hukuki ve düzenleyici gerekliliklerde, yeni teknolojilerde veya kaynaklarda beklenebilecek değişiklikler;

b) havacılık camiasının ve ilgili tarafların ihtiyaçları ve beklentilerine ilişkin olası değişiklikler;

c) belirlenmesi ve yönetilmesi gereken çeşitli öncelikler (örneğin: stratejik, operasyonel, kaynaklar);

d) yeni karar(lar)ın uygulanması için ihtiyaç duyulabilecek yeni kabiliyetler, yetkinlikler ve hatta değişim yönetimi süreçleri;

e) değerlendirilmesi, yönetilmesi veya en aza indirilmesi gereken riskler;

f) ilgili taraflar için halihazırda en büyük değeri oluşturan mevcut hizmetler, ürünler ve süreçler ve

g) yeni hizmetlere, ürünlere ve süreçlere ilişkin gittikçe gelişen talepler.

6.5.5.2 D3M gibi yapılandırılmış bir yaklaşım, karar alıcıları, emniyet verilerinin ifade ettikleri ile uyum sağlayan kararlara yönlendirmektedir. Bu, emniyet performansı yönetim çerçevesi kapsamında güven gerektirmekte olup, emniyet verilerini toplama ve işleme sistemi (SDCPS) içerisinde güven olması halinde, buradan hareketle alınan kararlarda da güven söz konusu olacaktır.

6.5.6 Veriye dayalı karar alma hususunda sıklıkla karşılaşılan zorluklar

6.5.6.1 Veri toplanmasına ve analizine ilişkin süreçlerin uygulanması, zaman ve paranın yanı sıra, organizasyonda mevcut olmayabilecek uzmanlık ve kabiliyetler de gerektirmektedir. Karar alma sürecine tahsis edilmesi gereken uygun zaman ve kaynak miktarı dikkatli bir şekilde göz önünde bulundurulmalıdır. Karar alma süreci kapsamındaki para miktarı, kararın etki alanı ve emniyet istikrarı göz önünde bulundurulması gereken faktörlerdendir. Organizasyonun sürece dahil olan hususları anlamaması halinde, D3M süreci, emniyet karar alıcılarının hayal kırıklığı yaşamalarına ve bu nedenle süreci baltalamalarına veya süreçten çekilmelerine neden olabilmektedir. SSP gibi; SMS, D3M ve emniyet performans yönetimi de D3M'nin sunduğu fırsatları azami düzeye çıkartmak için gereken yapıları ve kabiliyetleri oluşturma ve sürdürme taahhüdü gerektirmektedir.

6.5.6.2 Bir veriye ilişkin güven inşa etmek, bir uzmanın veri girdilerine ve fikrine güvenmekten daha zordur. D3M yaklaşımının benimsenmesi, kararların güvenilir emniyet performans göstergelerine (SPI'lar) ve diğer emniyet verileri analizi sonuçlarına dayalı olduğu kurum kültüründe ve zihniyetinde değişim yaşanmasını gerektirmektedir.

6.5.6.3 Bazı durumlarda, karar alma süreci, "mümkün olan en iyi" çözümü bulmaya çalışırken açmaza girebilmektedir ("analiz felci" olarak da bilinmektedir). Bunun önüne geçmek için kullanılabilecek stratejiler aşağıdakileri içermektedir:

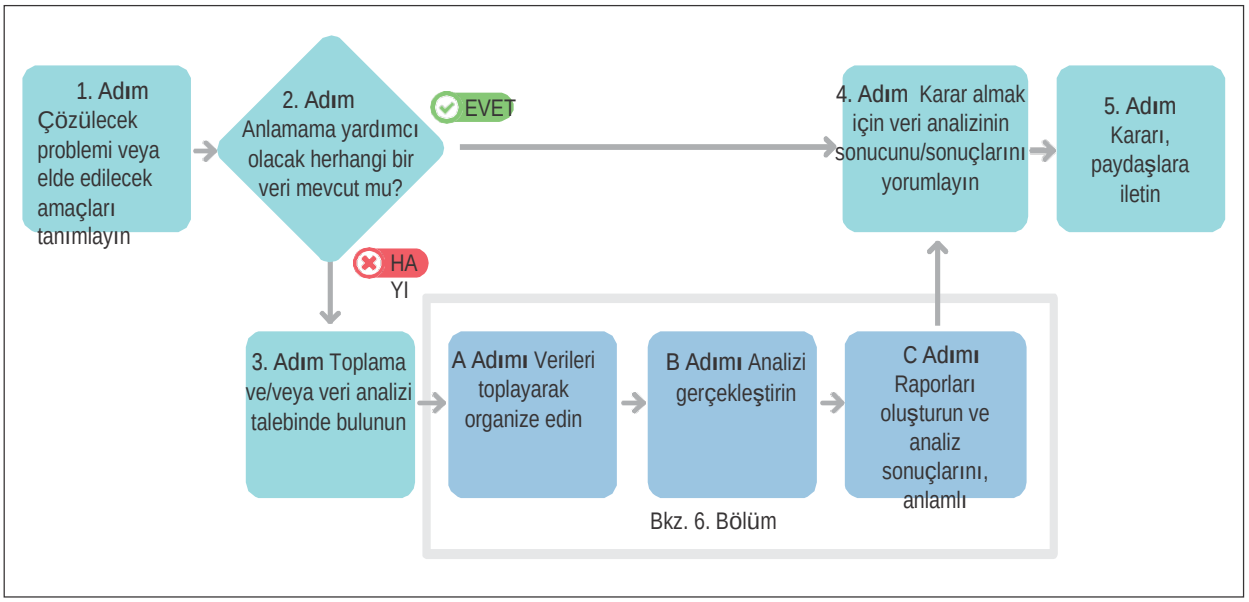
a) son teslim tarihinin belirlenmesi;

b) kapsamın ve amacın iyi bir şekilde tanımlanması ve

c) ilk seferde "mükemmel" bir karar veya çözümün amaçlanmasından ziyade "uygun" ve "uygulanabilir" bir karar alarak, bu kararların gittikçe geliştirilmesi.

6.5.7 Veriye dayalı karar alma süreci

6.5.7.1 D3M süreci, SSP ve SMS'nin değerini ve etkinliğini arttıran çok önemli bir araç olabilmektedir. Etkili emniyet yönetimi, savunulabilir ve bilinçli kararların alınmasına bağlıdır. Bunun karşılığında; etkili D3M, hepsi D3M sürecinin bileşenlerini oluşturan açık bir şekilde tanımlanmış emniyet verileri ve bilgileri gerekliliklerine, standartlara, toplama yöntemlerine, veri yönetimine, analizine ve paylaşımına dayanmaktadır. Şekil 6-3'te D3M süreci gösterilmektedir.



Şekil 6-3. Veriye dayalı karar alma aşamaları

1. Adım — Problemin veya amacın tanımlanması

6.5.7.2 D3M sürecinin planlanması ve tesis edilmesindeki ilk adım, çözülmesi gereken problemin veya elde edilmesi gereken emniyet amacını tanımlanmasıdır. Yanıtlanması gereken soru nedir? Emniyet karar alıcılarının alması gereken karar nedir? Bu, daha stratejik kurum amaçları ile nasıl uyumlu hale getirilecek? Problem tanımının yapılması sürecinde, karar alıcılar kendilerine aşağıdaki soruları sormalıdır:

a) Verilen toplanması ve analizi, organizasyonun emniyet amaçlarını veya emniyet hedeflerini destekliyor mu ve bunlarla ilgili mi?
b) İhtiyaç duyulan veriler mevcut mu? Yoksa makul bir şekilde elde edilebilir mi?
c) Verileri toplamak ve analiz etmek uygulanabilir ve makul mü?
d) İhtiyaç duyulan kaynaklar (insan, ekipman, yazılım, fonlar) mevcut mu?

6.5.7.3 Emniyet yönetim bağlamında; organizasyon bünyesindeki temel problem tanımlamaları, emniyet önceliklerinin, emniyet amaçları paralelinde değerlendirilerek seçilmesi ve emniyet riskinin hafifletilmesine yönelik tedbirlerin tesis edilmesi ile ilgilidir.

2. Adım — Karar almayı destekleyecek verilere erişim

6.5.7.4 Bir sonraki adım, problemin çözülmesi için (bilgilerin korunmasına yönelik hükümler göz önünde bulundurularak) hangi verilere ihtiyaç duyulduğunun tespit edilmesidir. Hiçbir veri, diğer verilerden daha önemli değildir. Mevcut verilerin, probleme yanıt bulunmasına ve çözülmesine yardımcı olup olmayacağına odaklanılmalıdır. İhtiyaç duyulan verilerin mevcut olması halinde, 4. adıma geçin. Uygun verilerin mevcut olmaması halinde, organizasyonun yeni emniyet verilerini ve emniyet bilgilerini anlamlı şekillerde toplaması, saklaması, analiz etmesi ve ortaya koyması gerekecektir.

3. Adım — Karar almayı destekleyecek verilerin talep edilmesi

6.5.7.5 Verilerin halihazırda mevcut olmaması halinde, organizasyonun verileri toplamak için yöntemler bulması gerekmektedir. Bu, başka bir emniyet performans göstergesinin (SPI'nın) ve belki de bununla uyumlu emniyet performans hedeflerinin (SPT'ler) tesis edilmesi anlamına gelebilecektir. İlave göstergelerin tesis edilmesi beraberinde masrafı da getirmektedir. Bu masrafın bilinmesi halinde, organizasyon, elde edilecek faydaların söz konusu masraflardan daha baskın olup olmadığına yönelik bir öngörüde bulunmalıdır. Esas odak noktası, veriye dayalı etkin emniyet kararlarının alınması için ihtiyaç duyulan emniyet verilerinin tespit edilmesi, izlenmesi ve hesaplanması olmalıdır. Masrafların elde edilecek faydalardan daha baskın olması halinde, alternatif veri kaynaklarını ve/veya göstergelerini göz önünde bulundurun.

6.5.7.6 D3M sürecinin planlama aşamasında, organizasyon, emniyet performans hedeflerini (STP'ler) ve emniyet performans göstergelerini (SPI'lar) tesis ederek ve verileri analiz ederek neyi elde etmek istediğini tanımlamalıdır. Organizasyonun neden tespit edilen problemi ele alması gerekiyor? Makul hedef nedir? Emniyet karar alıcıları, veri toplama ve analizinin sonuçlarını nasıl ve nerede kullanacak? Organizasyonun emniyet verilerini ve bilgilerini neden topladığının, analiz ettiğinin, paylaştığının ve değişiminin yapıldığının net bir şekilde anlaşılması, emniyet verileri toplama ve işleme sistemlerini (SDCPS) için elzemdir.

6.5.7.7 Aşağıda belirtilen unsurların tamamı, herhangi bir organizasyonun trendleri belirlemesine, bilinçli kararlar almasına, tanımlanan amaçlara ilişkin emniyet performansını değerlendirmesine, riskleri değerlendirmesine veya gerekliliklerini yerine getirmesine imkân sağlar:

a) emniyet performansı yönetimi - emniyet verileri ve bilgileri yönetişim çerçevesi olarak;

b) SDCPS - emniyet verilerinin toplanmasına ve işlenmesine ilişkin işlevsellik olarak ve

c) Güvenilir bir karar alma süreci olarak D3M.

4. Adım — Veri analizi sonuçlarının yorumlanması ve veriye dayalı kararların alınması

6.5.7.8 Toplanan veriler, karar alıcılara doğru zamanda ve anlamlı şekillerde sunulmalıdır. Veri setlerinin uygunluğu ve boyutu, mantıksal analizlerin karmaşıklığı ve veri analistlerinin kabiliyetleri, ancak verilerin ihtiyaç duyulduğu zamanda ve karar alıcıların bunları kolay bir şekilde anlayabileceği formatlarda sunulması halinde etkili olacaktır. Verilerden elde edilen fikirler, karar alma sürecine bilgi olarak geri dönmeli ve en nihayetinde emniyet performansını geliştirmelidir.

6.5.7.9 Pek çok karar alma modeli mevcuttur. Üzerinde mutabakata varılmış ve standardize edilmiş bir süreçten yararlanılması, organizasyonun veriye dayalı kararlarının tutarlılığını ve etkinliğini en üst düzeye çıkaracak olup, ekseriyetle aşağıdaki aşamaları içerecektir:

a) ihtiyaç duyulan kabiliyetlere ve deneyime sahip olan bir ekibin/grubun oluşturulması (örneğin: emniyet eylem grubu (SAG));

b) emniyet probleminin veya amacının ve bağlamın net bir şekilde tanımlanması;

c) sürekli uyumun sağlanması için organizasyonun emniyet performans hedeflerinin (SPT'ler) ve emniyet amaçlarının gözden geçirilmesi;

d) emniyet verilerinin neleri işaret ettiğini anlamak için söz konusu verilerin gözden geçirilmesi ve yorumlanması;

e) uygun alternatiflerin göz önünde bulundurulması ve analiz edilmesi;

f) uygulanabilir eylemlere (veya eylemsizliklere) ilişkin riskin göz önünde bulundurulması;

g) karar alma grubu arasında fikir birliğinin sağlanması;

h) veriye dayalı karara bağlı kalınması ve karara uygun şekilde hareket edilmesi (verinin eyleme dönüştürülmesi) ve

i) sonuçların izlenerek değerlendirilmesi.

5. Adım — Kararın iletilmesi

6.5.7.10 Emniyet kararının etkili olabilmesi için, aşağıdakileri içeren paydaşlara iletilmesi gerekir:

a) gerekli eylemleri kanunlaştırmak için gereken personel;

b) (gerekli olması halinde) durumu raporlayan şahıs;

c) emniyet iyileştirmelerinden haberdar olmalarını sağlamak için tüm personel (emniyetin teşviki; Devletler 8. bölümü, hizmet sağlayıcılar ise 9. bölümü incelemeli) ve

d) emniyet kararının, organizasyonun bilgilerine derç edilmesini sağlayacak kuruluş bilgi yöneticileri.

6.5.7.11 Emniyet iletişimleri ile ilgili ayrıntılı bilgiler için, Devletler 8.6, hizmet sağlayıcıları ise 9.6 sayılı maddeyi incelemelidir.

Bölüm 7

EMNİYET VERİLERİNİN, EMNİYET BİLGİLERİNİN VE İLGİLİ KAYNAKLARIN KORUNMASI

7.1 AMAÇLAR VE İÇERİK

7.1.1 Bu bölümde, emniyet raporlaması sistemleri tarafından yakalanan veya söz konusu sistemlerden elde edilen emniyet verilerinin ve emniyet bilgilerinin yanı sıra söz konusu verilerin ve bilgilerin kaynaklarının korunmasını düzenleyen temel ilkeler açıklanmaktadır.[1] Aynı zamanda söz konusu prensiplerin Devlet havacılık düzenleme otoriteleri, hizmet sağlayıcıları, kanun koyucular, hukukçular, savcılar, yargı görevlileri ile güvenlik verilerinin, güvenlik bilgilerinin ve bunlara ilişkin kaynakların kullanımı ve korunması ile ilgili kararların alınması konusunda sorumluluğu olan sair yetkili otoriteler tarafından uygulanmasına yönelik kılavuz bilgiler ve tavsiyeler de yer almaktadır. Bu bölüm; emniyet verilerine veya emniyet bilgilerine erişim sağlamak veya söz konusu verileri veya bilgileri paylaşmak isteyen sair kişiler için yararlı olabilir.

7.1.2 Bu bölüm kapsamında aşağıdaki konu başlıkları yer almaktadır:

a) temel prensipler;

b) koruma kapsamı ve seviyesi;

c) koruma prensipleri;

d) istisna prensipleri;

e) kamunun bilgilendirilmesi;

f) kayıtlı verilerin korunması ve

g) emniyet bilgilerinin değişimi ve paylaşılması.

7.2 TEMEL PRENSİPLER

7.2.1 Emniyet verilerinin, emniyet bilgilerinin ve bunlara ilişkin kaynakların korunmasındaki amaç, bireyleri ve organizasyonları emniyet verilerini ve emniyet bilgilerini raporlama konusunda teşvik ederken bunların havacılık güvenliğini sürdürmek veya geliştirmek için kullanılması amacıyla sürekli mevcut olmalarını sağlamaktır. Bu bağlamda; korumaların uygulanmasının önemi yadsınamaz. Korumalar, kaynakları, emniyetle ilgili yükümlülüklerinden kurtarma ya da adaletin uygun şekilde yönetilmesine müdahalede bulunma amacını taşımamaktadır.

7.2.2 Havacılık emniyeti, yalnızca Devletlerin veya hizmet sağlayıcıların sorumluluğu değildir. Aksine, tüm paydaşların, diğerlerinin yanı sıra, emniyet raporları yoluyla ilgili verileri ve bilgileri sağlamak suretiyle katkı sağlaması gereken ortak bir sorumluluktur.

1. Annex 19 uyarınca, emniyet verilerinin ve emniyet bilgilerinin kaynakları hem bireyleri hem de organizasyonları içermektedir.

7.2.3 Veri ve bilgiler çeşitli kaynaklardan gelebilirken, emniyet verilerinin ve emniyet bilgilerinin havacılık sistemi içerisinde bireyler ve organizasyonlar tarafından raporlanması, emniyet yönetimi için elzemdir. Etkin emniyet raporlaması sistemleri, Devletler ve hizmet sağlayıcıları tarafından mevcut ve olası emniyet eksikliklerine ve tehlikelerine işaret edilmesi için gerekli olan ilgili verilere ve bilgilere erişilecek şekilde, kişilerin kendi hatalarını ve deneyimlerini rapor etmeye istekli olmalarının ve isteklerini korumalarının sağlanmasına yardımcı olur. Bu güvence, insanların, istisna prensiplerinden biri geçerli olmadığı sürece, emniyet verilerinin ve emniyet bilgilerinin yalnızca emniyeti sürdürmek ve geliştirmek amacıyla kullanılacağından emin olabildikleri bir ortam oluşturulmak suretiyle sağlanır.

7.2.4 Annex 19 kapsamında, raporda bahsedilen bireylere veya organizasyonlara yönelik korumaya yer verilmemektedir. Ancak, Devletler, korumayı, raporda bahsedilen bireyleri veya organizasyonları kapsayarak şekilde genişletebilirler.

7.2.5 Raporladıkları emniyet verilerinin ve emniyet bilgilerinin yanı sıra hem bireylerin hem de organizasyonların korunması önemlidir. Bireyler ve organizasyonlar, aşağıdaki yollarla korunur:

a) raporlarına dayalı olarak cezalandırılmamalarını sağlayarak ve

b) raporlanan emniyet verilerinin ve emniyet bilgilerinin kullanımını, emniyetin sürdürülmesi veya geliştirilmesi amaçlarıyla sınırlandırarak.

Söz konusu korumalar, aşağıda ele alınan istisna prensiplerinden biri geçerli olmadığı sürece uygulanır.

7.2.6 Annex 19 kapsamında, Devletler tarafından, emniyet verilerinin ve emniyet bilgilerinin, herhangi bir istisna prensibi geçerli olmadığı sürece, **koruma prensiplerinde** ortaya konmakta olanlar haricinde hiçbir amaçla kullanılmamasının sağlanması öngörülmektedir. Söz konusu koruyucu ilkelerden sapmaya izin verilebilecek durumlar, **istisna prensipleri** kapsamında ortaya konmaktadır.

7.2.7 Raporlanan emniyet verilerine ve emniyet bilgilerine dayalı olarak; Devletler ve hizmet sağlayıcıları tarafından, emniyetin sürdürülmesi veya geliştirilmesi yani Devletler ve hizmet sağlayıcılarının aşağıdakilere yönelik uygun adımları atmasını sağlamak amacıyla önleyici, düzeltici veya iyileştirici faaliyetlerde bulunulması gerekebilecektir:

a) risk tespit edilerek hafifletilebilene kadar, herhangi bir emniyet riskinin sonucu olarak meydana gelebilecek ani hasar veya yaralanma potansiyeline karşı koruma sağlamak;

b) ileride böyle bir riskin ortaya çıkabilme ihtimalini en aza indirmek amacıyla uygun önlemin alınmasını sağlamak;

c) herhangi bir hafifletilmeyen emniyet riskine maruz kalınmasını önlemek veya

d) bizzat raporlama sisteminin ve söz konusu sistemin bir parçasını teşkil ettiği daha büyük sistemin bütünlüğünü sağlamak.

7.2.8 Söz konusu faaliyetlerin, herhangi bir emniyet yönetimi sisteminin amaçları ve etkinliği bakımından elzem olması nedeniyle, Annex 19 kapsamında, havacılık emniyetini sürdürecek veya geliştirecek önleyici, düzeltici ve iyileştirici faaliyetlerin engellenmeyeceği açık bir şekilde belirtilmektedir. Söz konusu faaliyetlerin geçerli emniyet yönetimi süreçlerinin bir fonksiyonu gibi değerlendirilebilmesi nedeniyle, Annex 19 kapsamında ortaya konmakta olan istisna prensiplerine tabi değildir.

7.2.9 Önleyici, düzeltici veya iyileştirici faaliyetler, tespit edilen emniyet riskleri etkin bir şekilde ele alınana kadar, birtakım ayrıcalıkların[3] uygulanmasının, hizmetlerin ifasının veya hava aracının işletilmesinin kısıtlanmasını, sınırlandırılmasını veya engellenmesini[2] gerektirebilir mi?

2. Ayrıcalıkların uygulanmasının engellenmesi, lisans ayrıcalıklarının askıya alınmasını veya iptal edilmesini içerebilir.
3. İzin sahibinin ayrıcalıkları, Devlet havacılık düzenleyici otoriteler tarafından düzenlenen lisans veya sertifika kapsamında belirtilmektedir.

Bu amaçlar göz önünde bulundurulduğunda, önleyici veya koruyucu tedbirler, tesis edilmiş protokoller kapsamında cezai veya disipliner olarak addedilmeyecektir. Söz konusu tedbirlerin amacı, hafifletilmemiş bir emniyet riskine maruz kalınmasını engellemek veya en aza indirmektir.

7.2.10 Emniyet verilerinin ve emniyet bilgilerinin yanı sıra bunlara ilişkin kaynakların korunmasına yönelik olarak Annex 19 dahilinde yer alan esaslar, Annex 19 kapsamında öngörüldüğü üzere, emniyet verilerinin ve emniyet bilgilerinin Devletler arasında değişiminin yapılmasının kolaylaştırmak amacıyla, eşit şartların yanı sıra daha keskin bir netlik ve şeffaflık sağlar.

7.3 KORUMA KAPSAMI

7.3.1 Koruma prensipleri kapsamında yer alan emniyet verilerinin ve emniyet bilgilerinin kapsamı

7.3.1.1 Koruma, gönüllü emniyet raporlaması sistemleri ve ilgili kaynaklar tarafından yakalanan emniyet verileri ve söz konusu sistemlerden ve ilgili kaynaklardan elde edilen emniyet bilgileri için geçerlidir. Bu, uygulanabilir olduğu hallerde, zorunlu emniyet raporlaması sistemleri için de geçerli olabilir (bkz. aşağıda yer alan 7.4.3 sayılı madde). Emniyet verilerinin ve emniyet bilgilerinin kaynakları bireyler veya organizasyonlar olabilir.

7.3.1.2 Bazı Devletlerde, emniyet raporlaması sistemleri, verilerin Devlet otoriteleri veya havacılık hizmet sağlayıcıları tarafından emniyet soruşturmalarına raporlanmasını, (otomatik veri yakalama sistemleri ve manuel veri yakalama sistemleri dahil olmak üzere) kendiliğinden açıklamalı raporlama sistemleri tarafından yakalanan veri ve bilgileri veya diğer ilgili emniyet verileri ve bilgilerini içerebilir. Bu nedenle koruma ve istisna prensipleri, bu sistemler tarafından yakalanan emniyet verilerini ve emniyet bilgilerini de içerecek şekilde genişletilebilir.

7.3.1.3 Koruma ve istisna prensiplerinin geçerli olacağı başka durumlar da mevcuttur. Örneğin, Annex 6 — *Hava Araçlarının İşletilmesi*, Kısım I — *Uluslararası Ticari Hava Taşımacılığı – Uçaklar* kapsamında uçuş verileri analiz (FDA) programları kaynaklarının, Annex 19 kapsamında yer alan esaslara uygun olarak korunması gerektiği belirtilmektedir.

7.3.1.4 Emniyet raporlaması sistemleri ve söz konusu sistemlerin bir parçası olabilecek türde sistemler tarafından yakalanabilecek emniyet verileri ve emniyet bilgileri türü, emniyet yönetimi sistemlerinin bizzat gelişimi ile birlikte zamanla değişebilir. Halihazırda Annex 19 kapsamında açık bir şekilde belirtilmeyen emniyet verileri, emniyet bilgileri ve emniyet raporlaması sistemleri, ileride Annex 19 kapsamında idare edilebilir.

7.3.2 Diğer Annex'ler kapsamında yer alan koruma prensipleriyle etkileşim

7.3.2.1 Annex 19 kapsamında korunmakta olan birtakım emniyet verisi ve emniyet bilgisi türleri, bazı durumlarda, sair koruma gerekliliklerine tabi olabilir.

7.3.2.2 Annex 13 kapsamında bir soruşturmanın başlatılması durumunda, Annex 13 kapsamında listelenmekte olan kaza ve olay soruşturma kayıtları, Annex 19 değil Annex 13 kapsamında belirtilen korumalara tabi olacağı Annex 19 kapsamında özellikle belirtilmektedir.

7.3.2.3 Bu ilke, Annex 13 kapsamında belirtilen herhangi bir kazanın veya olayın vuku bulmasından itibaren geçerli olup, Nihai Raporun yayınlanmasından sonra dahi geçerli olmaya devam eder. Kaza ve olay soruşturma kayıtlarının korunmasına ilişkin rehberlik, *Emniyet Bilgilerinin Korunmasına ilişkin El Kitabı* (Doc 10053) kapsamında yer almaktadır.

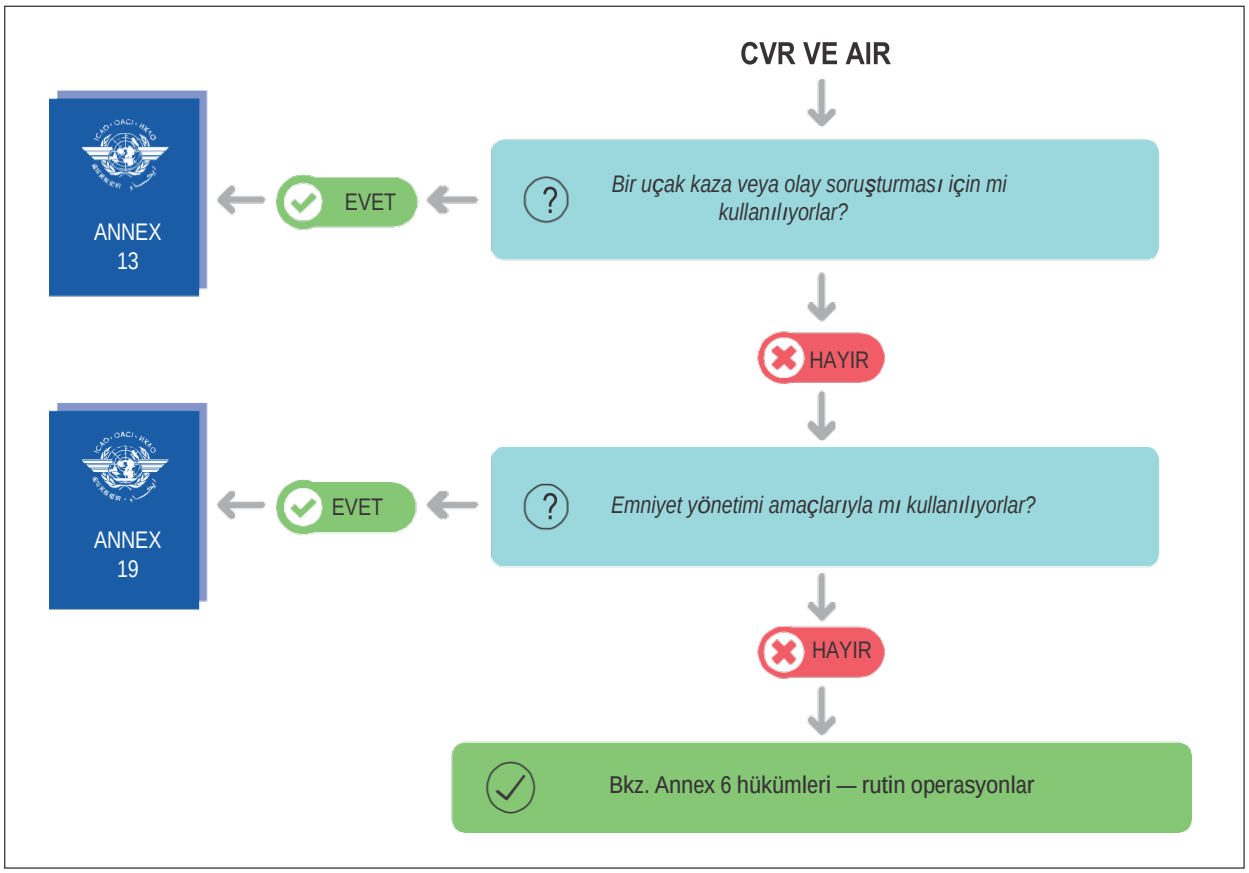
7.3.2.4 Benzer şekilde Annex 19, emniyet yönetimi amaçlarıyla kullanıldıklarında kayıtlı verilere koruma sağlarken Annex 6, Annex 13 türü soruşturmalar haricinde normal operasyonlarda uçuş kayıt cihazı tarafından gerçekleştirilen kayıtlara ilişkin koruma sağlamaktadır.

7.3.2.5 Annex 6 kapsamında kokpit ses kayıt cihazlarının (CVR'ler) ve hava görüntü kayıt cihazlarının (AIR'ler) kullanımını ele almakta olup, söz konusu cihazların kullanımı, uçuş kayıt cihazı sistemlerinin soruşturmasına yönelik uygun tedbirlerin alınması ile birlikte emniyete ilişkin amaçlarla kullanım ya da ilişkili kayıtların veya deşifre metinlerin cezai takibat amacıyla talep edilmesi halinde kullanımla sınırlandırılmalıdır. Söz konusu cezai takibat işlemleri, cezai suçların işlenmesi ve müdahil olan kabin ekibi üyelerinin söz konusu kullanıma muvafakat etmemiş olabileceği (örneğin: uçak kaçırma durumları) durumlarda yetkili otoritelerin bu tür kayıtlara ve deşifre metinlerine hiçbir sınırlama olmaksızın erişim sağlamalarına ve bunları kullanmalarına imkân sağlamak amacıyla, CVR'lere ve AIR'lere uyumlu hale getirilen korumalara ilişkin istisna olarak tadil metnine derç edilir.

7.3.2.6 Benzer şekilde uçuş veri kayıt cihazlarının (FDR'ler) ve uçak veri kayıt sistemlerinin (ADRS) yanı sıra B ve C Sınıfı hava görüntü kayıt cihazlarının ve hava görüntü kayıt sistemlerinin (AIRS) kullanımı, Annex 19'a uygun korumaların alınmasına tabi olarak, FDA programları dahil olmak üzere uçuşa elverişlilik veya bakım amaçlarıyla sınırlı olmalıdır.

7.3.2.7 Şekil 7-1; 6, 13 ve 19 sayılı Annex'ler kapsamındaki koruyucu çerçeveler arasındaki etkileşime yönelik genel kılavuz ilkeleri belirtmekte olup, geçerli hükümlerle istişare halinde kullanılması amaçlanır.

7.3.2.8 FDA programları ile ilgili olarak; kaynaklar, her halükârda, Annex 19 kapsamında yer alan esaslar tarafından korunmaya devam eder.



Şekil 7-1. Koruyucu hükümlerin etkileşimine yönelik kılavuz ilkeler

7.3.3 Annex 19 ilkelerinin hizmet sağlayıcılarına uygulanması

7.3.3.1 Annex 19 kapsamında, "çalışanların ve operasyon personelinin, eğitim ve deneyimleri ile uyumlu eylemlerinin veya ihmallerinin cezalandırılmayacağına güven duyabildiği" bir ortama ilişkin güven aşılayan bir raporlama ortamı tanımlanmaktadır. Herhangi bir eylem veya ihmal, kişinin eğitimi ve deneyimi ile uyumlu olup burada, aynı deneyim ve eğitim düzeyine sahip bir kişinin aynı şeyi yapabileceği veya yapamayabileceğinin beklenmesi makuldür. Böyle bir ortam, etkin ve verimli emniyet raporlaması bakımından esastır.

7.3.3.2 İnsanların ilgili emniyet verilerini veya emniyet bilgilerini raporlamak için teşvik edilmesi, söz konusu raporların kaynaklarının, Annex 19'a uygun olarak, bir Devlet tarafından alınan aksiyonların yanı sıra kendi çalışma ortamları dahilinde alınan aksiyonlardan korunmasını gerektirmektedir.

7.3.3.3 Annex hükümleri, kendi sivil havacılık faaliyetlerinin büyüklüğüne ve karmaşıklığına bakılmaksızın, bütün Devletler tarafından karşılanması gereken asgari gereklilikleri ortaya koymak amacıyla tasarlanmıştır. Devlet ve hizmet sağlayıcıları tarafından makul düzeyde uyumun sağlanması için yeterli olan gerekliliklerin geliştirilmesinden Devletler bizzat sorumludur.

7.3.3.4 Annex 19 kapsamında emniyet verileri, emniyet bilgileri ve bunlara ilişkin kaynaklar için uygulanan koruma ve istisna prensipleri, Devletler ve hizmet sağlayıcıları tarafından benzer şekilde uygulanmalıdır. Bu amacın elde edilmesi için, Devletlerin, Annex 19 kapsamında yer alan hükümlerin kendi hizmet sağlayıcıları tarafından uygulanmasını sağlamak amacıyla ilgili ulusal kanunları, düzenlemeleri ve politikaları hayata geçirmeleri beklenmektedir.

7.4 KORUMA SEVİYESİ

7.4.1 Annex 19 kapsamındaki korumaya elverişli olmak için şartlar

7.4.1.1 Annex 19, Devletlerin, emniyeti verilerinin ve emniyet durumlarının hangi şartlar altında korumaya elverişli olduğunu tespit etmelerini zorunlu kılmaktadır. Devletlerin bunu yaparken aşağıdaki hususları göz önünde bulundurması beklenmektedir:

a) emniyet verilerinin veya emniyet bilgilerinin Annex 19 kapsamında yer alıp almadığı;

b) Annex 6 veya Annex 13'ün Annex 19'dan öncelikli olduğu durumların mevcut olup olmadığı ve

c) herhangi bir istisna prensibinin geçerli olup olmadığı.

7.4.2 Havacılık emniyetinin sürdürülmesi ve geliştirilmesi için gerekli tedbirler

7.4.2.1 Annex 19; Devletlerin ve hizmet sağlayıcılarının, havacılık emniyetini sürdürmek veya geliştirmek için gerekli olan önleyici, düzeltici veya iyileştirici faaliyetleri gerçekleştirmesi için emniyet verilerini veya emniyet bilgilerini kullanmaktan alıkonmamasını sağlar. Bu amaçla uyumlu olarak; söz konusu faaliyet gerçekleştirildiğinde, emniyet verilerinin veya emniyet bilgilerinin kaynağı üzerindeki olası finansal, itibari veya sair olumsuz etkilerden mümkün olduğu her durumda kaçınmalıdır.

7.4.2.2 Önleyici, düzeltici veya iyileştirici faaliyetler, havacılık emniyetine yönelik kabul edilemez riskler teşkil eden durumların veya koşulların ele alınması amacını taşır.

7.4.2.3 *Önleyici faaliyet* emniyete yönelik risk teşkil eden herhangi bir olayın veya tehlikenin vuku bulmasını veya tekrarlanmasını önleyecek faaliyetleri içerir şekilde anlaşılabilir.

7.4.2.4 *Düzeltici faaliyet* geçerli emniyet veya yeterlilik standartlarına uyum gösteremeyen bir izin sahibi gibi, emniyetle ilgili belirli eksikliklerin veya yetersizliklerin ele alınması amacıyla gerçekleştirilen faaliyetleri içerir şekilde anlaşılabilir. Düzeltici faaliyet, bir izin sahibinin uyumlu hale döndürülmesi için gerekli olabilir.

7.4.2.5 *İyileştirici faaliyet* eğitim gibi emniyetle ilgili belirli eksikliklerin veya yetersizliklerin altta yatan nedenlerinin ele alınması amacıyla gerçekleştirilen faaliyetleri içerir şekilde anlaşılabilir. İyileştirici faaliyetler; ilgili ayrıcalıkları tatbik etmek için gerekli nitelikleri bir türlü karşılayamayan bir izin, sertifika veya lisans sahibinin ayrıcalıklarının kısıtlanmasını, sınırlandırılmasını, askıya alınmasını veya iptal edilmesini de içerebilir.

7.4.2.6 Bir veya başka bir amaca hizmet ettikleri belirtilmesine rağmen, söz konusu faaliyetler, birden fazla amaca hizmet edebilir. Örneğin; düzenleyici otorite veya bir hizmet sağlayıcısı tarafından, herhangi bir lisans veya sertifika sahibinin ilave eğitime tabi tutulmasını ve söz konusu eğitim başarılı bir şekilde tamamlanana kadar ilgili lisansın veya sertifikanın ayrıcalıklarını tatbik etmekten alıkonulmasını gerektiren bir tedbir alınabilir. Düzenleyici otorite tarafından, herhangi bir organizasyonun sertifikasının belirli ayrıcalıklarını iptal eden, bertaraf eden veya askıya alan bir tedbir de alınabilir. Emniyet sorununun altında yatan nedeni ele aldıkları için bir yandan iyileştirici özelliğe sahip bu faaliyetler, belirli bir eksikliği ele aldıkları için düzeltici faaliyet olarak da düşünülebilir. Alınan tedbirin niteliğine bakılmaksızın, alınan tedbir ile emniyetin sürdürülmesi veya geliştirilmesi arasında net ve kanıtlanabilir bir bağlantı olmalıdır.

7.4.2.7 Emniyet verileri veya emniyet bilgileri; önleyici faaliyetin, olası veya ortaya çıkan riskleri ele alarak havacılık emniyetini arttıracağı alanları tespit etmek veya emniyeti sürdürmek için iyileştirici veya düzeltici faaliyetlerin gerçekleştirilmesini gerektiren tehlikeleri veya eksiklikleri ortaya çıkarabilir. Önleyici, düzeltici veya iyileştirici faaliyeti haklı çıkaran temel durumu veya tehlikeyi kanıtlamak için Devletlerin emniyet verilerinden veya emniyet bilgilerinden yararlanması gerekebilir. Örneğin; herhangi bir idari lisans tedbirinin temelini oluşturmak veya ispat külfetini yerine getirmek için emniyet verileri ve emniyet bilgileri gerekli olabilir. Ya da lisans sahibinin ilave eğitim ihtiyacını veya işleticinin sistemlerinde yapılacak değişiklikleri ortaya koymak için emniyet verileri ve emniyet bilgileri gerekli olabilir. Raporlama sisteminin ve söz konusu sistemin bir parçasını teşkil ettiği daha büyük sistemin bütünlüğünü ve sorunsuz işleyişini sağlamak amacıyla da emniyet verilerinin veya emniyet bilgilerinin kullanılması gerekli olabilir.

7.4.2.8 Koşullara bakılmaksızın; önleyici, düzeltici veya iyileştirici faaliyetler, bu şekilde planlanmamış olmasına rağmen, söz konusu tedbire tabi tutulan birey veya hizmet sağlayıcısı tarafından cezai olarak algılanabilir. Gerçeği ifade etmek gerekirse, bazıları, yeterlilik eksikliklerini ele almak amacıyla uygulanan lisans tedbirlerini, emniyete yönelik bir riski düzeltmek veya iyileştirmek için gerekli olan bir tedbirden ziyade cezai işlem olarak değerlendirebilmektedir.

7.4.2.9 Tüm bu algılara rağmen, Annex 19 kapsamında, Devletler, havacılık emniyetini sürdürmek veya geliştirmek için gerekli olan faaliyetleri destekleyecek emniyet verilerini ve emniyet bilgilerini kullanmaktan alıkonmamaktadır. Havacılık emniyeti seviyesinin sürdürülmesi veya geliştirilmesi ya da havacılık sistemi emniyetinin kısa veya uzun vadede bozulmasının önlenmesi için tedbirlere ihtiyaç duyulduğu durumlarda, Devletler, kanıtlanabilir ölçüde önleyici, düzeltici veya iyileştirici amaca ve etkiye sahip olmadıkları sürece, söz konusu tedbirleri destekleyecek emniyet verilerinden veya emniyet bilgilerinden yararlanabilirler. Bu tür durumlarda, Devletler, emniyet amacını göstermek ve ileriye dönük raporlama üzerindeki olumsuz etkileri en aza indirmek amacıyla, alınan tedbirin arkasında yatak gerekçeyi net bir şekilde açıklayacak gerekli tedbirleri almayı düşünmelidir. Diğer taraftan; bu amaçlarından bir veya daha fazlasına hizmet ettiği gösterilemeyen, aksine yalnızca cezai veya disipliner amaca ve etkiye sahip olduğu gösterilebilen tedbirlerin alınmasına ilişkin emniyet verilerinin ve bilgilerinin kullanımı, herhangi bir istisna prensibi geçerli olmadığı sürece yasaklanmalıdır.

7.4.3 Zorunlu raporlama sistemlerinin korunması

7.4.3.1 Annex 19 kapsamında, gönüllü ve zorunlu emniyet raporlaması sistemleri tarafından yakalanan emniyet verilerinin, emniyet bilgilerinin ve bunlara ilişkin kaynakların korunmasına yönelik farklı gereklilikler belirtilmektedir. Gönüllü emniyet raporlaması sistemleri tarafından yakalanan emniyet verilerinin ve emniyet bilgilerinin korunması, Devletler arasında sürekli elverişliliğin ve daha büyük çaplı birörnekliğin sağlanması için bir Standart iken zorunlu emniyet raporlaması sistemleri bakımından söz konusu korumasın sağlanması bir Tavsiye Edilen Uygulamadır.

7.4.3.2 Belirli yargı yetki bölgelerinde, zorunlu ve gönüllü emniyet raporlaması sistemleri tarafından yakalanan emniyet verileri ve emniyet bilgileri farklı koruma düzeylerine tabi olduğundan, gönüllü sistemlerden elde edilen emniyet verileri ve emniyet bilgilerine, zorunlu sistemlerden elde edilenlere kıyasla daha geniş çaplı koruma sağlanır. Bu ayrım, emniyet verilerinin veya emniyet bilgilerinin zorunlu raporlama sistemi durumunda gerekli görülmeyen yollarla gönüllülük esasına dayalı olarak sağlanmasını teşvik etme ihtiyacı ile gerekçelendirilebilir.

7.4.3.3 Diğer Devletler, hem zorunlu hem de gönüllü emniyet raporlaması sistemlerinde emniyet verilerine ve emniyet bilgilerine aynı düzeyde yüksek koruma sağlar. Bunun gerekçesi, ilgili emniyet verilerinin ve emniyet bilgilerinin raporlanmasının sağlanması için kanunen raporlamada bulunma gerekliliğinin tek başına yeterli olamayabileceğine ve güvenilir bir ortamın değerinin, her tür raporlama için ne kadar elzem olduğuna dair farkındalık olabilir. Korumaların zorunlu raporlama sistemlerini kapsayacak şekilde genişletilmesi de, raporlamada bulunanları, aksi halde söz konusu korumalar mevcut olmasaydı sağlayamayabilecekleri ilave bilgileri sağlamaları konusunda cesaretlendirebilir.

7.4.3.4 Gönüllü emniyet raporlaması sistemleri ila zorunlu emniyet raporlaması sistemleri tarafından yakalanan emniyet verilerine ve emniyet bilgilerine sağlanan korumanın Devlet tarafından genişletilmesi halinde, söz konusu sistemler tarafından yakalanan emniyet verileri, emniyet bilgileri ve bunlara ilişkin kaynaklar için Annex 19 kapsamında yer alan koruma ve istisna prensipleri uygulanmalıdır.

7.4.4 Kamuya açık alandaki veri ve bilgilerin korunması

7.4.4.1 Emniyet verilerinin veya emniyet bilgilerinin kamuya açık alanda erişilebilir olduğu durumlar olabilir. Söz konusu emniyet verilerinin veya emniyet bilgilerinin hassas olmadığı ve söz konusu verilerin veya bilgilerin gelecekte ifşa edilmesinin, emniyet verilerinin veya emniyet bilgilerinin sürekli elverişliliğini olumsuz yönde etkilemeyeceği bazı durumlar da olabilir. Hava durumuna ilişkin emniyet verileri ve emniyet bilgileri, bu tür hassas olmayan veri ve bilgilere örnek olarak gösterilebilir.

7.4.4.2 Diğer durumlarda, normal şartlarda koruma prensiplerine tabi olan emniyet verileri ve emniyet bilgileri, örneğin medyaya sızdırılmaları suretiyle, kamuya açık bir hale gelebilirler. Bu tür durumlarda Devletler, koruma prensiplerinden otomatik olarak feragat edilmeyeceğinden, sızdırılan verilerin ve bilgilerin ifşa edilmeye devam edilmesinden kaçınmalıdır.

7.5 KORUMA PRENSİPLERİ

7.5.1 Koruma prensiplerinin uygulanması

7.5.1.1 Emniyet verilerinin, emniyet bilgilerinin ve bunlara ilişkin kaynakların korunması, Devletler için olağan bir görev olmalıdır. Bir Devlet, hukuken, kapsamlı ve net prosedürlerle desteklenen etkin bir koruma sağlayabilir.

7.5.1.2 Koruma sağlamanın temel amacı, bireylerin ve organizasyonların eksiklikleri tespit etmeleri, raporlamaları, analiz etmeleri ve düzeltmeleri yönünde teşvik edilmesi suretiyle, emniyet verilerinin ve emniyet bilgilerinin sürekli elverişliliğinin sağlanmasıdır. Bu da, sürece müdahil olan tarafların tamamının, korumaya yönelik amir kuralları ve süreçleri önceden biliyor olmasını gerektirir. Söz konusu kurallar ve süreçler resmileştirilmeli ve güvene dayalı bir sistemin temeli olacaklarsa keyfi uygulamalara açık olmamalıdır.

7.5.1.3 Emniyet verileri veya emniyet bilgileri korunurken, ilgili korumanın ulaşmak istediği amaç göz önünde bulundurulmalıdır. Amaç, korunacak veri ve bilgi türünden net bir şekilde anlaşılabilir. Pek çok durumda korumanın amacı, emniyet verilerinin ve emniyet bilgilerinin, belirli bir veriyi veya bilgiyi raporlayan bireye veya organizasyona karşı kullanılmasını engellemektir. Diğer durumlarda; emniyet verilerinin veya emniyet bilgilerinin, havalimanı operasyonları ve gürültü azaltma konuları ile ilgili ihtilaflar gibi emniyetle ilgili olmayan bağlamlarda genele yayınlanmasının veya kullanılmasının engellenmesi önemli olabilir.

7.5.1.4 Devlet tedbiri, koruyucu hükümlerin oluşturulmasına odaklanır. Hangi kanıtların sunulmasına izin verildiğinin kurallara tabi olduğu resmi işlemlerde, yalnızca Devlet tedbiri, korumaya tabi bilgilerin erişilebilirliğini yasaklayan ya da sert bir şekilde sınırlandıran uygun mevzuatın veya düzenlemelerin yasalaştırılması yoluyla gereken korumayı sağlayabilir. Örneğin; herhangi bir birey aleyhinde başlatılan cezai tahkikat kapsamında, öne sürülen cezai eylem ile doğrudan ilgili olmaması halinde, sanık tarafından yapılan gönüllü raporun kullanılması yasaklanmalıdır.

7.5.1.5 Herhangi bir hizmet sağlayıcısı aleyhinde başlatılan yasal işlemlerde, asgari olarak, korumaya tabi bilgilerin kullanılmayabileceğine yönelik aksi ispat edilebilir bir karineyi[4] zorunlu kılan bir kural mevcut olmalıdır. Herhangi bir olay sonucunda maruz kalınan hasarlara ilişkin olarak herhangi bir havayolu şirketi aleyhinde başlatılan işlem kapsamında, davacı, doğrudan olayla ilgili olmamasına rağmen işleticiyi olumsuz bir durumla karşı karşıya bırakabilecek genel bilgilerin ortaya çıkarılması amacıyla, işleticinin SMS dosyalarına genel erişim sağlamayı talep edebilir. Söz konusu soruların belirlenmesine ilişkin olarak tesis edilen prosedür, istisna prensiplerini (7.6 sayılı maddede daha ayrıntılı olarak ele alınmaktadır) uygulamakla görevlendirilen yetkili otoriteyi (bu durumda yüksek ihtimalle mahkemeyi), davacıyı tam olarak hangi bilgilerin ortaya çıkarılmasını amaçladığı, ilgili bilgilerin tedbirle alakasını göstermesini ve aynı ya da benzer bilgilere ilişkin alternatif kaynakların mevcut olmadığını kanıtlamasını istemeye yönlendirmelidir. Yetkili otorite, davacıdan, ilgili bilgilere erişim sağlayamamaları nedeniyle ne şekilde zarar gördüklerini göstermesini de isteyebilir. Söz konusu erişime izin verilmesine karar verildiği durumlarda, yetkili otorite tarafından, usule ilişkin geçerli gerekliliklere uygun olarak, genele yayın yapılmasını engelleyen ve işlemlerin ilgili kısımlarına erişimi kısıtlayan koruyucu bir karar gibi resmi korumalar tarh edilmelidir.

7.5.1.6 Herhangi bir bireyin veya organizasyonun belirli operasyonel veya teknik niteliklerinin, yetkinliklerinin ve kabiliyetlerinin söz konusu olduğu idari işlemlerde, emniyet hemen hemen her zaman söz konusu olacaktır. Bazı durumlarda emniyet verilerinin veya emniyet bilgilerinin kullanılması gerekli olabilmekle birlikte, icra edilebilir gereklilikler, söz konusu verilerin ve bilgilerin kontrollü ve sınırlı kullanımını sağlamalıdır. Emniyet verilerinin veya emniyet bilgilerinin, bu tür emniyetle ilgili durumlarda alınan karara temel teşkil ettiği hallerde, bahse konu verilerin ve bilgilerin kullanımı sonucunda bilgi kaynağı üzerinde oluşabilecek olumsuz veya zarar verici etkiyi önlemek için azami gayret sarf edilmelidir. Genellikle korumaya tabi raporlama düzeni kapsamında raporlamada bulunmaları teşvik edilen bireyler ve organizasyonlar, tamamen veya kısmen korumaya tabi rapora istinaden emniyet yararına tedbir alınması gereken durumların mevcut olduğunu kabul edeceklerdir. İcra edilebilir gereklilikler, emniyetin sürdürülmesi veya geliştirilmesi amacı güdülürken söz konusu tedbirin temel adalet kavramına uygun olmasını sağlamalıdır.

7.5.1.7 Çalışırken kısa bir süre dalgınlık yaşayan bir hava trafik kontrolörü tarafından yapılan raporlama, bu duruma örnek olarak gösterilebilir. Hiçbir ayrım kaybı yaşanmamıştır ve söz konusu olayın gerçekleştiğine dair tek kanıt söz konusu kontrolörün kendi raporu olmuştur. Emniyet ile ilgili amaçlar için, söz konusu raporun analizi ileri boyutta soruşturma gerektirmiş ve bu da akabinde, raporlama yapan kişinin bir takım süreçlerle kimliğinin tespit edilmesini gerektirmiştir. Acil düzeltici faaliyet, kapsamlı bir tıbbi muayene ve inceleme gerçekleştirilirken ilgili kontrolün (hiçbir mali veya itibari dezavantaja maruz kalmadan) faal görevinden alınmasını içerebilir. Tıbbi inceleme; tıbbi izin, tıbbi tedavi veya (yine hiçbir mali veya itibari dezavantaja maruz kalmadan) tıbbi nedenlere dayalı emeklilikle sonuçlanabilir. İlgili kontrol doğrudan görevden alınsa, benzer raporların ileride başkalarından da gelmesi pek mümkün olmayacaktır.

7.5.1.8 Bu noktaya kadar, gerekli olan ve uygun korumanın sağlanmasına yönelik doğrudan Devlet tedbiri üzerine odaklanılmıştır. Uygulamada ise, korumanın gerekli olduğu emniyet verilerinin ve emniyet bilgilerinin pek çoğu, hizmet sağlayıcının operasyonel ortamı dahilinde olup, işverenler ve çalışanlar arasındaki ilişkileri içerir. Mevzuat veya icra edilebilir Devlet gerekliliklerinin diğer türleri kapsamında, bu tür durumlarda her zaman koruma sağlanmayabilir. Ancak bu tür durumlarda bile Devletler, sertifikasyon, onay ve sürekli gözetim süreçleri ile etkin koruma talep etme pozisyonundadır. Annex 19 kapsamında, belirtilen hizmet sağlayıcıları tarafından etkin bir Emniyet Yönetimi Sisteminin (SMS) uygulanması öngörülmektedir. Etkin emniyet yönetimi; verilerin toplanmasına, analiz edilmesine ve korunmasına dayalıdır. Veri olmaması halinde, sistem etkinliğini kaybeder. Devlet Emniyet Programı (SSP), Devletlerin, organizasyonların, Emniyet Yönetimi Sisteminin (SMS) bir unsuru olan çalışanlarına koruma sağlayan politikaları uygulamaları konusunda yönlendirmesine imkân sağlamalıdır.

4. Aksi ispat edilebilir karine, kanıtlarla çürütülmediği süreci doğru olduğu addedilen bir karinedir.

7.5.1.9 Bu tür korumanın sağlanmasına ilişkin yollardan biri, raporlamada bulunan kişinin kimliksizleştirilmesini içerebilir. Raporların gizliliği faydalı bir strateji iken, mümkün olduğu durumlarda, tam kimliksizleştirme, analiz süreci boyunca takip imkanını ortadan kaldırır. Politikaların odak noktası, yetkili otoritenin söz konusu emniyet verilerini ve emniyet bilgilerini hangi amaçla kullanabildiği ve hangi amaçlara izin verdiği olmalıdır. İdari işlemlerle ilgili olarak yukarıda ele alınan husus (bkz. 7.5.1.6 sayılı madde), işveren/çalışan bağlamında eşit derecede geçerlidir. Ayrıca, söz konusu raporların veya diğer verilerin veya veri yakalama sürecinin, herhangi bir cezai veya disipliner uzaklaştırmayı veya işten çıkarımı desteklemek amacıyla kullanılması halinde, yaptıkları raporlamalara ihtiyaç duyulan kişiler söz konusu raporları temin etmeye gönülsüz olacaktır.

7.5.1.10 Emniyet verilerinin ve emniyet bilgilerinin FDR'ler, ses veya görüntü kayıt cihazları veya hava trafik ortamı kayıt cihazları gibi otomatik araçlarla yakalanması, koruma politikalarının veya düzenlemelerinin bir parçası olmalıdır. Düzenlemeler veya politikalar kapsamında izin verildiği durumlarda; söz konusu cihazların SMS veri yakalama kapsamında kullanılmasında, gönüllü olarak sunulan raporlamalara ne kadar riayet ediliyorsa, koruma prensiplerine de aynı şekilde tam riayet sağlanmalıdır. Raporlama popülasyonunun güveni, etkin emniyet yönetimi için elzemdir.

7.5.2 İşlemler

7.5.2.1 Annex 19 kapsamında, Devletler tarafından, emniyet verilerinin ve emniyet bilgilerinin, herhangi bir istisna prensibi geçerli olmadığı sürece, disipliner, yasal, idari ve cezai işlemler kapsamında çalışanlar, operasyon personeli veya organizasyonlar aleyhinde kullanılmamasının sağlanması öngörülmektedir.

7.5.2.2 "İşlem" terimi, "tedbir" teriminden daha kapsamlı ve geniş bir anlama sahip olabilir. Aynı zamanda, daha dar bir kapsamda, başka bir otorite (veya aynı otorite bünyesindeki herhangi bir kurum) tarafından alınan "tedbirlerin" incelenmesi veya uygulanmasına yönelik olarak belirli bir organın süreçlerine de atıfta bulunabilir. Genel anlamda "işlem" ve "tedbir" terimleri, herhangi bir otoritenin herhangi bir kişinin (geçerli kanunlar kapsamında tanımlanabilecek olan) haklarını, ayrıcalıklarını, meşru çıkarlarını veya makul beklentilerini etkileyen bir kararını devreye almak, uygulamaya koymak veya gözden geçirmek amacıyla atılan tüm adımları veya alınan tüm tedbirleri içerecek şekilde anlaşılabilir. Belirli tedbirlerin veya işlemlerin mahiyeti ve kapsamı, farklı hukuk sistemlerinde farklılık gösterebilir. Örneğin; bazı Devletlerde,

a) *Cezai ve yasal tedbirler veya işlemler* genellikle adli mercileri ilgilendirir. Söz konusu işlemler; tedbirin devreye alınmasını, davalının duruşmaya çıkmasını, atılan tüm tali veya geçici adımları, savunmaları, duruşmaya yönelik esasa ilişkin inceleme süreçleri ve diğer resmi sorgulamaları içerebilir. Bu tedbirlerin veya işlemlerin sonucunda, şahıslar maddi tazminata, para cezasına veya bazı durumlarda ömür boyu hapis cezasına çarptırılabilir.

b) *İdari tedbirler veya işlemler;* (bazı durumlarda açık bir şekilde emniyetle ilgili amaçlarla ve diğer durumlarda cezai amaçlarla) herhangi bir iznin değiştirilmesi, askıya alınması, yürürlükten kaldırılması veya iptal edilmesine yönelik eylemlerle ilgili olarak düzenleyici otorite veya mahkeme nezdinde gerçekleştirilen bir tahkikatı, soruşturmayı veya duruşmayı içerebilir.

c) *Disiplin tedbirleri veya işlemleri*; herhangi bir çalışan tarafından kuralların ve usullerin fiili veya görünür ihlallerine veya suiistimallerine işveren tarafından müdahale edildiği süreci ifade edebilir. Bu tedbirlerin veya işlemlerin sonucunda, çalışan iddia edilen suiistimalden aklanabilir veya iddiaların ispatlanması halinde, çalışan disiplin cezasına çarptırılabilir veya işten çıkarılabilir.

7.5.2.3 Bahse konu tedbirlere ve işlemlere idari mahkemeler ya da bir organizasyon bünyesindeki meslek, etik kuruluşları veya sair gözden geçirme kuruluşları gibi diğer otoriteler de müdahil olabilir.

7.5.2.4 Devletler tarafından, havacılık emniyetinin sürdürülmesi veya iyileştirilmesi için gerekli olan herhangi bir önleyici, düzeltici veya iyileştirici tedbirin alındığı durumlarda, koruma prensiplerinin geçerli olmadığı unutulmamalıdır (bkz. yukarıda yer alan 7.4.2 sayılı madde). Bu durum; emniyetin sürdürülmesi veya iyileştirilmesi amaçlarıyla alınan önleyici, düzeltici veya iyileştirici tedbirlerle ilişkili işlemler, tedbirler veya önlemler için de geçerlidir. Örneğin; önleyici, düzeltici veya iyileştirici bir tedbirin alınmasını gerekçelendirmek için emniyet verilerinin veya emniyet bilgilerinin kullanılmasına, söz konusu tedbire itirazda bulunmak isteyen bir birey veya organizasyon tarafından başlatılan işlemler kapsamında izin verilmektedir.

7.5.2.5 Emniyet verilerinin veya emniyet bilgilerinin, üçüncü bir tarafça rapor kaynağı aleyhinde başlatılan bir davada kullanıldığı durumlar olmasına rağmen, Devletler, emniyet verilerinin veya emniyet bilgilerinin havacılık emniyetinin sürdürülmesi veya iyileştirilmesi amaçları haricinde kullanılmamasını sağlamak üzere tüm gerekli tedbirleri almaları konusunda teşvik edilmektedir.

7.5.3 Zorunlu koruyucu tedbirler

7.5.3.1 Bazı faktörler, emniyet verilerinin veya emniyet bilgilerinin havacılık emniyetinin sürdürülmesi veya iyileştirilmesi amaçları haricinde paylaşılması veya kullanılması ile ilişkili olumsuz sonuçları en aza indirebilir. Emniyet verilerinin ve emniyet bilgilerinin paylaşılmasını veya kullanılmasını sınırlandıracak koruyucu tedbirlerin uygulanması suretiyle, söz konusu paylaşım veya kullanımdan kaynaklanabilecek zararların sınırlandırılması mümkün olabilir. Devletler, emniyet verilerinin veya emniyet bilgilerinin erişim izni kararının ardından gizli tutulmasına yönelik gerekliliklerin uygulamaya konmasına ilişkin olarak yetkili otoriteye bahşedilen yetkiyi, istisna prensiplerinin uygulanmasında göz önünde bulundurulması gereken mevzuatına veya düzenlemelerine derç edebilir.

7.5.3.2 Emniyet verisi ve emniyet bilgisi kaynağının kimliksizleştirilmesi de, havacılık emniyetinin sürdürülmesi veya iyileştirilmesi dışındaki amaçlarla yetkili otorite tarafından yayın izni verilmesinden önce yararlanılabilecek başka bir koruyucu tedbirdir. Bununla birlikte, emniyet verilerini veya emniyet bilgilerini sağlayan kaynakların, raporlanan verilerin veya bilgilerin içeriğinden kolaylıkla anlaşılabileceği durumlarda kimliksizleştirmek zor olabilir. Örneğin; belirli bir yargı yetki bölgesi dahilinde tek bir işletici tarafından kullanılan bir uçak tipinin müdahil olduğu bir olaya ilişkin rapor, yalnızca olaya müdahale olan uçak tipi belirtilerek söz konusu işleticiyi (veya hatta münferit bir çalışanı) işaret edebilir. Bu tür durumlarda, emniyet verilerinin veya emniyet bilgilerinin ne şekilde ve nerede paylaşılmasının veya kullanılmasının tasarlandığı ve ilgili bilgilerin mahiyeti büyük önem arz eder.

7.5.3.3 Emniyet verilerinin veya emniyet bilgilerinin, veri veya bilgi ile bağlantılı kişi veya organizasyonların bilgilerinin sınırlı olduğu bir forumda kullanılmasının tasarlanması halinde, yetkili otorite, kimliksizleştirmenin ilgili kaynaklara yönelik yeterli bir koruyucu tedbir sağlayacağından emin olabilir. Aynı şekilde, bilgi mahiyetinin ağırlıklı olarak teknik olması halinde, emniyet verilerinin veya emniyet bilgilerinin içeriğinde çıkarılması veya düzenlenmesi gereken çok fazla kimlik tanımlayıcı bilgi mevcut olmayabilir. Bu durumda, koruma görevi daha kolay bir şekilde yerine getirilebilir. Tasarlanan paylaşıma ilişkin forumun veya verilerin ya da bilgilerin kullanılmasının ve bilgilerin mahiyetinin, kaynakların kimliklerinin ne ölçüde tespit edilebileceğini etkileyip etkilemeyeceği ve kimlik tespiti yapılabilecek bilgilerin çıkarılmasının yeterli olup olmayacağı yetkili otorite tarafından ayrıca göz önünde bulundurulmalıdır. Tasarlanan paylaşımın veya kullanımın, bir organizasyonu ya da uçak işleticisi gibi bir şirketi olumsuz yönde etkileyebilecek olması halinde, verilerin veya bilgilerin kimliksizleştirilmesinin, söz konusu paylaşıma veya kullanıma izin verilmemiş olması halinde şirket veya işletici tarafından elde edilmiş olana benzer makul bir koruma sağlayıp sağlamayacağına yetkili otorite karar verecektir.

7.5.3.4 Yetkili otorite tarafından, emniyet verilerinin ve emniyet bilgilerinin kimliksizleştirilmesinin, söz konusu verilerin veya bilgilerinin amaçlanan veya sair şekilde izin verilebilir kullanımını engellemeyebileceğinin düşünülmesi halinde, kimliksizleştirme uygun olmayacaktır. Bu nedenle; Devletler, emniyet verilerinin veya emniyet bilgilerinin daha geniş kapsamlı kullanımını veya kamuya paylaşılmasını engellerken söz konusu paylaşımın özel bir amaçla sınırlandırılmış şekilde izin verilmesine yönelik farklı türde koruyucu tedbirler (veya koruyucu tedbirlerin kombinasyonları) uygulamayı tercih edebilirler. Koruyucu kararlar, basına kapalı işlemler, gizli inceleme ve özetler bu koruyucu tedbirlere örnektir.

7.5.3.5 Devletler ve organizasyonlar; bilgilerin toplandığı, saklandığı, işlendiği ve iletildiği ortamın yeterince güvenli olmasının ve erişim ile yetkiye yönelik kontrollerin, emniyet verilerini ve emniyet bilgilerini korumak için yeterli olmasının sağlanması gibi en iyi uygulamaları da hayata geçirebilirler.

7.6 İSTİSNA PRENSİPLERİ

Yetkili otorite tarafından üç istisna prensibinden herhangi birinin geçerli olduğu tespit edilmediği sürece, koruma prensipleri emniyet verileri, emniyet bilgileri ve bunlara ilişkin kaynaklar için geçerlidir. Emniyet Verilerini Toplama ve İşleme Sisteminin (SDCPS) sorumlusu; emniyet verilerine, emniyet bilgilerine ve bunlara ilişkin kaynaklara uygulanan korumalardan haberdar olmalı ve söz konusu korumaların, Annex 19 hükümlerine uygun olarak serbest bırakılmasını ve kullanılmasını sağlamalıdır.

7.6.2 Yetkili otoritenin tayin edilmesi

7.6.2.1 İstisna prensipleri bir dizi farklı amaç doğrultusunda uygulanacağı için, söz konusu verinin veya bilginin mahiyetine ve aranan kullanım türüne dayalı olarak yetkili otorite de farklı olacaktır. Her durumda, yetkili otoritenin görevi, belirli bir istisna prensibinin geçerli olup olmadığına karar vermek olacaktır. Yetkili otoritenin, karar alma yetkinliklerine kamunun güven duymasını sağlamak için, havacılık emniyeti ile ilgisi olmayan bilgi edinme hakkı kanunları düzenlemeleri, dava ifşa kuralları ve sair kurallar gibi çakışan çıkarları dengeleyebiliyor olması gerekecektir. Yetkili otoriteler, ulusal kanunlara ve diğer icra edilebilir gerekliliklere uygun olarak tayin edilmiş ve havacılık sorumlulukları ile görevlendirilmiş olan adli mercileri, düzenleyici otoriteleri veya diğerlerini sürece dahil edebilir.

7.6.2.2 Devletler ve organizasyonlar tarafından, istisna prensiplerinin farklı amaçlarla uygulanması görevine uygun olan yetkili otoritelerin belirlenmesi gerekecektir. Aşağıda yer alan Tablo 9 kapsamında, olası yetkili otorite ve durum örneklerine yer verilmektedir.

Tablo 9. Örnek durumlar ve olası yetkili otoriteler

Örnek Durum	*Olası Yetkili Otorite*
Bir vatandaş tarafından, bilgi edinme hakkı kanunları uyarınca, emniyet verilerinin veya emniyet bilgilerinin paylaşılmasının veya kullanılmasının talep edildiği durumlarda[5].	Devlet dairesi veya idari organ
Verilerin veya bilgilerin paylaşılması veya kullanılması hususunun, aynı bilgi edinme hakkı kanunları kapsamında başlatılan bir davanın bizzat konusu haline gelmiş olması ya da emniyet verilerinin veya emniyet bilgilerinin, adli işlemlerde kullanılmasının talep edilmesi halinde.	Mahkeme veya idari mahkeme
Emniyetin sürdürülmesi veya iyileştirilmesi amacıyla düzenleyici otorite tarafından tedbir alınacağı durumlarda.	Sivil Havacılık Otoritesi (CAA)
Emniyet verilerinin veya emniyet bilgilerinin, herhangi bir organizasyon nezaretinde paylaşılması veya kullanılması halinde.	Bir yönetici ya da yönetim, bir çalışan temsilcisi ve bazı Devletlerde bir düzenleyici otorite temsilcisinden oluşan bir kurul gibi, organizasyon bünyesinde havacılık emniyetinden sorumlu olan kişi

5. Bilgi edinme hakkı kanunlarına ilişkin ayrıntılı bilgiler için, bkz. Bu Bölüm kapsamında yer alan 7.7 sayılı madde.

7.6.2.3 Organizasyonun kendi yetkili otoritesini tespit ettiği durumlarda, yetkili otorite tarafından istisna ve koruma prensiplerinin uygulanmasına ilişkin olarak takdir hakkı ve yetkisinin bilinçli bir şekilde tatbik edilmesi, organizasyon bünyesinde yeterli düzeyde kendiliğinden koruma sağlayabilir. Yetkili otoritenin her amaca ilişkin nihai tespiti, geçerli kanunlara ve politikalara bağlı olarak, her Devlet ve organizasyon için önemli bir hususu teşkil eder.

7.6.2.4 Kararların hızlı bir şekilde alınmasına imkân sağlamak üzere, yetkili otorite dairesinin ve yargı yetki bölgesinin kalıcı olarak belirlenmesi göz önünde bulundurulabilir (örneğin: davayı içeren hususlar için adli merciler, düzenleyici tedbirleri içeren hususlar için Sivil Havacılık Otoritesi (CAA)). Söz konusu hususların kalıcı olarak belirlenmesi, aynı zamanda, yetkili otoritenin bu hususlar karşısındaki duruşunda netlik ve bu hususlarla mücadele etmesinde deneyim sağlar. Ayrıca, yetkili otoritenin karar alma sürecini idare eden kurallara ve prosedürlere sahip olması da çok önemlidir. Söz konusu kurallar ve prosedürler, geçerli ulusal kanunlara dayalı olmalıdır. Bu; ancak, belirli bir alanda tayin edilen yetkili otoritenin değişmemesi halinde gerçekleştirilebilir.

7.6.3 İstisna prensiplerinin uygulanması

7.6.3.1 İlki; yetkili otorite tarafından, "olayın ulusal kanunlar uyarınca ağır ihmal, kasti suiistimal veya suç faaliyeti teşkil eden bir davranış olarak addedilen herhangi bir fiilden/eylemden veya ihmalden kaynaklanmış olabileceğini makul ölçüde belirten gerçeklerin ve hallerin" söz konusu olduğu durumlarda korumaya yönelik istisnanın geçerli olduğunun tespit edildiği durumdur. Böylesi bir tespiti üstlenen ilgili yetkili otorite, pek çok durumda, adli, idari veya savcılık mercii olacaktır.

7.6.3.2 Söz konusu emniyet verilerinin veya emniyet bilgilerinin içerik değerlendirmesi ile, ilgili davranışın istisnai kullanım koşullardan herhangi birini karşılayıp karşılamadığı genellikle tespit edileceği için, duruma ilişkin gerçeklerin ve hallerin, söz konusu istisnai davranışın vuku bulduğunu su götürmez şekilde ortaya koyması gerekli değildir. Bunun yerine, söz konusu gerçeklerin ve hallerin, ilgili olayın böyle bir davranıştan kaynaklanmış olabileceğinin tespit edilebileceği makul bir dayanak sağlaması yeterli olacaktır. Yetkili otorite tarafından, bir duruma ilişkin gerçeklere ve hallere dayalı olarak, (ulusal hukuk kapsamında anlaşıldığı üzere) ağır ihmal, kasti suiistimal veya suç faaliyetinin sonucu olarak ortaya çıkmış olabileceğinin tespit edildiği durumlarda, istisna prensibi uygulanarak emniyet verileri, emniyet bilgileri veya bunlara ilişkin kaynaklar yayınlanabilir.

7.6.3.3 Bu terimlerle ifade edilmek istenen anlamlar ile ilgili olarak, farklı hukuk sistemleri, ulusal hukuk kapsamında farklı anlamlara sahip olabilir. Genel itibariyle; ağır ihmal, belirli bir riskin aktör tarafından tamamen değerlendirilmiş olup olmamasına bakmaksızın, söz konusu risk ciddi ölçüde göz önünde bulundurulmadan veya kayda alınmadan üstlenilen bir fiil/eylem veya ihmaldir. Bu, zaman zaman dikkatsiz davranış olarak tanımlanmaktadır. Kasti suiistimal; aktörün yanlış olduğunu bildiği veya yanlış olup olmadığını bilinçli bir şekilde umursamadığı yanlış bir fiil/eylem veya ihmaldir. Bu gibi hallerde, bilgi ve niyet, resmiyette kanunsuz olarak betimlenmesine karşın, kimi zaman eylemin sonuçlarına ilişkin de olabilecektir. Her halükarda, müdahil olunan davranışın mahiyetinin tespit edilmesi hususunda geçerli olan delil niteliğindeki testler ve tedbirler, ilgili yargı yetki bölgesinin kanunları ile uyumlu olmalıdır. Ayrıca istisna prensibinin, bir yanda "ağır ihmal" veya "kasti suiistimal" ve diğer yanda "suç faaliyeti" teşkil eden davranışlar arasında ayrım gözetmesi nedeniyle, "ağır ihmal" ya da "kasti suiistimal" teşkil edebilecek bir davranışın (ancak, söz konusu davranış geçerli ulusal kanun kapsamında tanımlanabilecektir), cezai değil sivil standart bağlamında değerlendirilmesi gerekmektedir.

7.6.3.4 Yetkili bir otorite tarafından koruma kuralına ilişkin istisnanın geçerli olduğuna karar verebileceği ikinci bir durum ise, ilgili emniyet verilerini veya emniyet bilgilerini inceleyen yetkili otoritenin, söz konusu verilerin veya bilgilerin yayınlanmasının "adaletin uygun şekilde yönetilmesi için gerekli" olduğunu ve "söz konusu verilerin veya bilgilerin yayınlanmasına ilişkin faydaların, söz konusu verilerin veya bilgilerin yayınlanmasının, emniyet verilerinin ve emniyet bilgilerinin geleceğe dönük toplanmaları ve elverişliliği üzerinde sahip olabileceği olumsuz ulusal ve uluslararası etkiden daha baskın" olduğunu tespit ettiği durumdur.

7.6.3.5 Bu; iki aşamalı bir değerlendirme sürecini içermekte olup, söz konusu süreç kapsamında, yetkili otorite tarafından öncelikle verilerin veya bilgilerin "adaletin uygun şekilde yönetilmesi için gerekli" olup olmadığının tespit edilmesi gerekmekte olup, bu durum, aynı bilgilere ilişkin alternatif kaynakların mevcut olması halinde söz konusu olmayabilir; ikinci olarak ise, söz konusu verilerin veya bilgilerin yayınlanmasının adaletin uygun şekilde yönetilmesi için gerekli olduğuna karar vermesi halinde, tüm ilişkili hususlar göz önünde bulundurulduğunda, emniyetin sürdürülmesi veya iyileştirilmesi amaçlarıyla, söz konusu verilerin veya bilgilerin değerinin, bunların yayınlanmasının, emniyet verilerinin ve emniyet bilgilerinin geleceğe dönük toplanmaları ve elverişliliği üzerinde sahip olabileceği olumsuz etkiden daha baskın olup olmadığını tespit etmelidir.

7.6.3.6 Emniyet verilerinin veya emniyet bilgilerinin, herhangi bir fiilde/eylemde veya (hukuki, idari, cezai veya disipliner) işlemde kullanılmasının önerilmesi halinde, söz konusu kullanımın olası olumsuz etkisi, söz konusu verilerin veya bilgilerin kaynağına ilişkin olabilir. Emniyet verilerinin veya emniyet bilgilerinin, fiilin/eylemin veya işlemin sınırları dışında paylaşılmasının önüne geçilmesi amacıyla koruyucu tedbirler uygulanabilir olsa da, herhangi bir işlem sırasında söz konusu verilerin veya bilgilerin kullanımından kaynaklanan olumsuz etki, emniyetin sürdürülmesi veya iyileştirilmesi amaçlarıyla, emniyet verilerinin ve emniyet bilgilerinin ileriye dönük raporlanmasını veya paylaşılmasını teşvik etmeyebilir. Emniyet verilerinin veya emniyet bilgilerinin önerilen kullanımının, söz konusu verilerin veya bilgilerin işlem sınırlarının ötesinde yayılmasını veya yayınlanmasını içermesi halinde, yetkili otorite, (ulusal ve uluslararası) daha geniş toplum üzerindeki olası olumsuz etkiyi de göz önünde bulundurmalıdır.

7.6.3.7 Bireysel düzeyde ise, bilgilerin kamuya açıklanması, müdahil olan kişi aleyhinde, utanç ve/veya geçim kaynağının olası kaybı gibi, olumsuz etkiye sebep olabilir. Daha kapsamlı düzeyde ise, emniyet verilerinin veya emniyet bilgilerinin belirli bir durumda yayınlanması veya dağıtılması, söz konusu fiile/eyleme veya işleme müdahil olmayan ancak benzer durumda olan kişiler için, söz konusu verilerin ve bilgilerin raporlanması veya toplanmasına katkı sağlanması bakımından genel anlamda caydırıcı bir etki oluşturabilir.

7.6.3.8 İlk iki istisna prensibine ilişkin tespitte bulunurken, yetkili otorite aşağıdaki hususlara ilişkin olarak kani olmalıdır:

a) İlk durumda; paylaşılmak veya kullanılmak istenen emniyet verilerinin veya emniyet bilgilerinin içeriği, söz konusu fiilin/eylemin veya ihmalin ağır ihmal, kasti suiistimal veya suç faaliyeti teşkil edip etmediğinin tespit edilmesi için gereklidir veya

b) İkinci durumda; ilgili veriler, bilgiler veya bunlara ilişkin kaynak, hukukun uygun bir şekilde yönetilmesi için gereklidir.

7.6.3.9 Yetkili otorite tarafından, emniyet verilerinin, emniyet bilgilerinin veya bunlara ilişkin kaynağın kimliğinin duruma ilişkin olarak gerekli olup olmadığı tespit edilecektir. Yetkili bir otorite tarafından, korumaya tabi verilere, bilgilere veya kaynağa atıf yapılmaksızın makul ölçüde karar verilebilmesi halinde, emniyet verilerinin, emniyet bilgilerinin ve bunlara ilişkin kaynakların korunmasına daha çok önem verilmelidir. Yetkili otorite tarafından, söz konusu verilerin ve bilgilerin paylaşılması (veya kullanılması) gerekli olmaksızın karar verilebildiği durumlarda, emniyet verilerinin, emniyet bilgilerinin ve bunlara ilişkin kaynakların toplanmasını ve elverişliliğini tehlikeye atmaya gerek yoktur. Bu, emniyetin sürdürülmesi ve iyileştirilmesi için emniyet verilerinin ve emniyet bilgilerinin sürekli elverişliliğinin sağlanmasına yardımcı olacaktır.

7.6.3.10 Emniyet verilerinin, emniyet bilgilerinin ve bunlara ilişkin kaynakların paylaşılmasından veya kullanımından, havacılık operasyon personelinin denetçilerle işbirliği yapma konusunda gönülsüz olmaları gibi olumsuz sonuçlar ortaya çıkabilir. Söz konusu verilerin, bilgilerin veya bunlara ilişkin kaynaklara yönelik bilgilerin, herhangi bir işlem kapsamında esasa ilişkin bir gerçeği ortaya koymak için gerekli olmaması halinde, emniyet verilerinin, emniyet bilgilerinin ve bunlara ilişkin kaynakların geleceğe dönük toplanması ve elverişliliği, ilgili istisna prensiplerinden herhangi biri kapsamında gereksiz yayınlanma dolayısıyla zarar görmemelidir. Ayrıca, gerekli bilgilerin alternatif kaynaklardan elverişli bir şekilde elde edilebilmesi halinde, yetkili otorite tarafından, bilgilerin elde edilmesi için tüm makul alternatif yollara başvurulana kadar, emniyet verilerine veya emniyet bilgilerine erişime izin verilmesi aleyhinde karar verebilir.

7.6.3.11 Benzer şekilde; bilgi edinme hakkı kanununun mevcut olmadığı bir Ülkedeki herhangi bir yetkili otoriteden, emniyet verilerinin veya emniyet bilgilerinin kamuya açıklanmasının gerekli olup olmadığı konusunda karar vermesinin istenmesi halinde (örneğin; medyadan gelen bir talebe cevaben), yetkili otorite, büyük ihtimalle, söz konusu verilerin veya bilgilerin içeriğinin kamu nezdinde bilinir olmasının ne denli önemli olduğunu bilmek isteyecektir. Böyle bir durumda, yetkili otorite şöyle bir soru sorabilir: "Verilerin veya bilgilerin içerikleri bilinmese, olay kamu nezdinde olması gerektiği şekilde anlaşılır mı veya olay, seyahat eden kamu kesimine yönelik emniyet sonuçlarına neden olur mu?" Emniyet verilerine veya emniyet bilgilerine erişim sağlanmazsa, kamu nezdindeki bilginin tehlikeye gireceğine dair görüşün doğru olduğunu kanıtlayabilmek, söz konusu verilerin veya bilgilerin paylaşılmasına yönelik görüşü güçlendirebilir.

Ancak; bu veriler veya bilgiler, yalnızca bahse konu gerekçeler ortaya konduğu için paylaşılmak zorunda değildir. Paylaşımın, geleceğe dönük emniyet raporlamasına ilişkin olarak insanların cesaretini kırarak, emniyet verilerinin ve emniyet bilgilerinin sürekli elverişliliğine ciddi ölçüde zarar vermesi halinde, durumun, paylaşım lehine çevrilmesi gerekmez.

7.6.3.12 Üçüncü istisna ise, "emniyet verilerini veya emniyet bilgilerini inceleyen" yetkili otorite tarafından "söz konusu verilerin veya bilgilerin yayınlanmasının emniyetin sürdürülmesi veya iyileştirilmesi için gerekli olduğunun ve söz konusu verilerin veya bilgilerin yayınlanmasının faydalarının, bunların yayınlanmasının, ilgili emniyet verilerinin ve emniyet bilgilerinin geleceğe dönük toplanmaları ve elverişliliği üzerinde sahip olabileceği olumsuz ulusal ve uluslararası etkiden daha baskın olduğunun" tespit edildiği durumdur. Bu istisna, emniyetin sürdürülmesi veya iyileştirilmesi için emniyet verilerinin veya emniyet bilgilerinin yayınlanmasının gerekli olduğu durumlar için geçerlidir. Emniyet verilerinin veya emniyet bilgilerinin, havacılık emniyetini sürdürmek veya iyileştirmek için gerekli olan ve düzenleyici bir otorite tarafından alınan önleyici, düzeltici veya iyileştirici faaliyetler ile bağlantılı olarak kullanılmasında geçerli değildir.

7.6.3.13 Annex 19 kapsamında öngörülen haller; örneğin eğitim ve öğretim amaçlarıyla veya emniyet bilgilerinin ve tavsiyelerinin daha geniş toplumun yararına yayınlanması da dahil olmak üzere emniyetin sürdürülmesi veya iyileştirilmesi ile ilgili olarak daha genel amaçlarla yayınlanmasına yönelik faydaların yetkili otorite tarafından göz önünde bulundurulmasını kapsar. Bu durumlara yönelik analiz, yukarıda yer alan 7.6.3.5 sayılı iki aşamalı sürecin aynısını içermektedir: öncelikle, yetkili otorite tarafından "ilgili verilerin veya bilgilerin yayınlanmasının, emniyetin sürdürülmesi veya iyileştirilmesi için gerekli" olduğuna karar verilmesi; ikinci olarak ise, yetkili otorite tarafından, söz konusu verilerin veya bilgilerin yayınlanmasına ilişkin faydaların, söz konusu verilerin veya bilgilerin yayınlanmasının, bunların geleceğe dönük toplanmaları ve elverişliliği üzerinde sahip olabileceği olası olumsuz etkiden daha baskın olduğunun tespit edilmesi gerekmektedir.

7.6.3.14 Bu analizin ikinci aşamasının değerlendirilmesi ile ilgili olarak; Annex 19 kapsamında, yetkili otoriteler "emniyet verilerinin ve emniyet bilgilerinin kaynağının onayının" göz önünde bulundurulması konusunda teşvik edilmektedir. Bu farkındalığın önemi, emniyet verilerinin ve emniyet bilgilerinin emniyetin sürdürülmesi veya iyileştirilmesi ile ilgili genel amaçlara yönelik olarak yayınlanması (bu durumda, bu istisna prensibi geçerli olacaktır) ile emniyet verilerinin ve emniyet bilgilerinin, emniyetin sürdürülmesi veya iyileştirilmesini destekleyici nitelikteki belirli önleyici, düzeltici ve iyileştirici amaçlarla kullanılması (bu durumda, söz konusu kullanıma halihazırda koruma prensipleri kapsamında izin verildiği için hiçbir istisna prensibi gerekliliğinin yerine getirilmesi gerekli olmayacaktır) arasındaki ayrımı gözeten, yukarıda yer alan 7.4.2 sayılı madde kapsamında ele alınan kritik ayrımı vurgular.

7.6.3.15 Koruma prensiplerinin ruhuna uyum sağlanması konusunda, emniyet verilerinin veya emniyet bilgilerinin emniyetin sürdürülmesi veya iyileştirilmesi amacıyla alınan önleyici, düzeltici veya iyileştirici tedbirleri desteklemek amacıyla kullanılması göz önünde bulundurulurken, yetkili otorite tarafından, söz konusu verilere veya bilgilere ilişkin uygun alternatif kaynağın elverişli olup olmayabileceğinin ortaya konması mümkün olabilir. Böyle bir durumda, korumaya tabi emniyet verilerinin veya emniyet bilgilerinin istisnasız kullanımından kaçınılabilir.

7.6.3.16 Ancak, söz konusu elverişlilik değerlendirmesi, Annex 19 kapsamında bahsedilen istisna prensibinin resmi olarak uygulanmasını gerektirmez veya buna yönelik bir çağrıda bulunmaz. Bunun nedeni, istisna prensibinin, emniyetin sürdürülmesi veya iyileştirilmesi menfaatinin diğer birtakım çakışan kamu yararından daha baskın geldiği durumlarda (örneğin: adaletin uygun bir şekilde yönetilmesi, verilere veya bilgilere kamu erişiminin sağlanması, veya korumaya tabi verilerin veya bilgilerin kapsama dahil edilmesine izin verilerek eğitim veya öğretim süreçlerinin kolaylaştırılması) geçerli olmasıdır. Emniyetin sürdürülmesi veya iyileştirilmesi amacıyla alınan önleyici, düzeltici veya iyileştirici tedbirler, koruma prensipleri kapsamına girmekte olup, söz konusu kullanımı dengelemesi gereken hiçbir emniyet dışı dengeleyici menfaat söz konusu değildir.

7.6.4 İstisna prensipleri uygulanırken göz önünde bulundurulması gereken ilave hususlar

7.6.4.1 Bir durumda herhangi bir istisna prensibinin geçerli olup olmadığına karar verilirken, yetkili otorite, emniyet verilerinin veya emniyet bilgilerinin kaynağının onayını daima göz önünde bulundurmalıdır. Herhangi bir şahsa, kaynağı olduğu emniyet verilerinin veya emniyet bilgilerinin gizliliğine yönelik güvence verilmiş olması halinde, söz konusu verilerin veya bilgilerin, bu güvencelerle çatışacak şekilde kullanılması, ilgili şahıs tarafından gelecekte sağlanabilecek emniyet verileri ve emniyet bilgileri üzerinde olumsuz etkiye sahip olabilir. Ayrıca emniyet verilerinin veya emniyet bilgilerinin, kaynağa sunulan gizlilik güvencelerine rağmen yayınlanması veya kullanılması halinde, bu, ilgili durumdan haberdar olabilecek şahıslar üzerinde benzer bir olumsuz etkiye sahip olabilir.

7.6.4.2 7.6.4.1 sayılı madde kapsamında bahsedilen türden istenmeyen olayların önüne geçmek amacıyla, bireylerin ve organizasyonların sağladıkları verilerin ve bilgilerin istisna prensiplerinin uygulanmasına uygun olarak nasıl, ne zaman, nerede ve hangi amaçlarla kullanılabileceğini önceden net bir şekilde anlamalarını sağlamak ihtiyatlı bir adım olacaktır. Bunun sağlanması, güvene dayalı bir öngörülebilir raporlama ortamının tesis edilmesi ve idame ettirilmesi için elzemdir.

7.6.4.3 Yetkili otorite tarafından, istisna prensiplerinin Annex 19 kapsamındaki hükümlerle uyumlu bir şekilde uygulanmasına ilişkin genel nitelikli kılavuz ilkeler, Şekil 7-2 [6]kapsamında gösterilmektedir.

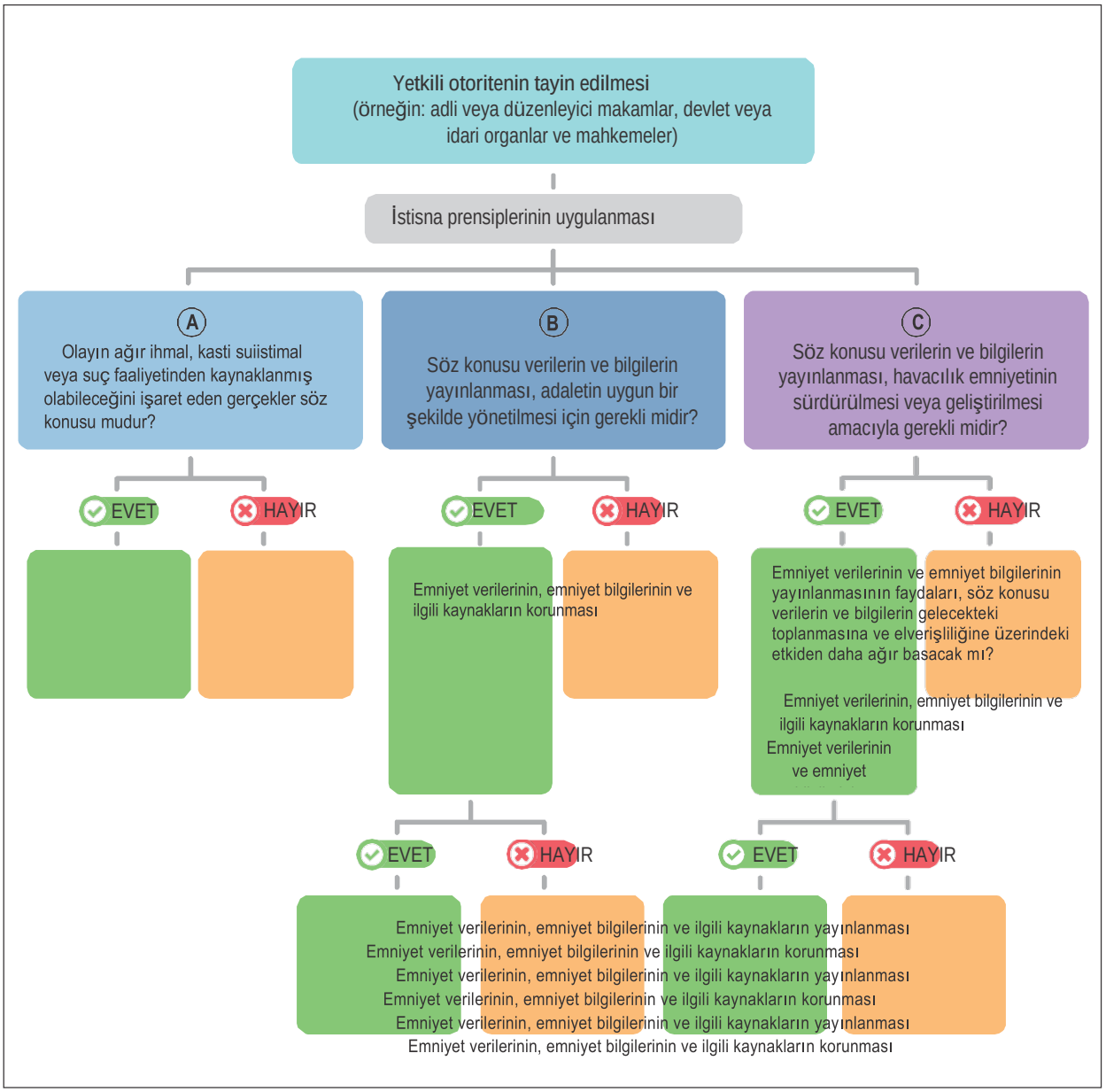
7.7 KAMUNUN BİLGİLENDİRİLMESİ

7.7.1 Halk, emniyet verilerine veya emniyet bilgilerine karşı büyük bir ilgi duyar. Halkın ilgisi; açıklık, şeffaflık ve hesap verilebilirlikte toplanır; böylece sistem emniyeti hakkında genel bir farkındalığa ve emniyetin ele alınması için gereken her şeyin yapıldığına dair güvenceye sahip olabilirler. Bazı bireyler veya ilgi grupları, doğrudan emniyetle ilgili olanlar haricinde nedenlerle emniyet verileri veya emniyet bilgileriyle de ilgilenebilir. İfşa, hükümete sunulan bir bilgi talebinin sonucu olarak veya bir adli kovuşturmanın süreçleri kapsamında gönüllülük esasına dayalı olarak gerçekleşebilir. Herhangi bir emniyet verisinin veya emniyet bilgisinin kamuya açıklanmasının uygun olup olmadığı, emniyet verilerinin ve emniyet bilgilerinin mahiyetine bağlıdır. Söz konusu karar, daha önceki bölümler kapsamında ele alındığı üzere, yetkili otoritenin yetki alanına girer.

7.7.2 Emniyet verilerinin veya emniyet bilgilerinin kamuya açıklanması halinde, bilgilerin nasıl kullanılacağını kısıtlamak genelde mümkün değildir. Açıklık ve şeffaflık kesinlikle teşvik edilmelidir; ama aynı zamanda, emniyet verilerinin ve emniyet bilgilerinin raporlanmasına ve analizine müdahil olanların hakları ve meşru beklentilerinin yanı sıra bunların ilgili şahısların menfaatlerine veya itibarlarına gelebilecek uygunsuz zararlardan korunması ihtiyacı da göz önünde bulundurulmalıdır. Ancak; bu, bilgi edinme hakkı kanunlarının yürürlükte olduğu Devletler için her zaman geçerli olmayabilir.

7.7.3 Pek çok Devlet, Devlet kurumlarının elinde bulunan bilgilerinin tamamının yayınlanmasını gerektiren geçerli mevzuata sahiptir. Bu tür kanunlar zaman zaman bilgi edinme hakkı kanunları olarak adlandırılmaktadır. Bu kanunlar kapsamında, belirli bir tür bilgiye ilişkin istisna söz konusu olmadığı sürece, bu bilgiler, talep üzerine devlet tarafından ifşa edilmelidir. Gizli bilgiler, ticari açıdan hassas bilgiler veya mahremiyet kanunları kapsamında korunmakta olan tıbbi kayıtlar gibi bilgiler istisnalara ilişkin örneklerdendir. Emniyet verileri veya emniyet bilgileri genellikle istisnaya tabi değildir. Annex 19'a uygun olarak; Devletler, bilgi edinme hakkı kanunları veya havacılık mevzuatı dahil olmak üzere herhangi bir türden kanun kapsamında kamuya ifşanın önüne geçecek muafiyetler veya kurallar oluşturmayı tercih edebilir.

6. Devletlerin, havacılık emniyetini sürdürmek veya geliştirmek için gerekli olan önleyici, düzeltici veya iyileştirici faaliyetleri gerçekleştirmesi için emniyet verilerini veya emniyet bilgilerini *kullanmaktan* alıkonmayacağını unutmamak gerekir.



Şekil 7-2. İstisna prensiplerinin uygulanmasına ilişkin kılavuz ilkeler

7.7.4 Bilgi edinme hakkı kanunları genellikle hükümetin elinde bulunan bilgiler için geçerlidir. İfşadan korunması gereken pek çok emniyet verisinin ve emniyet bilgisinin operasyonel personel veya hizmet sağlayıcılardan elde edilmesi nedeniyle, söz konusu verilerin ve bilgilerin herhangi bir devlet otoritesine emanet edilmesi yerine organizasyon bünyesinde kalmasına imkân sağlamak faydalı bir yaklaşım olacaktır. Böylece, idari işlem gibi birtakım ilave hükümet tedbiri alınmadıkça, kamunun aydınlatılması mevzusu ortaya çıkmaz. İdari veya adli bir işlem kapsamında kamunun aydınlatılması mevzusuyla karşı karşıya kalındığı durumlarda, yetkili otorite, yukarıda ele alınan temel koruma prensiplerini uygulamalıdır. Hizmet sağlayıcılarının emniyet verilerini ve emniyet bilgilerini bir devlet makamına bildirmek zorunda olması veya hizmet sağlayıcısının, bir devlet makamı veya kurumu olması ya da bir devlet makamı veya kurumu bünyesinde yer alması halinde, bu yaklaşım faydalı olmayabilir.

7.7.5 Emniyet verilerine veya emniyet bilgilerine erişime yönelik ortaya atılan çatışan hak taleplerinin uygun şekilde değerlendirilmemesi, mevcut ve geleceğe dönük çabaları iki şekilde etkileyebilir. Birtakım verilerin veya bilgilerin kamuya açıklanması, bireylerin mahremiyetinin ya da organizasyonların emniyet verilerine veya emniyet bilgilerine ilişkin gizlilik beklentilerinin ihlali olarak algılanabilir. Birtakım verilerin veya bilgilerin, müdahil olan bireyler veya organizasyonlar aleyhindeki yaptırımları destekleyici nitelikteki bir argüman kapsamında kullanılması, temel dürüstlük ilkelerinin ihlali olarak görülebilir. İfşasına veya suç teşkil edecek kullanımına yönelik tehdit algısından kaynaklanan, bilgilerin saklanması şeklindeki öngörülebilir insan davranışı, emniyet verilerinin ve emniyet bilgilerinin geleceğe dönük elverişliliğini etkileyebilir. Bunun hem emniyet yönetimine ilişkin veri toplama ve veri analizi fonksiyonları üzerinde açık bir etkisi olabilir.

7.7.6 Yetkili otorite tarafından emniyet verilerinin veya emniyet bilgilerinin kamuya açıklanabileceğine karar verilmesi halinde, Devletin, kamuya yapılan açıklamaların geçerli mahremiyet kanunlarına uygun olarak ya da kimliksizleştirilmiş olarak, özet veya toplu şekilde yapılmasını sağlaması beklenmektedir. Zorunlu koruyucu tedbirler ile ilgili ayrıntılı bilgiler 7.5.3 sayılı maddede yer almaktadır.

7.8 KAYITLI VERİLERİN KORUNMASI

7.8.1 Çalışma ortamı kayıtlarının korunması

7.8.1.1 Çalışma ortamı kayıtları, koruma politikalarının veya düzenlemelerinin bir parçası olmalıdır. Düzenlemeler veya politikalar kapsamında izin verildiği durumlarda, söz konusu kayıtlar emniyet yönetimi kapsamında kullanılırken, koruma ve istisna prensiplerine tam olarak riayet edilmelidir. Raporlama popülasyonunun güveni, etkin emniyet yönetimi için elzemdir. Bu güvenden ödün verilmemelidir.

7.8.1.2 Annex 19 kapsamında yer alan Hükümler, hava aracının emniyetli bir şekilde işletilmesi ile ilgili olan veya hava aracının emniyetli bir şekilde işletilmesini doğrudan destekleyen emniyet yönetimi işlevleri için geçerlidir. Çalışma ortamı kayıtları, Annex 19 kapsamında tanımlanmayan ulusal mahremiyet kanunları ile idare edilebilir.

7.8.1.3 Çalışma ortamı kayıtları; kokpit ses kayıt cihazları (CVR'ler), hava görüntü kayıt cihazları (AIR'ler), diğer uçuş kayıt cihazı kayıtları veya hava trafik kontrolörü iş istasyonlarındaki geri plan iletişimi ve işitsel çevre kayıtlarını içerebilir.

7.9 EMNİYET BİLGİLERİNİN PAYLAŞILMASI VE DEĞİŞİMİ

7.9.1 Devletler arasında paylaşılan bilgilerin korunması

7.9.1.1 Emniyet bilgilerinin paylaşılmasının ve değişiminin yapılmasının ana amaçlarından birinin, emniyet bilgilerinin paylaşılması ve değişiminin yapılması sürecinde hem Devlet düzeyindeki hem de küresel düzeydeki emniyet sorunlarına tutarlı, gerçeklere dayalı ve şeffaf bir müdahalede bulunulmasını sağlamak olduğu göz önünde bulundurulduğunda, Devletler aşağıdaki ilkelere uygun olarak hareket edecektir:

a) Uluslararası Sivil Havacılık Sözleşmesine (Chicago Konvansiyonu), Eklerine ve Devletlerin sair çok taraflı ve iki taraflı yükümlülüklerine riayet edilecektir;

b) Emniyet bilgilerinin paylaşımı ve değişimi; Devlet sırlarına, kişisel verilerin korunmasına, ticari sırlara ve bireylerin ve tüzel kişilerin haklarının ihlaline ilişkin ulusal kanunlar ve düzenlemeler dahil olmak ancak bunlarla sınırlı kalmamak üzere, emniyet bilgilerinin korunmasına ilişkin ulusal kanunların ilgili Devletlerin otoriteleri tarafından ihlal edilmesine yol açmaz;

c) Herhangi bir Devlet tarafından paylaşılan ve değişimi yapılan emniyet bilgileri, söz konusu Devletin kendisini, havayollarını, kamu görevlilerini ve vatandaşlarını olumsuz yönde etkileyecek şekilde ve ekonomik avantaj elde edilmesi dahil olmak üzere sair uygunsuz amaçlar için kullanılmamalıdır;

d) Emniyet ile ilgili bilgilerin uygunsuz kullanıma karşı korunmasının tek amacı, önleyici tedbirlerin doğru bir şekilde ve zamanında alınmasını ve havacılık emniyetinin iyileştirilmesini sağlamak üzere bunların sürekli olarak kullanıma hazır bulunmasını temin etmek olacaktır ve

e) Emniyet bilgileri, Annex 19 kapsamında yer alan koruma prensiplerine uygun olarak paylaşılmalı ve değişimi yapılmalıdır.

7.9.1.2 Bilgilerin paylaşımına ve değişiminin yapılmasına ilişkin yasal bir çerçeve, Devletler arasında yapılarak örneğin hava ulaştırma (hava hizmetleri) anlaşmalarına derç edilen ikili düzenlemelere dayalı olabilecektir. Bilgilerin paylaşımını ve değişiminin yapılmasını kolaylaştırmak amacıyla Devletler, geçerli olması halinde, onaylanarak yürürlüğe girmeyi bekleyen bu tür ikili düzenlemelerin geçici olarak uygulanacağı konusunda da mutabakata varabilir.

7.9.1.3 Devletler, havacılık sistemlerinin kullanıcıları arasında emniyet bilgilerinin paylaşımına ve değişiminin yapılmasına ilişkin ağlar tesis edilmesini teşvik etmeli ve kolaylaştırmalıdır. Emniyet bilgilerinin paylaşımı ve değişiminin yapılması, hem Devlet düzeyindeki hem de küresel düzeydeki emniyet sorunlarına tutarlı, gerçeklere dayalı ve şeffaf bir müdahalede bulunulmasını sağlamak için elzemdir.

Bölüm 8

DEVLET EMNİYET YÖNETİMİ

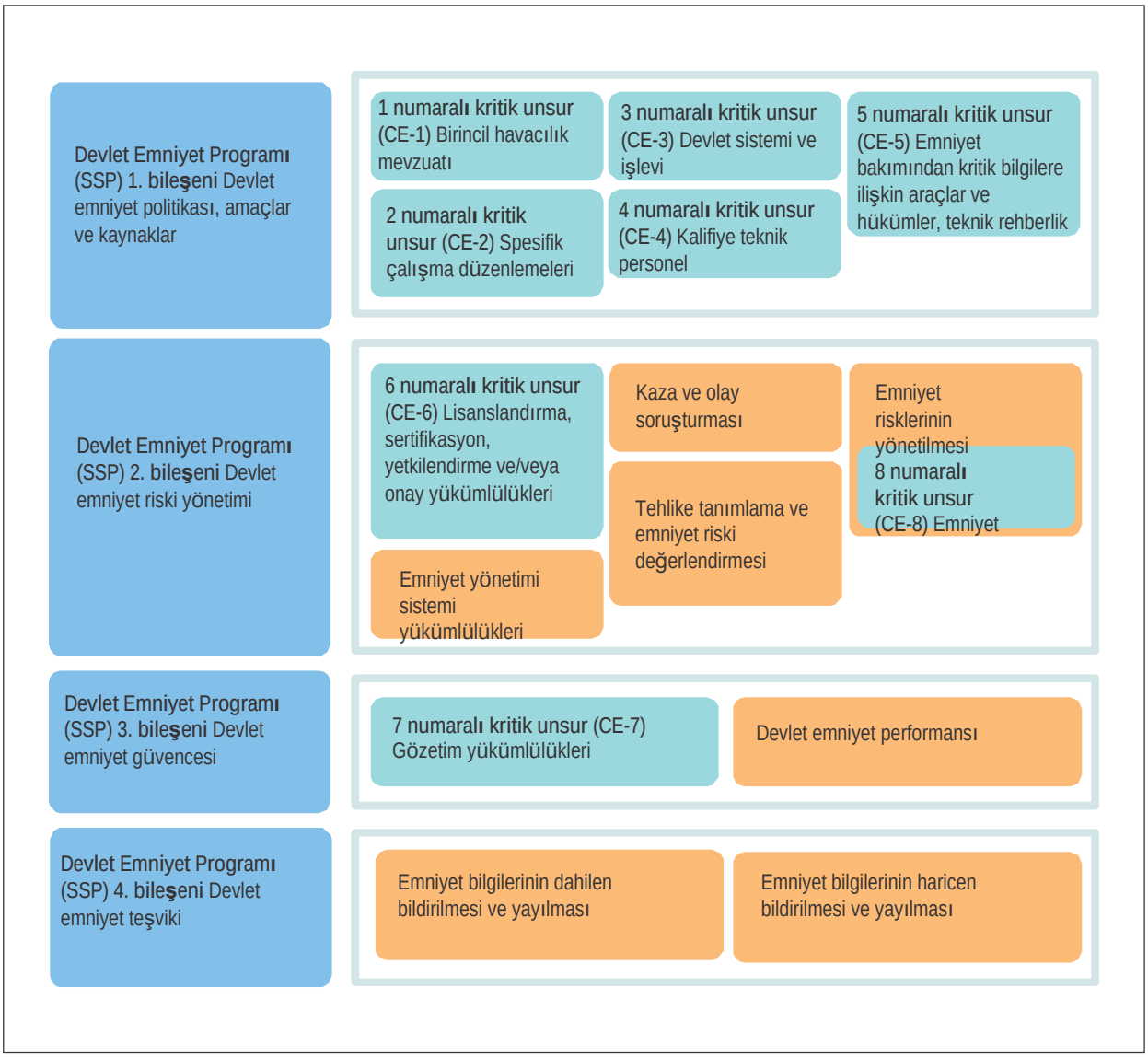
8.1 GİRİŞ

8.1.1 Annex 19'un 3. Bölümünde, Devletlerin emniyet yönetimi sorumluluklarına ilişkin Standartlar ve Tavsiye Edilen Uygulamalar (SARP'ler) yer almaktadır. Entegre bir şekilde emniyetin yönetilmesine yönelik Devlet emniyet programının (SSP) tesis edilmesi ve sürdürülmesi buna dahildir.

8.1.2 Annex 19'un İlk Baskısı ile Devletlerden iki hüküm dizisini tesis etmeleri ve uygulamaları beklenmiş olup, bunlar herhangi bir Devletin emniyet gözetimi (SSO) sisteminin sekiz kritik unsuru (CE'ler) ve Devlet Emniyet Programının (SSP) dört bileşeni olmuştur. Emniyet gözetimi hususu, Devletin, Devlet Emniyet Programı (SSP) kapsamında emniyet yönetimi ilkelerinin oluşturulması temsil edilirken kural koyucu Standartların ve Tavsiye Edilen Uygulamaların (SARP'lar) havacılık endüstrisi tarafından etkin bir şekilde uygulanmasını sağlamak olan geleneksel rolünü yansıtmıştır. Söz konusu sekiz kritik unsura ilişkin detaylar, Standartlar ve Tavsiye Edilen Uygulamalar (SARP'lar) statüsündeki Annex'in Ek 1'inde yer almış, Devlet Emniyet Programının (SSP) uygulanmasına ve sürdürülmesine yönelik çerçevenin detaylı unsurları ise kılavuz materyal olarak Ek A kapsamında sunulmuştur.

8.1.3 Emniyet gözetimi sistemi ile Devlet Emniyet Programı (SSP), her birinin ulaşmayı amaçladığı emniyet amaçları bakımından yakın bir şekilde bağlantılı olmuştur. Önceki ağırlıklı olarak emniyet gözetimine, sonraki ise emniyet yönetimine ve emniyet performansına ilişkin olmak üzere, her ikisi de Devletin işlevlerine ve sorumluluklarına işaret etmektedir. Emniyetin yönetilmesinde proaktif bir yaklaşıma geçişi yansıtan sekiz kritik unsur (CE) dahilinde açık bir şekilde emniyet yönetimine ilişkin bazı yönler mevcuttur. Örneğin, gözetim yükümlülükleri (7 numaralı kritik unsur (CE-7)), emniyet güvencesine ve birincil havacılık mevzuatına (1 numaralı kritik unsur (CE-1)) ilişkin bir öge olarak değerlendirilebilmekte iken ilk Devlet Emniyet Programı (SSP) çerçevesinde spesifik işletme düzenlemeleri (2 numaralı kritik unsur (CE-2)) de önemli emniyet riski kontrolleri olarak yansıtılmıştır.

8.1.4 Bu sorumluluklar Annex 19'un İkinci Baskısında entegre edilmiştir ve birlikte, söz konusu Devletin emniyet yönetimi sorumlulukları olarak anılmaktadır. Hem emniyet gözetimini hem de emniyet yönetimini kapsayan, Devletin emniyet yönetimi sorumluluklarına ilişkin Standartlar ve Tavsiye Edilen Uygulamalar (SARP'ler) birbirine bağımlıdırlar ve etkin emniyet yönetimine yönelik entegre bir yaklaşım teşkil ederler. Annex 19'un İkinci Baskısında halen Devlet Emniyet Programı (SSP) teriminin kullanılmasına karşın, anlam, 3. Bölümde yer alan Standartlara ve Tavsiye Edilen Uygulamalara (SARP'lar) ilişkin entegre seti kapsayacak şekilde değişmiştir. Böylelikle, Devlet Emniyet Programı (SSP) artık bir çerçeve olmaktan ziyade, söz konusu Devletin, emniyet gözetimini içeren emniyet yönetimi sorumluluklarının karşılanmasına yönelik bir program olarak tanımlanmaktadır. Bu sebeple, Devlet Emniyet Programı (SSP), Devlet emniyet yönetimine ilişkin geniş kavram kapsamındadır. Bu gelişim Şekil 8-1'de gösterilmektedir.



Şekil 8-1. Entegre Devlet emniyet programı

8.2 DEVLET EMNİYET PROGRAMI (SSP)

8.2.1 Devlet emniyet gözetim sistemi kritik unsurları

Devlet emniyet gözetimi (SSO) sisteminin kritik unsurları (CE'ler) Devlet Emniyet Programının (SSP) temelini teşkil eder. Annex 19'un İkinci Baskısında, Standart seviyesindeki sekiz Kritik Unsura (CE'ler) ilişkin hükümler muhafaza edilerek emniyet gözetimi sisteminin önemi vurgulanmaktadır. Devlet Emniyet Programı (SSP) çerçevesinden kaynaklanan gerekliliklerin çoğu, birkaçı Standarda yükseltilerek Tavsiye Edilen Uygulamalara yükseltilmiştir. Devlet Emniyet Gözetimi (SSO) sistemine ilişkin detaylar, *Emniyet Gözetimi El Kitabı*, Kısım A — *Devlet Emniyet Gözetimi Sisteminin Oluşturulması ve Yönetimi* (Doc 9734) kapsamında ele alınmaktadır.

8.2.2 Devlet emniyet programına genel bakış

8.2.2.1 Devlet Emniyet Programı (SSP), emniyetin iyileştirilmesini amaçlayan entegre düzenlemeler ve faaliyetler setidir. Devlet Emniyet Programının (SSP) oluşturulması ve muhafaza edilmesi için, ICAO Standartları ve Tavsiye Edilen Uygulamaları(SARP'lar) aşağıdaki dört bileşende yapılandırılmaktadır:

a) Devlet emniyet politikası, amaçlar ve kaynaklar;

b) Devlet emniyet risk yönetimi;

c) Devlet emniyet güvencesi ve

d) Devlet emniyet teşviki.

8.2.2.2 Devlet Emniyet Programının (SSP) uygulanması, söz konusu Devletin havacılık işlevlerinden sorumlu olan birden fazla otoritesi arasında koordinasyon gerektirir. Devlet Emniyet Programının (SSP) uygulanması, söz konusu Devletin havacılık organizasyonlarının ilgili rollerini veya birbirleriyle olan normal etkileşimini değiştirmez. Daha ziyade, Devlet Emniyet Programı (SSP), söz konusu Devlet dahilinde emniyetin daha da iyileştirilmesi için kolektif emniyet işlevlerini ve kabiliyetlerini desteklemeyi amaçlar. Devlet Emniyet Programını (SSP) uygulamaya başlarken, çoğu Devlet, Devlet Emniyet Programının (SSP) bir çok unsuruna işaret eden mevcut süreçlere ve faaliyetlere sahip olduğunu fark eder. Devlet Emniyet Programının (SSP) uygulanması, ilave performans ve emniyet riskine dayalı unsurlarla bu süreçlerin iyileştirilmesini ve söz konusu Devletteki havacılık endüstrisi tarafından Emniyet Yönetimi Sisteminin (SMS) etkin bir şekilde uygulanmasının kolaylaştırılmasını amaçlar.

8.2.2.3 Devlet Emniyet Programının (SSP) amaçları şunlardır:

a) söz konusu Devletin, destekleyici nitelikte spesifik çalışma düzenlemelerinin uygulandığı etkin bir mevzuat çerçevesine sahip olmasının sağlanması;

b) ilgili Devlet havacılık otoriteleri arasında Emniyet Riski Yönetimi (SRM) ve emniyet güvence koordinasyonunun ve sinerjisinin sağlanması;

c) hizmet sağlayıcılarının Emniyet Yönetimi Sistemi (SMS) ile uygun etkileşimin ve etkin uygulamanın desteklenmesi;

d) söz konusu Devletin havacılık endüstrisinin emniyet performansının izlenmesinin ve ölçülmesinin kolaylaştırılması ve

e) söz konusu Devletin genel emniyet performansının muhafaza edilmesi ve/veya sürekli olarak iyileştirilmesi.

8.2.3 Emniyet yönetimi işlevlerinin ve faaliyetlerinin devredilmesi

8.2.3.1 Bazı emniyet yönetimi faaliyetleri, emniyet riski değerlendirmelerinin yürütülmesi, emniyet verileri analizlerinin gerçekleştirilmesi veya Emniyet Performansı Göstergelerinin (SPI'ler) değerlendirilmesi gibi yeni yetkinlikler gerektirir.

8.2.3.2 Devletler, Devlet Emniyet Programı (SSP) kapsamındaki bazı spesifik işlevleri başka bir Devlete, bölgesel emniyet gözetimi organizasyonuna (RSOO) veya ticari birlik, sektör temsilcisi organizasyon veya özel kuruluş gibi diğer yetkili otoriteye devretmeyi seçebilirler. Devletler tarafından spesifik işlevlerin devredilebilecek olmasına karşın, devrin yapıldığı kuruluş ile arayüz bağlantısı kurmak ve devrin yapıldığı kuruluş tarafından sağlanan bilgileri işlemek için Devletlerin yine de yeterli personele sahip olmaları gerekecektir.

8.2.3.3 Devletler tarafından aynı zamanda, devredilen işlevlerin kendilerini memnun edecek şekilde yürütülmesini sağlamak için uygun teknik ve idari süreçlerin oluşturulması değerlendirilmelidir.

8.2.3.4 Düzenlemeye bakılmaksızın, devredilen görevlerin ulusal gerekliliklere ve Standartlara ve Tavsiye Edilen Uygulamalara (SARP'lar) uygun olarak gerçekleştirilmesini sağlama sorumluluğu ilgili Devlete aittir.

8.2.3.5 Yetki devri, nispeten düşük seviyede havacılık faaliyetlerine sahip olan Devletler tarafından trendlerin saptanması ve hafifletme stratejilerinin koordine edilmesi için emniyet verilerinin kolektif bir şekilde toplanmasına imkan verebilir.

8.2.3.6 Herhangi bir Devletin gözetim süreçlerinin geliştirilmesi için yardım almayı seçmesi halinde, hizmet sağlayıcılarına yönelik organizasyonel emniyet riski profillerinin oluşturulması, onaylanmış organizasyonlara/hizmet sağlayıcılarına yönelik incelemelerin, denetimlerin ve izleme faaliyetlerinin planlanması ve önceliklendirilmesi buna dahil olmalıdır.

8.2.3.7 Herhangi bir Devlet tarafından gözetim faaliyetlerinin devrinin seçilmesi halinde, söz konusu Devlet, belgelenmiş sonuçlarla gözetim kayıtlarına erişim imkanına sahip olduğundan emin olmalıdır. Söz konusu Devletin aynı zamanda her bir hizmet sağlayıcısının emniyet performansını periyodik olarak izlemesi ve gözden geçirmesi ve emniyet sorunlarının çözüme kavuşturulmasının kimin tarafından izleneceğinin ve (ihtiyaç duyulduğunda) yürütüleceğinin açık bir şekilde belirlenmiş olmasını sağlaması gerekir.

8.2.3.8 Yetki devri, sınırlı kaynaklara sahip olan Devletler için uygun uzmanlığa erişim imkanına sahip olunmasına yönelik bir yöntemdir. Bölgesel Emniyet Gözetimi Organizasyonunun (RSOO) tesis edilmesine ilişkin rehberlik *Emniyet Gözetimi El Kitabı*, Kısım B — *Bölgesel Emniyet Gözetimi Organizasyonu* (Doc 9734) kapsamında yer almaktadır.

8.3 1. BİLEŞEN: DEVLET EMNİYET POLİTİKASI, AMAÇLAR VE KAYNAKLAR

8.3.1 Devlet Emniyet Programının (SSP) birinci bileşeni, emniyetin herhangi bir Devlet tarafından kendi havacılık sistemi genelinde nasıl yönetileceğini tanımlar. Gerekliliklerin, Devlet Emniyet Programına (SSP) ilişkin farklı Devlet havacılık otoritelerinin yükümlülüklerinin, işlevlerinin ve faaliyetlerinin ve ulaşılacak geniş kapsamlı emniyet amaçlarının tespit edilmesini içerir. Devlet emniyet politikası ve amaçları, açık beklentiler sunmak ve söz konusu Devletin Sivil Havacılık Otoritesi'nin (CAA) emniyet yönetimi çalışmaları ile diğer Devlet havacılık otoritelerinin bu yöndeki çalışmalarının emniyet performansının sürdürülmesine ve iyileştirilmesine yoğunlaşmış halde tutmak üzere belgelenmelidir. Bu sayede, söz konusu Devlet tarafından, büyümeye devam eden ve daha karmaşık hale gelen hava ulaştırma sisteminin desteklenmesine yönelik açık emniyet kılavuz ilkelerinin sunulmasına imkan verilir.

8.3.2 Söz konusu Devletin yasal çerçevesi kapsamında havacılık emniyetinin nasıl yönetileceği öngörülür. Hizmet sağlayıcıları, ürünlerinin ve hizmetlerinin emniyetinden hukuken sorumludurlar. Söz konusu Devlet tarafından tesis edilen emniyet düzenlemelerine riayet eder nitelikte olmalıdırlar. Söz konusu Devlet, Devlet Emniyet Programının (SSP) uygulanmasına ve sürdürülmesine dahil olan havacılık otoritelerinin Devlet Emniyet Programının (SSP) etkili bir şekilde uygulanabilmesi için gerekli kaynaklara sahip olmalarını sağlamalıdır.

8.3.3 Devlet Emniyet Programının (SSP) Devlet emniyet politikası, amaçlar ve kaynaklar başlıklı 1. bileşeni aşağıdaki unsurlardan oluşur:

a) birincil havacılık mevzuatı;

b) spesifik çalışma düzenlemeleri;

c) Devlet sistemi ve işlevleri;

d) kalifiye teknik personel ve

e) teknik kılavuzluk, araçlar ve emniyet bakımından kritik bilgilerin sağlanması.

8.3.4 Birincil havacılık mevzuatı

8.3.4.1 Birincil havacılık mevzuatına (1 numaralı kritik unsur (CE-1)) ilişkin rehberliğe Doc 9734 Kısım A kapsamında ulaşılabilir.

Not.— Bu el kitabı genelinde "mevzuat" terimi, birincil havacılık mevzuatını ve spesifik çalışma düzenlemelerini içermek üzere genel bir terim olarak kullanılmaktadır.

8.3.4.2 Çeşitli Devlet havacılık otoritelerini (örneğin, Sivil Havacılık Otoritesi (CAA) veya Kaza Soruşturma Otoritesi) görevlerini ifa etmek üzere yetkilendiren mevzuat hükümlerine ihtiyaç olabilecektir. Birincil havacılık mevzuatında Devlet Emniyet Programının (SSP) uygulanmasının Sivil Havacılık Otoritesinin (CAA) görevi olarak özellikle belirtilmesinin gerekip gerekmediği söz konusu Devletin hukuk sistemine bağlıdır. Bazı Devletler tarafından, Devlet Emniyet Programının (SSP) uygulanmasının söz konusu Devletlerin birincil havacılık mevzuatında daha önceden belirtilen işlevler kapsamında ifade edildiği değerlendirilebilir. Bu durumda, birincil havacılık mevzuatının tadil edilmesi gerekli olmayabilir. Devlet Emniyet Programının (SSP) uygulanmasına ilişkin kanıtın resmi Devlet belgelerinde açık bir şekilde mevcut olması gerekir. Söz konusu Devlet tarafından aynı zamanda, Annex 19 kapsamında belirtildiği şekilde, emniyet yönetimi sorumluluklarını ele alma taahhüdünün kanıtlanabilmesi gerekir.

8.3.4.3 Kendi Devlet Emniyet Programı (SSP) kapsamında, söz konusu Devlet tarafından aşağıdaki türden bir yürütme politikasının tesis edilmesi beklenir:

a) pozitif emniyet kültürünü destekleyen ve teşvik eden;

b) özellikle, sağlanan bilgilerin kendi aleyhine tanıklık yapan türden olması halinde olmak üzere, emniyet verilerinin ve emniyet bilgilerinin ve ilgili kaynakların korunmasının söz konusu Devlet tarafından nasıl güvence altına alındığını açıklayan ve

c) Emniyet Yönetimi Sistemine (SMS) sahip olan hizmet sağlayıcılarının, söz konusu Emniyet Yönetimi Sisteminin (SMS) Emniyet Yönetimi Sistemi (SMS) çerçevesine uygun olması ve etkin ve olgunlaşmış olduğunun gösterilmesi koşuluyla, belirli emniyet sorunlarını içeren olaylara, kendilerinin Emniyet Yönetimi Sistemi (SMS) bağlamı dahilinde ve ilgili Devlet otoritesinin memnuniyeti sağlanacak şekilde işlem yapmalarına ve bu olayları çözüme kavuşturmalarına izin verilen koşulları ve durumları belirten.

8.3.4.4 Emniyet yönetimi prensipleri kullanılarak, herhangi bir Devlet ile söz konusu Devletin hizmet sağlayıcıları arasındaki ilişkinin uyum ve yürütmenin ötesinde emniyet performansının sürdürülmesine veya sürekli olarak iyileştirilmesine yönelik bir ortaklığa dönüşmesi gerekir.

8.3.5 Spesifik çalışma düzenlemeleri

8.3.5.1 Başka bir Devletten düzenlemelerin uyarlanması veya benimsenmesi de dahil olmak üzere, spesifik çalışma düzenlemelerine (2 numaralı Kritik Unsur (CE-2)) ilişkin rehberliğe Doc 9734, Kısım A kapsamında ulaşılabilir.

Kural koyucu ve performansa dayalı düzenlemeler

8.3.5.2 Emniyet düzenlemeleri, Devletler tarafından emniyet risklerini kontrol etmek için kullanılabilen önemli bir araçtır. Emniyet yönetimine geçilmesiyle, performansa dayalı düzenlemelerin uygulamaya konmasına yönelik bir trend de meydana gelmiştir. Performansa dayalı düzenlemelerin neler olduğunu anlamak için öncelikle kural koyucu düzenlemelerin anlaşılması gerekir. Kural koyucu düzenlemeler, neyin yapılması ve nasıl yapılması gerektiğini açık bir şekilde ortaya koyan düzenlemelerdir. Bu düzenlemelere riayetin arzu edilen emniyet seviyesine ulaşması beklenir. Bir çok kural koyucu düzenleme bir kaza sonrasında oluşturulmuştur ve öğrenilen derslere ve gelecekte aynı sebeplerden dolayı herhangi bir kazanın meydana gelmesini önleme isteğine dayalıdır. Hizmet sağlayıcısının perspektifinden, kural koyucu gerekliliklerin karşılanması söz konusu düzenlemelerin sapma olmadan uygulanmasını gerektirir. Hizmet sağlayıcısından veya otoriteden herhangi bir başka analiz veya gerekçelendirme beklenmez.

8.3.5.3 Yakın geçmişe kadar ICAO Standartları ve Tavsiye Edilen Uygulamaları (SARP'lar), kural koyucu gerekliliklere, asgari standartların belirlenmesine ve birlikte çalışmanın sağlanmasına yönelik bir yol olarak odaklanmıştır. Bununla birlikte, performansa dayalı düzenlemelerin etkinlikleri geliştirebilecek olan ve emniyet amaçlarını karşılayabilen veya aşabilen yenilikçi uygulama yaklaşımlarını desteklemesinin sağlanmasına yönelik olarak giderek artan bir ihtiyaç söz konusudur.

8.3.5.4 Gerek kural koyucu gerek performansa dayalı düzenlemelere imkan veren Standartlara ilişkin örnekler ICAO Annex'lerinde belirtilmektedir. Aşağıda, Annex 14 — *Havaalanları*, Cilt I — *Havaalanı Tasarımı ve İşletimi* kapsamındaki, kural koyucu düzenlemelere imkan veren bir Standart örneği yer almaktadır:

> *3.3.1 Pist sonunda taksi yolunun veya taksi yolu dönüşünün bulunmadığı ve kod harfinin D, E veya F olduğu hallerde, uçakların 180 derecelik dönüşünü kolaylaştırmak için bir pist dönüş cebi sağlanacaktır.*

8.3.5.5 Pistin belirtilen kriterlerde olması halinde, pist dönüş cebinin sağlanması olmak üzere uyumun sağlanmasına yönelik sadece tek bir yol belirtmekte olması sebebiyle, bu örnekte kural koyucu bir düzenlemeye imkan verilmektedir. Kural koyucu düzenlemelerden farklılık genellikle, düzenlemelerden muafiyet tanınmasıyla verilir.

8.3.5.6 Bunun aksine, performansa dayalı düzenlemelere imkan veren Standartlar istenen sonuç bakımından ifade edilir. Ortaya çıkan performansa dayalı düzenlemeler, hizmet sağlayıcısı tarafından önerilen yaklaşımının istenen sonuca ulaşacağının kanıtlanmasını öngörür. Aşağıda, Annex 6, Kısım I kapsamındaki performansa dayalı bir Standart örneği mevcuttur.

> *7.2.11 Uçuşun herhangi bir aşamasında herhangi bir teçhizat kaleminin arızalanması halinde geri kalan teçhizatın söz konusu uçağın 7.2.1'e ve uygulanabildiği hallerde 7.2.2., 7.2.5 ve 7.2.6'ya uygun olarak seyrine imkan vermesinin sağlanması için uçak yeterli şekilde seyrüsefer teçhizatı ile donatılacaktır.*

8.3.5.7 Yukarıdaki Standardın gerekli spesifik seyrüsefer teçhizatını belirtmediği dikkate alınmalıdır. Bunun yerine, söz konusu Standartta istenilen sonuç, yani bir kalemin arızalanması halinde geri kalan teçhizatın söz konusu uçağın halen emniyetli bir şekilde seyrine imkan vermesi gerektiği açıklanmaktadır. Gerekli teçhizat, söz konusu uçağın tasarımına bağlı olacaktır. Bu şekilde yazılan düzenlemeler, söz konusu havayolu işletmesi tarafından bu gerekliliğe nasıl riayet edildiğinin gösterilmesi için otoriteye gerekli verilerin temin edilmesini gerektirecektir. Bu işlem, söz konusu havayolu işletmesinin kendi analizi vasıtasıyla yapılabilir, ancak bu tür performansa dayalı düzenlemeler için, ihtiyaç duyulan bilgiler genellikle başka kaynaklardan elde edilir. Bu durumda, gerek söz konusu otorite gerek havayolu işletmesi tarafından, kararın yönlendirilmesi için uçak imalatçılarından alınan veriler kullanılacaktır ve söz konusu havayolu işleticisi tarafından kendi yeni çözümünün geliştirilmesine gerek bulunmamaktadır. Performansa dayalı düzenlemeler yazılırken, Devletler tarafından riayetin nasıl kanıtlanabildiği unutulmamalıdır. Söz konusu Devlet için, sektörün söz konusu gerekliliğin karşılanmasında desteklenmesi için kılavuz materyal ve/veya kabul edilebilir uygulama yöntemlerinin oluşturulması gerekebilecektir.

8.3.5.8 Aşağıda, Annex 19'un 2. Ekinden başka bir performansa dayalı Standart örneği yer almaktadır.

> *2.1.1 Hizmet sağlayıcısı tarafından, kendi havacılık ürünleri veya hizmetleri ile ilişkili tehlikeleri tanımlayan bir süreç geliştirilecek ve muhafaza edilecektir.*

8.3.5.9 Yukarıdaki örnekte, söz konusu Standart kapsamında tehlikeleri tanımlamak için bir sürecin uygulanması öngörülmemekle birlikte, böyle bir sürecin neye benzemesi gerektiği belirtilmemektedir. Devletler tarafından hizmet sağlayıcılarına kendi metodolojilerinin tasarlanmasına izin verilebilir. Düzenleyici otoritenin rolü, söz konusu hizmet sağlayıcısının metodolojisinin, süreçlerinin ve sisteminin gerçekte tanımlanmakta olan tehlikelerle sonuçlanıp sonuçlanmayacağının değerlendirilmesi olacaktır. Söz konusu otorite tarafından aynı zamanda, tanımlanan tehlikelerin büyüklüğünün, türlerinin ve öneminin değerlendirilmesi gibi, hizmet sağlayıcısının tehlike tanımlama sürecinin performansına yönelik bir değerlendirme yapılacaktır. Bu şekilde yazılan performansa dayalı düzenlemeler, düzenleyici otoriteler tarafından, sadece düzenlemelerin metnine zorunlu riayetin değerlendirilmesinden ziyade, sistemin performansının değerlendirilmesine yönelik becerilere ve uzmanlığa sahip olunmasını gerektirir. Uygulamanın hizmet sağlayıcıları arasında değişiklik gösterecek olmasına bağlı olarak değerlendirme için daha fazla kaynak da gereklidir.

Kural koyucu ve performansa dayalı opsiyonların sunulması

8.3.5.10 Bazı hallerde, ICAO Standartları ve Tavsiye Edilen Uygulamaları (SARP'lar), kural koyucu düzenlemelerin tesis edilmesini ve aynı zamanda Devletlere alternatif uygulama yöntemlerini destekleyecek performansa dayalı düzenlemeleri tesis etme seçiminin sunulmasını öngörür. Devletler tarafından hem kural koyucu hem de performansa dayalı düzenleyici opsiyonların tesis edildiği hallerde, performansa dayalı düzenlemeleri karşılamak üzere kendi yaklaşımını oluşturma uzmanlığına sahip olmayan hizmet sağlayıcıları tarafından kural koyucu düzenlemelere riayet edilmesi seçilebilir. Böyle bir uzmanlığa sahip olan hizmet sağlayıcıları için, ortaya çıkan düzenlemeler, hizmet sağlayıcıları tarafından kendi operasyonlarına uygun olan uygulama yöntemlerinin oluşturulmasına imkan verecek ve aynı zamanda artan operasyonel esnekliğe ve kaynakların daha etkin bir şekilde kullanılmasına yönelik potansiyel sunabilecektir. Annex 6, Kısım I, tadil 43 kapsamındakiler gibi yorgunluk yönetimi Standartları bu konuda iyi bir örnek sunmaktadır:

> *4.10.1 İşleticinin Devleti tarafından yorgunluğun yönetilmesine yönelik düzenlemeler tesis edilecektir. Bu düzenlemeler, uçuş ve kabin ekibi üyeleri tarafından yeterli tetiklik düzeyinde görev yapılmasını sağlamak amacıyla bilimsel ilkelere, bilgiye ve operasyon tecrübesine dayalı olacaktır. Bu doğrultuda, İşleticinin Devleti tarafından;*
>
> *a) uçuş süresi, uçuş görev süresi, görev süresi sınırlamalarına ve istirahat süresi gerekliliklerine yönelik olarak kural koyucu düzenlemeler tesis edilecek ve*
>
> *b) işleticiye Yorgunluk Riski Yönetimi Sisteminin (FRMS) kullanılmasına izin verildiği hallerde, FRSM düzenlemeleri tesis edilecektir.*
>
> *4.10.2 İşleticinin Devleti tarafından işleticinin, 4.10.1'e uygun olarak ve yorgunluk ile ilgili emniyet risklerinin yönetilmesi amacıyla;*
>
> *a) İşleticinin Devleti tarafından tesis olunan kural koyucu yorgunluk yönetimi düzenlemeleri dahilinde olan uçuş süresi, uçuş görev süresi, görev süresi sınırlamaları ve istirahat süresi gerekliliklerinin tesis edilmesi veya*
>
> *b) tüm operasyonlar için 4.10.6'ya uygun olan bir Yorgunluk Riski Yönetimi Sisteminin (FRMS) tesis edilmesi veya*
>
> *c) operasyonlarının bir kısmı için 4.10.6'ya ve operasyonlarının geri kalanı için 4.10.2 a) gerekliliklerine uygun olan bir FRMS tesis edilmesi öngörülecektir.*

8.3.5.11 Yukarıdaki örnekte, söz konusu Standart kapsamında, Devletler tarafından kural koyucu uçuş ve görev sınırlaması düzenlemelerinin tesis edilmesi öngörülmekte iken FRMS'nin desteklenmesine yönelik düzenlemelerin tesis edilmesi opsiyoneldir. FRMS, söz konusu havayolu işletmesine kendisine özgü yorgunluk risklerini daha iyi bir şekilde ele alma imkanı vermekte ve aynı zamanda, kural koyucu uçuş ve görev sınırlaması düzenlemeleri dışında operasyonel esneklik potansiyeli sunmaktadır. Devletler tarafından, zorunlu kural koyucu sınırlama düzenlemelerine alternatif olarak FRMS düzenlemelerinin sunulmasının gerekli olup olmadığı ve FRMS'ye ilişkin olarak uygun gözetim sunulması için gerekli kaynaklara sahip olup olunmadığı değerlendirilmelidir. 4.10.2 Standardı, bunun akabinde, havayolu işletmelerinin kendilerinin yorgunlukla ilgili emniyet risklerini yönetmelerinin gerektiğini açıklamaya geçmektedir. FRMS düzenlemelerinin tesis edildiği hallerde, 4.10.2(a) kapsamında belirtilen kural koyucu sınırlama düzenlemeleri dahilinde veya 4.10.2(b) ve (c) kapsamında belirtilen performansa dayalı FRMS uygulanarak bu şekilde hareket edilebilir. FRMS oluşturma uzmanlığına sahip olmayan ve ilişkili düzenleyici gereklilikleri karşılamayan havayolu işletmeleri tarafından kural koyucu düzenlemelere riayet edilmesi gerekecektir.

8.3.5.12 Performansa dayalı düzenlemelerin daima uygun olmadığı aşikar olmalıdır. Koruyucu gereklilikler, birlikte çalışabilirliği kolaylaştırmak için olması gibi, standart hale getirilmiş uygulama yöntemleri gerekli olduğunda uygun olmaya devam ederler. Örneğin, pist işaretlemelerine yönelik gereklilikler doğası gereği mutlaka kural koyucudur.

8.3.5.13 Uygulamada, düzenlemeler nadiren tümüyle kural koyucu veya tümüyle performansa dayalıdır, daha ziyade her ikisinin unsurlarını içerirler. Aynı zamanda, farklı derecelerde performansa dayalıdırlar. Herhangi bir Devlet tarafından performansa dayalı düzenlemelerin uygulanması düşünüldüğünde, söz konusu Devlet tarafından, endüstrinin kabiliyeti ve olgunluğu, endüstrinin spesifik sektörleri ve hatta münferit hizmet sağlayıcılarının olgunluğu ve Emniyet Yönetim Sistemleri (SMS) göz önünde bulundurulmalıdır. Performansa dayalı düzenlemeler aynı zamanda, riayete yönelik kontrolün yanı sıra, her bir hizmet sağlayıcısının spesifik operasyon bağlamını dikkate alarak sistemleri değerlendirebilmesini ve emniyet performansına yönelik değerlendirme yapabilmesini öngörerek düzenleyici otoriteden çok şey isterler. Devletler, daha yüksek seviyelerde uzmanlığın yanı sıra daha fazla kaynağın gerekli olduğu göz önünde bulundurularak endüstriyi gözetmeye ve yönetmeye devam edebildiklerinden emin olmalıdırlar. Emniyet Yönetimi Sistemi (SMS), hizmet sağlayıcıları için performansa dayalı düzenlemelerin karşılanmasına yönelik bir temel ve araçlar sunmakla birlikte, Emniyet Yönetimi Sistemine (SMS) sahip olan her hizmet sağlayıcısının bu kabiliyete sahip olduğu yönünde otomatik bir güvence teşkil etmez. İş, spesifik performansa dayalı gerekliliğin taleplerine bağlıdır.

8.3.5.14 Performansa dayalı düzenlemeler aynı zamanda yürütme üzerinde etkiye sahiptirler. Riayetsizliğin kolaylıkla tespit edilebilmesi sebebiyle, kural koyucu düzenlemelerin yürütülmesi ileri yönlüdür. Performansa dayalı düzenlemeler bakımından yürütme daha zorludur. Örneğin, herhangi bir hizmet sağlayıcısı, söz konusu düzenlemeyi karşılayan bir süreci uygulamakta olduğunu gösterebilecektir (örneğin, uygulanmakta olan bir tehlike raporlaması sistemine sahip olması), ancak söz konusu sürecin amaçlanan sonucu ortaya koyabildiğini gösterememektedir (örneğin, söz konusu tehlike raporlaması sisteminin etkin olup olmadığı). Bu, sadece "kanun metnini" karşılayan ancak öngörülen emniyet sonucunu ortaya koymayan sistemlerin veya süreçlerin tesis edilmesine yol açabilecektir. Düzenleyici otoriteler tarafından, uygulanabilirliklerini sağlamak üzere, performansa dayalı düzenlemelerin oluşturulmasında ilgili yürütme kurumlarının dahil edilmesi gerekecektir.

8.3.6 Devlet sistemi ve işlevleri

8.3.6.1 Devlet sistemine ve işlevlerine (3 numaralı kritik unsur (CE-3) ilişkin rehberliğe Doc 9734, Kısım A kapsamında ulaşılabilir.

Devlet Emniyet Programının (SSP) koordinasyonundan sorumlu organizasyon

8.3.6.2 Devletin emniyet yönetimi sorumlulukları, söz konusu Devlet dahilindeki birden fazla havacılık otoritesi, örneğin, Sivil Havacılık Otoritesi (CAA) ve bağımsız Kaza Soruşturma Otoritesi (AIA) tarafından yerine getirilebilir. Devletler tarafından, Devlet Emniyet Programının (SSP) sürdürülmesinin ve uygulanmasının koordinasyonundan söz konusu Devlet dahilindeki hangi otoritenin sorumlu olduğu açıklığa kavuşturulmalıdır. Sivil Havacılık Otoritesinin (CAA) normalde çoğu Devlet Emniyet Programı (SSP) sorumluluklarından sorumlu olduğu göz önünde bulundurularak bu görev bir çok Devlet tarafından Sivil Havacılık Otoritesine (CAA) verilir. Dahil olan tüm otoritelerin görevleri ve sorumlulukları belirlenmeli ve belgelenmelidir.

Devlet Emniyet Programı (SSP) koordinasyon grubu

8.3.6.3 Söz konusu Devlet tarafından, Kaza Soruşturma Otoritelerinin yanı sıra askeri havacılık otoriteleri de dahil olmak üzere, Devlet Emniyet Programının (SSP) uygulanmasına ve sürdürülmesine ilişkin sorumluluklara sahip olan, etkilenen havacılık otoritelerinden temsil ile uygun bir koordinasyon grubu oluşturulmalıdır. Koordinasyon grubunun tayini, iyi iletişimi kolaylaştıracak, mükerrer çalışmayı ve çatışan politikaları önleyecek ve Devlet Emniyet Programının (SSP) etkili ve verimli bir şekilde uygulanmasını sağlayacaktır. Söz konusu grup, Devlet Emniyet Programının (SSP) koordinasyonundan sorumlu olan organizasyonun başkanı tarafından başkanlık edilen bir tür komitedir.

8.3.6.4 Söz konusu Devlet tarafından aynı zamanda, Devlet Emniyet Programının (SSP) uygulanmasının günlük planlamasının ve yönetiminin bir kişiye, departmana veya ekibe tahsis edilmesi faydalı bulunabilir. Söz konusu kişi, departman veya ekip, Devletin emniyet amaçlarının ortaya konulması için çeşitli unsurların birlikte çalışmasını sağlayabilir.

Devlet Emniyet Programı (SSP) işlevleri ve faaliyetleri

8.3.6.5 Annex 19'a uygun olarak hizmet sağlayıcıları tarafından Emniyet Yönetimi Sisteminin (SMS) uygulanmasının kabulüne ve izlenmesine işaret etmek üzere iş gücünün ve organizasyon yapısının nasıl Devletler nasıl düzenlendiği, her Devlet için karara bağlanması gereken bir husustur. Devletler, yeni bir daire oluşturmayı veya bu sorumluluğu, uçuşa elverişlilik dairesi, uçuş işletme dairesi, hava seyrüsefer ve havaalanı dairesi gibi mevcut dairelerin sorumluluklarına eklemeyi seçebilirler. Bu karar, söz konusu Devletin yeni yetkinlik gerekliliklerini ele almayı nasıl seçtiğine bağlı olacaktır.

8.3.6.6 Görevlerin açıklığa kavuşturulması çeşitli havacılık otoriteleri için önem arz etmektedir. Devlet Emniyet Programı (SSP) yükümlülüklerinin, işlevlerinin ve faaliyetlerinin tümü buna dahil olmalıdır. Söz konusu Devlet, en önemlisi söz konusu Devlette emniyetin yönetilmesine yönelik sorumluluğu olmak üzere, her bir Annex 19 gerekliliğinin karşılanmasına yönelik katkısının her bir otorite tarafından anlaşılmasını sağlamalıdır. Muğlaklığın önlenmesi için her bir havacılık otoritesinin Devlet Emniyet Programının (SSP) uygulanmasına ilişkin yükümlülükleri ve işlevleri belgelenmelidir.

8.3.6.7 Emniyete dahil olan personelin coğrafi olarak dağıtıldığı Devletlerde uygun yönetişim yapıları olmalıdır. Emniyet yönetimine az sayıda kişinin dahil olduğu daha az karmaşık havacılık sistemleri için karmaşık bir yönetişim yapısı gerekli olmayabilir. Söz konusu Devlet tarafından tüm personelin ulusal seviyede Devlet Emniyet Programının (SSP) uygulanmasına yönelik aynı anlayışa sahip olması sağlanmalıdır. Devlet Emniyet Programına (SSP) ilişkin uygulama yaklaşımı belgelenmelidir.

Devlet emniyet politikası ve emniyet amaçları

8.3.6.8 Devlet Emniyet Programının (SSP) etkin bir şekilde uygulanması, söz konusu Devletin üst yönetiminin taahhüdünü ve tüm seviyelerdeki personelin desteğini gerektirir. Devlet emniyet politikaları ve Devlet emniyet amaçları, söz konusu Devletin havacılık otoriteleri tarafından onaylanan üst düzey beyanlardır. Birleştirildiklerinde, emniyet davranışını ve kaynak tahsisatını yönlendirirler. Söz konusu Devlet için yerinde ve uygun halde kalmaya devam etmelerini sağlamak üzere, Devlet emniyet politikası ve amaçları periyodik olarak yayınlanmalı ve gözden geçirilmelidir.

Devlet emniyet politikası

8.3.6.9 Üst yönetimin taahhüdünün Devlet emniyet politikasında açık bir şekilde ifade edilmesi gerekir. Devlet emniyet politikası, söz konusu Devletin emniyet gayelerini ve yönünü açıklayan resmi bir belgedir. Devlet emniyet politikası, üst yönetimin emniyete ve söz konusu Devlette pozitif emniyet kültürünün teşvik edilmesine yönelik tutumunu yansıtır. Söz konusu Devletin emniyet misyonu ve vizyon bildirisi olarak düşünülebilir.

8.3.6.10 Emniyet politikasında, emniyet yönetimi için elzem olan kilit uygulamaların ve üst yönetim tarafından emniyet sorumluluklarının nasıl ortaya konmasının beklendiğinin (örneğin, veriye dayalı yaklaşımın kullanımı) ele alınması gerekir. Emniyet politikasında yansıtılan prensiplerin, söz konusu Devletin günlük uygulamalarında açık bir şekilde görünür olması gerekir.

8.3.6.11 Devlet emniyet politikası, emniyet niyetini kanıtlamak için Devlet havacılık otoriteleri tarafından onaylanır ve bir prosedür veya protokol olarak uygulanır. Aşağıda tipik bir politika beyanı verilmektedir: "Emniyete, (1) emniyetli koşullara ve davranışlara yönelik sorumluluğumuzu kabul ederek (2) emniyet liderliği, ortak çalışma, açık iletişim, vb. kültürü ile ulaşacağız."

Devlet emniyet amaçları

8.3.6.12 Emniyet amaçlarının oluşturulması, havacılık sistemindeki en yüksek emniyet risklerinin açık bir şekilde kavranmasıyla başlar. Havacılık sistemindeki emniyet riski, havacılık sisteminin boyutu ve karmaşıklığı ile çalışma ortamı gibi birçok farklı etkenden etkilenir. İyi bir sistem tanımının oluşturulması iyi bir geri plan ve kavrama sağlayacaktır. Bu bölümün 8.7 maddesindeki Devlet Emniyet Programının (SSP) uygulanmasını referans alınız.

8.3.6.13 En üst emniyet risklerine yönelik anlayışın oluşturulması için, mevcut olduğunda, kantitatif verilerin kullanılması gerekir. Kantitatif bilgiler ve uzman analizi Devlet tarafından da kullanılabilir. Havacılık sisteminin genelindeki geniş kapsamlı emniyet risklerinin anlaşılması için yönlendirilen tartışmalara katılmak üzere seçilmiş bir uzmanlar grubu oluşturulabilir. Bu grup, bu kez Devlet seviyesinde olmak üzere, 9. Bölümün 9.3.6 Maddesi kapsamında ele alınan hizmet sağlayıcısının emniyet gözden geçirme kurulu (SRB) ile benzer bir role sahip olacaktır. Bu uzmanlar, mevcut emniyet trendi bilgileri, bilinen kazalar ve ciddi olaylar, katkıda bulunan faktörler veya söz konusu Devletin Devlet Emniyet Gözetimi (SSO) süreçlerindeki bilinen eksiklikler ile yönlendirilebilir. Aynı zamanda, Global Havacılık Emniyeti Planı (GASP) kapsamında tanımlanan global amaçları veya bölgesel amaçları değerlendirebilirler. Her bir havacılık sektörüne ilişkin "bilinen" emniyet sorunlarını tanımlamak için hizmet sağlayıcıları ile ortaklaşa biçimde beyin fırtınası türü yaklaşım uygulanabilir.

8.3.6.14 Devlet emniyet amaçları, tüm ilgili Devlet havacılık otoriteleri için yönlendirme sağlayan kısa ve öz, üst seviye beyanlardır. Söz konusu Devlet tarafından ulaşılması amaçlanan istenilen emniyet sonuçlarını temsil ederler. Emniyet amaçlarını tanımlarken söz konusu Devletin istenilen sonuçlara etki etme kabiliyetinin göz önünde bulundurulması da önem arz eder. Emniyet amaçları, emniyetin yönetilmesine yönelik olarak söz konusu Devletin önceliklerini temsil eder ve söz konusu Devletin kaynaklarının tahsis edilmesine ve yönlendirilmesine yönelik bir model sunarlar.

8.3.6.15 Emniyet amaçları, söz konusu Devletin Emniyet Performansı Göstergelerinin (SPI'ler) ve Emniyet Performansı Hedeflerinin (SPT'ler) tanımlanmasını ve akabinde, bu Bölümün ileriki kısımlarında ele alınan kabul edilebilir emniyet performansı seviyesinin (ALoSP) oluşturulmasını desteklerler. Emniyet amaçları, söz konusu Devlet tarafından emniyet performansının izlenmesini ve ölçülmesini sağlamak üzere Emniyet Performansı Göstergeleri (SPI'ler) ve Emniyet Performansı Hedefleri (SPT'ler) ile bir paket olarak birlikte çalışırlar. Emniyet Performansı Göstergelerine (SPI'ler) ve Emniyet Performansı Hedeflerine (SPT'ler) ilişkin daha fazla rehberliğe 4. Bölüm kapsamında ulaşılabilir.

8.3.6.16 Devlet Emniyet Programının (SSP) uygulanmasına müteakiben, Devlet Emniyet Programı (SSP) tarafından üretilen emniyet bilgileri analiz edilerek söz konusu Devlet tarafından tanımlanan emniyet risklerinin periyodik olarak yeniden değerlendirilmesi gerekir. Bu analiz aynı zamanda ortaya yeni çıkan sorunların tanımlanmasını destekleyecektir. Emniyet analizine ilişkin rehberliğe 6. Bölüm kapsamında ulaşılabilir. Güncel risklere ilişkin yeniden değerlendirmeler göz önünde bulundurularak, söz konusu Devlet tarafından emniyet amaçlarına ulaşılmasına yönelik ilerleme ve bu amaçların sürekli yerindeliği periyodik olarak gözden geçirilmelidir.

Devlet emniyet kaynakları

8.3.6.17 Söz konusu Devlet tarafından, emniyet sorumluluklarına sahip olan kurumlara salahiyetlerini hayata geçirmek için yeterli kaynakların verilmesi sağlanmalıdır. Mali kaynakların yanı sıra insan kaynakları da buna dahildir.

8.3.6.18 Bazı havacılık otoriteleri, Devlet tarafından tahsis edilen bütçeye dayalı olarak finansman alırlar. Diğerleri ise, havacılık sistemine katılanlardan (lisans ve onay ücretleri gibi) veya havacılık sistemi dahilindeki hizmetleri kullananlardan (örneğin yolculara veya yakıta uygulanan vergiler) tahsil edilen ücret ve harçlarla finanse edilirler. Söz konusu Devlete en uygun olan finansman kaynağı, söz konusu Devletin içerisinde bulunduğu koşullara bağlıdır. Örneğin, küçük bir havacılık endüstrisine sahip olan herhangi bir Devlet, düzenleyici faaliyetlerinin finanse edilmesi için Sivil Havacılık Otoritesi (CAA) tarafından sadece ücretlere ve harçlara dayanılmasını yeterli bulmayabilir. Devletin, havacılık faaliyetlerini finanse etmek için birden fazla kaynağa ihtiyacı olabilir.

8.3.6.19 Herhangi bir Devlet tarafından Devlet Emniyet Programının (SSP) tümüyle uygulanmaya ve emniyet yönetimi uygulamalarını benimsenmeye başlanmasıyla, söz konusu Devletin yeterli bir gelir akışına sahip olmaya devam etmesini sağlamak için bütçesini ve finansmanını tekrar değerlendirmesi gerekebilir. Örnek olarak Emniyet Riski Yönetimi (SRM), verilerin toplanması ve analiz edilmesi ve emniyetin teşvik edilmesi de dahil olmak üzere, emniyet yönetimi yaklaşımının başarılı olabilmesi için yeni işlevler uygulamaya konulur ve iradenin sürdürülmesi gerekir. Emniyet yönetimi aynı zamanda söz konusu Devletin havacılık otoritelerinin riskin yönetilmesine yönelik olarak kendi süreçlerini sürekli olarak izleyebilmesini ve gözden geçirebilmesini gerektirir. Denetçilerin ve diğer personelin yeniden eğitime tabi tutulmaları gerekebilir. Böylelikle, söz konusu Devlet, emniyet yönetimi yaklaşımına geçiş yapılırken Devlet kurumları için yeterli mali kaynakların tahsis edilmesini gerekli bulabilir.

Ulusal Havacılık Emniyet Planı (NASP)

8.3.6.20 Emniyete yönelik ICAO global planlamasına ilişkin A39-12 sayılı genel kurul kararı kapsamında, ulusal havacılık emniyeti planlarının etkin bir şekilde uygulanmasının önemi kabul edilmektedir. Söz konusu kararda, Devletler tarafından Global Havacılık Emniyeti Planının (GASP, Doc 10004) hedefleri doğrultusunda ulusal havacılık emniyeti planlarının oluşturulmasına ve uygulanmasına hükmedilmektedir. Uluslararası seviyede, Global Havacılık Emniyeti Planı (GASP), havacılık emniyetinin önceliklendirilmesini ve sürekli olarak iyileştirmesini destekleyen bir strateji ortaya koymaktadır. Bölgesel ve ulusal havacılık emniyet planlarının Global Havacılık Emniyeti Planına (GASP) uyumlu olarak oluşturulması gerekir.

8.3.6.21 Bölgesel seviyede, planlama süreci, bölgesel havacılık emniyeti grupları (RASG'ler) tarafından koordine edilir. İlgili Devletler tarafından karşılaşılan sorunlara dayalı olarak bölgesel ve ulusal emniyet iyileştirme inisiyatifleri (SEI'ler) uyarlanmalıdır. Ulusal havacılık emniyeti planı, belirli bir süre boyunca (örneğin, önümüzdeki beş yıl boyunca), ulusal seviyede havacılık emniyetinin yönetilmesine yönelik stratejik bir yönlendirme sunar. Tüm paydaşlara, Devlet havacılık otoriteleri tarafından gelecek yıllarda kaynakların nerelere hedeflenmesi gerektiğini ana hatlarıyla belirtir.

8.3.6.22 Ulusal havacılık emniyeti planı, söz konusu Devlet tarafından ulusal seviyede emniyetin iyileştirilmesine yönelik stratejisinin, diğer hükümet bölümleri ve seyahat eden halk da dahil olmak üzere, tüm paydaşlara açık bir şekilde bildirilmesine imkan verir. Sivil Havacılık Otoritelerinin (CAA'lar) ve sivil havacılığa dahil olan diğer kuruluşlar tarafından tehlikelerin tanımlanması ve operasyonel emniyet risklerinin ve diğer emniyet sorunlarının yönetilmesi için nasıl çalışacaklarının açıklanmasına yönelik şeffaf bir yol sunar. Aynı zamanda, planlanan Emniyet İyileştirme İnisiyatiflerinin belirlenen hedeflerin karşılanmasında söz konusu Devlete nasıl yardımcı olacağını açıklar. Ulusal havacılık emniyeti planı, söz konusu Devletin havacılık emniyetine yönelik taahhüdünü vurgular.

8.3.6.23 Her bir Devlet tarafından bir ulusal havacılık emniyeti planı oluşturulmalıdır. Herhangi bir Devletin halihazırda uygulanmakta olan herhangi bir Devlet Emniyet Programına (SSP) sahip olması halinde, ulusal havacılık emniyeti planı 1. Bileşen - Devlet emniyet politikası, amaçlar ve kaynaklar - kapsamında ele alınabilir. Ulusal havacılık emniyeti planı, kamu ve Sivil Havacılık Otoritesi (CAA) dışındaki diğer kuruluşlarla iletişimin kolaylaştırılması için ayrı bir üst seviye doküman olarak yayınlanmalıdır.

Devlet Emniyet Programı (SSP) Dokümantasyonu

8.3.6.24 Söz konusu Devlet, tüm ilgili personelin ortak bir anlayışa sahip olmasını sağlamak için Devlet Emniyet Programını (SSP) bir doküman kapsamında açıklamalıdır. Söz konusu dokümanda, dokümanın yapısı ve ilişkili programları, çeşitli bileşenlerle nasıl birlikte çalıştığı ve farklı Devlet havacılık otoritelerinin rolleri yer almalıdır. Dokümantasyonun, mevcut süreçleri ve prosedürleri tamamlaması ve emniyetin iyileştirilmesi için çeşitli Devlet Emniyet Programı (SSP) alt programlarının birlikte nasıl çalıştığı geniş kapsamlı olarak tanımlanmalıdır. Dokümantasyonun desteklenmesinde otoritelerin emniyet sorumluluklarına ve mesuliyetlerine ilişkin çapraz referanslara da yer verilebilir. Söz konusu Devlet tarafından, fiziki bir dokümanda veya uygun bir şekilde kontrollü bir web sitesinde olması gibi, ortamı için en elverişli olacak bir dokümantasyon ve dağıtım yöntemi seçilmelidir. İletişim kanalına bakılmaksızın, buradaki amaç, tüm ilgili personel tarafından Devlet Emniyet Programına (SSP) ilişkin ortak bir anlayışın kolaylaştırılmasıdır.

8.3.7 Kalifiye teknik personel

8.3.7.1 Emniyet ile ilgili işlevleri icra eden kalifiye teknik personele (4 numaralı kritik unsur (CE-4)) ilişkin rehberliğe Doc 9734, Kısım A kapsamında ulaşılabilir.

Genel rehberlik

8.3.7.2 Devletlerin, personelleri tarafından icra edilen Devlet Emniyet Programı (SSP) kapsamındaki görevleri ve sorumlulukları göz önünde bulundurularak Devlet Emniyet Programının (SSP) etkili bir şekilde uygulanması için gerekli olan yetkinlikleri belirlemeleri ve ele almaları gerekmektedir. Bu yetkinlikler, uyum gözetiminin icrası için gerekli olanlara ilaveten olup, mevcut personelin eğitime tabi tutulması veya ilave personelin işe alınması suretiyle ele alınabilecektir ve bunlarla sınırlı kalmamak üzere aşağıdakileri içerir:

a) geliştirilmiş liderlik becerileri;

b) iş süreçlerinin anlaşılması;

c) performansın ve etkinliğin değerlendirilmesi için gerekli deneyim ve muhakeme;

d) emniyet riskine dayalı gözetim;

e) emniyet verilerinin toplanması ve analiz edilmesi;

f) emniyet performansı ölçümü ve izlemesi ve

g) emniyeti teşvik faaliyetleri.

8.3.7.3 Güçlü bir denetim iş gücünün geliştirilmesine ve sürdürülmesine ilişkin rehberliğe *Sivil Havacılık Emniyet Denetçilerinin Yetkinliklerine ilişkin El Kitabı* (Doc 10070) kapsamında ulaşılabilir.

8.3.7.4 Söz konusu Devlet tarafından, organizasyonda farklı görevlere ve sorumluluklara sahip olan personel için en uygun eğitimin tespit edilmesi gerekir. Değerlendirilmesi gereken eğitim türlerine ilişkin örnekler şunlardır:

a) Devlet Emniyet Programına (SSP), Emniyet Yönetimi Sistemine (SMS), emniyet politikasına, amaçlara ve kabul edilebilir emniyet performansı seviyesine (ALoSP) ilişkin olarak üst yönetime yönelik brifingler veya alıştırma eğitimi;

b) Devlet Emniyet Programı (SSP) ve Emniyet Yönetimi Sistemi (SMS) prensiplerine, Emniyet Yönetimi Sistemi (SMS) değerlendirmelerinin nasıl gerçekleştirileceğine, herhangi bir hizmet sağlayıcısının Emniyet Performansı Göstergelerinin (SPI'ler) kabul için nasıl değerlendirilmesi gerektiğine ve hizmet sağlayıcısının emniyet yönetimi ortamında genel olarak nasıl denetleneceğine ilişkin olarak denetçilere yönelik eğitim;

c) tesis edilen düzenlemelere sürekli riayet sağlanırken emniyet performansının iyileştirilmesi için hizmet sağlayıcıları ile ortaklaşa çalışılmasında denetçilere destek verilmesine yönelik teknik olmayan eğitim (etkili iletişim becerileri, müzakere becerileri, çatışma çözümü, vb.);

d) veri analizinden, emniyet amaçlarından, Emniyet Performansı Göstergelerinden (SPI'ler) ve Emniyet Performansı Hedeflerinden (SPT'ler) sorumlu olan personele yönelik eğitim;

e) havacılık tıp doktorlarına ve tıbbi durum değerlendiricilerine yönelik eğitim;

f) hukuk personeli, vb. için emniyet verilerinin, emniyet bilgilerinin ve ilgili kaynakların korunmasına ve yürütme politikasına ilişkin eğitim ve

g) hizmet sağlayıcısı emniyet soruşturmacılarına yönelik Devlet Emniyet Programı (SSP) ve Emniyet Yönetimi Sistemi (SMS) eğitimi.

8.3.7.5 Devlet Emniyet Programı (SSP) ile ilgili görevlerde bulunan personele yönelik emniyet eğitimi programları, Devlet organizasyonları arasında, uygun görüldüğü şekilde, koordine edilmelidir. Devlet Emniyet Programı (SSP) ve Emniyet Yönetimi Sistemi (SMS) eğitiminin veya alıştırmanın kapsamı, gerçek Devlet Emniyet Programı (SSP) süreçlerini ve gelişmesine ve olgunlaşmasına bağlı olarak Devlet Emniyet Programının (SSP) kendisini yansıtmalıdır. Başlangıç Devlet Emniyet Programı (SSP) ve Emniyet Yönetimi Sistemi (SMS) eğitimi, genel Devlet Emniyet Programı (SSP) unsurlarıyla veya Emniyet Yönetimi Sistemi (SMS) çerçevesi unsurları ve rehberliğiyle sınırlı olabilir.

8.3.7.6 Tüm ilgili teknik personelin uygun bir şekilde eğitime tabi tutulmasını sağlamak için, söz konusu Devlet tarafından;

a) kurum içi eğitim politikaları ve prosedürleri geliştirilmeli ve

b) ilgili personel için bir Devlet Emniyet Programı (SSP) ve Emniyet Yönetimi Sistemi (SMS) eğitim programı oluşturulmalıdır. Devlet Emniyet Programı (SSP)-Emniyet Yönetimi Sistemi (SMS) uygulama personeline ve hizmet sağlayıcılarının Emniyet Yönetimi Sistemlerinin (SMS) gözetimine / izlenmesine dahil olan operasyon/saha denetçilerine öncelik verilmelidir (Devlete özgü Devlet Emniyet Programı (SSP) süreçleri ve bu süreçlerin yerindeliği de dahil olmak üzere).

8.3.7.7 Online kurslar, sınıf kursları, atölyeler vb. de dahil olmak üzere, bir çok farklı türden Devlet Emniyet Programı (SSP) ve Emniyet Yönetimi Sistemi (SMS) eğitimi mevcuttur. Sunulan eğitimin türü ve miktarı, ilgili personel tarafından görevlerinin ifası için ihtiyaç duyulan yetkinliğin oluşturulmasını ve Devlet Emniyet Programına (SSP) yönelik katkılarının anlaşılmasını sağlamalıdır. Buradaki amaç, herhangi bir kişi veya ekip tarafından Devlet Emniyet Programının (SSP) her bir yönünün ele alınmasını ve bunların kendilerine verilen görevi ifa etmek üzere eğitimli olmalarını sağlamaktır.

8.3.7.8 Denetçilere yönelik uygun ve yeterli eğitim tutarlı gözetimi ve gerekli görülen kabiliyetlerin emniyet yönetimi ortamında etkin olmasını sağlayacaktır. Devletler tarafından aşağıdakilerin göz önünde bulundurulması gerekir:

a) Hizmet sağlayıcılarının Emniyet Yönetimi Sistemlerinin (SMS) gözetimi ve izlenmesi, Emniyet Yönetimi Sistemi (SMS) gerekliliklerinin uygulamaya konması öncesinde kritik olmayabilecek yetkinlikler gerektirecektir. Denetçilerin, hizmet sağlayıcılarının Emniyet Yönetimi Sistemlerinin (SMS) uygulanmasının uygunluğunu ve etkinliğini değerlendirmek için mevcut teknik bilgilerini ilave becerilerle tamamlamaları gerekecektir. Bu yaklaşım, emniyet verilerinin ve emniyet bilgilerinin paylaşılmasını kolaylaştırmak üzere hizmet sağlayıcılarının güveninin kazanılması için endüstri ile ortak çalışmayı gerektirir. Devletlerin, endüstri ile olan etkileşimden sorumlu personelin Emniyet Yönetimi Sistemi (SMS) ortamında gözetim faaliyetlerini ifa etmek üzere yetkinliklere ve esnekliğe sahip olmasının sağlanması için uygun eğitim vermeleri gerekecektir. Uygun eğitimin belirlenmesi için eğitim ihtiyaçları analizi kullanılabilir.

b) Söz konusu eğitimin aynı zamanda, personelde, kendi havacılık otoritelerinin bünyesindeki diğer departmanların ve diğer Devlet havacılık otoritelerinin görevlerine ve katkılarına yönelik bir farkındalık oluşturması gerekir. Bu sayede, denetçilerin yanı sıra farklı Devlet havacılık otoritelerinden personelin tutarlı bir yaklaşıma sahip olmalarına imkan verilecektir. Ayrıca, çeşitli sektörler genelinde emniyet risklerinin daha iyi bir şekilde anlaşılması kolaylaştırılacaktır. Denetçiler aynı zamanda, Devlet emniyet amaçlarına ulaşılmasına nasıl katkı sağladıklarını daha iyi bir şekilde anlayabilirler.

8.3.8 Teknik kılavuzluk, araçlar ve emniyet bakımından kritik bilgilerin sağlanması

8.3.8.1 Teknik kılavuzluğa, araçlara ve emniyet bakımından kritik bilgilerin sağlanmasına (5 numaralı kritik unsur (CE-5)) ilişkin rehberliğe Doc 9734, Kısım A kapsamında ulaşılabilir.

8.3.8.2 Söz konusu Devlet tarafından, emniyet yönetimi düzenlemelerinin yorumlanmasına yardımcı olunmak üzere denetçilere ve hizmet sağlayıcılarına kılavuzluk sağlanması düşünülmelidir. Bu sayede, pozitif emniyet kültürü teşvik edilecek ve hizmet sağlayıcısına, kendi emniyet amaçlarının ve sonrasında, genellikle düzenleme vasıtasıyla ulaşılan Devletin emniyet amaçlarının karşılanmasında yardım sağlanacaktır. Emniyet Yönetimi Sisteminin (SMS) değerlendirilmesi, hizmet sağlayıcılarının Emniyet Yönetimi Sistemlerinin (SMS) uygunluğunun ve performansının tespit edilmesi için ilave araçlar gerektirebilir. Geliştirilen araçlar, uygulanması öncesinde, etkilenen personele yönelik eğitim gerektirecektir.

8.4 2. BİLEŞEN: DEVLET EMNİYET RİSKİ YÖNETİMİ

8.4.1 Devletlerin, havacılık sistemindeki olası emniyet risklerini saptamaları gerekir. Söz konusu Devlet tarafından, herhangi bir kazanın veya olayın sebeplerinin analiz edilmesine ilişkin geleneksel yöntemlerin bunun başarılmasına yönelik proaktif süreçlerle arttırılması gerekir. Proaktif süreçler, söz konusu Devlet tarafından kazaların öncüllerinin ve kazalara katkıda bulunanların ele alınmasına ve emniyet iyileştirmelerinin azami hale getirilmesine yönelik olarak emniyet kaynaklarının stratejik bir şekilde yönetilmesine imkan verir. Devletler tarafından;

a) havacılık ile ilgili faaliyetlerinin emniyetinin yönetilmesi ve iyileştirilmesi için hizmet sağlayıcıları tarafından Emniyet Yönetimi Sisteminin (SMS) uygulanması öngörülmeli;
b) hizmet sağlayıcılarının Emniyet Riski Yönetiminin (SRM) kabul edilebilir olup olmadığının tespit edilmesine yönelik yollar tesis edilmeli ve
c) söz konusu hizmet sağlayıcısının Emniyet Yönetimi Sistemi (SMS) gözden geçirilmeli ve etkin olduğundan emin olunmalıdır.

8.4.2 Devlet Emniyet Riski Yönetimi (SRM) bileşeni, tehlike tanımlama süreçleri ve ilişkili emniyet risklerinin yönetilmesi de dahil olmak üzere, hizmet sağlayıcıları tarafından Emniyet Yönetimi Sisteminin (SMS) uygulanmasını kapsar.

8.4.3 Devletler tarafından aynı zamanda Emniyet Riski Yönetimine (SRM) ilişkin prensiplerin kendi faaliyetleri için de uygulanması gerekir. Düzenlemelerin oluşturulması ve değerlendirilen riske dayalı olarak gözetim faaliyetlerinin önceliklendirilmesi gibi faaliyetler buna dahildir.

8.4.4 Diğer kuruluşlarla olan arayüzler vasıtasıyla başlatılan emniyet riski, hizmet sağlayıcıları ve düzenleyici otoriteler tarafından genellikle gözden kaçırılan bir alandır. Devlet Emniyet Programı (SSP) ve Emniyet Yönetimi Sistemi (Sistemleri) (SMS) (SMS'ler) arasındaki arayüz, Devletler ve hizmet sağlayıcıları için belirli bir arayüz zorluğu teşkil edebilir. Söz konusu Devlet tarafından, kendi düzenlemeleri ve destekleyici rehberliği vasıtasıyla Emniyet Yönetimi Sistemi (SMS) arayüz riski yönetiminin öneminin vurgulanması değerlendirilmelidir. Arayüz riskine ilişkin örnekler şunlardır:

a) Bağımlılık — A organizasyonunun, malların veya hizmetlerin sunulması için B organizasyonuna bağımlı olması. B organizasyonunun beklenti ve A organizasyonunun bağımlılığı bakımından net olmaması ve teslimatı yapmaması.

b) Kontrol — arayüz bağlantısına sahip olan organizasyonlar genellikle, arayüz bağlantılı olan organizasyonun (organizasyonların) niteliğinin veya etkinliğinin minimal kontrolüne sahiptirler.

8.4.5 Bu olayların her ikisinde de arayüz riski yönetimi söz konusu riski aydınlığa kavuşturabilir, karşılıklı beklentileri açıklığa kavuşturabilir ve karşılıklı olarak kararlaştırılan sınır kontrolleri vasıtasıyla istenmeyen sonuçları hafifletebilir. Hizmet sağlayıcıları arasındaki arayüzlere ilişkin ilave bilgilere 2. Bölüm kapsamında ulaşılabilir.

8.4.6 Lisanslandırma, sertifikasyon, yetkilendirme ve onay yükümlülükleri

8.4.6.1 Lisanslandırma, sertifikasyon, yetkilendirme ve onay yükümlülüklerine (6 numaralı kritik unsur (CE-6)) ilişkin rehberliğe Doc 9734, Kısım A kapsamında ulaşılabilir.

8.4.6.2 Lisanslandırma, sertifikasyon, yetkilendirme ve onay yükümlülükleri, Devlet emniyet riski kontrol stratejisinin önemli bileşenleridir. Söz konusu Devlete, hizmet sağlayıcılarının ve diğer ilgili sektör temsilcisi organizasyonların havacılık sisteminde emniyetli bir şekilde faaliyet gösterilmesine yönelik olarak gerekli görülen standartlara ulaştığına dair güvence sağlarlar. Diğer Devletler tarafından tanzim olunan lisansların, sertifikaların, yetkilendirmelerin ve onayların tanınmasını veya kabulünü kolaylaştırmak için bazı Devletler tarafından ortak çalışma düzenlemeleri tesis edilmiştir. Bu tür düzenlemeler, söz konusu Devleti Şikago Sözleşmesi kapsamındaki yükümlülüklerinden kurtarmaz.

8.4.7 Emniyet yönetimi sistemi yükümlülükleri

Emniyet Yönetimi Sistemi (SMS) düzenleyici gereklilikleri

8.4.7.1 Annex 19'a uygun olarak söz konusu Devlet tarafından hizmet sağlayıcıları ve uluslararası genel havacılık işletmeleri tarafından Emniyet Yönetimi Sisteminin (SMS) uygulanması öngörülecektir. Söz konusu gereklilikler, Annex 19 Ek 2 kapsamında yer alan Emniyet Yönetimi Sistemi (SMS) çerçevesini ve bu el kitabının 9. Bölümünde yer alan destekleyici rehberliğe değinmektedir. Bu gerekliliklerin nasıl tesis edileceği, söz konusu Devletin düzenleyici çerçevesine bağlı olacaktır.

8.4.7.2 Devletler tarafından, Emniyet Yönetimi Sisteminin (SMS) söz konusu Devlet nezdinde kabul edilebilir olmasını sağlayan bir süreç oluşturulacaktır. Bu hususlaki yaklaşımlardan biri, Devlet seviyesinde, öngörülen Emniyet Yönetimi Sistemi uygulamasının ilerlemesini temsil eden zaman çizelgelerinin ve kilometre taşlarının tesis edilmesidir. Emniyet Yönetimi Sistemi (SMS) boşluk analizinin ve uygulama planının nasıl oluşturulması ve uygulanması gerektiğine dair hizmet sağlayıcılarına yönelik ilave rehberliğe 9. Bölümde ulaşılabilir.

8.4.7.3 Söz konusu Devletin Emniyet Yönetimi Sistemi (SMS) düzenleyici gerekliliklerinin ve Emniyet Yönetimi Sistemi (SMS) kılavuz materyalinin periyodik olarak gözden geçirilmesi gerekir. Söz konusu gözden geçirmede, endüstri geri bildirimi, söz konusu Devletin emniyet riski profilinin periyodik olarak gözden geçirilmesi, güncel durum ve ICAO Emniyet Yönetimi Sistemi (SMS) Standartları ve Tavsiye Edilen Uygulamaları (SARP'lar) ve kılavuz materyal göz önünde bulundurulmalıdır.

Uluslararası genel havacılık

8.4.7.4 Uluslararası genel havacılığa (IGA) yönelik Emniyet Yönetimi Sistemi (SMS) hükümleri Annex 19 kapsamında bir miktar esneklikle ele alınmakta ve dolayısıyla hizmet sağlayıcıları listesinde yer verilmemektedir. Havacılığın bu sektörü tarafından Emniyet Yönetimi Sistemi (SMS) çerçevesinin uygulanması beklenmektedir. Bu sektör ile diğer sektörler arasındaki fark, bu durumda, Devletlere, söz konusu gereklilikleri nasıl tesis edeceklerine dair bir derece esneklik verilmesidir. Annex 6, Kısım II — *Uluslararası Genel Havacılık — Uçaklar* kapsamında yer alan diğer hükümlerle tutarlı olarak, Tescil Devleti tarafından Uluslararası Genel Havacılık (IGA) işletmeleri tarafından Emniyet Yönetimi Sisteminin (SMS) uygulanmasına yönelik kriterler belirlenecektir.

8.4.7.5 Söz konusu kriterlerin tesis edilmesi, Annex 19 kapsamında tanımlanan şekilde Emniyet Yönetimi Sistemi (SMS) çerçevesinin uygulanmasını gerektirmelidir, ancak buna bir dizi yolla ulaşılabilecektir:

a) kriterlerin Uluslararası Genel Havacılığa (IGA) yönelik mevcut spesifik çalışma düzenlemeleri dahilinde tesis edilmesi;

b) gerekliliklerin, söz konusu kriterleri tanımlayan spesifik çalışma düzenlemeleri haricindeki yasal bir belge kapsamındaki düzenleyici çerçeve dahilinde yayınlanması veya

c) düzenleyici çerçeve dahilinde, söz konusu Devlet tarafından kabul edilen bir Emniyet Yönetimi Sistemi (SMS) endüstri uygulama esasına atıfta bulunulması.

8.4.7.6 Uluslararası Genel Havacılığa (IGA) ilişkin Emniyet Yönetimi Sistemi (SMS) kriterlerinin tesis edilmesine yönelik en iyi yaklaşımın seçilmesinde, Tescil Devleti tarafından, herhangi bir üçüncü tarafa gözetim yetkisinin olası devri de dahil olmak üzere, Emniyet Yönetimi Sisteminin (SMS) izlenmesinin nasıl gerçekleştirileceği göz önünde bulundurulmalıdır. Hizmet sağlayıcılarının Emniyet Yönetimi Sistemleri (SMS) için olduğu gibi, söz konusu Emniyet Yönetimi Sisteminin kabul edilebilirliği tespit edilirken Tescil Devleti tarafından, boyuta, operasyon ortamına ve operasyonun karmaşıklığına dayalı ölçeklenebilirliğe imkan verilmelidir.

8.4.7.7 Annex 6, Kısım I'e uygun olarak hava işletme ruhsatı (AOC) düzenlenmiş, birden fazla Tescil Devletindeki büyük veya turbojet uçaklar durumunda, söz konusu işletici bir hizmet sağlayıcısı olarak değerlendirilecek ve Emniyet Yönetimi Sisteminin (SMS) İşleticinin Devleti nezdinde kabul edilebilir kılınması için söz konusu işleticiye bu şekilde muamele edilecektir.

Emniyet Yönetimi Sistemi (SMS) kabulü

8.4.7.8 Pek çok hizmet sağlayıcısı birden fazla Devlet alınmış sertifikalara, yetkilendirmelere veya onaylara sahiptir veya birden fazla Devlette operasyonlar gerçekleştirmektedir. Söz konusu Devletin sorumluluğu dışında olan hizmet sağlayıcısının Emniyet Yönetimi Sisteminin (SMS) gözetime tabi tutulmasına yönelik olarak hiçbir Annex 19 gerekliliği mevcut değildir. Bununla birlikte, Emniyet Yönetimi Sistemi (SMS) gerekliliğinin uyumlaştırılması, Devletler arasında Emniyet Yönetimi Sisteminin (SMS) kabulünü kolaylaştırmaz. Uyumlaştırma, gözetim tekrarını ve hizmet sağlayıcıları tarafından (potansiyel olarak) farklı gereklilikler vasıtasıyla benzer Emniyet Yönetimi Sistemi (SMS) yükümlülüklerine riayet edilmesine yönelik ihtiyacı azaltır. Devletler, kanıtlanabilir emniyet değeri eklemeden sertifika sahipleri için idari ve mali külfeti arttıran politikaların farkında olmalıdırlar. Burada önemli olan, sertifikasyonlarının, yetkilendirmelerinin veya onaylarının ortak kabulünden yararlanmayan hizmet sağlayıcıları için, Emniyet Yönetimi Sisteminin (SMS) uygulamaya konmasının durumu kötüleştirmiş olmasıdır. Devletler, hizmet sağlayıcılarına yönelik gereksiz külfet yüklemeden uygulamanın faydalarına ulaşmaya çalışmalıdırlar.

8.4.7.9 Ayrıca, Devletler, diğer Devletlerin hizmet sağlayıcılarına sertifikalar, yetkilendirmeler veya onaylar verilirken aşırı teknik, hukuki veya idari külfetler olmadan, söz konusu gereklilikleri eşit bir şekilde uygulamaya teşvik edilirler. Birçok hizmet sağlayıcısı, birden fazla Devlet tarafından ilk kabul ve Emniyet Yönetimi Sistemlerini (SMS) kabul etmiş olan Devletlerden periyodik izlemenin veya denetimlerin desteklenmesi için ilave kaynaklara ihtiyaç duyarlar. Gereklilikler değişiklik arz ettiğinde, farklı bir şekilde yorumlandıklarında veya çatışma halinde olduklarında da ilave çalışma gerekir.

8.4.7.10 Emniyet Yönetimi Sistemi (SMS) çerçevesi gereklilikleri Annex 19 kapsamında ortaya konmaktadır. Bu gereklilikler Devletler tarafından söz konusu Devletin düzenleyici çerçevesine aktarılır. Herhangi bir organizasyonel sistemin veya sürecin performansı, uygulamada, söz konusu gerekliliklerin nasıl uygulandığına bağlıdır. Devletler arasındaki Emniyet Yönetimi Sistemi (SMS) denkliğine ve Emniyet Yönetimi Sistemi (SMS) kabulünün yansımalarına ilişkin iki ana bileşen mevcuttur.

8.4.7.11 İlk bileşen, Emniyet Yönetimi Sisteminin (SMS) tanınmasının veya kabulünün resmi yönleridir. Devletler arasındaki bir dizi diplomatik, hukuki ve teknik düzenlemeleri içeren ikili veya çok taraflı anlaşmalara karşın bazı Devletler tarafından bu husus ele alınmıştır. Bazı hallerde, kabul, her durumda olmamak üzere, karşılıklıdır.

8.4.7.12 İkinci bileşen ise teknik denkliktir. Teknik denklik beş alana ayrılabilir:

a) *Ortak gereklilikler*. Denkliğin belirlenmesi için yeterli olmamakla birlikte, ortak bir gereklilikler setinin kullanılması teknik değerlendirmelere yönelik yapıya ve etkinliğe imkan verir. Bunlar, çeşitli ICAO Annex'leri kapsamında belirlenmiştir.

b) *Uygulama beklentileri*. Her bir Devlet tarafından, uygulamanın ve performansın kanıtlanması için diğer otoriteye ilişkin süreçlere, programlara, yöntemlere ve araçlara yönelik spesifik beklentiler belirlenir.

c) *Kabul metodolojisi*. Devletler tarafından, süreçlerin ve yönetim kabiliyetlerinin Devletler arasında nasıl değişkenlik arz ettiğinin değerlendirilmesi için kullanılan yöntemlerdir. Bu genellikle, söz konusu Devletin emniyet gözetimi sisteminin bir işlevidir (6 numaralı Kritik Unsur (CE-6), lisanslandırma, sertifikasyon, yetkilendirme ve onay yükümlülükleri).

d) *Performans ölçümü*. Her bir Devlet tarafından, sertifikalandırılmış ve onaylanmış organizasyonlarının emniyet performansını ölçmek için kullanılan metodolojinin amacı, söz konusu Devlet tarafından her bir organizasyonun performans potansiyelinin ve durumunun anlaşılmasını geliştirmektir.

e) *Politikaların ve yöntemlerin izlenmesi*. İzleme, organizasyonların ve Emniyet Yönetimi Sistemlerinin (SMS'ler) performans durumunu güvence altına almalıdır. Bu, söz konusu Devletin gözetim yükümlülüklerinin bir unsurudur. Her bir Devlet tarafından, Emniyet Yönetimi Sistemlerinin (SMS'ler) gözetimi için başka bir otorite tarafından kullanılan yöntemlere yönelik bir anlayış ve güven oluşturulmalıdır. Bu sayede Emniyet Yönetimi Sistemlerinin (SMS'ler) kabulü veya tanınması desteklenir.

8.4.7.13 Hizmet sağlayıcılarının Emniyet Yönetimi Sisteminin (SMS) ilgili Devlet otoritesi nezdinde kabul edilebilir kılınması gerekir. Hizmet sağlayıcıları tarafından bir boşluk analizinin gerçekleştirilmesi ve işletilebilir bir uygulama planının oluşturulması beklenir (söz konusu Devlet tarafından planlanmış bir görev olarak kabul de dahil olmak üzere). Emniyet Yönetimi Sistemi (SMS) uygulamaları genel olarak üç veya dört aşamada yürütülür. Hizmet sağlayıcısı ile söz konusu Devlet arasındaki erken işbirliğinin daha sorunsuz bir oluşturma ve kabul sürecine yol açması muhtemeldir. Emniyet Yönetimi Sistemi (SMS) uygulaması hakkında bilgi için bakınız Bölüm 9.

Emniyet Performansı Göstergelerinin (SPI'ler) ve Emniyet Performansı Hedeflerinin (SPT'ler) Kabulü

8.4.7.14 Hizmet sağlayıcılarının önerilen Emniyet Performansı Göstergeleri (SPI'ler), ilgili Devletin düzenleyici otoritesi tarafından Emniyet Yönetimi Sistemi (SMS) kabulü kapsamında gözden geçirilir ve kabul edilir. Devletler, hizmet sağlayıcılarının Emniyet Performansı Göstergelerinin (SPI'ler) kabulünün uygulama sürecinde daha sonradan planlanmasını değerlendirebilirler. Bu, genellikle anlamlı yansımaların oluşturulmasına yönelik yeterli verilere sahip olmamalarına bağlı olarak özellikle ilk sertifikasyonda hizmet sağlayıcıları için kullanışlıdır. Söz konusu düzenleyici otorite, önerilen Emniyet Performansı Göstergelerinin (SPI'ler) münferit hizmet sağlayıcısının havacılık faaliyetleri bakımından münasip ve uygun olduğuna kanaat getirebilir. Hizmet sağlayıcısının Emniyet Performansı Göstergelerinden (SPI'ler) ve Emniyet Performansı Hedeflerinden (SPT'ler) bazıları, kabul edilebilir emniyet performansı seviyesinin (ALoSP) ölçülmesine ve izlenmesine yönelik olarak söz konusu Devletin Emniyet Performansı Göstergeleri (SPI'ler) ve Emniyet Performansı Hedefleri (SPT'ler) ile bağlantılı olabilir. Tüm Emniyet Performansı Göstergeleri (SPI'ler) ve Emniyet Performansı Hedefleri (SPT'ler) için durum böyle olmayabilir. Emniyet performansı ölçümü hakkında daha fazla bilgiye 4. Bölüm kapsamında ulaşılabilir.

8.4.7.15 Hizmet sağlayıcısının Emniyet Performansı Göstergelerinin (SPT'ler) kabulü, söz konusu Emniyet Performansı Göstergelerinin (SPI'ler) zamanla izlenmesi sonrasında ele alınabilir. Bu sayede temel performans belirlenir. Temel performans, söz konusu Devlette, bölgesel veya global seviyede belirlenen hedeflere dayalı olabilir. Devlet Emniyet Performansı Hedeflerine (SPT'ler) ulaşılması, hizmet sağlayıcısı ile emniyet riskini hafifletici tedbirlerin koordine edilmesini gerektirecektir.

Birden fazla hizmet sağlayıcısı genelinde tek bir Emniyet Yönetimi Sistemi (SMS)

8.4.7.16 Birden fazla hizmet sağlayıcısı sertifikasyonuna sahip olan organizasyonlar, Emniyet Yönetimi Sisteminin (SMS) faydalarından yararlanmak ve arayüz unsurlarını daha iyi bir şekilde ele almak için bu sertifikasyonlara tek bir Emniyet Yönetimi Sistemi (SMS) kapsamında yer vermeyi seçebilirler. Söz konusu Devletin düzenleyici otoritesi tarafından, bu ana organizasyonların Emniyet Yönetimi Sistemi (SMS) veya daha geniş bir Emniyet Yönetimi Sisteminin (SMS) kapsamında yer verilen hizmet sağlayıcılarına yönelik Emniyet Yönetimi Sistemi (SMS) gerekliliklerinin uygulanmasını değerlendirilirken aşağıdaki hususlar değerlendirilmelidir:

a) Bilhassa, söz konusu düzenleyici otorite bünyesindeki farklı organizasyonlardan denetçilerin farklı hizmet sağlayıcılarının gözetiminden ve izlenmesinden sorumlu olduğu hallerde olmak üzere, Emniyet Yönetimi Sistemi (SMS) izleme politikalarının ve süreçlerinin söz konusu Devlet genelinde tutarlı bir şekilde uygulanmasının sağlanması:

   1) düzenlemelerin tutarlı bir şekilde yorumlanmasına ve gözetimin ve izlemenin uygulanmasına yönelik yönetim taahhüdüne dair kanıtın mevcut olması;

   2) ideal olarak farklı disiplinlerden katılımcıları içermek üzere, tüm gözetim ve izleme personeline standart hale getirilmiş eğitimin verilmiş olması;

   3) farklı gözetim ve izleme organizasyonları söz konusu olduğunda, ortak politikaların, prosedürlerin ve denetim araçlarının oluşturulmasının ve uygulanmasının gerekmesi;

   4) her bir hizmet sağlayıcısına tayin edilen sorumlu denetçiler arasında tutarlı ve sık iletişimin olması;

   5) gözetim ve izleme faaliyetlerinin standart hale getirilme derecesini izleyen mekanizmaların uygulamada olması. Saptanan sorunların ele alınması gerekir;

   6) söz konusu hizmet sağlayıcısının faaliyetlerinin Emniyet Yönetimi Sistemi (SMS) tarafından kurumsal ("ana") seviyede ele alınabileceğinin kabul edilmesi. Annex 19'un uygulanabilirliği dışındaki faaliyetleri ve Emniyet Yönetimi Sistemini (SMS) öngören faaliyetler buna dahil olabilir.

   7) ana organizasyon tarafından aşağıdakilerin belgelenmiş olması:

      i) emniyet verilerinin ve emniyet bilgilerinin nasıl paylaşıldığına, iletişimlerin nasıl iletildiğine, kararların nasıl alındığına ve farklı faaliyet alanları genelinde ve uygulanabildiği hallerde farklı düzenleyici otoritelerde kaynakların nasıl tahsis edildiğine yönelik politikaları ve prosedürleri;

      ii) Emniyet Yönetimi Sistemi (SMS) ile ilişkili görevleri ve sorumlulukları ve Emniyet Yönetimi Sistemine (SMS) yönelik sorumluluk çerçevesi ve

      iii) organizasyon yapısı ve sistem tanımındaki farklı sistemler ve faaliyetler arasındaki arayüz bağlantıları.

b) Bazıları yabancı düzenleyici otoriteler tarafından tanzim olunmuş sertifikaları içeren, birden fazla sertifikaya sahip olan ana organizasyonlar tarafından birden fazla hizmet sağlayıcısı genelinde tek bir Emniyet Yönetimi Sisteminin (SMS) uygulanmasının seçilebileceğine dair farkındalığın sağlanması.

   1) Emniyet Yönetimi Sisteminin (SMS) kapsamının sistem tanımında açık bir şekilde tanımlandığının ve münferit faaliyetleri detaylandırdığının kabul edilmesi. Söz konusu hizmet sağlayıcısı tarafından kendi Emniyet Yönetimi Sistemi (SMS) süreçleri ve kurumsal Emniyet Yönetimi Sistemi (SMS) arasındaki uyumluluğun kanıtlanabilmesi.

2) söz konusu ana organizasyon tarafından hem yurt içi hem de yurt dışı onaylara sahip olunduğunda, bu senaryonun, farklı düzenleyici otoriteler tarafından Emniyet Yönetimi Sisteminin (SMS) kabulü gibi ilave zorluklara yol açabileceğinin bilincinde olunması. Emniyet Yönetimi Sistemi (SMS) kabulüne yönelik düzenlemelerin henüz tesis edilmediği hallerde, gözetimin ve izlemenin nasıl paylaşılacağına, delege edileceğine veya ayrı bir şekilde (mükerrer olarak) sürdürüleceğine dair diğer düzenleyici otoriteler ile bir anlaşma yapılması gerekir.

Entegre yönetim sistemleri

8.4.7.17 Emniyet Yönetim Sistemlerini (SMS) diğer yönetim sistemleri ile entegre etmiş olan hizmet sağlayıcıları değerlendirmeye tabi tutulurken düzenleyici otorite tarafından aşağıdaki hususlar göz önünde bulundurulmalıdır:

a) yetkilerinin kapsamını açıklığa kavuşturan bir politikanın hazırlanması (ilgili yönetim sistemlerinin gözetiminden sorumlu olmayabileceklerdir) ve

b) entegre yönetim sisteminin değerlendirilmesi ve izlenmesi için gerekli kaynaklar (uygun uzmanlığa sahip personeli, süreçleri, prosedürleri ve araçları içerebilecektir).

8.4.7.18 Emniyet Yönetim Sisteminin (SMS) diğer yönetim sistemlerine entegrasyonu hizmet sağlayıcısı için faydalıdır. Söz konusu entegrasyon, Sivil Havacılık Otoritesinin (CAA) memnuniyeti doğrultusunda ve söz konusu Sivil Havacılık Otoritesi (CAA) tarafından Emniyet Yönetimi Sistemi (SMS) etkin bir şekilde "görülebilecek" ve izlenebilecek bir şekilde tamamlanmalıdır. Entegre yönetim sistemi kapsamında Emniyet Yönetimi Sistemi (SMS) uygulayan hizmet sağlayıcılarına ilişkin rehberlik 9. Bölümde yer almaktadır.

8.4.8 Kaza soruşturması

8.4.8.1 Kaza soruşturma otoritesi (AIA), diğer organizasyonlardan işlevsel olarak bağımsız olmalıdır. Söz konusu Devletin Sivil Havacılık Otoritesinden (CAA) bağımsız olunması özellikle önemlidir. Sivil Havacılık Otoritesinin (CAA) menfaatleri ile Kaza Soruşturma Otoritesine (AIA) verilen görevler çelişebilecektir. Bu işlevin diğer organizasyonlardan bağımsız olma gerekçesi, kazalardaki neden-sonuç ilişkisinin düzenleyici veya Devlet Emniyet Programı (SSP) ile ilgili etkenlerle bağlantılı olabilmesidir. Ayrıca, böyle bir bağımsızlık Kaza Soruşturma Otoritesinin (AIA) yaşayabilirliğini geliştirir ve gerçek veya algılanan çıkar çatışmalarını engeller.

8.4.8.2 Kaza soruşturma süreci, Devlet Emniyet Programında (SSP) büyük bir role sahiptir. Söz konusu Devlet tarafından havacılık sistemindeki katkıda bulunan etkenlerin ve olası aksaklıkların saptanmasına ve tekrarı önleyecek gerekli karşı tedbirlerin oluşturulmasına imkan verir. Bu faaliyet, aktif kırılmaları ve kazaların/olayların katkıda bulunan etkenlerini ortaya çıkararak ve olayların analizinden öğrenilen derslere ilişkin raporlar sunarak havacılık emniyetinin sürekli olarak iyileştirilmesine katkı sağlar. Bu sayede düzeltici faaliyet kararlarının ve tekabül eden kaynak tahsisinin geliştirilmesi sağlanabilir ve havacılık sistemindeki gerekli iyileştirmeler belirlenebilir. Daha fazla bilgi için ICAO Annex 13'ü ve ilgili rehberliği referans alınız.

8.4.8.3 Annex 13'e uygun olarak resmi soruşturma gerektirmeyen birçok emniyet olayı vardır.
Bu olaylar ve belirlenen tehlikeler sistemik problemlerin göstergesi olabilir. Bu problemler, hizmet sağlayıcısı tarafından liderlik edilen emniyet soruşturmasıyla ortaya çıkarılabilir ve çözüme kavuşturulabilir. Hizmet sağlayıcısı emniyet soruşturmaları hakkında bilgi için 9. Bölümü referans alınız.

8.4.9 Tehlike tanımlama ve emniyet riski değerlendirmesi

Genel rehberlik

8.4.9.1 Havacılık otoritelerinin en önemli rollerinden biri, havacılık sisteminin genelindeki tehlikeleri ve yükselen trendleri belirlemektir. Buna genellikle birden fazla kaynaktan bir araya getirilen emniyet verilerinin analiz edilmesiyle ulaşılır. Herhangi bir Devletin Emniyet Riski Yönetimi (SRM) sürecinin karmaşıklık ve kapsamlılık seviyesi, söz konusu Devletteki havacılık sisteminin boyutuna, olgunluğuna ve karmaşıklığına dayalı olarak değişkenlik arz edecektir. Emniyet Riski Yönetimi (SRM) sürecine ilişkin genel rehberliğe 2. Bölüm kapsamında ulaşılabilir.

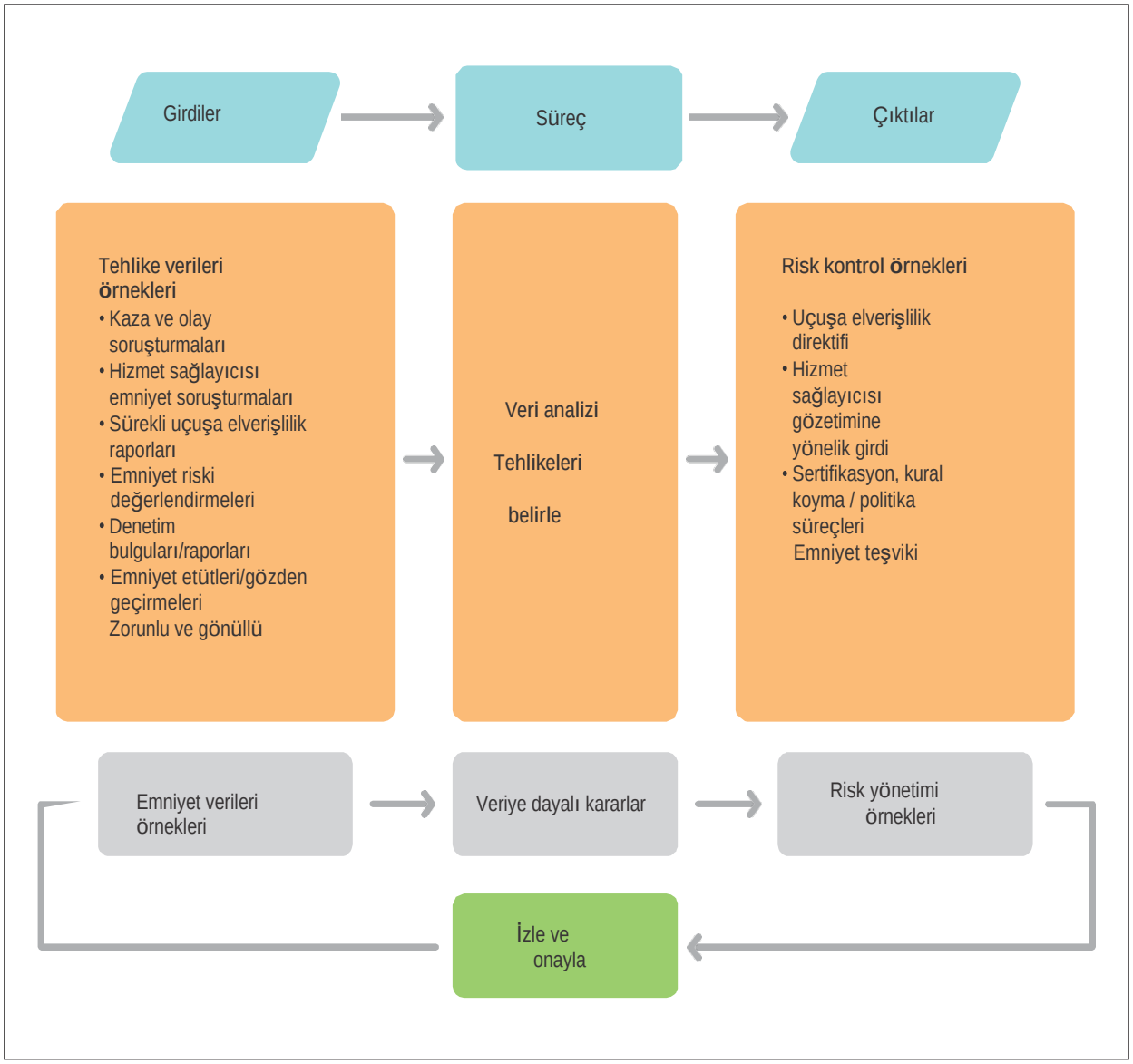
8.4.9.2 Dahili ve harici emniyet verilerinin ve emniyet bilgilerinin toplanması, etkin bir Devlet Emniyet Programına (SSP) ulaşılması bakımından elzemdir. Karmaşık olmayan havacılık sistemleri tarafından sınırlı veriler üretilebilir. Bu durumda, harici verilerin toplanması ve değişimi bir öncelik olmalıdır. Harici veriler genellikle, soruşturma raporları, yıllık emniyet raporları (kazalara ilişkin bilgiler ve analizler de dahil), emniyet ikazları, emniyet bültenleri, emniyet etütleri, iSTARS vb. gibi, diğer Devletlerden alınır. Bölgesel seviyede, ICAO grupları (örneğin, Bölgesel Havacılık Emniyeti Grupları (RASG'ler), planlama ve uygulama bölge grupları (PIRG'ler), vb. tarafından da emniyet bilgilerine ilişkin iyi bir kaynak sağlanabilir. Söz konusu Devletin emniyet verilerini toplama ve işleme sisteminde (SDCPS) kaza ve olay raporlarının ICAO'ya sunulmasına yönelik prosedürlere yer verilmelidir ve bu sayede global emniyet bilgilerinin toplanması ve paylaşılması kolaylaştırılacaktır.

8.4.9.3 Emniyet Riski Yönetiminin (SRM) birincil amacı, mevcut emniyet verileri kullanılarak tehlikelerin olası sonuçlarının saptanması ve kontrolüdür. Emniyet Riski Yönetimine (SRM) ilişkin prensipler Devletler ve hizmet sağlayıcıları için aynıdır.

8.4.9.4 Hizmet sağlayıcıları kendi emniyet verilerine erişim imkanına sahiptirler. Devletler, birden fazla hizmet sağlayıcısından emniyet verilerine erişme imkanına sahiptirler. Bu sebeple, topladığı emniyet verilerini sınıflandırmak için yaygın sınıflandırmaları uygulayan Devlet, Devlet Emniyet Riski Yönetimi (SRM) sürecinin etkinliğini büyük ölçüde iyileştirecektir. Bu sayede, farklı havacılık sektörleri genelindeki birden fazla kaynaktan elde edilen verilerin daha etkili bir şekilde analiz edilmesine imkan verilir. Veri analizi süreci girdileri ve çıktıları aşağıdaki Şekil 8-2'de gösterilmektedir.

8.4.9.5 Girdiler, kaza soruşturmaları, hizmet sağlayıcısı emniyet soruşturmaları, sürekli uçuşa elverişlilik raporları, tıbbi değerlendirme raporları, emniyet riski değerlendirmeleri, denetim bulguları ve denetim raporları ve emniyet etütleri ve gözden geçirmeleri de dahil olmak üzere, havacılık sisteminin herhangi bir kısmından alınabilir.

8.4.9.6 Gerektiğinde, tehlikenin giderilmesi veya emniyet riski seviyesinin kabul edilebilir bir seviyeye azaltılması için çıktılar veya emniyet riski kontrolleri uygulanır. Söz konusu Devlet için mevcut olan birçok hafifletme opsiyonundan bazıları şunları içerir: uçuşa elverişlilik direktifleri, hizmet sağlayıcısının (hizmet sağlayıcılarının) geliştirilmiş gözetimine ve izlenmesine girdi sağlanması, sertifikasyon, kural koyma veya emniyet politikalarında yapılan değişiklikler, emniyet teşvik programı, öğrenilen derslere ilişkin atölye çalışmalarının kolaylaştırılması. Seçilen tedbir açıkça, ele alınan sorunun önem derecesine ve türüne bağlıdır.



Şekil 8-2. Veriye dayalı analiz programı

Tehlike tanımlama

8.4.9.7 Tehlike tanımlama, örnek verilerin toplanmasına dayandırılır. Her bir tehlikenin kapsamlı bir şekilde anlaşılmasını sağlamak için birden fazla sektörden verilerin toplanması veya bir araya getirilmesi uygun olabilir. Şekil 8-2'de gösterilen süreç, reaktif veya proaktif tehlike tanımlama için eşit ölçüde geçerlidir. Herhangi bir olay veya kaza soruşturması sırasında tanımlanan tehlikelerin analiz edilmesi, reaktif metodolojiye bir örnektir. Proaktif olan da ise denetimler veya incelemeler sırasında veya zorunlu raporlardan tanımlanan tehlikeler yer alabilecektir. Günlük sistem güvenilirliği izlemesinden elde edilen emniyet performansı bozulmasına ilişkin erken işaretlerle uyarılmayı içerebilecektir.

8.4.9.8 Tehlikeler, söz konusu Devletin havacılık sistemindeki tüm seviyelerde mevcuttur. Kazalar veya olaylar, tehlikeler belirli tetikleyici etkenlerle etkileşimde bulunduğunda ortaya çıkar. Sonuç olarak, tehlikelerin, kazalara, olaylara veya emniyet ile ilgili diğer hadiselere yol açmaları öncesinde tanımlanmaları gerekir.

8.4.9.9 Devletler, mevcut verilerin toplanması, bir araya getirilmesi ve analiz edilmesi için herhangi bir kişinin veya ekibin tayin edilmesine teşvik edilir. Devlet emniyet analisti tarafından verilerin, potansiyel tehlikelerin yanı sıra tekabül eden etkilerin ve sonuçların belirlenmesi için analiz edilmesi gerekir. Tehlike tanımlama sürecinde öngörülen detay, değerlendirilmekte olan sürecin karmaşıklığına bağlıdır.

8.4.9.10 Etkin tehlike tanımlamasını sağlamak için sistematik bir süreç geliştirilmelidir. Bu süreçte aşağıdaki unsurlar yer almalıdır:

a) söz konusu Devletteki emniyet riskinin yönetilmesinin desteklenmesi için gerekli veri kaynaklarına erişim;

b) uygun analitik becerilere ve operasyon tecrübesine sahip olan emniyet analizi ekibi ve geniş bir dizi tehlike analizi tekniklerinde eğitim ve tecrübe ve

c) toplanmakta olan (veya toplanacak) verilere ve söz konusu Devletteki havacılık faaliyetlerinin kapsamına uygun tehlike analizi aracı (araçları).

Tehlike tanımlama tetikleyicileri

8.4.9.11 Tehlike tanımlamanın başlatılması gereken birçok durum mevcuttur. Bunların başlıcalarının bazıları şunlardır:

a) *Sistem tasarımı:* Tehlike tanımlama, operasyonların başlangıcı öncesinde, belirli havacılık sisteminin ve çevresinin detaylı bir şekilde tanımlanmasıyla başlar. Emniyet analizi ekibi tarafından söz konusu sistem ile ilişkili çeşitli potansiyel tehlikelerin yanı sıra arayüz bağlantısına sahip olan diğer sistemlere yönelik etkiler belirlenir.

b) *Sistem değişikliği:* Tehlike tanımlama, sistemde herhangi bir (operasyonel veya organizasyonel) değişiklik yapılmadan önce başlar ve havacılık sistemindeki belirli değişikliğin detaylı bir şekilde tanımlanmasını içerir. Emniyet analizi ekibi tarafından, bunun ardından, önerilen değişik ile ilişkili potansiyel tehlikelerin yanı sıra arayüz bağlantısına sahip olan diğer sistemlere yönelik etkiler belirlenir.

c) *Talebe bağlı ve sürekli izleme:* Tehlike tanımlama, işler durumda olan mevcut sistemlere uygulanır. Tehlike durumundaki değişiklikler tespit etmek için veri izlemesi kullanılır. Örneğin, tehlikenin ortaya çıkması beklenenden daha sık veya daha şiddetli olabilir veya kararlaştırılan hafifletme stratejileri beklenenden daha az etkin olabilir. Bir dizi ilgilenilmesi gereken kritik unsura dayalı bildirim eşikleriyle sürekli izleme ve analiz tesis edilebilir.

Emniyet riski değerlendirmesi

8.4.9.12 Emniyet riski değerlendirmesine ilişkin genel rehberliğe 2. Bölüm kapsamında ulaşılabilir. Emniyet riskinin herhangi bir havacılık sektörü veya herhangi bir bölge genelinde görüntülenebilmesi ve kontrol edilebilmesi dikkate alınmalıdır.

8.4.9.13 Verilerin analiz edilmesi ve farklı emniyet riski modelleme yaklaşımlarının kullanılması için birçok farklı araç mevcuttur. Emniyet riski değerlendirmesini seçerken veya oluştururken, Devletler tarafından söz konusu sürecin kendi ortamları için iyi bir şekilde çalıştığından emin olunmalıdır.

8.4.10 Emniyet risklerinin yönetimi

8.4.10.1 Emniyet sorunlarının çözüme kavuşturulmasına (8 numaralı Kritik Unsur (CE-8)) ilişkin rehberliğe Doc 9734, Kısım A kapsamında ulaşılabilir.

8.4.10.2 Emniyet risklerinin yönetilmesindeki amaç, emniyet risklerinin kontrol altında tutulmasını ve kabul edilebilir emniyet performansı seviyesine (ALoSP) ulaşılmasını sağlamaktır. Uygun Devlet havacılık otoritesi tarafından uygun emniyet riski hafifletme veya emniyet riski kontrol stratejileri geliştirilir, belgelenir ve tavsiye edilir. Örnekler şunları içerir; herhangi bir hizmet sağlayıcısına doğrudan müdahale, ilave politikaların veya düzenlemelerin uygulanması, operasyonel direktiflerin yayınlanması veya emniyeti teşvik edici faaliyetlerle tesir edilmesi.

8.4.10.3 Bir sonraki adım olarak her bir önerilen emniyet riski kontrolüne yönelik bir değerlendirme yapılmalıdır. İdeal emniyet riski kontrolü adayları maliyet etkin, gerçekleştirilmesi kolay, hızlıca uygulanabilir, etkindirler ve istenmeyen sonuçları getirmezler. Çoğu durumum bu idealleri karşılamaması sebebiyle, aday emniyet risk kontrollerinin etkinlik, maliyet, uygulamanın güncelliği ve karmaşıklık özelliklerinin dengelenmesine dayalı olarak değerlendirilmesi ve seçilmesi gerekir. Seçilmeleri ve uygulanmaları sonrasında, emniyet riski kontrollerinin, amaçlanan hedeflere ulaşıldığından emin olmak için izlenmesi ve doğrulanması gerekir.

8.4.10.4 Bir çok emniyet riski kontrolü hizmet sağlayıcısı (hizmet sağlayıcıları) tarafından eylem gerektirir. Hizmet sağlayıcısının (hizmet sağlayıcılarının) etkin uygulama için Devletler tarafından yönlendirilmesi gerekir. Devletlerin, emniyet riski kontrollerinin etkinliğini ve bunların hizmet sağlayıcıları üzerindeki etkisini, birlikte Devletlerin emniyet performansını izlemeleri gerekli olabilir. Emniyet riski hafifletme yaklaşımları 2. Bölüm kapsamında özetlenmektedir.

8.5 3. BİLEŞEN: DEVLET EMNİYET GÜVENCESİ

8.5.1 Devlet emniyet güvencesi faaliyetlerinin amacı, işlevlerinin amaçlanan emniyet amaçlarına ve hedeflerine ulaştığına yönelik olarak söz konusu Devlete güvence vermektir. Hizmet sağlayıcıları tarafından Emniyet Yönetimi Sistemleri (SMS) kapsamında bir emniyet güvencesi sürecinin uygulanması öngörülür. Emniyet Yönetimi Sistemi (SMS) güvence kabiliyeti, her bir hizmet sağlayıcısına, emniyet süreçlerinin etkili bir şekilde işlediğine ve emniyet amaçlarına ulaşılmasında doğru yolda olduklarına dair güvence verir. Benzer şekilde, Devlet emniyet güvencesi faaliyetleri, Devlet Emniyet Programı (SSP) kapsamında, söz konusu Devlete, emniyet süreçlerinin etkili bir şekilde işlediğine ve söz konusu Devletin, söz konusu Devletin havacılık endüstrisinin müşterek gayretleriyle emniyet amaçlarına ulaşmada doğru yolda olduğuna dair güvence sağlar.

8.5.2 Gözetim faaliyetleri ve emniyet verilerini/bilgilerini toplama, analiz etme, paylaşma ve bunların değişimini yapma mekanizmaları, düzenleyici emniyet riski kontrollerinin hizmet sağlayıcısının Emniyet Yönetimi Sistemine (SMS) uygun bir şekilde entegre edilmesini sağlar. Bu sayede, söz konusu sistemin tasarlandığı gibi uygulandığına ve düzenleyici kontrollerin Emniyet Riski Yönetiminin (SRM) planlanan etkisine sahip olduğuna dair güven sağlanır. Havacılık emniyeti verileri/bilgileri, Devletler tarafından, gözetim süreçleri ve emniyet raporlaması programları da dahil olmak üzere, bir çok kaynaktan toplanabilir. Bu verilerin çeşitli seviyelerde analiz edilmesi ve analizden elde edilen çıkarımların söz konusu Devletin havacılık sistemindeki gözetim faaliyetlerine ve emniyete ilişkin tamamen bilgiye dayalı karar almaya yönelik dayanak olarak kullanılması gerekir.

8.5.3 Gözetim yükümlülükleri

8.5.3.1 Uyum izlemesine ilişkin Gözetim yükümlülüklerine (7 numaralı Kritik Unsur (CE-7)) ilişkin rehberliğe Doc 9734, Kısım A kapsamında ulaşılabilir.

Gözetim faaliyetlerinin önceliklendirilmesi

8.5.3.2 Emniyet riskine dayalı gözetim (SRBS) yaklaşımı, Devletin emniyet yönetimi kaynaklarının her bir sektörün veya münferit hizmet sağlayıcısının emniyet riski profiliyle örtüşecek şekilde önceliklendirilmesine ve tahsis edilmesine imkan verir. Devletler, kendi emniyet süreçlerinin ve bilhassa emniyet performansını yönetimlerinin sürekli gelişen olgunluğunu izleyerek her bir hizmet sağlayıcısı hakkında aşinalık ve tecrübe kazanırlar. Zamanla, Devletler tarafından, bilhassa emniyet riskini yönetmeleri bakımından olmak üzere, hizmet sağlayıcısının emniyet becerilerine ilişkin net bir resim oluşturulacaktır.

Hizmet sağlayıcısının emniyet kabiliyetine ilişkin güven ve kanıt oluştukça, söz konusu Devlet tarafından gözetimin kapsamının ve/veya sıklığının değiştirilmesi seçilebilecektir.

8.5.3.3 Emniyet riskine dayalı gözetim (SRBS), olgun bir Emniyet Yönetimi Sistemine (SMS) sahip olan organizasyonlar için en uygun olandır. Emniyet riskine dayalı gözetim (SRBS) aynı zamanda, Emniyet Yönetimi Sisteminin (SMS) henüz uygulanmadığı organizasyonlar için de geçerli olabilir. Etkin Emniyet Riskine Dayalı Gözetimin (SRBS) temeli yeterince güvenilirdir ve anlamlı veriler içerir. Güvenilir ve anlamlı veriler olmadan, gözetim kapsamında veya sıklığında yapılan düzeltmelerin savunulması zordur.

8.5.3.4 Devletlerin, (veriye dayalı) kararlarının dayandırıldığı güvenilir ve kapsamlı verilere sahip olmalarını sağlamak için veri yönetimi kabiliyetlerini geliştirmeleri ve güçlendirmeleri gerekir. Münferit sektör emniyet riski analizleri de söz konusu Devlet tarafından benzer operasyon türlerine sahip olan birden fazla hizmet sağlayıcısına (örneğin, kısa mesafeli havayolları) etki eden ortak emniyet risklerinin değerlendirilmesine imkan verebilir. Böylelikle, herhangi bir spesifik havacılık sektörü dahilindeki veya sektörler genelindeki hizmet sağlayıcıları arasındaki emniyet riski sıralaması kolaylaştırılır ve kaynakların, en büyük emniyet etkisine sahip olan sektörlere veya faaliyetlere tahsisi desteklenir.

8.5.3.5 Sektör seviyesindeki analizler, söz konusu Devlet tarafından havacılık sisteminin genel bağlamda, parçaların bütüne nasıl katkı yaptığı bakımından görüntülenmesine imkan verir. Bu analizler, söz konusu Devlete, daha yüksek seviyelerdeki destekten veya müdahaleden hangi sektörün (sektörlerin) fayda göreceğinin ve daha işbirlikçi bir yaklaşım için hangi sektörlerin en iyi aday olduğunun belirlenmesinde güç verir. Bu sayede söz konusu Devlete, havacılık sistemi genelindeki düzenlemenin orantılı ve en çok ihtiyaca sahip olan alanlara yönelik olduğuna dair güvence sağlanır. Minimal müdahaleyle maksimum düzenleyici etkinliğe ulaşılması için spesifik düzenlemelerde değişikliklere ihtiyaç duyulan yerlerin belirlenmesi kolaydır.

8.5.3.6 Emniyet Riskine Dayalı Gözetimin (SRBS) bir bedeli vardır. Söz konusu Devlet ile havacılık topluluğu arasında uyuma dayalı denetimlerin ve incelemelerin ötesinde kesintisiz etkileşim gerektirir. Emniyet Riskine Dayalı Gözetim (SRBS) yaklaşımı, gözetim faaliyetlerinin uyarlanması için hizmet sağlayıcısının emniyet riski profilini kullanır. Hizmet sağlayıcısının sistemindeki iç gözden geçirmelerin, analizin ve karar almanın girdisi, önemli emniyet risklerine ve bunları etkin bir şekilde işaret eden hafifletmelere işaret eden hedeflenen bir eylem planı haline gelir. Gerek Devletten gerek hizmet sağlayıcısından elde edilen analiz, emniyet kaygısına ilişkin öncelik alanlarını tanımlar ve bu alanlara işaret edilmesindeki en etkili yolları özetler.

8.5.3.7 Burada önemli olan, emniyet riskine dayalı gözetimin, gerçekleştirilen gözetimin veya kaynakların miktarını mutlaka düşürmeyebileceği, öte yandan, gözetimin niteliğinin ve düzenleyici otorite ile hizmet sağlayıcısı arasındaki etkileşimin niteliğinin büyük ölçüde gelişecek olmasıdır.

Hizmet sağlayıcısı organizasyonel emniyet riski profilleri

8.5.3.8 Devletler, gözetim faaliyetlerinin kapsamının ve sıklığının değiştirilmesine ilişkin süreci desteklemek üzere her bir havacılık sektörü genelinde tutarlı olan organizasyonel emniyet riski profilleri oluşturmak isteyebileceklerdir. Bu tür araçlar, hizmet sağlayıcılarına yönelik olarak halihazırda mevcut olması gereken bilgileri elde etmeyi ve bir araya getirmeyi amaçlamalıdır ve aşağıdakiler gibi etkenleri içerebilir:

a) söz konusu organizasyonun finansal sağlığı;

b) faaliyette bulunulan yıl sayısı;

c) sorumlu yönetici ve emniyet yöneticisi gibi kilit personelin değişim oranı;

d) sorumlu yöneticinin yetkinliği ve performansı;

e) emniyet yöneticisinin yetkinliği ve performansı (sorumlu yönetici veya emniyet yöneticisi yetkinliği hakkında daha fazla bilgi için bakınız Bölüm 9)

f) önceki denetimlerin sonuçları;

g) önceki bulguların zamanında ve etkin bir şekilde çözüme kavuşturulması;

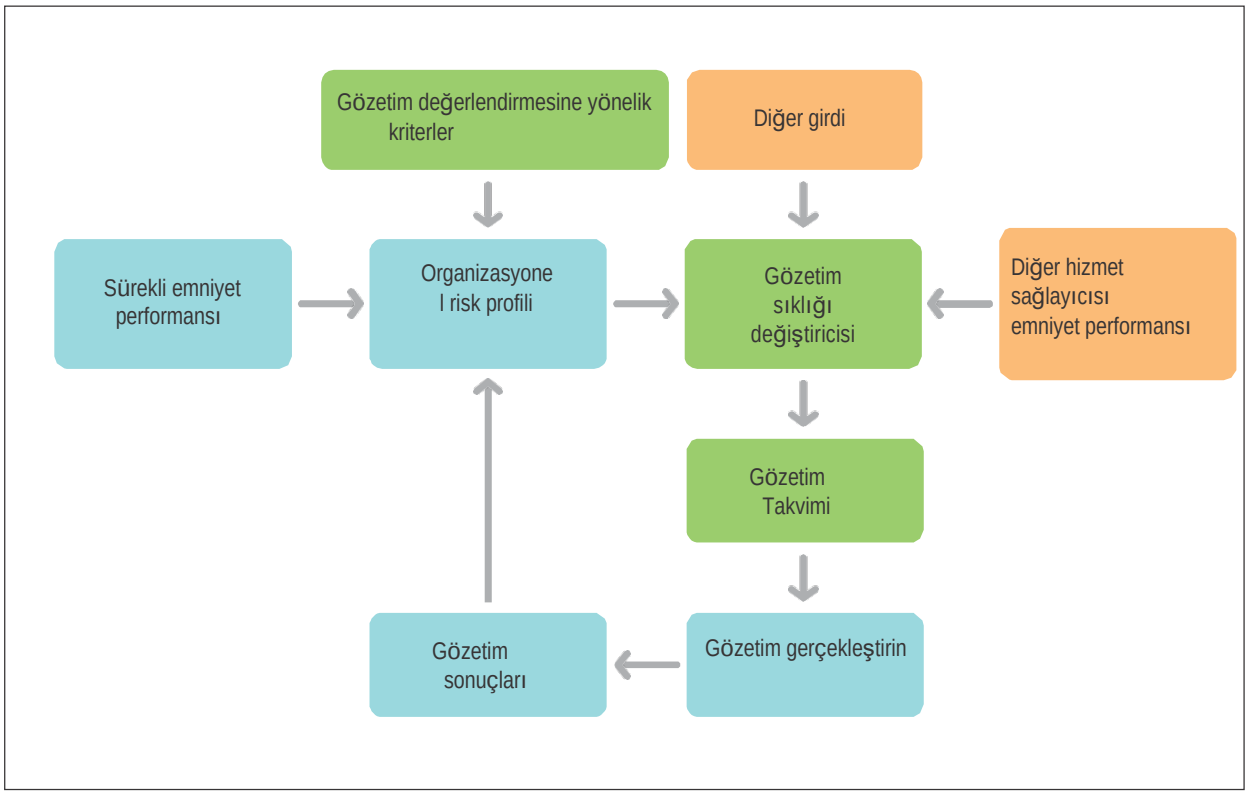
h) nispi faaliyet seviyesine ilişkin tedbirler (emniyet riskine maruz kalma hali);

i) gerçekleştirilmekte olan faaliyetlerin nispi kapsamına ve karmaşıklığına yönelik göstergeler;

j) tehlike tanımlama ve emniyet riski değerlendirme sürecinin olgunluğu ve

k) Devlet emniyet verileri analizi ve performans izlemesi faaliyetlerinden emniyet performansı tedbirleri.

8.5.3.9 Hizmet sağlayıcısının gözetiminin kapsamının veya sıklığının değiştirilmesi için kullanılabilen sürece ilişkin örnek Şekil 8-3'de gösterilmektedir.



Şekil 8-3. Emniyet riskine dayalı gözetim kavramı

8.5.4 Hizmet sağlayıcılarının emniyet performansının izlenmesi

Söz konusu Devlet tarafından her bir hizmet sağlayıcısının Emniyet Performansı Göstergelerinin (SPI'ler) ve Emniyet Performansı Hedeflerinin (SPT'ler) periyodik olarak gözden geçirilmesi gerekir. Bu gözden geçirmede, her bir Emniyet Performansı Göstergesinin (SPI) ve Emniyet Performansı Hedefinin (SPT) performansı ve etkinliği göz önünde bulundurulmalıdır. Söz konusu gözden geçirme, sürekli emniyet iyileştirmesinin desteklenmesine yönelik düzeltmelerin yapılmasına yönelik ihtiyacı gösterebilecektir.

8.5.5 Devlet emniyet performansı

8.5.5.1 Emniyet performansı yönetimi hakkındaki genel bilgiler için 4. Bölümü referans alınız.

Kabul edilebilir emniyet performansı seviyesi

8.5.5.2 Devletler tarafından, kendi Devlet Emniyet Programları (SSP) vasıtasıyla ulaşılacak kabul edilebilir emniyet performansı seviyesinin (ALoSP) belirlenmesi gerekmektedir. Buna aşağıdakiler vasıtasıyla ulaşılabilir:

a) Devlet Emniyet Programının (SSP) uygulanması ve sürdürülmesi ve

b) emniyetin etkili bir şekilde yönetilmekte olduğunu gösteren Emniyet Performansı Göstergelerinin (SPI'ler) ve Emniyet Performansı Hedeflerinin (SPT'ler) uygulanması ve sürdürülmesi.

8.5.5.3 Kabul edilebilir emniyet performansı seviyesi (ALoSP), emniyete ilişkin olarak her bir sektör tarafından ulaşılması ve muhafaza edilmesi gereken hedefler ile emniyete etki eden kendi faaliyetlerinin ve işlevlerinin etkinliğinin tespit edilmesine yönelik tedbirler de dahil olmak üzere, söz konusu Devletin kendi havacılık sisteminden beklediği emniyet seviyelerini ifade eder. Kabul edilebilir emniyet performansı seviyesi (ALoSP) aynı zamanda, söz konusu Devlet tarafından önemli görülen ve Devlet seviyesindeki havacılık paydaşları tarafından mutabık kalınan hususların bir yansımasıdır. Kabul edilebilir emniyet performansı seviyesi (ALoSP) başkalarından ayrı bir şekilde geliştirilmemelidir. Daha ziyade, daha yüksek seviyede stratejik rehberlik (Global Havacılık Emniyeti Planından (GASP), Bölgesel Planlardan, vb.) ve Devlet Emniyet Programı (SSP) kapsamında belirlenen emniyet amaçları göz önünde bulundurularak tanımlanmalıdır.

Kabul edilebilir emniyet performansı seviyesinin (ALoSP) belirlenmesi

8.5.5.4 Kabul edilebilir emniyet performansı seviyesinin (ALoSP) belirlenmesine ilişkin sorumluluk söz konusu Devletin havacılık otoritelerine aittir ve söz konusu Devlete, söz konusu Devletin yetkisi altındaki sektörlere ve hizmet sağlayıcılarına yönelik Emniyet Performansı Göstergeleri (SPI'ler) seti vasıtasıyla ifade edilecektir. Amaç, 4. Bölümde ana hatlarıyla belirtilen tüm havacılık sistemi ölçüm sürecinin emniyet performansının sürdürülmesi veya sürekli olarak iyileştirilmesidir. Bu sayede, söz konusu Devlet tarafından emniyete ilişkin olarak neler yaptığının anlaşılmasına ve gerektiğinde duruma tesir etmek üzere harekete geçilmesine imkan verilir. Hizmet sağlayıcılarının Emniyet Performansı Göstergelerinin (SPI'ler) ve hedeflerinin kabulü bu süreç kapsamındadır.

8.5.5.5 Kabul edilebilir emniyet performansı seviyesi (ALoSP), söz konusu Devletin havacılık sistemi tarafından ortaya konması gereken beklenen emniyet performansı seviyesine dair tüm Devlet havacılık otoritelerinin mutabakatını yansıtır ve iç ve dış paydaşlara, söz konusu Devletin havacılık emniyetini nasıl yönetmekte olduğunu kanıtlar. Bunlarla sınırlı kalmamakla birlikte, söz konusu Devletin yetkisi altındaki her bir sektöre ve hizmet sağlayıcısına yönelik emniyet performansına yönelik beklentileri içerir. Kabul edilebilir emniyet performansı seviyesinin (ALoSP) belirlenmesi, tüm geçerli Standart ve Tavsiye Edilen Uygulamalar (SARP'lar) da dahil olmak üzere, Devletin Uluslararası Sivil Havacılık Sözleşmesine tabi olma yükümlülüğünü değiştirmez veya geçersiz kılmaz.

8.5.5.6 Şekil 8-4'de, Emniyet Performansı Göstergelerine (SPI'ler) ve Emniyet Performansı Hedeflerine (SPT'ler) dayalı olarak kabul edilebilir emniyet performansı seviyesi (ALoSP) kavramı ortaya konmaktadır. Emniyet amaçlarına, Emniyet Performansı Göstergelerine (SPI'ler) ve Emniyet Performansı Hedeflerine (SPT'ler) ilişkin daha fazla bilgiye 4. Bölüm ve sonraki paragraflar kapsamında ulaşılabilir.

Emniyet performansı göstergeleri ve emniyet performansı hedefleri

8.5.5.7 Anlamlı Emniyet Performansı Göstergelerinin (SPI'ler) spesifik çalışma ortamını yansıtması ve emniyet risklerinin nasıl kontrol edildiğinin belirlenmesi için kullanılabilen koşulları vurgulamaya hizmet etmesi gerekir. Devlet izleme ve ölçüm stratejisinde, söz konusu Devletin sorumlu olduğu havacılık sisteminin tüm alanlarını çevreleyen Emniyet

Performansı Göstergeleri (SPI'ler) setinin yer alması gerekir. Hem sonuçları (örneğin, kazalar, olaylar, mevzuat ihlalleri) hem de işlevleri ve faaliyetleri (uygulamadaki emniyet riski hafifletmelerinin beklendiği gibi gerçekleştirildiği operasyonlar) yansıtması gerekir.

Bu kombinasyon, emniyet performansının sadece neyin çalışmadığına (başka bir deyişle, sonuçlar) göre değil, aynı zamanda neyin çalıştığına (başka bir deyişle, emniyet riski hafifletmelerinin beklenen sonuçları ürettiği faaliyetler) göre değerlendirilmesine imkan verir. Uygulamada, bu yaklaşım, iki ayrı türden emniyet risklerini yansıtan Emniyet Performansı Göstergelerinin (SPI'ler) değerlendirilmesini kapsar:

a) **Operasyonel emniyet riskleri** (şemanın sol tarafında gösterilmektedir), herhangi bir istenmeyen sonuca yol açabilecek olan koşullara odaklanır. Bunlar, kazalarla, olaylarla, aksaklıklarla ve kusurlarla ilişkili olan koşullardır. Operasyonel emniyet riski aslen hizmetlerin sunumuna ilişkin bir yan üründür. Bu sebeple, operasyonel emniyet riskine odaklı Emniyet Performansı Göstergeleri (SPI'ler) çoğunlukla, dolaylı olarak, hizmet sağlayıcılarının Emniyet Yönetimi Sistemleri (SMS) ile bağlantılı olacaktır. Şekil 8-4 kapsamında üç operasyonel riskin gösterilmesine karşın, gerçek sayının her bir Devletteki duruma dayalı olması gerekir.

   Bu Emniyet Performansı Göstergeleri (SPI'ler) ağırlıklı olarak hizmet sağlayıcılarının Emniyet Riski Yönetimi (SRM) süreci tarafından belirlenen operasyonel emniyet sorunlarını yansıtır. Söz konusu Devletin Emniyet Riski Yönetimi (SRM) süreci aynı zamanda, hizmet sağlayıcısı operasyonel emniyet riski Emniyet Performansı Göstergelerinin (SPI'ler) bir araya getirilmesinden elde edilen Devlet havacılık sistemi genelindeki operasyonel emniyet sorunlarını yansıtan bir girdi olarak kullanılabilir. Herhangi bir operasyonel emniyet sorunu ve ilgili Emniyet Performansı Göstergeleri (SPI'ler) arasında sık bir şekilde birden çoğa ilişki olacaktır. Başka bir deyişle, tek bir operasyonel emniyet sorunu birden fazla Emniyet Performansı Göstergesi (SPI) tarafından gösterilebilecektir.

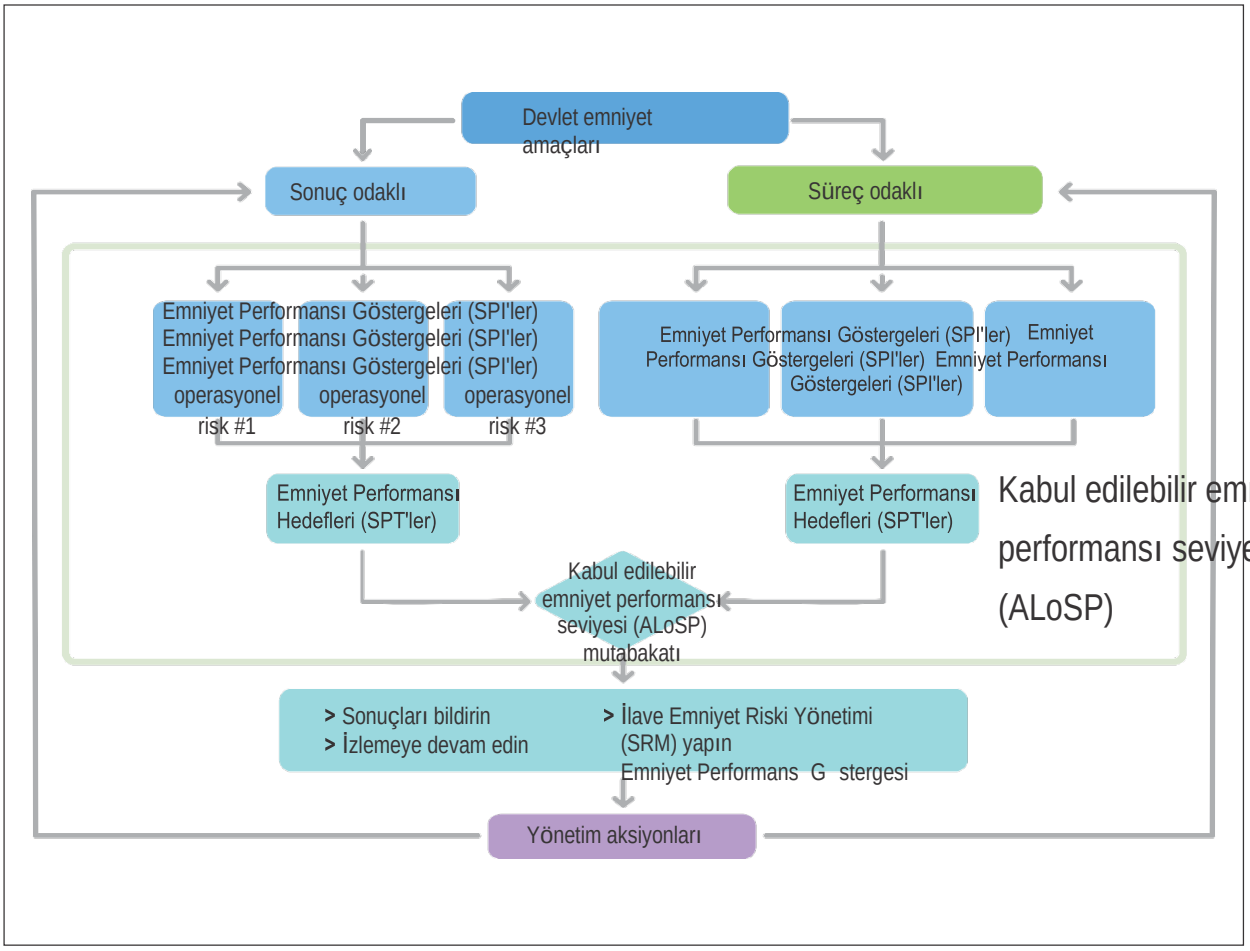
b) **Süreç uygulaması emniyet riskleri** (şemanın sağ tarafında gösterilmektedir), operasyonel emniyet riskinin yönetilmesi için gerekli olan araçlara ve kaynaklara odaklanmaktadır. Emniyet risklerinin süreç uygulaması perspektifinden yönetimi, ICAO Standartları ve Tavsiye Edilen Uygulamaları (SARP'lar) uygulama durumunun (emniyet ile ilgili ulusal kanunlar ve düzenlemeler), endüstri dahilindeki Emniyet Yönetimi Sistemi (SMS) süreçlerinin uygulanmasının ve Devlet seviyesinde Devlet Emniyet Programının (SSP) uygulanmasının (endüstrinin etkin gözetimini ve izlenmesini içeren) değerlendirilmesinden başlar. Yukarıdakilerden herhangi birine yönelik iyileştirmelerin gerekli olması halinde, bu iyileştirmelerin sağlanılmasına yönelik faaliyetlerin planlanması, uygulanması ve izlenmesi ve bu faaliyetler için yeterli kaynakların tahsis edilmesi gerekir. Söz konusu değişikliklerin planlanmasının, uygulanmasının ve/veya etkinliğinin izlenmesine imkan veren Emniyet Performansı Göstergeleri (SPI'ler) bunun akabinde oluşturulur.

   "Süreç uygulaması emniyet riskine" odaklanan Emniyet Performansı Göstergeleri (SPI'ler), söz konusu Devlete, hizmet sağlayıcıları tarafından Emniyet Yönetimi Sisteminin (SMS) kurumsal olarak düzenlenmesinin ve Emniyet Riski Yönetiminin (SRM)/emniyet güvencesi süreçlerinin uygulanmasının yeterliliğinin izlenmesine yönelik sıkı riayet dışında alternatif yöntemler sunar. Bu Emniyet Performansı Göstergeleri (SPI'ler) aynı zamanda, Evrensel Emniyet Gözetimi Denetim Programı (USOAP) analizleri ve Devlet Emniyet Programı (SSP) sürekli iyileştirme faaliyetleri tarafından gösterilen, ihtiyaç duyulan iyileştirmelere ilişkin olarak da belirlenebilir. Evrensel Emniyet Gözetimi Denetim Programı (USOAP) denetimlerinin sonuçları, Emniyet Yönetimi Sistemi (SMS) değerlendirmelerinin bir araya getirilmesi ve Devlet Emniyet Programı (SSP) sürekli iyileştirme bilgileri, iyileştirmeye yönelik potansiyel alanları belirler. Bunların, en büyük faydaya göre önceliklendirilmesi gerekir. Bu sayede, söz konusu Devletin havacılık sisteminin emniyet performansında iyileştirmeye katkıda bulunulur. Bu Emniyet Performansı Göstergelerinin (SPI'ler), operasyonel emniyet riski Emniyet Performansı Göstergelerinden (SPI'ler) farklı olmaları gerekir.

8.5.5.8 Gerek operasyonel gerek süreç uygulaması emniyet risklerine yönelik Emniyet Performansı Göstergeleri (SPI'ler), söz konusu Devletin emniyet güvencesi sürecinin kilit kısmı haline gelir. Operasyonel emniyet riski Emniyet Performansı Göstergelerinin (SPI'ler) ve süreç uygulaması emniyet riski Emniyet Performansı Göstergelerinin (SPI'ler) bir araya getirilmesi, Devletin kabul edilebilir emniyet performansı seviyesinin (ALoSP) belirlenmesine yönelik geri bildirim kaynağını genişletir.

Emniyet performansı göstergelerinin periyodik olarak gözden geçirilmesi

8.5.5.9 Devlet Emniyet Performansı Göstergelerinin (SPI'ler) belirlenmesi sonrasında periyodik bir gözden geçirme elzemdir. Başlangıçta en üstteki emniyet risklerinin belirlenmesi, geçmişe ait verilere dayalı analiz tarafından yardımcı olunan bir faaliyettir. Bununla birlikte, havacılık sistemi dinamiktir ve sürekli olarak değişir. Yeni emniyet sorunları doğabilir, söz konusu Devletteki süreçler değişebilir ve bu gibi haller söz konusu olabilir. Devlet operasyonel emniyet sorunlarının ve süreçlerinin periyodik olarak gözden geçirilmesi, Devlet emniyet amaçlarının ve sonuçta Emniyet Performansı Göstergelerinin (SPI'ler) ve Emniyet Performansı Hedeflerinin (SPT'ler) güncellenmesini ve geliştirilmesini destekler.



Şekil 8-4. Kabul edilebilir emniyet performansı seviyesi (ALoSP)

Kabul edilebilir emniyet performansı seviyesinin (ALoSP) periyodik olarak gözden geçirilmesi

8.5.5.10 Başlangıçtaki kabul edilebilir emniyet performansı seviyesinden (ALoSP) sorumlu olan üst yönetim ekibi tarafından söz konusu kabul edilebilir emniyet performansı seviyesinin (ALoSP) sürekli uygunluğunun tespit edilmesi gerekir. Kabul edilebilir emniyet performansı seviyesinin (ALoSP) periyodik olarak gözden geçirilmesi aşağıdakilere odaklanmalıdır:

a) bu alanlarda emniyet performansı yönetimine imkan veren Emniyet Performansı Göstergelerinin (SPI'ler) dahil edilmesini sağlayarak havacılık sektörleri dahilindeki kritik emniyet sorunlarının belirlenmesi;

b) söz konusu Devletin tüm havacılık sisteminin genelinde emniyet performansı yönetiminin geliştirilmesi amacıyla, her bir sektördeki ilgili Emniyet Performansı Göstergesi (SPI) için ulaşılacak istenilen iyileştirmeyi veya sürdürülecek emniyet performansı seviyesini tanımlayan Emniyet Performansı Hedeflerinin (SPT'ler) belirlenmesi;

c) herhangi bir Emniyet Performansı Göstergesi (SPI) bir takım tedbir gerektiren herhangi bir noktaya ulaştığında (uygun görülmesi halinde) tetikleyicilerin belirlenmesi ve

d) kararlaştırılan kabul edilebilir emniyet performansı seviyesine (ALoSP) ulaşılması için mevcut Emniyet Performansı Göstergelerinde (SPI'ler), Emniyet Performansı Hedeflerinde (SPT'ler) ve tetikleyicilerde değişikliklere veya ilavelere gerek bulunup bulunmadığının tespit edilmesi için Emniyet Performansı Göstergelerinin (SPI'ler) gözden geçirilmesi.

8.5.5.11 Söz konusu Devletin en üstteki risklerine yönelik periyodik gözden geçirmenin sonuçlarından biri, söz konusu veriler tarafından elverildiği kadar detaylı olarak her bir operasyonel emniyet sorununun mahiyetinin daha iyi bir şekilde anlaşılmasıdır. Söz konusu Devlet tarafından tehlikelerinin ve bunların olası sonuçlarının Devlet havacılık sisteminin tüm seviyelerinde değerlendirilmesi gerekir. Ayrıca, Devlet süreçlerinin (lisanslandırma, sertifikasyon, yetkilendirme, onay, gözetim ve buna benzer) Emniyet Riski Yönetimine (SRM) nasıl katkı sağladığı analiz edilmelidir. Her bir operasyonel emniyet riski, gerekli emniyet riski hafifletmelerini saptamak üzere değerlendirilir. Bu tedbirler, etkinliklerini ölçen Emniyet Performansı Göstergeleri (SPI'ler) vasıtasıyla izlenir.

8.5.5.12 Operasyonel emniyet riskinin emniyet performansının iyileştirilmesi reaktif olma eğiliminde iken emniyet riski yönetimi süreçlerinin iyileştirilmesi proaktif olma eğilimindedir. Emniyet riskinin yönetilmesini daha iyi destekleyen Devlet süreçlerinin iyileştirilmesi, olumsuz sonuçlar ortaya koymaları öncesinde tehlikelerin tanımlanmasına ve kontrol edilmesine imkan verir.

Kabul edilebilir emniyet performansı seviyesine (ALoSP) ulaşılması

8.5.5.13 Herhangi bir Devletin, Emniyet Performansı Göstergeleri (SPI'ler) ve Emniyet Performansı Hedefleri (SPT'ler) ile gösterilen emniyet performansı, ulaşılan kabul edilebilir emniyet performansı seviyesini (ALoSP) kanıtlar. Emniyet Performansı Hedeflerinden (SPT'ler) herhangi bir karşılanmaması halinde, bunun nedeninin daha iyi bir şekilde anlaşılması ve hangi tedbirlerin alınması gerektiğinin tespiti için bir değerlendirmeye ihtiyaç duyulabilir. Sebep aşağıdakiler olabilir:

a) söz konusu hedefler ulaşılabilir veya gerçekçi olmamıştır;

b) hedefe ulaşmak için alınan tedbirler uygun olmamış veya başlangıçtaki niyetten sapmıştır (pratik kopma);

c) diğer emniyet riski önceliklerindeki değişiklikler, kaynakları belirli bir hedefin karşılanmasından uzaklaştırmıştır veya

d) söz konusu hedefler belirlendiğinde düşünülmemiş olan yükselen riskler ortaya çıkmıştır.

8.5.5.14 Karşılanmayan hedefler için, sebebin anlaşılmasına ve hedefin karşılanmaması halinde dahi emniyet iyileştirmesinin yeterli olup olmadığına ve başka hangi tedbirlerin gerektiğine dair bir yönetim kararına ihtiyaç duyulacaktır. Burada, ele alınmayan bazı risk faktörlerini tanımlayabilecek ilave analiz gerekebilecek veya etkin olmayan bir takım risk hafifletmeleri söz konusu olabilecektir.

8.5.6 Değişik yönetimi: Devlet perspektifi

8.5.6.1 Annex 19 kapsamında, Devletler tarafından Devlet Emniyet Programı (SSP) kapsamındaki değişikliğin yönetimine yönelik resmi faaliyetlerin tesis edilmesi açık bir şekilde öngörülmemektedir. Bununla birlikte, değişiklikler, çağdaş havacılık sisteminde hep var olan bir gerçektir. Herhangi bir sistemde değişiklikler getirildiğinde, söz konusu sistemin belirlenmiş emniyet riski resmi değişecektir. Değişiklikler, mevcut savunmaların etkinliğini etkileyebilecek tehlikeler getirebilecektir. Bu da yeni riske veya mevcut emniyet risklerinde değişikliklere yol açabilecektir. Devletler tarafından kendi havacılık sistemlerindeki değişikliğin etkisi değerlendirilmeli ve yönetilmelidir.

8.5.6.2 Devlet Emniyet Programı (SSP), değişikliklerin Devlet seviyesindeki etkisinin değerlendirilmesine yönelik prosedürler geliştirmelidir. Bu prosedürler, uygulanmaları öncesinde havacılık sistemindeki değişikliklerin emniyet etkisinin Devlet tarafından proaktif bir şekilde belirlenmesine ve önerilen değişikliklerin yapılandırılmış bir şekilde planlanmasına ve uygulanmasına imkan vermelidir.

8.5.6.3 Değişiklikler planlanırken, söz konusu Devlet tarafından söz konusu değişikliğin mevcut sistem üzerindeki etkisi analiz edilmeli ve Emniyet Riski Yönetimi (SRM) süreci kullanılarak yeni veya değişen emniyet riskleri analiz edilmeli ve uygun görüldüğü takdirde hafifletilmelidir. Değişen sistemde veya operasyonel bağlamda, tüm emniyet riskleri değerlendirilene kadar hiçbir operasyon gerçekleştirilmemelidir.

8.5.6.4 Devletler tarafından kendi Devlet Emniyet Programları (SSP) kapsamında iki tür değişiklik ile karşılaşılacaktır: organizasyonel değişiklik (örneğin, sorumlulukların yeniden dağıtılması veya Devlet havacılık otoriteleri bünyesindeki yeniden yapılanma) ve operasyonel değişiklik (örneğin, hava sahası kullanımındaki herhangi bir değişiklik). Devlet Emniyet Programı (SSP) kapsamındaki değişiklik yönetimi, söz konusu Devletin yasal yükümlülüklerini yerine getirme kabiliyeti üzerinde (süreç değişikliği) ve Devlet emniyet yönetimi kabiliyetleri üzerinde belirgin bir etkiye sahip olabilecek olan değişikliklere odaklanmalıdır. Süreç değişikliklerinin ve operasyonel değişikliklerin kombinasyonu buna dahil olabilir.

8.5.6.5 Söz konusu Devletin emniyet risklerine belirgin etki potansiyele sahip olan değişiklik örnekleri, bunlarla sınırlı kalmamak üzere, şunları içerir:

a) Devlet havacılık otoritelerinin yeniden yapılandırılması (küçülme dahil);

b) Emniyet Riskine Dayalı Gözetim (SRBS), Emniyet Riski Yönetimi (SRM) ve emniyet güvencesi süreçleri gibi metodolojideki değişiklikler de dahil olmak üzere, Devlet Emniyet Programı (SSP) süreçlerindeki değişiklikler.

c) mevcut Devlet emniyet politikalarındaki, programlarındaki ve düzenlemelerdeki değişiklikler gibi, düzenleyici ortamdaki değişiklikler;

d) yeni teknolojilerin getirilmesi, altyapıdaki, ekipmanlardaki ve hizmetlerdeki değişiklikler gibi, operasyon ortamındaki değişiklikler;

e) hızla değişen endüstri (genişleme, sözleşmeyle yaptırma, biçim değiştirme) ve bunun Devlet gözetim ve performans izleme kabiliyetleri üzerindeki potansiyel etkisi.

8.5.6.6 Değişikliklerin bildirilmesi, değişik yönetiminin etkinliği bakımından esastır. Söz konusu Devlet dahilindeki etkilenen personelin ve etkilenen hizmet sağlayıcısının (hizmet sağlayıcılarının) söz konusu değişiklikten ve söz konusu değişikliğin zamanlamasından ve etkilerinden tümüyle haberdar olması elzemdir.

8.6 4. BİLEŞEN: DEVLET EMNİYET TEŞVİKİ

8.6.1 Devlet perspektifinden bakıldığında, dahili ve harici Devlet emniyet teşviki tedbirinin uygulanmasına yönelik ihtiyaç, Annex 19 kapsamında Devletlerin emniyet yönetimi sorumluluklarındaki bileşenlerden biri olarak belirlenmiştir. Dahilen, Sivil Havacılık Otoriteleri (CAA'lar) ve Devlet Emniyet Programına (SSP) dahil olan diğer havacılık otoriteleri tarafından, etkin ve verimli bir Devlet Emniyet Programını (SSP) besleyen bir kültürün geliştirilmesini desteklemek üzere personellerine ilgili emniyet bilgilerinin sağlanmasına yönelik mekanizmalar tesis edilmelidir. Emniyet politikalarının, emniyet planlarının yanı sıra diğer önemli Devlet Emniyet Programı (SSP) dokümantasyonunun iletilmesi, aynı zamanda, Devlet tarafından uygulamaya koyulan emniyet yönetimi süreçlerinin etkin kalmaya devam etmesini sağlayacak şekilde personeli arasındaki farkındalığı ve işbirliğini geliştirebilir.

8.6.2 Herhangi bir Devlet veya spesifik havacılık sektörü dahilinde emniyet performansının iyileştirilmesi ziyadesiyle, söz konusu Devletin veya havacılık sektörünün emniyet kültürüne bağlıdır. Emniyetin yönetilmesi ile ilgili tedbirler, söz konusu organizasyon pozitif emniyet kültürüne sahip olduğunda daha etkin olma eğilimindedir. Üst ve orta düzey yönetim tarafından gözle görülür bir şekilde desteklendiğinde, ön saflardaki çalışanlar, emniyet amaçlarına ulaşılmasına yönelik olarak ortak sorumlulukları hissetme eğiliminde olurlar.

8.6.3 Herhangi bir havacılık sistemi dahilinde emniyet kültürünün iyileştirilmesine yönelik diğer tedbirler arasında, iletişime yönelik ihtiyaç önemiyle öne çıkar. Önceliklerini, en iyi uygulamalarını, belirli bir operasyonda öne çıkan riskleri sürekli olarak bildirmek suretiyle, Devletler tarafından pozitif emniyet kültürü beslenebilir ve Sivil Havacılık Otoritelerinin (CAA'lar) veya hizmet sağlayıcılarının profesyonelleri arasındaki emniyet amaçlarına ulaşma potansiyeli azami hale getirilebilir. Emniyet kültürüne ilişkin daha fazla detaya 3. Bölüm kapsamında ulaşılabilir.

8.6.4 Çalışanların emniyet performansına yönelik sorumluluklarını sahiplenmeleri ve kavramaları sonrasında, sorumluluklarının emniyetli bir havacılığa yönelik olarak etkili bir şekilde yerine getirilmesi için kullanılabilen yolları ve bilgileri faal bir şekilde aramaları beklenir. Bu, emniyet yönetiminde kilit bir rol oynaması için emniyet teşvikine yönelik bir fırsattır. Haricen, hizmet sağlayıcıları ile iletişim kanallarının tesis edilmesi, öğrenilen derslerin, en iyi uygulamaların, Emniyet Performansı Göstergelerinin (SPI'ler) ve spesifik emniyet risklerine ilişkin bilgi sunumunun paylaşılmasına imkan vermelidir.

Bu sayede, emsal organizasyonlar arasında pozitif emniyet kültürünün geliştirilmesi desteklenerek hizmet sağlayıcıları dahilinde emniyet yönetimi uygulamalarının uygulanması desteklenmelidir. Ayrıca, hizmet sağlayıcıları ile rutin iletişim çalışmalarının tesis edilmesi, havacılık emniyeti sorunlarına ilişkin genel farkındalığı arttırabilecek ve emniyet iyileştirme inisiyatiflerinin belirlenmesinde daha fazla işbirliğini teşvik edebilecektir.

8.6.5 Devletler tarafından havacılık emniyetinin iyileştirilmesine yönelik kararlar veya tedbirler alındıkça (örneğin, düzenlemelerin tesis edilmesi veya gözetim yöntemlerine yönelik değişikliklerin uygulanması), dahili iletişimin yanı sıra harici iletişimde bulunulması da önem arz etmektedir. Bu sayede, söz konusu Devletin taahhüdünün havacılık topluluğu genelindeki algısı güçlendirilebilir. Böylelikle, Devlet emniyet amaçlarına ulaşılmasına katkıda bulunulabilecektir.

8.6.6 Devletlere, emniyet teşviki tedbirlerinin tesis edilmesinde destek verecek birçok kaynak ve araç mevcuttur. Devletler tarafından benimsenebilecek birçok teşvik tedbirinin yapılandırılmasına yönelik yollardan biri bir iletişim planının oluşturulmasıdır. Böyle bir plan, asgari olarak, havacılık topluluğunun ilgili üyelerinin belirlenmesini, gruplarından her birine iletilen mesajları ve bilgileri ve bu bilgilerin aktarılacağı yolları içerebilecektir. Söz konusu iletişim planı, aynı zamanda, bu dahili ve harici kitlelerle iletişimde bulunulmasına yönelik kabiliyetin ve kanalların etkili bir şekilde geliştirilmesinde Sivil Havacılık Otoritesini (CAA) destekleyen bir yol haritası işlevi de görebilecektir. Bu sayede, Devletlere, emniyet kültürünün inşa edilmesinin yanı sıra, gerek Devletlerin gerekse de hizmet sağlayıcılarının perspektifinden olmak üzere, başarılı emniyet yönetimi tarafından öngörülen gerekli verilerin ve araçların sağlanması bakımından fayda sağlanabilir.

8.6.7 Bazı bilgiler, sosyal medya kullanılarak nispeten daha az resmi olan bültenler ve ilanlar vasıtasıyla iletilebilirken bazıları ise özel toplantılarda veya seminerlerde daha iyi bir şekilde ele alınır. Söz konusu Devlet dahilinde pozitif emniyet kültürünün geliştirilmesinde en iyi sonuçlara ulaşacaklarına ve sonuçta etkin bir Devlet Emniyet Programına (SSP) ve söz konusu Devlet dahilinde daha emniyetli bir sivil havacılık sistemine ulaşacaklarına inanılan yeterli emniyet teşviki kanallarının ve medyanın uygulanması söz konusu Devletin görevidir.

8.6.8 Bilgilerin dahilen bildirilmesi ve yayılması

Not.— Herhangi bir koruma prensibi uygulanmadığı sürece, gönüllü emniyet raporlaması sistemlerinden alınan emniyet bilgileri korunacaktır. Bu koruma, zorunlu raporlama sisteminden alınan emniyet bilgilerini kapsayacak şekilde genişletilebilir. Emniyet verilerinin, emniyet bilgilerinin ve ilgili kaynakların korunmasına ilişkin detaylar için bakınız Bölüm 7.

8.6.8.1 Emniyet teşviki tedbirleri ve yayınları aynı zamanda herhangi bir Devlet dahilinde emniyet gözetimine katılan farklı organizasyonlar arasındaki koordinasyonu ve işbirliğini geliştirebilir. Devlet Emniyet Programı (SSP) dokümanı ve ilişkili Devlet emniyet ve yürütme politikaları, eğitimin entegrasyonunun ilgili bilgilerin bildirilmesinin ve yayılmasının başarılı bir şekilde gerçekleştirilmesi bakımından esastır. Farklı havacılık sektörlerinden sorumlu olan Devlet düzenleyici otoritelerinin yanı sıra Kaza Soruşturma Otoritesi (AIA) gibi diğer bağımsız idari kuruluşların, Devlet emniyet teşvikindeki ilgili rollerine yönelik entegre bir yaklaşıma sahip olmaları gerekir. Devletler tarafından Devlet Emniyet Programı (SSP) Koordinasyon Grubunun üyeleri (Devlet Emniyet Programının (SSP) uygulanmasına ve sürdürülmesine dahil olan Devlet kuruluşları) arasında resmi bir iletişim kanalı tesis edilmelidir.

8.6.8.2 Operasyonel perspektiften, uyumlaştırılmış Emniyet Yönetimi Sistemi (SMS) gereklilikleri ve ilgili hizmet sağlayıcılarının izlenmesi de dahil olmak üzere, operasyonel stratejilerin Devlet havacılık otoriteleri arasında paylaşılması, iletilmesi ve koordine edilmesi önemlidir. Açık bir iletişim kanalı, farklı havacılık sektörlerine yönelik çelişen kabul kriterlerinin veya Emniyet Yönetimi Sistemi (SMS) gerekliliklerinin oluşturulmasının önüne geçebilecektir.

8.6.8.3 Devletler tarafından dahili iletişimlerinde ve bilgi dağıtımlarında ele alınması gereken bilgi örnekleri aşağıdakileri içerir:

a) Devlet Emniyet Programı (SSP) dokümantasyonu, politikaları ve prosedürleri;

b) Emniyet Performansı Göstergeleri (SPI'ler);

c) sektöre ilişkin emniyet performansı bilgileri;

d) sektöre ilişkin organizasyonel emniyet riskleri profilleri;

e) sistem emniyeti sorumluluğunun iletilmesi;

f) kazalardan ve olaylardan öğrenilen dersler ve

g) emniyet yönetimine ilişkin kavramlar ve en iyi uygulamalar.

8.6.8.4 Hizmet sağlayıcılarının birden fazla Devlet tarafından onaylandığı hallerde, emniyet iletişimine ilişkin açık hatlara yönelik belirli bir ihtiyaç söz konusudur.

8.6.8.5 Diğerlerinin yanı sıra haber bültenleri, bültenler, kitapçıklar, yayınlar, seminerler, toplantılar, eğitim, web siteleri, posta listeleri, sosyal medyadaki yayınlar, işbirliği gruplarında gerçekleştirilen tartışmalar gibi, Devlet organizasyonları tarafından emniyet iletişimlerinin dahilen iletilmesi için benimsenebilecek birçok yöntem mevcuttur.

8.6.8.6 Belirli bir mesajın iletilmesi için hangi tür medyanın kullanılması gerektiği değerlendirilirken, söz konusu organizasyon tarafından her bir mesaj ve söz konusu mesajın hedef kitlesi için hangisinin daha uygun olduğu değerlendirilmelidir. Devlet Emniyet Programı (SSP) dokümanları, ihtiyaç duyulduğunda personel için kolaylıkla ulaşılabilir halde olan bir web sitesinde ilan edilebilecektir. Öğrenilen dersler ve en iyi uygulamalar gibi diğer bilgiler ise periyodik bülten veya haber bülteni için daha uygun olabilecektir.

8.6.8.7 Birden fazla medya kullanılarak belirli bir kaygıya veya tehlikeye işaret edilmesine yönelik kampanyaların oluşturulması söz konusu soruna yönelik farkındalığın arttırılmasında ve personelin tutumunun değiştirilmesinde etkili olabilecektir.

8.6.9 Emniyet bilgilerinin haricen bildirilmesi ve yayılması

8.6.9.1 Söz konusu Devlet tarafından, Emniyet Yönetimi Sisteminin (SMS) uygulanmasını kolaylaştırmak ve sistem genelindeki emniyet kültürünü geliştirmek için uygun iletişim platformları veya ortam tesis edilmelidir.

8.6.9.2 Emniyet bilgilerinin havacılık endüstrisi genelinde haricen bildirilmesi ve yayılması sırasında, bir önceki madde kapsamında sunulan unsurlara ilaveten, Devletler tarafından aşağıdakilerin göz önünde bulundurulması gerekir:

a) Emniyet Yönetimi Sisteminin (SMS) uygulanmasına yönelik kılavuz materyal;

b) raporlamanın önemi;

c) havacılık topluluğuna yönelik mevcut emniyet eğitiminin belirlenmesi;

d) aşağıdakiler arasında emniyet bilgilerinin alışverişinin teşvik edilmesi;

1) hizmet sağlayıcıları ile ve hizmet sağlayıcıları arasında ve

2) Devletler arasında.

8.6.9.3 Söz konusu Devletin Devlet Emniyet Programı (SSP) dokümantasyonunun ve ilgili emniyet ve yürütme politikalarının aynı zamanda hizmet sağlayıcılarına, uygun görüldüğü şekilde temin edilmesi gerekir.

8.6.9.4 Esas itibariyle, içerik her iki kitle için de faydalı olduğu sürece, dahili iletişimler için kullanılan aynı destek ortamı haricen de kullanılabilir. Bununla birlikte, harici iletişim için, emniyet bilgilerinin alışverişine yönelik sektörel topluluklar oluşturan ve bu sayede mesajların ulaşmasını arttıran sosyal medya, postalama listesi bültenleri, seminerler gibi, daha büyük kitlelere ulaşan çözümlere özel dikkat gösterilmesi gerekebilecektir.

8.6.9.5 Ulusal hukuk kapsamında aksi öngörülmediği sürece, Devletler tarafından havacılık topluluğu arasında emniyet bilgilerinin paylaşılmasına veya alışverişine yönelik ağların oluşturulması teşvik edilmelidir.

8.7 DEVLET EMNİYET PROGRAMININ (SSP) UYGULANMASI

Herhangi bir büyük çaplı proje uygulaması çalışmasında olduğu gibi, Devlet Emniyet Programı (SSP) uygulaması belirlenmiş bir zaman aralığı dahilinde tamamlanması gereken bir çok görev ve alt görev içerir. Görevlerin sayısının yanı sıra her bir görevin kapsamı, söz konusu Devletin emniyet gözetimi sisteminin olgunluğa bağlıdır. Çoğu Devlette, Devlet Emniyet Programının (SSP) geliştirilmesine ve uygulanmasına birçok organizasyon ve kuruluş dahil olur. Bir uygulama planının geliştirilmesi bu sürecin kolaylaştırılmasına yardımcı olur. Bu bölümde, kapsamlı bir sistem tanımının geliştirilmesinden, ölçeklendirilebilirliğe yönelik olarak dikkate alınması gereken hususlardan, boşluk analizinin gerçekleştirilmesinden ve sağlam bir Devlet Emniyet Programı (SSP) temelinin oluşturulmasının sağlanmasını içeren uygulama planının oluşturulmasından adımlar ortaya konmaktadır. Bu bölümde ayrıca, Devlet Emniyet Programının (SSP) olgunluğuna yönelik sürekli değerlendirme ele alınmaktadır.

8.7.1 Devletin sivil havacılık sistemi tanımı ve ölçeklendirilebilirliğe yönelik olarak dikkate alınması gereken hususlar

8.7.1.1 Devletin havacılık sisteminin boyutunun ve karmaşıklığının ve unsurlar arasındaki etkileşimlerin anlaşılması, Devlet Emniyet Programının (SSP) planlanması bakımından esastır. Devlet tarafından Devlet Emniyet Programının (SSP) uygulanması gerekli olmakla birlikte, gerekliliklerin nasıl karşılandığı havacılık sisteminin boyutuna ve karmaşıklığına bağlı olacaktır. Ölçeklendirilebilirliğe ilişkin daha fazla bilgiye 1. Bölüm kapsamında ulaşılabilir.

8.7.1.2 Devlet Emniyet Programında (SSP) aynı zamanda, her bir havacılık alanındaki hizmet sağlayıcısı sayısı, bunların boyutu ve karmaşıklığı ile bölgesel ortam göz önünde bulundurulacaktır. Küçük sayıda hizmet sağlayıcılarına sahip olan Devletler tarafından bölgesel ortaklıkların kurulması göz önünde bulundurulmalıdır. Diğer Devletler ile veya Bölgesel Emniyet Gözetimi Organizasyonları (RSOO'lar) vasıtasıyla bölgesel ortaklıklar ve öğrenilen derslerin ve emniyet riski bilgilerinin paylaşılması, Devlet Emniyet Programının (SSP) uygulanmasının faydalarını azami hale getirirken etkiyi minimuma indirecektir.

8.7.1.3 Söz konusu Devlet tarafından, sivil havacılık sistemi tanımında çeşitli Devlet havacılık otoriteleri ile havacılık sistemi tanımlanmalıdır. Organizasyonel yapılara ve arayüz bağlantılarına ilişkin genel bakış buna dahil olmalıdır. Bu tanımlama, Devlet Emniyet Programı (SSP) uygulama planlama süreci kapsamındadır. Böyle bir gözden geçirmede aşağıdakilere ilişkin bir açıklamaya yer verilmelidir:

a) çeşitli Devlet havacılık otoriteleri de dahil olmak üzere, mevcut havacılık düzenleyici çerçevesinin yapısı;

b) çeşitli düzenleyici otoritelerin emniyet yönetimi görevleri ve sorumlulukları;

c) organizasyonlar arasında Devlet Emniyet Programının (SSP) koordinasyonuna yönelik platform veya mekanizma ve

d) Devlet seviyesinde ve her bir organizasyon bünyesinde olmak üzere dahili bir gözden geçirme mekanizması.

8.7.2 Devlet Emniyet Programı (SSP) boşluk analizi ve uygulama planı

Devlet Emniyet Programı (SSP) boşluk analizi

8.7.2.1 Devlet Emniyet Programı (SSP) uygulama planının oluşturulması öncesinde boşluk analizi gerçekleştirilmelidir. Boşluk analizinin amacı, mevcut Devlet yapıları ve süreçleri ile söz konusu Devlette etkin bir Devlet Emniyet Programı (SSP) uygulaması için gerekli olanlar arasındaki boşluğa ilişkin detaylı bir anlayışa ulaşılmasıdır. Birçok Devlet için, boşluk analizi, hatırı sayılır ölçüde emniyet yönetimi kabiliyetinin halihazırda mevcut olduğunu ortaya çıkarır. Buradaki zorluk ise, tipik olarak, söz konusu mevcut kabiliyetlerin geliştirilmesi, tekrar uyumlu hale getirilmesi ve desteklenmesidir. Tedbir gerektiren olarak belirlenen unsurlar veya süreçler, Devlet Emniyet Programı (SSP) uygulama planının temelini teşkil eder.

Devlet Emniyet Programı (SSP) temeli

8.7.2.2 Devletler tarafından, etkin Devlet Emniyet Programı (SSP) uygulamasını desteklemek üzere olgun bir temelin oluşturulması elzemdir. Global Havacılık Emniyeti Planı (GASP) amaçları, Devletler tarafından etkin emniyet gözetimi sistemlerinin, Devlet Emniyet Programlarının (SSP'ler) ve gelecekteki havacılık sistemlerini destekleyecek gelişmiş emniyet yönetimi kabiliyetlerinin aşamalı olarak uygulanmasını gerektirmektedir. Bu temel, daha performansa dayalı bir yaklaşımın desteklenmesi için ihtiyaç duyulan emniyet gözetimi sisteminin unsurlarından oluşur.

8.7.2.3 Bu temeldeki eksikliklerin belirlenmesi için ICAO Evrensel Emniyet Gözetimi Denetim Programı (USOAP) vasıtasıyla toplanan veriler kullanılabilir. Etkin Devlet Emniyet Programı (SSP) uygulamasıyla bağlantılı olan sorunlara ilişkin tatminkar olmayan Evrensel Emniyet Gözetimi Denetim Programı (USOAP) protokolü sorularının ele alınması, Devlet Emniyet Programının (SSP) uygulanmasındaki ilk adım olmalıdır.

Devlet Emniyet Programı (SSP) uygulama planı

8.7.2.4 Devlet Emniyet Programı (SSP) uygulamasının amacı, mevcut Devlet Emniyet Gözetiminin (SSO) ve emniyet yönetimi süreçlerinin aşamalı olarak iyileştirilmesidir. Uygun görevler/alt görevler bir eylem planı kapsamında önceliklendirilir ve belgelendirilir. Devlet Emniyet Programı (SSP) üst seviye (açıklama) dokümanı ile birlikte Devlet Emniyet Programı (SSP) uygulama planı, söz konusu Devletin etkin Devlet Emniyet Programına (SSP) ve emniyet performansının sürekli olarak iyileştirilmesine yönelik yolculuğunu yönlendiren "modelleri" ortaya koyar. Dahil olan herkesin Devlet Emniyet Programının ve uygulamaya yönelik planlarının bilincinde olmasını sağlamak için bu iki kilit dokümanın tüm ilgili personel tarafından kolaylıkla ulaşılabilir olması sağlanmalıdır.

8.7.3 Devlet Emniyet Programı (SSP) olgunluk değerlendirmesi

Geri plan ve amaç

8.7.3.1 Devlet Emniyet Programının (SSP) olgunluğuna yönelik değerlendirme, ICAO Standartlarını ve Tavsiye Edilen Uygulamaları (SARP'lar) ve söz konusu Devlet tarafından ihtiyaçlarını karşılamak üzere oluşturulan kılavuz materyali yansıtan bir araç kullanılarak gerçekleştirilmelidir. Söz konusu araç, Devletler tarafından, Devlet Emniyet Programının (SSP) sürekli olarak iyileştirilmesine ilişkin iç denetimlerin gerçekleştirilmesi için kullanılmalıdır. Bunlara, aynı zamanda, ICAO ve uygun görüldüğü üzer diğer harici kuruluşlar tarafından başvurulmalıdır. Söz konusu araç, söz konusu Devlet tarafından Devlet Emniyet Programının (SSP) etkinliğinin değerlendirilmesi için kullanılabilen bir sorular (veya beklentiler) dizisine dayalı olmalıdır. Devlet Emniyet Programı (SSP) olgunluk değerlendirmesi, tüm ilgili taraflardan bir çapraz kesitle, yüz yüze tartışmalar ve görüşmeler gibi etkileşimlerden faydalanacaktır. Söz konusu araç esnek olmalı ve söz konusu Devletin havacılık sisteminin boyutuna ve karmaşıklığına tekabül etmelidir.

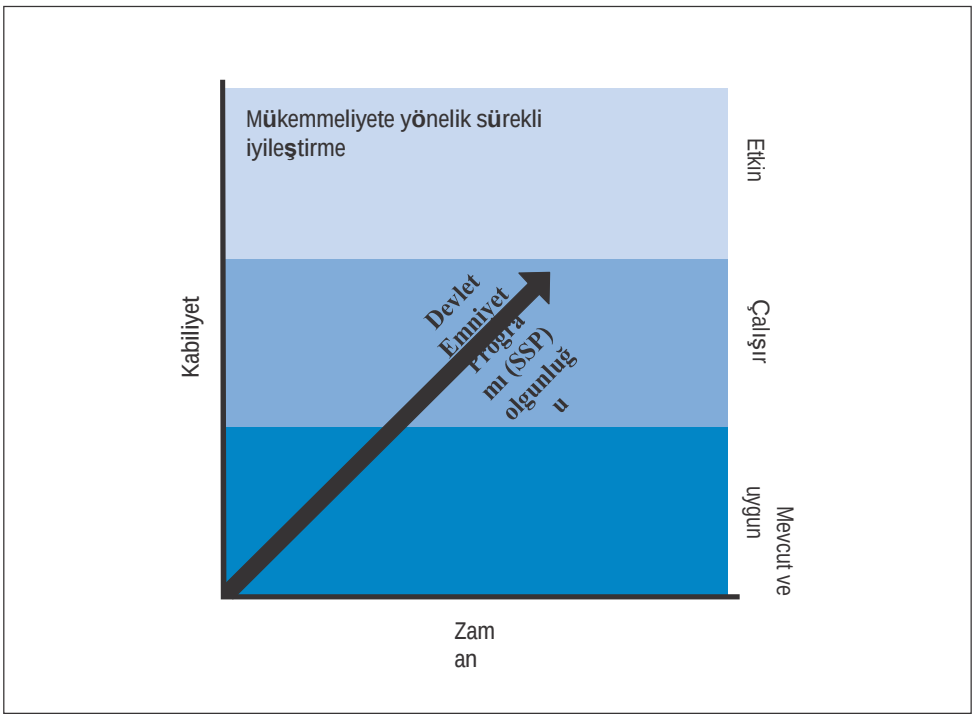
Değerlendirme

8.7.3.2 Devlet Emniyet Programının (SSP) temel unsurlarının oluşturulması sonrasında, dokümantasyona yönelik bir değerlendirme gerçekleştirilebilir. Bu değerlendirmenin amacı, Devlet Emniyet Programına (SSP) yönelik uyum ve performans beklentilerinin mevcut ve uygun olup olmadığını tespit etmektir. Değerlendirmeyi destekleyecek kanıt toplanmalıdır. Daha sonraki bir aşamada, Devlet Emniyet Programı (SSP), ne kadar iyi çalıştığının ve amaçlarına ulaşılmasında ne denli etkin olduğunun anlaşılabilmesi için değerlendirmeye tabi tutulabilir. Netice her defasında arzu edilen sonucu ortaya koyduğunda etkinliğe ulaşılır. Değerlendirme, normalde, uygun Devlet Emniyet Programı (SSP) yetkinliğine ve teknik uzmanlığa sahip olan bir ekip tarafından gerçekleştirilir ve kanıt, yine bu ekip tarafından toplanır. Değerlendirmenin, söz konusu organizasyon genelindeki etkinliğinin tespit edilmesi için organizasyonun farklı seviyelerindeki bir dizi kişi ile etkileşime imkan veren bir şekilde yapılandırılması önemlidir. Örneğin, emniyet politikasının yürürlüğe konduğu ve personel tarafından anlaşıldığı derecenin belirlenmesi, personelin çapraz kesitiyle etkileşim gerektirecektir.

Kesintisiz izleme ve sürekli iyileştirme

8.7.3.3 Söz konusu Devlet tarafından aynı araç, kesintisiz izleme ve sürekli iyileştirme sırasında Devlet Emniyet Programının (SSP) etkinliğinin değerlendirilmesi için kullanılabilecektir. Değerlendirmenin havacılık sistemindeki değişiklikleri saptaması muhtemel olacaktır. Çoğu Devlet için, Devlet Emniyet Programının (SSP) uygulanması zaman alacak ve tüm unsurların etkin bir şekilde çalıştığı bir olgunluk seviyesine gelmesi birkaç yıl alacaktır. Şekil 8-5 kapsamında, Devlet tarafından Devlet Emniyet Programı (SSP) uygulandıkça ve geliştirildikçe Devlet Emniyet Programının (SSP) olgunluğuna ilişkin farklı seviyeler gösterilmektedir.

8.7.3.4 Başlangıçta kilit unsurların mevcudiyetine ve uygunluğuna bakılarak çeşitli aşamalarda Devlet Emniyet Programı (SSP) değerlendirmesi gerçekleştirilebilir. Daha sonraki bir aşamada, Devlet Emniyet Programı (SSP), ne kadar iyi çalıştığının ve amaçlarına ulaşılmasında ne denli etkin olduğunun anlaşılabilmesi için değerlendirmeye tabi tutulabilir. Devletler, mükemmeliyete yönelik sürekli iyileştirmeyi desteklemek için periyodik olarak değerlendirmeler gerçekleştirmeye devam edebilirler.



Şekil 8-5. Devlet Emniyet Programı (SSP) olgunluk yolculuğu

Bölüm 9

EMNİYET YÖNETİMİ SİSTEMLERİ (SMS)

9.1 GİRİŞ

9.1.1 Bu bölümde, Annex 19'a uygun olarak Emniyet Yönetimi Sistemi (SMS) çerçevesinin uygulanmasına ilişkin olarak hizmet sağlayıcılarına yönelik rehberlik ile Emniyet Yönetimi Sisteminin (SMS) gözetimine ilişkin olarak Devletlere yönelik rehberlik sunulmaktadır.

9.1.2 Emniyet Yönetimi Sisteminin (SMS) amacı, hizmet sağlayıcılarına, emniyetin yönetilmesine yönelik sistematik bir yaklaşımın sağlanmasıdır. Tehlikelerin tanımlanması, emniyet verilerinin ve emniyet bilgilerinin toplanması ve analiz edilmesi ve emniyet risklerinin sürekli olarak değerlendirilmesi vasıtasıyla emniyet performansının sürekli olarak iyileştirilmesi için tasarlanmıştır. Emniyet Yönetimi Sistemi (SMS), havacılık kazalarıyla ve olaylarıyla sonuçlanmaları öncesinde emniyet risklerinin proaktif bir şekilde hafifletmeyi amaçlar. Hizmet sağlayıcılarına, havacılık emniyetine sağladıkları katkıya dair daha fazla anlayış kazandırırken, faaliyetlerini, emniyet performansını ve kaynakları etkin bir şekilde yönetme imkanı verir. Etkin bir Emniyet Yönetimi Sistemi (SMS), Devletlere, söz konusu hizmet sağlayıcısının emniyet risklerini yönetme becerisini sergiler ve Devlet seviyesinde ekin emniyet yönetimine imkan verir.

9.1.3 Uluslararası genel havacılık işletmeleri tarafından işletmekte oldukları uçaklara yönelik Emniyet Yönetimi Sistemi (SMS) kriterleri Tescil Devleti tarafından belirlendiği şekilde tespit edilmeli ve Emniyet Yönetimi Sistemlerinin (SMS) Tescil Devleti nezdinde kabul edilebilir olması sağlanmalıdır. Emniyet Yönetimi Sisteminin (SMS) kabul edilebilirliğini kolaylaştırmak üzere, uluslararası genel havacılık işletmeleri tarafından Tescil Devletinden herhangi bir sektörel uygulama esasına izin verilip verilmediği sorulmalıdır.

9.1.4 Annex 6, Kısım I'e uygun olarak tanzim olunan Hava İşletme Ruhsatına (AOC) sahip olarak birden fazla Tescil Devleti kapsamındaki büyük veya turbojet uçakların işleticilerinin hizmet sağlayıcıları olduğu değerlendirilmektedir ve bu sebeple, Emniyet Yönetimi Sistemi (SMS), İşletici Devleti nezdinde kabul edilebilir kılınmalıdır.

9.2 EMNİYET YÖNETİMİ SİSTEMİ (SMS) ÇERÇEVESİ

9.2.1 Emniyet Yönetimi Sisteminin (SMS) uygulanmasına ve sürdürülmesine yönelik çerçeve Annex 19 kapsamında belirtilmektedir. Söz konusu hizmet sağlayıcısının boyutuna ve karmaşıklığına bakılmaksızın, Emniyet Yönetimi Sistemi (SMS) çerçevesinin tüm unsurları uygulanır. Uygulamanın, söz konusu organizasyona ve söz konusu organizasyonun faaliyetlerine uyarlanması gerekir.

9.2.2 ICAO Emniyet Yönetimi Sistemi (SMS) çerçevesi aşağıdaki dört bileşenden ve on iki unsurdan oluşur:

Tablo 10. ICAO EMNİYET YÖNETİMİ SİSTEMİ (SMS) çerçevesinin bileşenleri ve unsurları

BİLEŞEN	*UNSUR*
1. Emniyet politikası ve amaçları	1.1 Yönetim taahhüdü
	1.2 Emniyet mesuliyeti ve sorumlulukları
	1.3 Kilit öneme sahip olan emniyet personelinin tayini
	1.4 Acil durum müdahale planlamasının koordinasyonu
	1.5 Emniyet Yönetimi Sistemi (SMS) dokümantasyonu
2. Emniyet riski yönetimi	2.1 Tehlike tanımlama
	2.2 Emniyet riski değerlendirmesi ve hafifletmesi
3. Emniyet güvencesi	3.1 Emniyet performansı izlemesi ve ölçümü
	3.2 Değişiklik yönetimi
	3.3 Emniyet Yönetimi Sisteminin (SMS) sürekli iyileştirilmesi
4. Emniyet teşviki	4.1 Eğitim ve öğretim
	4.2 Emniyet iletişimi

9.3 1. BİLEŞEN: EMNİYET POLİTİKASI VE AMAÇLARI

9.3.1 Emniyet Yönetimi Sistemi (SMS) çerçevesinin ilk bileşeni, emniyet yönetiminin etkin olabileceği bir ortamın oluşturulmasına odaklanır. Üst yönetimin emniyete yönelik taahhüdünü, hedeflerini ve destekleyici organizasyon yapısını ortaya koyan bir emniyet politikasına ve amaçlarına dayandırılır.

9.3.2 Yönetim taahhüdü ve emniyet liderliği, etkin bir Emniyet Yönetimi Sisteminin (SMS) uygulanması bakımından kilit öneme sahiptir ve emniyet politikası ve emniyet amaçlarının belirlenmesiyle ortaya koyulur. Emniyete yönelik yönetim taahhüdü, yönetim karar alma ve kaynak tahsisatı vasıtasıyla kanıtlanır; pozitif emniyet kültürünün oluşturulması için bu kararların ve tedbirlerin daima emniyet politikası ve amaçları ile tutarlı olması gerekir.

9.3.3 Emniyet politikasının üst yönetim tarafından geliştirilmesi ve onaylanması ve sorumlu yönetici tarafından imzalanması gerekir. Karşılıklı sorumluluk hissinin teşvik edilmesi için emniyet politikasının ve emniyet amaçlarının geliştirilmesinde kilit öneme sahip olan personele ve uygun olduğunda personeli temsil eden organlara (çalışan forumları, işçi sendikaları) danışılması gerekir.

9.3.4 Yönetim taahhüdü

Emniyet politikası

9.3.4.1 Emniyet politikasının üst yönetim ve sorumlu yönetici tarafından görülür bir şekilde onaylanması gerekir. "Görülür onay", yönetim tarafından emniyet politikasına verilen aktif desteğin organizasyonun geri kalanı tarafından görülür hale getirilmesi anlamına gelir. Bu, herhangi bir iletişim yöntemiyle ve faaliyetlerin emniyet politikasına uyumlu hale getirilmesiyle yapılabilir.

9.3.4.2 Tüm personelin emniyet politikasını anlamasını ve emniyet politikasına uygun olarak çalışmasını sağlamak için organizasyon genelinde emniyet politikasının iletilmesi yönetimin sorumluluğundadır.

9.3.4.3 Organizasyonun emniyete yönelik taahhüdünü yansıtmak üzere, emniyet politikasında aşağıdakilere yönelik taahhüde yer verilmelidir:

a) emniyet performansı seviyesinin sürekli olarak iyileştirilmesi;

b) organizasyon dahilinde pozitif emniyet kültürünün teşvik edilmesi ve sürdürülmesi;

c) tüm geçerli düzenleyici gerekliliklere riayetin sağlanması;

d) emniyetli bir ürün veya hizmet sunulması için gerekli kaynakların sağlanması;

e) emniyetin tüm yöneticilerin birincil sorumluluğu olmasının sağlanması ve

f) tüm seviyelerde anlaşılmasının, uygulanmasının ve sürdürülmesinin sağlanması.

9.3.4.4 Emniyet politikasının, aynı zamanda, emniyet sorunlarının rapor edilmesini teşvik etmek ve rapor edilen emniyet olayları veya emniyet sorunları halinde uygulanan disiplin politikası hakkında personeli bilgilendirmek üzere emniyet raporlaması sistemine atıfta bulunması gerekir.

9.3.4.5 Disiplin politikası, organizasyon tarafından herhangi bir disiplin tedbirinin alınmasının gerekli olup olmadığının belirlenmesi için herhangi bir hatanın veya kural ihlalinin gerçekleşip gerçekleşmediğini tespit etmek için kullanılır. Dahil olan kişilere adil muamelede bulunulmasını sağlamak için, bu tespitte bulunulmasından sorumlu olanların, söz konusu olayın bağlamı tümüyle değerlendirilebilecek şekilde gerekli teknik uzmanlığa sahip olmaları elzemdir.

9.3.4.6 Emniyet verilerinin ve emniyet bilgilerinin yanı sıra raporlamada bulunanların korunmasına yönelik bir politika raporlama kültürü üzerinde pozitif bir etkiye sahip olabilir. Söz konusu hizmet sağlayıcısı ve Devlet tarafından, personeli veya spesifik hizmet sağlayıcılarını belirtmek zorunda kalmadan anlamlı emniyet analizlerinin gerçekleştirilmesine imkan vermek üzere raporların kimliksizleştirilmesine ve bir araya getirilmesine imkan verilmesi gerekir. Büyük çaplı olaylar hizmet sağlayıcısının Emniyet Yönetimi Sisteminin (SMS) dışında olan süreçleri ve prosedürleri başlatabilecek, ilgili Devlet otoritesi tarafından her durumda raporların önceden kimliksizleştirilmesine izin verilmeyebilecektir. Yine de raporların uygun bir şekilde kimliksizleştirilmesine imkan veren bir politika, toplanan verilerin niteliğini iyileştirebilir.

Emniyet amaçları

9.3.4.7 Kendi emniyet politikasını göz önünde bulundurarak, söz konusu hizmet sağlayıcısı tarafından, aynı zamanda, emniyet sonuçlarına ilişkin olarak neye ulaşmayı amaçladığının tanımlanması için emniyet amaçlarının belirlenmesi gerekir. Emniyet amaçlarının, söz konusu organizasyonun emniyet önceliklerine ilişkin kısa, üst seviye beyanlar olmaları ve en belirgin emniyet risklerine işaret etmeleri gerekir. Emniyet amaçlarına emniyet politikasında yer verilebilir (veya emniyet amaçları ayrı olarak belgelenebilir) ve emniyet amaçları, söz konusu organizasyon tarafından emniyet bakımından ulaşılması amaçlanan şeyleri tanımlar. Bu emniyet amaçlarının başarısının izlenmesi için emniyet performansı göstergelerine (SPI'ler) ve emniyet performansı hedeflerine (SPT'ler) ihtiyaç duyulur ve bu Bölümde 3. Bileşen kapsamında bunlara ilişkin ayrıntılar ayrıca belirtilmektedir.

9.3.4.8 Güncel halde kalmaya devam ettiklerinden emin olmak için emniyet politikasının ve emniyet amaçlarının periyodik olarak gözden geçirilmesi gerekir (örneğin, sorumlu yönetici değişikliği bunların gözden geçirilmesini gerektirecektir).

9.3.5 Emniyet mesuliyeti ve sorumlulukları

Sorumlu yönetici

9.3.5.1 Tipik olarak genel müdür olmak üzere, sorumlu yönetici, söz konusu organizasyonun emniyetli operasyonu üzerinde nihai yetkiye sahip olan kişidir. Sorumlu yönetici, emniyeti ana bir organizasyonel değer olarak aşılayan emniyet amaçlarını ve emniyet politikasını belirler ve teşvik eder. Sorumlu yöneticinin, söz konusu organizasyon hesabına karar alma yetkisine sahip olması, gerek mali kaynaklar gerek insan kaynakları olmak üzere, kaynakların kontrolüne sahip olması, emniyet sorunlarına ve emniyet risklerine işaret edilmesi için uygun tedbirlerin alınmasının sağlanmasından sorumlu olması ve kazalara ve olaylara karşılık verilmesinden sorumlu olması gerekir.

9.3.5.2 Söz konusu hizmet sağlayıcısı için, özellikle birden fazla kuruluşa ve birden fazla sertifikaya, yetkilendirmeye veya onaya sahip olan büyük çaplı karmaşık organizasyonlarda olmak üzere, sorumlu yönetici olmaya en uygun kişinin belirlenmesine yönelik zorluklar söz konusu olabilecektir. Seçilen kişinin organizasyonel olarak söz konusu organizasyonun en yüksek seviyesinde konumlandırılması ve bu sayede doğru stratejik emniyet kararlarının alınmasının sağlanması önemlidir.

9.3.5.3 Hizmet sağlayıcısı tarafından, sorumlu yöneticinin, Emniyet Yönetimi Sisteminin (SMS) etkin olmasının sağlanmasına yönelik işlem yapma yetkisiyle söz konusu organizasyondaki herhangi bir seviyedeki genel emniyet performansına ilişkin sorumluluk verilerek belirlenmesi gerekmektedir. Yönetimin tüm üyelerinin spesifik emniyet mesuliyetlerinin tanımlanması ve bu kişilerin Emniyet Yönetimi Sistemine (SMS) ilişkin görevlerinin bu kişiler tarafından pozitif emniyet kültürüne nasıl katkı sağlanabildiğini yansıtması gerekir. Emniyet sorumlulukları, mesuliyetleri ve yetkileri, organizasyonun genelinde belgelenmeli ve bildirilmelidir. Yöneticilerin emniyet mesuliyetleri, Emniyet Yönetimi Sisteminin (SMS) etkin ve etkili performansı için gerekli olan insan kaynaklarının, teknik, mali veya diğer kaynakların tahsis edilmesini kapsamalıdır.

Not.— "Mesuliyet" terimi, delege edilemeyen yükümlülüklere atıfta bulunmaktadır. "Sorumluluklar" terimi, delege edilebilecek olan işlevlere ve faaliyetlere atıfta bulunmaktadır.

9.3.5.4 Emniyet Yönetimi Sisteminin (SMS), tümü aynı tüzel kişiliğin kapsamında olan birçok farklı sertifikaya, yetkilendirmeye veya onaya uygulandığı hallerde, tek bir sorumlu yöneticinin olması gerekir. Bunun mümkün olmadığı hallerde, her bir organizasyonel sertifika, yetkilendirme veya onay için münferit sorumlu yöneticilerin belirlenmesi ve mesuliyete ilişkin aşık hatların tanımlanması gerekir; bu kişilerin emniyet mesuliyetlerinin nasıl koordine edileceğinin belirlenmesi de önemlidir.

9.3.5.5 Sorumlu yöneticinin görülür şekilde dahil olabileceği en etkili yollardan biri düzenli olarak üst düzey emniyet toplantılarına liderlik edilmesidir. Söz konusu organizasyonun emniyetinden nihai olarak sorumlu olan kişi olması sebebiyle, bu toplantılara faal bir şekilde dahil olunması sorumlu yönetici tarafından aşağıdakilerin yapılmasına imkan verir:

a) emniyet amaçlarının gözden geçirilmesi;

b) emniyet performansının ve emniyet hedeflerine ulaşılmasının izlenmesi;

c) zamanında emniyet kararlarının alınması;

d) uygun kaynakların tahsis edilmesi;

e) yöneticilerin emniyet sorumluluklarından, performanstan ve uygulama zaman aralıklarından mesul tutulması ve

f) tüm personel tarafından emniyet ile ilgili ve emniyetten sorumlu olan bir üst düzey yetkili olarak görülme.

9.3.5.6 Sorumlu yönetici, söz konusu organizasyonun günlük faaliyetlerine veya işyerinde karşılaşılan problemlere genellikle dahil olmaz ve Emniyet Yönetimi Sistemini (SMS) yönetmek ve işletmek üzere uygun bir organizasyonel yapının olmasını sağlamalıdır. Emniyet yönetimi sorumluluğu genellikle üst yönetim ekibine veya diğer kilit öneme sahip personele delege edilir.

Emniyet Yönetimi Sisteminin (SMS) günlük çalışmasına ilişkin sorumluluğun delege edilebilmesine karşın, sorumlu yönetici tarafından ne sisteme ilişkin mesuliyet ne de emniyet risklerine ilişkin kararlar delege edilebilir. Örneğin, aşağıdaki emniyet mesuliyetleri delege edilemez:

a) emniyet politikalarının uygun olduğundan ve iletildiğinden emin olunması;

b) kaynakların gerekli şekilde tahsis edilmesinin sağlanması (finansman, personel, eğitim, iktisap) ve

c) kabul edilebilir emniyet riski limitlerinin belirlenmesi ve gerekli kontrollere kaynak sağlanması.

9.3.5.7 Sorumlu yöneticinin aşağıdaki emniyet mesuliyetlerine sahip olması uygundur:

a) etkin bir Emniyet Yönetimi Sisteminin (SMS) gereğince uygulanması için yeterli mali kaynakların ve insan kaynaklarının sağlanması;

b) pozitif emniyet kültürünün teşvik edilmesi;

c) emniyet politikasının belirlenmesi ve teşvik edilmesi;

d) organizasyonun emniyet amaçlarının belirlenmesi;

e) Emniyet Yönetimi Sisteminin (SMS) gereğince uygulanmasının ve gerekliliklere göre işlemesinin sağlanması ve

f) Emniyet Yönetimi Sisteminin (SMS) sürekli olarak iyileştirilmesine çalışılması.

9.3.5.8 Sorumlu yöneticinin yetkileri, bunlarla sınırlı kalmamak üzere, aşağıdakilere ilişkin nihai yetkiyi içerir:

a) tüm emniyet sorunlarının çözüme kavuşturulması ve

b) söz konusu operasyonu veya faaliyeti durdurma yetkisi de dahil olmak üzere, organizasyonun sertifikası, yetkilendirmesi veya onayı kapsamındaki operasyonlar.

9.3.5.9 Emniyet riski tolere edilebilirliğine ilişkin kararlar alma yetkisinin tanımlanması gerekir. Risklerin kabul edilebilirliğine ilişkin kararların kimin tarafından alınabildiği ve herhangi bir değişikliğin uygulanabileceğinin kabulüne dair yetki buna dahildir. Söz konusu yetki herhangi bir kişiye, yönetim pozisyonuna veya komiteye verilebilecektir.

9.3.5.10 Emniyet riski tolere edilebilirliğine ilişkin kararları alma yetkisinin söz konusu yöneticinin genel karar alma ve kaynak tahsisi yetkisi ile örtüşmesi gerekir. Daha düşük seviyedeki bir yönetici (veya yönetim grubu), belirli bir seviyeye kadar tolere edilebilirlik kararları almak üzere yetkilendirilebilir. Söz konusu yöneticinin yetkisini aşan risk seviyeleri, değerlendirilmek üzere daha fazla yetkiye sahip olan daha yüksek bir yönetim seviyesine intikal ettirilmelidir.

Mesuliyet ve sorumluluklar

9.3.5.11 Emniyetli ürünlerin ve operasyonların sunulmasını destekleyen emniyet ile ilgili görevlere dahil olan tüm personelin, yönetimin ve çalışanların mesuliyetleri ve sorumlulukları açık bir şekilde tanımlanmalıdır. Emniyet sorumlulukları, söz konusu çalışanın organizasyonun emniyet performansına (organizasyonel emniyet sonuçları) yönelik katkısına odaklanmalıdır. Emniyetin yönetimi ana bir işlevdir ve bu itibarla, her bir üst düzey yöneticinin, Emniyet Yönetimi Sisteminin (SMS) çalışmasına bir derece dahli söz konusudur.

9.3.5.12 Tanımlanan tüm mesuliyetler, sorumluluklar ve yetkiler, söz konusu hizmet sağlayıcısının Emniyet Yönetimi Sistemi (SMS) dokümantasyonunda belirtilmeli ve organizasyon genelinde bildirilmelidir. Her bir üst düzey yöneticinin emniyet mesuliyetleri ve sorumlulukları kendi görev tanımının ayrılmaz bileşenleridir. Bölüm yöneticileri ile emniyet yöneticisi arasındaki farklı emniyet yönetimi işlevleri de bu kapsamda yer almalıdır (detaylar için bakınız 9.3.6).

9.3.5.13 Organizasyon genelindeki emniyet mesuliyetine ilişkin çizgiler ile bunların nasıl tanımlandığı, söz konusu organizasyonun türüne ve karmaşıklığına ve tercih edilen iletişim yöntemlerine bağlı olacaktır. Tipik olarak emniyet mesuliyetleri ve sorumlulukları organizasyon şemalarında, departmanların sorumluluklarını ve personelin görev veya iş tanımlarını tanımlayan dokümanlarda yansıtılacaktır.

9.3.5.14 Hizmet sağlayıcısı tarafından, çalışanların emniyet sorumlulukları ile organizasyonel sorumlulukları arasındaki çıkar çatışmalarının önlenmesi amaçlanmalıdır. Emniyet Yönetimi Sistemi (SMS) mesuliyetlerini ve sorumluluklarını, çakışmaları ve/veya boşlukları en aza indirgeyen bir şekilde tahsis etmelidirler.

Harici organizasyonlara ilişkin olarak mesuliyet ve sorumluluklar

9.3.5.15 Herhangi bir Emniyet Yönetimi Sistemi (SMS) arayüz bağlantısı söz konusu olduğunda, harici organizasyonların emniyet performansından hizmet sağlayıcısı sorumludur. Harici organizasyonların Emniyet Yönetimi Sistemine (SMS) sahip olmalarının gerekli olmaması halinde dahi, harici organizasyonlar tarafından sunulan ve söz konusu hizmet sağlayıcısının faaliyetlerini destekleyen ürünlerin veya hizmetlerin emniyet performansından hizmet sağlayıcısı mesul tutulabilir. Emniyet Yönetimi Sistemi (SMS) ile söz konusu hizmet sağlayıcısının ürünlerinin veya hizmetlerinin emniyetli bir şekilde sunulmasına katkıda bulunan harici organizasyonların emniyet sistemleri ile arayüz bağlantısına sahip olması hizmet sağlayıcısı için elzemdir.

9.3.6 Kilit öneme sahip olan emniyet personelinin tayini

9.3.6.1 Emniyet yöneticisi görevini ifa etmek üzere yetkin bir kişinin veya kişilerin tayin edilmesi, etkin bir şekilde uygulanan ve işleyen bir Emniyet Yönetimi Sistemi (SMS) için elzemdir. Emniyet yöneticisi farklı unvanlarla belirlenebilir. Bu el kitabının amaçları doğrultusunda, "emniyet yöneticisi" genel terimi, söz konusu kişiden çok görev için kullanılır ve bu anlama gelir. Emniyet yöneticisi görevini yürüten kişi, Emniyet Yönetimi Sisteminin (SMS) uygulanması ve söz konusu organizasyondaki diğer departmanlara emniyet hizmetlerinin sunulması konusunda sorumlu yöneticiye karşı sorumludur.

9.3.6.2 Emniyet yöneticisi, sorumlu yöneticiye ve bölüm yöneticilerine emniyet yönetimi konuları hakkında tavsiyelerde bulunur ve emniyet sorunlarının organizasyon dahilinde ve havacılık topluluğunun harici üyeleriyle koordine edilmesinden ve bildirilmesinden sorumludur. Emniyet yöneticisinin görevleri, bunlarla sınırlı olmamak üzere, aşağıdakileri içerir:

a) (ilk uygulamaya müteakiben) sorumlu yönetici adına Emniyet Yönetimi Sistemi (SMS) uygulamasını yönetmek;

b) tehlike tanımlama ve emniyet riski analizini gerçekleştirmek/kolaylaştırmak;

c) düzeltici faaliyetleri izlemek ve sonuçlarını değerlendirmek;

d) organizasyonun emniyet performansına yönelik olarak periyodik raporlar sunmak;

e) Emniyet Yönetimi Sistemi (SMS) dokümantasyonunu ve kayıtlarını muhafaza etmek;

f) personel emniyet eğitimini planlamak ve kolaylaştırmak;

g) emniyet konularına yönelik olarak bağımsız tavsiyelerde bulunmak;

h) havacılık endüstrisindeki emniyet kaygılarını ve bunların söz konusu organizasyonun ürün ve hizmet sunumunun amaçlandığı çalışmaları üzerinde algılanan etkisini izlemek ve

i) emniyete ilişkin sorunlara yönelik olarak söz konusu Devletin Sivil Havacılık Otoritesi (CAA) ve diğer gerekli Devlet otoriteleriyle (sorumlu yönetici adına) koordinasyonda ve iletişimde bulunmak.

9.3.6.3 Çoğu organizasyonda, emniyet yöneticisi olarak bir birey tayin edilir. Organizasyonun boyutuna, mahiyetine ve karmaşıklığına bağlı olarak, emniyet yöneticisi rolü, özel bir görev olabilir veya diğer görevlerle birleştirilebilir. Ayrıca, bazı organizasyonlar tarafından bu görevin bir kişiler grubuna tahsis edilmesi gerekli olabilir. Söz konusu organizasyon, seçilen tercihin herhangi bir çıkar çatışmasıyla sonuçlanmadığından emin olmalıdır. Mümkün olduğu hallerde, emniyet yöneticisi, ürün veya hizmet sunumuna doğrudan dahil olmamalı, ancak bunlara ilişkin çalışma bilgisine sahip olmalıdır. Söz konusu tayinde, aynı zamanda, diğer görevler ve işlevler ile olası çıkar çatışmaları da göz önünde bulundurulmalıdır. Bu çıkar çatışmaları aşağıdakileri içerebilecektir:

a) finansman rekabeti (örneğin, finans yöneticisinin emniyet yöneticisi olması);

b) kaynaklara ilişkin çatışan öncelikler ve

c) Emniyet yöneticisinin operasyonel role ve emniyet yöneticisinin dahil olduğu operasyonel faaliyetlerin Emniyet Yönetimi Sistemi (SMS) etkinliğini değerlendirme becerisine sahip olduğu haller.

9.3.6.4 Söz konusu görevin bir kişiler grubuna tahsis edildiği hallerde (örneğin, hizmet sağlayıcıları tarafından Emniyet Yönetim Sistemleri (SMS) birden fazla faaliyete genişletildiğinde), söz konusu kişilerden birinin, sorumlu yöneticiye doğrudan ve dolambaçsız bir raporlama hattının sürdürülmesi için "baş" emniyet yöneticisi olarak görevlendirilmesi gerekir.

9.3.6.5 Emniyet yöneticisinin yetkinlikleri, bunlarla sınırlı kalmamakla birlikte, aşağıdakileri içermelidir:

a) emniyet/kalite yönetimi deneyimi;

b) organizasyon tarafından sunulan ürüne veya hizmete ilişkin operasyonel deneyim;

c) operasyonları veya sunulan ürünü/hizmeti destekleyen sistemin kavranmasına yönelik teknik geri plan;

d) çevresiyle uyum becerisi;

e) analitik ve problem çözme becerisi;

f) proje yönetimi becerileri;

g) sözlü ve yazılı iletişim becerileri ve

h) insan faktörlerinin kavranması.

9.3.6.6 Organizasyonun boyutuna, mahiyetine ve karmaşıklığına bağlı olarak emniyet yöneticisine ilave personel tarafından destek verilebilir. Emniyet yöneticisi ve destek personeli, emniyet verilerinin hızlıca toplanmasının ve analiz edilmesinin, emniyet riski kararları ve kontrolleri gerektiği şekilde alınıp yapılabilecek şekilde ilgili emniyet bilgilerinin organizasyon dahilinde uygun bir şekilde dağıtılmasının sağlanmasından sorumludurlar.

9.3.6.7 Hizmet sağlayıcıları tarafından, organizasyon genelinde Emniyet Yönetimi Sistemi (SMS) işlevlerini destekleyen uygun emniyet komiteleri tesis edilmelidir. Emniyet komitesinde kimlere yer verilmesinin gerektiği ve toplantıların sıklığının belirlenmesi buna dahil olmalıdır.

9.3.6.8 Bazen emniyet gözden geçirme kurulu (SRB) olarak anılan en üst düzey emniyet komitesi, danışman sıfatıyla katılmak üzere emniyet yöneticisi de dahil olmak üzere, sorumlu yönetici ile üst düzey yöneticileri içerir. Emniyet gözden geçirme kurulu (SRB) stratejiktir ve emniyet politikalarına, kaynak tahsisatına ve organizasyonel performansa ilişkin üst seviye konularla ilgilenir. Emniyet gözden geçirme kurulu (SRB) tarafından aşağıdaki konular izlenir:

a) Emniyet Yönetimi Sisteminin (SMS) etkinliği;

b) gerekli emniyet riski kontrol tedbirlerinin uygulanmasına zamanında karşılık verilmesi;

c) organizasyonun emniyet politikası ve amaçları karşısında emniyet performansı;

d) emniyet riski hafifletme stratejilerinin genel etkinliği;

e) organizasyonun, aşağıdakileri destekleyen emniyet yönetimi süreçlerinin etkinliği:

1) emniyet yönetimine ilişkin olarak ilan edilen organizasyonel öncelik ve

2) organizasyon genelinde emniyetin teşvik edilmesi.

9.3.6.9 En üst düzey emniyet komitesi tarafından stratejik bir yönlendirmenin oluşturulması sonrasında, emniyet stratejilerinin uygulanmasının organizasyon genelinde koordine edilmesi gerekir. Bu koordinasyon, operasyonel olarak daha odaklanmış olan emniyet eylem gruplarının (SAG'ler) oluşturulmasıyla sağlanabilir. Emniyet eylem grupları (SAG'ler) normalde yöneticilerden ve ön saftaki personelden oluşur ve bu gruplara, tayin edilen bir yönetici tarafından başkanlık edilir. Emniyet eylem grupları (SAG'ler), Emniyet Gözden Geçirme Kurulu (SRB) tarafından geliştirilen stratejilere uygun olarak spesifik uygulama sorunlarıyla ilgilenen taktik oluşumlardır. Emniyet Eylem Grupları (SAG'ler):

a) söz konusu organizasyonun kendi görev alanları dahilindeki operasyonel emniyet performansını izler ve uygun Emniyet Riski Yönetimi (SRM) faaliyetlerinin yürütülmesini sağlar;

b) mevcut emniyet verilerini gözden geçirir ve uygun emniyet riski kontrolü stratejilerinin uygulanmasını belirler ve çalışan geri bildiriminin sunulmasını sağlar;

c) operasyonel değişikliklerin veya yeni teknolojilerin uygulamaya koyulmasına ilişkin emniyet etkisini değerlendirir;

d) emniyet riski kontrollerine ilişkin tedbirlerin uygulanmasını koordine eder ve söz konusu tedbirlerin hızlı bir şekilde alınmasını sağlar ve

e) spesifik emniyet riski kontrollerinin etkinliğini gözden geçirir.

9.3.7 Acil durum müdahale planlamasının koordinasyonu

9.3.7.1 Tanım gereği, acil durum, derhal eylem gerektiren, ani, planlanmamış bir durum veya olaydır. Acil durum müdahale planlamasının koordinasyonu, herhangi bir plansız havacılık operasyonu acil durumu sırasında sınırlı bir zaman dilimi içerisinde gerçekleşen faaliyetlere yönelik planlama anlamına gelmektedir. Acil durum müdahale planı (ERP), herhangi bir hizmet sağlayıcısının sürecinin havacılık ile ilgili acil durumların, krizlerin veya olayların ele alınmasına yönelik Emniyet Riski Yönetimi (SRM) sürecinin ayrılmaz bir bileşenidir. Herhangi bir hizmet sağlayıcısının havacılık operasyonlarının veya faaliyetlerinin kamu sağlığı acil durumu/salgını gibi acil durumlarla tehlikeye düşmesine dair ihtimal olduğu hallerde, bu senaryoların aynı zamanda, uygun görüldüğü şekilde, Acil Durum Müdahale Planında (ERP) ele alınması gerekir. Acil Durum Müdahale Planında (ERP), Emniyet Yönetimi Sistemi (SMS) vasıtasıyla belirlenen önceden görülebilir acil durumların ele alınması ve havacılık ile ilgili acil durumların etkili bir şekilde yönetilmesine yönelik hafifletme tedbirlerine, süreçlere ve kontrollere yer verilmesi gerekir.

9.3.7.2 Acil Durum Müdahale Planının (ERP) genel amacı, operasyonların emniyetli bir şekilde devamını ve mümkün olan en kısa süre içerisinde normal operasyonlara geri dönülmesini sağlamaktır. Bu sayede, acil durum sorumluluklarının tayini ve yetki devri de dahil olmak üzere, normalden acil durum operasyonlarına intizamlı ve etkin bir geçiş sağlanmalıdır. Acil durum sonrasında "normal" operasyonların yeniden tesis edilmesi için gereken zaman dilimi buna dahildir. Acil Durum Müdahale Planında (ERP), herhangi bir acil durum sırasında sorumlu personel tarafından alınması gereken tedbirler belirlenir. Çoğu acil durum, farklı organizasyonlar arasında, muhtemelen diğer hizmet sağlayıcıları ve havacılık dışı ilgili acil durum hizmetleri gibi harici organizasyonlar ile koordineli eylem gerektirecektir. Acil Durum Müdahale Planının (ERP), uygun kilit personelin yanı sıra koordinasyon yapılan harici organizasyonlar tarafından kolaylıkla erişilebilir olması gerekir.

9.3.7.3 Acil durum müdahale planlamasının koordinasyonu sadece, Acil Durum Müdahale Planı (ERP) tesis ve idame ettirmesi gereken hizmet sağlayıcıları için geçerlidir. Annex 19 kapsamında Acil Durum Müdahale Planının (ERP) oluşturulması veya geliştirilmesi öngörülmemektedir; acil durum müdahale planı sadece ilgili ICAO Annex'lerinde belirlenen spesifik hizmet sağlayıcıları için geçerlidir (diğer Annex'lerde acil durum hallerinde yapılacak işlemlere ilişkin farklı şartlar kullanılabilecektir). Bu koordinasyonun, Acil Durum Müdahale Planının (ERP) periyodik olarak test edilmesi kapsamında tatbik edilmesi gerekir.

9.3.8 Emniyet Yönetimi Sistemi (SMS) Dokümantasyonu

9.3.8.1 Emniyet Yönetimi Sistemi (SMS) dokümantasyonunda, söz konusu hizmet sağlayıcısının Emniyet Yönetimi Sisteminin (SMS) organizasyon dahilindeki idaresinin, bildirilmesinin ve sürdürülmesinin kolaylaştırılmasına yönelik Emniyet Yönetimi Sistemi (SMS) politikalarını, süreçlerini ve prosedürlerini açıklayan üst seviye bir "Emniyet Yönetimi Sistemi (SMS) el kitabı" yer almalıdır. Söz konusu el kitabı, personelin, söz konusu organizasyonunun Emniyet Yönetimi Sisteminin (SMS) nasıl işlediğini ve emniyet politikasının ve amaçlarının nasıl karşılanacağını anlamasına yardımcı olmalıdır. Dokümantasyonda, Emniyet Yönetimi Sisteminin (SMS) sınırlarını öngören bir sistem tanımı yer almalıdır. Aynı zamanda, çeşitli politikalar, süreçler ve prosedürler ile uygulamalar arasındaki ilişkinin açıklanmasına yardımcı olmalı ve bunların söz konusu hizmet sağlayıcısının emniyet politikası ve amaçlarıyla nasıl bağlantılı olduğunu tanımlamalıdır. Dokümantasyon, organizasyon genelindeki personel tarafından kolaylıkla anlaşılabilecek günlük emniyet yönetimi faaliyetleri ele alınacak şekilde uyarlanmalı ve yazılmalıdır.

9.3.8.2 Emniyet Yönetimi Sistemi (SMS) el kitabı, aynı zamanda, hizmet sağlayıcısı ile önemli emniyet paydaşları (örneğin, Emniyet Yönetimi Sisteminin (SMS) mevzuata dayalı kabulü, değerlendirmesi ve sonraki izlemesi amacıyla Sivil Havacılık Otoritesi (CAA)) arasındaki birincil emniyet iletişimi aracı işlevini görür. Emniyet Yönetimi Sistemi (SMS) el kitabı bağımsız bir doküman olabilir veya söz konusu hizmet sağlayıcısı tarafından muhafaza edilen diğer organizasyonel dokümanlarla (veya dokümantasyonla) entegre edilebilir. Söz konusu organizasyonun Emniyet Yönetimi Sistemi (SMS) süreçlerine ilişkin detayların mevcut dokümanlar kapsamında halihazırda ele alınmış olduğu hallerde, bu dokümanlara çapraz referans yapılması yeterlidir. Bu Emniyet Yönetimi Sistemi (SMS) dokümanı güncel halde tutulmalıdır. Kontrollü el kitabı olması sebebiyle, Emniyet Yönetimi Sistemi (SMS) el kitabında önemli değişikliklerin yapılması öncesinde Sivil Havacılık Otoritesi (CAA) mutabakatı gerekebilir.

9.3.8.3 Emniyet Yönetimi Sistemi (SMS) el kitabında, aşağıdakiler de dahil olmak üzere, söz konusu hizmet sağlayıcısının politikalarına, süreçlerine ve prosedürlerine ilişkin detaylı bir açıklama yer almalıdır:

a) emniyet politikası ve emniyet amaçları;

b) geçerli mevzuata dayalı Emniyet Yönetimi Sistemi (SMS) gerekliliklerine atıf;

c) sistem tanımı;

d) emniyet mesuliyetleri ve kilit öneme sahip olan emniyet personeli;

e) gönüllü ve zorunlu emniyet raporlaması sistemi süreçleri ve prosedürleri;

f) tehlike tanımlama ve emniyet riski değerlendirmesi süreçleri ve prosedürleri;

g) emniyet soruşturması prosedürleri;

h) emniyet performansı göstergelerinin belirlenmesine ve izlenmesine yönelik prosedürler;

i) Emniyet Yönetimi Sistemi (SMS) eğitimi süreçleri ve prosedürleri ve iletişimi;

j) emniyet iletişimi süreçleri ve prosedürleri;

k) iç denetim prosedürleri;

l) değişiklik yönetimi prosedürleri;

m) Emniyet Yönetimi Sistemi (SMS) dokümantasyon yönetimi prosedürleri ve

n) uygulanabildiği hallerde, acil durum müdahale planlamasının koordinasyonu.

9.3.8.4 Emniyet Yönetimi Sistemi (SMS) dokümantasyonu aynı zamanda, Emniyet Yönetimi Sisteminin (SMS) varlığını ve sürekli çalışmasını doğrulayan operasyonel kayıtların derlenmesini ve muhafaza edilmesini de kapsar. Operasyonel kayıtlar, Emniyet Riski Yönetimi (SRM) ve emniyet güvencesi faaliyetleri gibi Emniyet Yönetimi Sistemi (SMS) süreçlerinin ve prosedürlerinin çıktılarıdır. Emniyet Yönetimi Sistemi (SMS) operasyonel kayıtlarının mevcut saklama sürelerine uygun olarak saklanması ve muhafaza edilmesi gerekir. Tipik Emniyet Yönetimi Sistemi (SMS) operasyonel kayıtları şunları içermelidir:

a) tehlike kayıt defteri ve tehlike/emniyet raporları;

b) Emniyet Performansı Göstergeleri (SPI'ler) ve ilgili çizelgeler;

c) tamamlanan emniyet riski değerlendirmelerine ilişkin kayıtlar;

d) Emniyet Yönetimi Sistemi (SMS) iç gözden geçirme ve denetim kayıtları;

e) iç denetim kayıtları;

f) Emniyet Yönetimi Sistemi (SMS) kayıtları/emniyet eğitimi kayıtları;

g) Emniyet Yönetimi Sistemi (SMS)/emniyet komitesi toplantı tutanakları;

h) Emniyet Yönetimi Sistemi (SMS) uygulama planı (ilk uygulama sırasında) ve

i) uygulama planının desteklenmesine yönelik boşluk analizi.

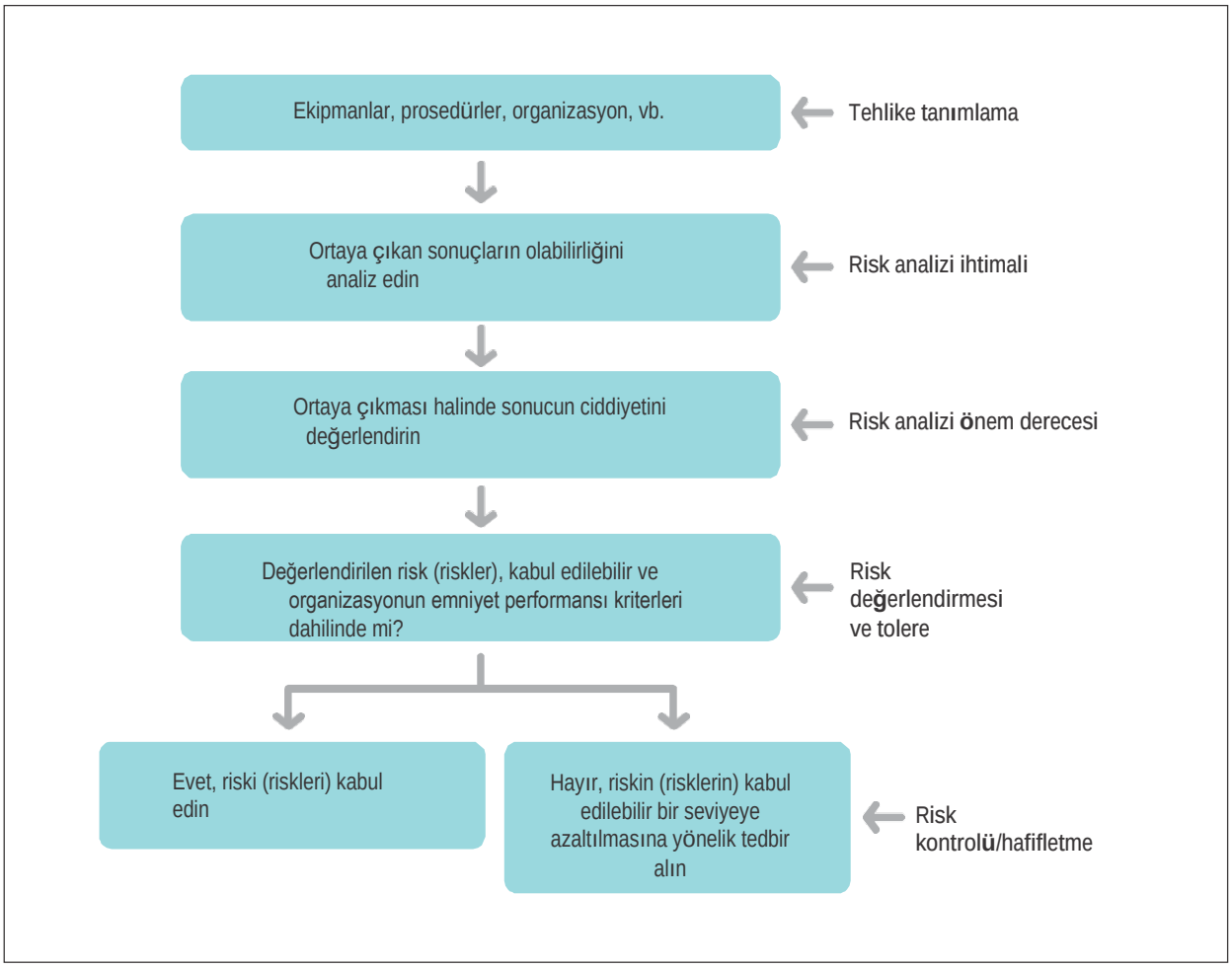
9.4 2. BİLEŞEN: EMNİYET RİSKİ YÖNETİMİ

9.4.1 Hizmet sağlayıcıları, emniyet risklerini yönetmekte olduklarından emin olmalıdırlar. Bu süreç, tehlike tanımlamayı, emniyet riski değerlendirmesini ve emniyet riski hafifletmesini içeren emniyet riski yönetimi (SRM) olarak bilinir.

9.4.2 Emniyet Riski Yönetimi (SRM) süreci sistematik olarak söz konusu hizmet sağlayıcısının ürünlerinin veya hizmetlerinin sunumu bağlamında mevcut olan tehlikeleri tanımlar. Tehlikeler, tasarımı, teknik işlevi, insan arayüzü veya diğer süreçlerle ve sistemlerle etkileşimleri bakımından yetersiz olan sistemlerin sonucu olabilir. Aynı zamanda, söz konusu hizmet sağlayıcısının çalışma ortamındaki değişikliklere adapte olunmasında mevcut süreçlerin veya sistemlerin herhangi bir aksaklığından doğabilirler. Bu etkenlerin dikkatli bir şekilde analiz edilmesi, genellikle, operasyon veya faaliyet yaşam döngüsündeki herhangi bir noktada potansiyel tehlikeleri belirleyebilir.

9.4.3 Yüksek emniyet performansına ulaşılması için söz konusu sistemin ve çalışma ortamının anlaşılması elzemdir. Sistemi ve sistemin arayüzlerini tanımlayan detaylı bir sistem tanımına sahip olunması işe yaracaktır. Tehlikeler, iç ve dış kaynaklardan operasyonel yaşam döngüleri boyunca tanımlanabilir. Etkin halde kalmaya devam ettiklerinden emin olmak için emniyet riski değerlendirmelerinin ve emniyet riski hafifletmelerinin sürekli olarak gözden geçirilmesi gerekecektir. Şekil 9-1 kapsamında, hizmet sağlayıcısına yönelik tehlike tanımlama ve emniyet riski yönetimi sürecine ilişkin genel bilgiler yer almaktadır.

Not.— Tehlike tanımlama ve emniyet riski değerlendirmesi prosedürlerine ilişkin detaylı rehberlik 2. Bölüm kapsamında ele alınmaktadır.



Şekil 9-1. Tehlike tanımlama ve risk yönetim süreci

9.4.4 Tehlike tanımlama

Tehlike tanımlama, Emniyet Riski Yönetimi (SRM) sürecindeki birinci adımdır. Söz konusu hizmet sağlayıcısı tarafından, operasyonun ve faaliyetlerin tüm alanlarında havacılık emniyetine etki edebilecek olan tehlikelerin tanımlanmasına yönelik resmi bir süreç geliştirilmeli ve sürdürülmelidir. Ekipmanlar, tesisler ve sistemler buna dahildir. Tanımlanan ve kontrol edilen havacılık emniyeti ile ilgili tehlikeler, operasyonun emniyeti için faydalıdır. Harici organizasyonlar ile olan Emniyet Yönetimi Sistemi (SMS) arayüz bağlantıları sonucunda var olabilecek tehlikelerin göz önünde bulundurulması da önemlidir.

Tehlike tanımlamasına ilişkin kaynaklar

9.4.4.1 Söz konusu organizasyona dahili veya harici nitelikte olsun, tehlike tanımlamasına ilişkin çeşitli kaynaklar mevcuttur. Dahili kaynaklardan bazıları şunları içerir:

a) *Normal operasyon izlemesi*; hat operasyonları emniyet denetimi (LOSA) gibi günlük operasyonların ve faaliyetlerin izlenmesine yönelik gözlemsel teknikleri kullanır.

b) *Otomasyonlu izleme sistemleri*; uçuş verilerini izleme (FDM) gibi analiz edilebilen parametrelerin izlenmesine yönelik otomasyonlu kayıt sistemlerini kullanır.

c) *Gönüllü ve zorunlu emniyet raporlaması sistemleri*; harici organizasyonlardan çalışanlar da dahil olmak üzere, herkese, tehlikeleri ve diğer emniyet sorunlarını organizasyona rapor etme imkanı sağlar.

d) *Denetimler*; denetlenmekte olan görevdeki veya süreçteki tehlikelerin tanımlanması için kullanılabilir. Değişikliğin uygulanmasına ilişkin tehlikeleri tanımlamak için bunların aynı zamanda organizasyonel değişiklikler ile koordine edilmesi gerekir.

e) *Eğitimden geri bildirim*; interaktif (iki yollu) olan eğitim, katılımcılardan yeni tehlikelerin tanımlanmasını kolaylaştırabilir.

f) *Hizmet sağlayıcısı emniyet soruşturmaları*; dahili emniyet soruşturmasında ve kazalara/olaylara ilişkin takip raporlarında tanımlanan tehlikeler.

9.4.4.2 Tehlike tanımlamaya ilişkin harici kaynaklara ilişkin örnekler şunlardır:

a) *Havacılık kazası raporları*; kaza raporlarının gözden geçirilmesi; aynı Devletteki kazalara veya herhangi bir benzer uçak tipine, bölgeye veya çalışma ortamına ilişkin olabilir.

b) *Devlet zorunlu ve gönüllü emniyet raporlaması sistemleri*; bazı Devletler tarafından hizmet sağlayıcılarından alınan emniyet raporlarına ilişkin özetler sunulur.

c) *Devlet gözetim denetimleri ve üçüncü taraf denetimleri*; bazı hallerde harici denetimler tehlikeleri tanımlayabilir. Bunlar, tanımlanamayan tehlike olarak belgelenebilir veya herhangi bir denetim bulgusu dahilinde daha az açık olarak yakalanabilir.

d) *Ticari birlikler ve bilgi değişimi sistemleri*; birçok ticari birlik ve sektör grubu, tanımlanan tehlikeleri içerebilecek olan emniyet verilerini paylaşabilir.

Emniyet raporlaması sistemi

9.4.4.3 Tehlikelerin tanımlanmasına ilişkin ana kaynaklardan biri, özellikle gönüllü emniyet raporlaması sistemi olmak üzere, emniyet raporlaması sistemidir. Zorunlu sistem normalde, ortaya çıkmış olan olaylar için kullanılırken, gönüllü sistem, tehlikeler, ramak kalalar veya hatalar gibi potansiyel emniyet sorunlarına yönelik ilave raporlama kanalı sunmaktadır. Devlete ve hizmet sağlayıcısına düşük sonuçlu olaylara ilişkin değerli bilgiler sağlarlar.

9.4.4.4 Kişilerin gördüklerini veya tecrübe ettiklerini rapor etmeye teşvik etmek için hizmet sağlayıcıları tarafından uygun korumaların sağlanması önemlidir. Örneğin, hatalara ilişkin raporlar veya bazı hallerde kural ihlali için yürütme tedbirinden feragat edilebilir. Rapor edilen bilgilerin sadece emniyetin iyileştirilmesini desteklemek üzere kullanılacağının açık bir şekilde belirtilmesi gerekir. Amaç, etkin bir raporlama kültürü ve potansiyel emniyet eksikliklerinin proaktif bir şekilde tanımlanmasını teşvik etmektir.

9.4.4.5 Gönüllü emniyet raporlaması sistemleri, rapor eden kişi hakkındaki tanımlayıcı bilgilerin takip işlemine imkan vermek üzere sadece saklayıcı tarafından bilinmesini gerektirecek şekilde gizli olmalıdır. Saklayıcının rolü, tipik olarak emniyet yöneticisi ve emniyet soruşturmasına dahil olan personel ile kısıtlı olmak üzere birkaç kişi ile sınırlı olmalıdır. Gizliliğin muhafaza edilmesi, cezalandırma veya mahcubiyet korkusu olmaksızın, insan hatasına yol açan tehlikelerin açıklanmasının kolaylaştırılmasına yardımcı olacaktır. Gönüllü emniyet raporları, takip tedbirlerinin gerekli olması halinde kimliksizleştirilebilir ve arşivlenebilir. Kimliksizleştirilmiş raporlar, risk hafifletmesinin etkinliğini izlemek ve yükselen tehlikeleri tanımlamak üzere gelecekteki trend çıkarma analizlerini destekleyebilir.

9.4.4.6 Tüm seviyelerden ve tüm disiplinler genelinde personel, kendi emniyet raporlaması sistemleri vasıtasıyla tehlikeleri tanımlamaya ve diğer emniyet sorunlarını raporlamaya teşvik edilir. Etkin olması için, emniyet raporlaması sistemlerinin tüm personel tarafından kolaylıkla erişilebilir olması gerekir. Duruma bağlı olarak kağıt temelli, web temelli veya masaüstü bir form kullanılabilir. Kullanılabilen birden fazla giriş yöntemine sahip olunması, personelin katılım ihtimalini azami düzeye çıkarır. Emniyet raporlamasının faydalarından ve nelerin rapor edilmesi gerektiğinden herkes haberdar edilmelidir.

9.4.4.7 Emniyet raporu sunan herkesin hangi kararların veya tedbirlerin alındığına dair geri bildirim alması gerekir. Raporlama sistemi gerekliliklerinin, analiz araçlarının ve yöntemlerinin uyumlu hale getirilmesi, emniyet bilgilerinin değişiminin yanı sıra, belirli emniyet performansı göstergelerine ilişkin kıyaslamaları kolaylaştırabilir. Gönüllü raporlama düzeninde rapor eden kişilere sağlanan geri bildirim aynı zamanda, söz konusu raporların ciddiye alındığının kanıtlanmasına hizmet eder. Bu sayede, pozitif emniyet kültürünün teşvik edilmesine ve gelecekteki raporlamanın cesaretlendirilmesine yardımcı olunur.

9.4.4.8 Çok sayıda emniyet raporu söz konusu olduğunda, girişte raporların filtrelenmesine ihtiyaç duyulabilir. Bu filtreleme, daha fazla soruşturmanın gerekli olup olmadığının ve hangi seviyede soruşturmanın gerekli olduğunun tespit edilmesine yönelik ilk emniyet riski değerlendirmesini içerebilir.

9.4.4.9 Emniyet raporları genellikle bir sınıflandırma veya tasnif sisteminin kullanılması vasıtasıyla filtrelenir. Sınıflandırma kullanılarak bilgilerin filtrelenmesi yaygın sorunların ve trendlerin belirlenmesini kolaylaştırabilir. Hizmet sağlayıcıları tarafından kendi operasyon türünü (türlerini) kapsayan sınıflandırmalar geliştirilmelidir. Sınıflandırma kullanılmasının dezavantajı, bazı hallerde, tanımlanan tehlikenin tanımlanan kategorilerden herhangi biriyle tam olarak uymamasıdır. Burada ortaya çıkan zorluk, uygun detay derecesine sahip olan, tehlikelerin kolaylıkla tahsis edilmesine yeterli olacak kadar spesifik, ancak analiz için değerli olacak kadar genel sınıflandırmaların kullanılmasıdır. Bazı Devletler ve uluslararası ticari birlikler tarafından, kullanılabilecek sınıflandırmalar geliştirilmiştir. Sınıflandırmalara ilişkin ilave bilgiler 5. Bölüm kapsamında yer almaktadır.

9.4.4.10 Tehlike tanımlamasına yönelik diğer yöntemler, konu uzmanları tarafından detaylı analiz senaryolarının yürütüldüğü atölyeleri veya toplantıları kapsar. Bu oturumlar, bir dizi deneyimli operasyon personelinin ve teknik personelin sağladığı katkılardan faydalanır. Bu tür faaliyetler için mevcut emniyet komitesi toplantıları (Emniyet Gözden Geçirme Kurulu (SRB), Emniyet Eylem Grubu (SAG), vb.) kullanılabilir; ilişkili emniyet risklerinin değerlendirilmesi için de aynı gruptan yararlanılabilir.

9.4.4.11 Tanımlanan tehlikelerin ve potansiyel sonuçlarının belgelenmesi gerekir. Bu belgeleme emniyet riski değerlendirmesi süreçleri için kullanılacaktır.

9.4.4.12 Tehlike tanımlama süreci kapsamında, gerek söz konusu organizasyon dahilinde gerek söz konusu organizasyon haricinde olmak üzere diğer sistemlerle olan arayüz bağlantıları da dahil olmak üzere, hizmet sağlayıcısının havacılık faaliyetlerinin kapsamı dahilinde mevcut olabilecek tüm olası tehlikeler göz önünde bulundurulur. Tehlikelerin tanımlanması sonrasında, sonuçlarının (başka bir deyişle, spesifik olaylar veya sonuçlar) tespit edilmesi gerekir.

Tehlikelerin soruşturulması

9.4.4.13 Tehlike tanımlama sürekli ve söz konusu hizmet sağlayıcısının devam eden faaliyetleri kapsamında olmalıdır. Bazı koşullar için daha detaylı soruşturma gerekebilecektir. Bunlar aşağıdakileri içerebilecektir:

a) söz konusu organizasyon tarafından havacılık emniyeti ile ilgili olaylarda veya mevzuata riayetsizlikte açıklanamayan bir artışın yaşandığı haller veya

b) söz konusu organizasyondaki veya faaliyetlerindeki önemli değişiklikler.

9.4.5 Hizmet sağlayıcısı emniyet soruşturması

9.4.5.1 Etkin emniyet yönetimi, emniyet olaylarının ve emniyet tehlikelerinin analiz edilmesine ve çalışma ortamındaki emniyetin iyileştirilmesine yönelik tavsiyelerin ve bulguların rapor edilmesine yönelik kalite soruşturmalarına bağlıdır.

9.4.5.2 Annex 13 kapsamındaki kaza ve olay soruşturmaları ile hizmet sağlayıcısı soruşturmaları arasında açık bir ayrım mevcuttur. Annex 13 kapsamındaki kazalara ve ciddi olaylara ilişkin soruşturmadan, Annex 13 kapsamında tanımlandığı üzere söz konusu Devlet sorumludur. Bu tür bilgiler, kazalardan ve olaylardan öğrenilen derslerin yayılması bakımından elzemdir. Hizmet sağlayıcısı emniyet soruşturmaları, hizmet sağlayıcıları tarafından, tehlike tanımlama ve risk değerlendirme süreçlerini desteklemek üzere kendi Emniyet Yönetimi Sistemleri (SMS) kapsamında yürütülür. Tehlike tanımlamasına yönelik değerli kaynak sunabilecek veya risk kontrollerindeki zayıflıkları belirleyebilecek olan, Annex 13 kapsamı dışında kalan birçok emniyet olayı söz konusudur. Bu problemler, hizmet sağlayıcısı tarafından liderlik edilen emniyet soruşturmasıyla ortaya çıkarılabilir ve çözüme kavuşturulabilecektir.

9.4.5.3 Hizmet sağlayıcısı emniyet soruşturmasının birincil amacı, neyin gerçekleştiğini ve emniyet eksikliklerinin ortadan kaldırılması veya hafifletilmesi suretiyle gelecekte benzer durumların ortaya çıkmasının nasıl engelleneceğinin anlaşılmasıdır. Bu anlayışa, söz konusu olayın dikkatli ve metotlu bir şekilde incelenmesi ve gelecekteki tekerrürlerin ihtimalinin ve/veya akıbetinin azaltılması için öğrenilen derslerin uygulanmasıyla ulaşılabilir. Hizmet sağlayıcısı emniyet soruşturmaları, söz konusu hizmet sağlayıcısının Emniyet Yönetimi Sisteminin (SMS) ayrılmaz bir parçasıdır.

9.4.5.4 Emniyet olaylarına ve tehlikelerine yönelik hizmet sağlayıcısı soruşturmaları, havacılıktaki genel risk yönetimi sürecine ilişkin elzem bir faaliyettir. Emniyet soruşturması yürütülmesinin faydaları şunları içerir:

a) olaya yol açan olaylara yönelik olarak daha iyi bir anlayışın kazanılması;

b) katkıda bulunan insan faktörlerinin, teknik ve organizasyonel faktörlerin belirlenmesi;

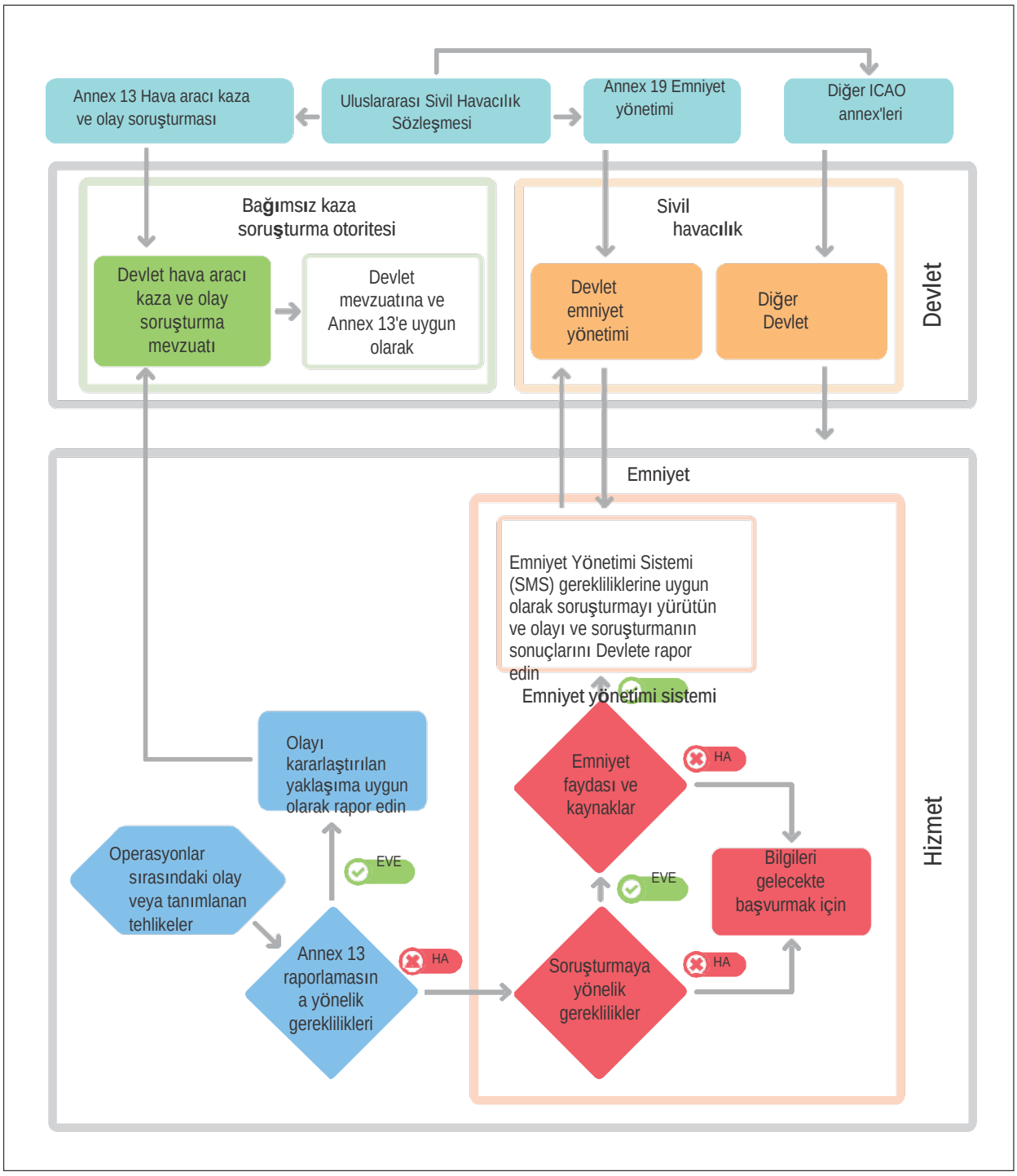
c) tehlikelerin tanımlanması ve risk değerlendirmelerinin gerçekleştirilmesi;

d) kabul edilemez risklerin azaltılması veya giderilmesi için tavsiyelerde bulunulması ve

e) havacılık topluluğunun uygun üyeleri ile paylaşılması gereken öğrenilen derslerin belirlenmesi.

Soruşturma tetikleyicileri

9.4.5.5 Hizmet sağlayıcısı emniyet soruşturması genellikle, emniyet raporlaması sistemi vasıtasıyla sunulan bir bildirim (rapor) ile tetiklenir. Şekil 9-2'de emniyet soruşturması kararı süreci ve hizmet sağlayıcısı emniyet soruşturmasının ne zaman gerçekleştirilmesi gerektiği ile Annex 13 hükümleri kapsamında ne zaman soruşturma başlatılması gerektiği arasındaki ayrım ortaya konmaktadır.



Şekil 9-2. Emniyet soruşturması karar süreci

9.4.5.6 Tüm olaylar veya tehlikeler soruşturulmayabilir veya tüm olayların veya tehlikelerin soruşturulması gerekli değildir; soruşturma yürütülmesine ve söz konusu soruşturmanın derinliğine yönelik karar, söz konusu olayın veya tehlikenin fiili veya olası sonuçlarına bağlı olmalıdır. Yüksek risk potansiyeline sahip olduğu değerlendirilen olayların ve tehlikelerin soruşturulması daha muhtemeldir ve düşük risk potansiyeline sahip olanlardan daha derinlemesine soruşturulması gerekir. Hizmet sağlayıcıları tarafından tanımlanmış tetikleme noktalarına sahip olan yapılandırılmış bir karar alma yaklaşımı kullanılmalıdır. Bu sayede emniyet soruşturması kararları, neyin soruşturulması gerektiği ve soruşturmanın kapsamı yönlendirilecektir. Aşağıdakiler buna dahil olabilecektir:

a) sonucun önem derecesi veya olası önem derecesi

b) soruşturmanın yürütülmesine yönelik mevzuata dayalı veya organizasyonel gereklilikler;

c) elde edilecek emniyet değeri;

d) alınacak emniyet tedbirine yönelik imkan;

e) soruşturma yapılmamasıyla ilişkili riskler;

f) hedeflenen emniyet programlarına katkı;

g) belirlenen trendler;

h) eğitim faydası ve

i) kaynak elverişliliği.

Soruşturmacının görevlendirilmesi

9.4.5.7 Soruşturma başlatılacak olması halinde, ilk işlem, gerekli becerilere ve uzmanlığa sahip olan bir soruşturmacının veya kaynakların elverişli olduğu hallerde bir soruşturma ekibinin tayin edilmesi olacaktır. Söz konusu ekibin boyutu ve üyelerinin uzmanlık profili, soruşturulmakta olan olayın mahiyetine ve önem derecesine bağlıdır. Soruşturma ekibi tarafından diğer uzmanların yardımı gerekli görülebilecektir. Genellikle, operasyon ve emniyet ofisi uzmanlarından destek alarak iç soruşturmanın yürütülmesi için tek bir kişi görevlendirilir.

9.4.5.8 Hizmet sağlayıcısı emniyet soruşturmacıları ideal olarak söz konusu olay veya tanımlanan tehlike ile ilişkili alandan organizasyonel bakımından bağımsızdırlar. Soruşturmacının (soruşturmacıların) hizmet sağlayıcısı emniyet soruşturmalarında bilgi sahibi (eğitimli) ve becerikli (tecrübeli) olması/olmaları halinde daha iyi sonuçlar elde edilecektir. Soruşturmacılar bu görev için ideal olarak sahip oldukları bilgi, beceriler ve dürüstlüğü, tarafsızlığı, mantıklı düşünmeyi, faydacılığı ve etraflıca düşünmeyi içermesi gereken karakter özellikleri için seçileceklerdir.

Soruşturma süreci

9.4.5.9 Soruşturmada neyin gerçekleştiği ve neden gerçekleştiği belirlenmelidir ve bunun için, soruşturma kapsamında uygulanmak üzere kök neden analizi gerekebilecektir. İdeal olarak, söz konusu olaya dahil olan kişiler ile olaydan sonra mümkün olan en kısa süre içerisinde görüşme yapılmalıdır. Soruşturma aşağıdakileri içermelidir:

a) dahil olan kişilerin eylemleri de dahil olmak üzere, önemli olaylara ilişkin zaman çizelgelerinin belirlenmesi;

b) faaliyetlere ilişkin politikaların ve prosedürlerin gözden geçirilmesi;

c) olaya ilişkin alınan kararların gözden geçirilmesi;

d) söz konusu olayın ortaya çıkmasını engellemiş olması gereken, uygulanan risk kontrollerinin belirlenmesi ve

e) önceki veya benzer olaylara ilişkin emniyet verilerinin gözden geçirilmesi.

9.4.5.10 Emniyet soruşturması, suçlamaya veya cezalandırmaya değil, tanımlanan tehlikelere ve emniyet risklerine ve iyileştirme imkanlarına odaklanmalıdır. Soruşturmanın yürütülme şekli ve daha da önemlisi, raporun nasıl yazıldığı, muhtemel emniyet etkisine, söz konusu organizasyonun gelecekteki emniyet kültürüne ve gelecekteki emniyet inisiyatiflerinin etkinliğine tesir edecektir.

9.4.5.11 Soruşturma, emniyet eksikliklerini gideren veya hafifleten, açık bir şekilde tanımlanmış bulgular ve tavsiyeler ile sonuçlanmalıdır.

9.4.6 Emniyet riski değerlendirmesi ve hafifletmesi

9.4.6.1 Hizmet sağlayıcısı tarafından, emniyet risklerinin değerlendirilmesine yönelik tutarlı ve sistematik bir yaklaşıma imkan verecek bir emniyet riski değerlendirmesi modeli geliştirilmelidir. Bu model, hangi emniyet risklerinin kabul edilebilir veya kabul edilemez olduğunun belirlenmesine ve tedbirlerin önceliklendirilmesine yardımcı olacak bir yöntem içermelidir.

9.4.6.2 Hizmet sağlayıcısının çalışma ortamına uygun olduklarından emin olunması için, kullanılan Emniyet Riski Yönetimi (SRM) araçlarının periyodik olarak gözden geçirilmesi ve uyarlanması gerekebilecektir. Hizmet sağlayıcısı tarafından, söz konusu hizmet sağlayıcısının Emniyet Yönetimi Sistemi (SMS) olgunlaştıkça operasyonunun ihtiyaçlarını daha iyi bir şekilde yansıtan daha sofistike yaklaşımlar bulunabilecektir. Hizmet sağlayıcısı ile Sivil Havacılık Otoritesi (CAA) tarafından bir metodoloji kararlaştırılmalıdır.

9.4.6.3 Emniyet riski sınıflandırmasına yönelik daha sofistike yaklaşımlar mevcuttur. Hizmet sağlayıcısının emniyet yönetiminde deneyimli olması veya yüksek riskli bir ortamda faaliyet göstermesi halinde bunlar daha uygun olabilecektir.

9.4.6.4 Emniyet riski değerlendirmesi sürecinde mevcut olan her nevi emniyet verileri ve emniyet bilgileri kullanılmalıdır. Emniyet risklerinin değerlendirilmesi sonrasında, hizmet sağlayıcısı tarafından hangi emniyet riski kontrollerine ihtiyaç duyulduğunu tespit etmek üzere veriye dayalı karar alma sürecine girişilecektir.

9.4.6.5 Emniyet riski değerlendirmelerinde bazı hallerde, verilerin elverişsizliğine bağlı olarak kantitatif verilerden ziyade kalitatif bilgilerin (uzman değerlendirmesi) kullanılması gerekir. Emniyet riski matrisinin kullanılması, söz konusu kullanıcıya, tanımlanan tehlikeye ilişkin emniyet riskini (risklerini) kantitatif bir formatta ifade etme imkanı verir. Böylelikle, tanımlanan emniyet riskleri arasında doğrudan büyüklük karşılaştırmasına imkan verilir. Kantitatif veriler mevcut olmadığında, tanımlanan her bir emniyet riskine "oluşması muhtemel" veya "ihtimal dışı" gibi kalitatif bir emniyet riski kriteri tayin edilebilecektir.

9.4.6.6 Spesifik çalışma ortamlarına sahip olan birden fazla lokasyonda operasyonları olan hizmet sağlayıcıları için, emniyet riski değerlendirmelerinin ve emniyet riski kontrolü tanımlamasının gerçekleştirilmesi için yerel emniyet komitelerinin tesis edilmesi daha efektif olabilecektir. Genellikle, operasyon alanındaki bir uzmandan (söz konusu hizmet sağlayıcısının bünyesindeki veya haricindeki) görüş talep edilir. Uygun kaynakların sağlanması için daha üst otoritelerden nihai kararlar veya kontrol kabulü gerekli olabilir.

9.4.6.7 Hizmet sağlayıcıları tarafından kendi emniyet riski değerlendirmelerinin önceliklendirilmesi ve emniyet riski kontrollerinin benimsenmesi kendi kararlarıdır. Rehberlik teşkil etmesi amacıyla, hizmet sağlayıcısı tarafından aşağıdaki türden önceliklendirme süreci bulunmalıdır:

a) en yüksek emniyet riskini değerlendiren ve kontrol eden;

b) kaynakları en yüksek emniyet risklerine tahsis eden;

c) emniyeti etkin bir şekilde muhafaza eden veya iyileştiren;

d) belirtilen ve kararlaştırılan emniyet amaçlarına ve Emniyet Performansı Hedeflerine (SPT'ler) ulaşan ve

e) emniyet risklerinin kontrolüne ilişkin olarak söz konusu Devletin düzenlemeleri kapsamındaki gereklilikleri karşılayan.

9.4.6.8 Emniyet risklerinin değerlendirilmesi sonrasında, uygun emniyet riski kontrolleri uygulanabilir. Uygun emniyet riski kontrollerinin belirlenmesine "son kullanıcıların" ve konu uzmanlarının dahil edilmesi önemlidir. Doğru insanların dahil edilmesinin sağlanması, emniyet riski seçilen hafifletmelerin uygulanabilirliğini azami düzeye çıkaracaktır. Emniyet riski kontrollerinin uygulanması öncesinde, bilhassa yeni tehlikelerin getirilmesi olmak üzere, istenmeyen sonuçlara yönelik bir tespitte bulunulmalıdır.

9.4.6.9 Emniyet riski kontrolünün kararlaştırılması ve uygulanması sonrasında, emniyet riski kontrolünün etkinliğinin güvence altına alınması için emniyet performansı izlenmelidir. Operasyon koşulları altında yeni emniyet riski kontrollerinin doğruluğunun, verimliliğinin ve etkinliğinin doğrulanması için bu gereklidir.

9.4.6.10 Emniyet Riski Yönetimi (SRM) çıktıları belgelenmelidir. Söz konusu tehlike ve sonuçları, emniyet riski değerlendirmesi ve alınan emniyet riski kontrol tedbirleri buna dahil olmalıdır. Bunlar genellikle, takip edilebilmeleri ve izlenebilmeleri için bir kayıt defteri kapsamında tutulmalıdır. Söz konusu Emniyet Riski Yönetimi (SRM) dokümantasyonu, emniyet kararları alınırken referans olarak ve emniyet bilgilerinin değişimi için kullanılabilen organizasyonel emniyet bilgisine ilişkin geçmişe yönelik bir kaynak haline gelir. Bu emniyet bilgisi, emniyet trendi analizlerine ve emniyet eğitimine ve iletişimine yönelik materyal sunar. Aynı zamanda, emniyet riski kontrollerinin ve tedbirlerinin uygulanıp uygulanmadığının ve etkin olup olmadığının tespit edilmesine yönelik iç denetimler için de faydalıdır.

9.5 3. BİLEŞEN: EMNİYET GÜVENCESİ

9.5.1 Annex 19, Ek 2, 3.1.1 kapsamında hizmet sağlayıcıları tarafından, söz konusu organizasyonun emniyet performansının doğrulanmasına ve emniyet riski kontrollerinin etkinliğinin onaylanmasına yönelik araçların geliştirilmesi ve muhafaza edilmesi öngörülmektedir. Bu kabiliyetler, hizmet sağlayıcısının Emniyet Yönetimi Sisteminin (SMS) emniyet güvencesi bileşeni tarafından sağlanır.

9.5.2 Emniyet güvencesi, söz konusu Emniyet Yönetimi Sisteminin (SMS) beklentilere ve gerekliliklere uygun bir şekilde işleyip işlemediğinin tespit edilmesi için gerçekleştirilen süreçlerden ve faaliyetlerden oluşur. Yükselen emniyet risklerini getirebilecek değişikliklerin veya sapmaların veya mevcut emniyet riski kontrollerinin kötüleşmesinin tespit edilmesi için süreçlerinin yanı sıra çalışma ortamının sürekli olarak izlenmesini içerir. Bu sayede, Emniyet Riski Yönetimi (SRM) süreci vasıtasıyla bu tür değişiklikler veya sapmalar ele alınabilecektir.

9.5.3 Emniyet güvencesi faaliyetleri, potansiyel bir emniyet etkisine sahip olan belirlenmiş sorunlara cevaben alınan tedbirlerin geliştirilmesini ve uygulanmasını içermelidir. Bu tedbirler, söz konusu hizmet sağlayıcısının Emniyet Yönetimi Sisteminin (SMS) performansını sürekli olarak iyileştirir.

9.5.4 Emniyet performansının izlenmesi ve ölçümü

Emniyet performansının doğrulanması ve emniyet riski kontrollerinin etkinliğinin onaylanması, iç denetimlerin bir kombinasyonunun kullanımı ile Emniyet Performansı Göstergelerinin (SPI'ler) tesis edilmesini ve izlenmesini gerektirir. Uygulanmalarının daima amaçlanan sonuçlara ulaşmamasına bağlı olarak emniyet riski kontrollerinin etkinliğinin değerlendirilmesi önemlidir. Bu değerlendirme, doğru emniyet riski kontrolünün seçilip seçilmediğinin belirlenmesine yardımcı olacak ve farklı bir emniyet riski kontrolü stratejisinin uygulanmasıyla sonuçlanabilecektir.

İç denetim

9.5.4.1 İç denetimler, Emniyet Yönetimi Sisteminin (SMS) etkinliğini değerlendirmek ve potansiyel iyileştirme alanlarını belirlemek üzere gerçekleştirilir. Çoğu havacılık emniyeti düzenlemesi, ilgili Devlet tarafından tesis edilmiş olan genel emniyet riski kontrolleridir. İç denetim vasıtasıyla söz konusu düzenlemelere riayetin sağlanması, emniyet güvencesinin başlıca unsurudur.

9.5.4.2 Aynı zamanda, emniyet riski kontrollerinin etkin bir şekilde uygulanmasının ve izlenmesinin sağlanması da gereklidir. Uygunsuzluklar ve diğer sorunlar belirlendiğinde, sebepler ve katkıda bulunan etkenler soruşturulmalı ve analiz edilmelidir. İç denetimin ana odak noktası, emniyet riski kontrollerini öngören politikalar, süreçler ve prosedürlerdir.

9.5.4.3 İç denetimler, denetlenmekte olan işlevlerden bağımsız olan kişiler veya departmanlar tarafından gerçekleştirildiğinde en üst düzeyde etkili olur. Bu tür denetimler, sorumlu yöneticiye ve üst yönetime aşağıdakilerin durumuna ilişkin geri bildirim sağlamalıdır:

a) düzenlemelere riayet;

b) politikalara, süreçlere ve prosedürlere riayet;

c) emniyet riski kontrollerinin etkinliği;

d) düzeltici faaliyetlerin etkinliği ve

e) Emniyet Yönetimi Sisteminin (SMS) etkinliği.

9.5.4.4 Bazı organizasyonlar tarafından iç denetimlerin uygun derecede bağımsızlığı sağlanamayabilir; bu gibi hallerde, söz konusu hizmet sağlayıcısı tarafından harici denetçilerin (örneğin, bağımsız denetçiler veya başka bir organizasyondan denetçiler) görevlendirilmesi değerlendirilmelidir.

9.5.4.5 İç denetimlerin planlanmasında söz konusu süreçlerin emniyet bakımından kritikliği, önceki denetimlerin ve değerlendirmelerin (tüm kaynaklardan) sonuçları ve uygulanan emniyet riski kontrolleri dikkate alınmalıdır. İç denetimlerde, düzenlemelere ve politikalara, süreçlere ve prosedürlere uyumsuzluk belirlenmelidir. İç denetimler aynı zamanda, sistem eksikliklerini, emniyet riski kontrollerinin etkinliğindeki eksikliği ve iyileştirme imkanlarını da belirlemelidir.

9.5.4.6 Uyuma ve etkinliğe yönelik değerlendirme emniyet performansına ulaşılması bakımından elzemdir. İç denetim süreci, gerek uyumun gerek etkinliğin tespit edilmesi için kullanılabilir. Her bir sürecin veya prosedürün uyumunun ve etkinliğinin değerlendirilmesi için aşağıdaki sorular sorulabilir:

a) Uyumun tespit edilmesi
   1) Öngörülen süreç veya prosedür mevcut mudur?

   2) Söz konusu süreç veya prosedür belgelenmiş midir (girdiler, faaliyetler, arayüzler ve çıktılar tanımlanmış mıdır)?

   3) Söz konusu süreç veya prosedür gereklilikleri (kriterleri) karşılamakta mıdır?

   4) Söz konusu süreç veya prosedür kullanılmakta mıdır?

   5) Etkilenen tüm personel tarafından söz konusu süreç veya prosedür devamlı olarak takip edilmekte midir?

   6) Tanımlanan girdiler üretilmekte midir?

   7) Herhangi bir süreç veya prosedür değişikliği belgelenmiş ve uygulanmakta mıdır?

b) Etkinliğin değerlendirilmesi

   1) Söz konusu süreç veya prosedür kullanıcılar tarafından anlaşılmakta mıdır?

   2) Söz konusu sürecin veya prosedürün amacına devamlı olarak ulaşılmakta mıdır?

3) Söz konusu sürecin veya prosedürün sonuçları "müşteri" tarafından talep edilenler midir?

4) Söz konusu süreç veya prosedür düzenli olarak gözden geçirilmekte midir?

5) Söz konusu süreçte veya prosedürde değişiklikler olduğunda emniyet riski değerlendirmesi gerçekleştirilmekte midir?

6) Süreç veya prosedür iyileştirmeleri beklenen faydalarla sonuçlanmış mıdır?

9.5.4.7 İlaveten, iç denetimlerin daha önceden belirlenen uyumsuzlukların kapatılmasındaki ilerlemeyi izlemesi gerekir. Bunlar, kök neden analizi ve düzeltici ve önleyici faaliyet planlarının geliştirilmesi ve uygulanması vasıtasıyla ele alınmış olmalıdır. Herhangi bir uyumsuzluğa ilişkin nedenin (nedenlerin) ve katkıda bulunan etkenlerin analizinden elde edilen sonuçların söz konusu hizmet sağlayıcısının Emniyet Riski Yönetimi (SRM) süreçlerini beslemesi gerekir.

9.5.4.8 İç denetim sürecinin sonuçları, Emniyet Riski Yönetimi (SRM) ve emniyet güvencesi işlevlerinin çeşitli girdilerinden biri haline gelir. İç denetimler, söz konusu hizmet sağlayıcısının yönetimini organizasyon dahilindeki uyum seviyesi, emniyet riski kontrollerinin etkinlik derecesi ve nerelerde düzeltici veya önleyici faaliyete gerekli olduğu hakkında bilgilendirir.

9.5.4.9 Sivil Havacılık Otoriteleri (CAA'lar) tarafından düzenlemelere uyum durumuna, Emniyet Yönetimi Sisteminin (SMS) etkinliğine ve kendi organizasyonunun ve süreçlerinin denetlenmesi için söz konusu hizmet sağlayıcısı tarafından seçilen sektörel birliklerin veya diğer üçüncü tarafların etkinliğine ilişkin ilave geri bildirim sağlanabilir. Bu tür ikinci ve üçüncü taraf denetimlerinin sonuçları, emniyet güvencesi işlevine, söz konusu hizmet sağlayıcısına kendi Emniyet Yönetimi Sisteminin (SMS) iyileştirilmesine yönelik imkanların ve kendi iç denetim süreçlerinin etkinliğine dair göstergeler sunan girdilerdir.

Emniyet performansı izlemesi

9.5.4.10 Emniyet performansı izlemesi, herhangi bir organizasyon için tipik olarak mevcut olan bir dizi kaynaktan emniyet verilerinin ve emniyet bilgilerinin toplanması vasıtasıyla gerçekleştirilir. Bilgiye dayalı karar almanın desteklenmesine yönelik veri elverişliliği, Emniyet Yönetimi Sisteminin (SMS) en önemli unsurlarından biridir. Bu verilerin emniyet performansı izlemesi ve ölçümü için kullanılması, emniyet riski karar almasına yönelik gerekli bilgileri üreten elzem faaliyetlerdir.

9.5.4.11 Emniyet performansı izlemesi ve ölçümü bir takım temel prensipler gözetilerek gerçekleştirilmelidir. Ulaşılan emniyet performansı, organizasyonel davranışın bir göstergesi ve aynı zamanda Emniyet Yönetimi Sisteminin (SMS) etkinliğinin ölçüsüdür. Bunun için söz konusu organizasyon tarafından aşağıdakilerin tanımlanması gerekir:

a) öncelikle, söz konusu organizasyonun operasyonel bağlamına özgü emniyet kaygılarına ilişkin stratejik kazanımları veya arzu edilen sonuçları yansıtmak üzere tesis edilmesi gereken emniyet amaçları;

b) emniyet amaçlarına ilişkin taktik parametreler olan ve dolayısıyla da verilerin toplanmasına yönelik referans olan Emniyet Performansı Göstergeleri (SPI'ler) ve

c) emniyet amaçlarına ulaşılmasına yönelik ilerlemenin izlenmesi için kullanılan taktik parametreler olan Emniyet Performansı Hedefleri (SPT'ler).

9.5.4.12 Emniyet Performansı Göstergelerinin (SPI'ler) geniş bir göstergeler yelpazesini kapsaması halinde, söz konusu hizmet sağlayıcısının daha eksiksiz ve gerçekçi bir resmine ulaşılacaktır. Burada aşağıdakiler kapsanmalıdır:

a) düşük ihtimale/yüksek önem derecesine sahip olan olaylar (örneğin, kazalar ve ciddi olaylar);

b) yüksek ihtimale/düşük önem derecesine sahip olan olaylar (örneğin, sorunsuz operasyonel olaylar, uygunsuzluk raporları, sapmalar, vb.) ve

c) süreç performansı (örneğin, eğitim, sistem iyileştirmeleri ve raporların işlenmesi).

9.5.4.13 Emniyet Performansı Göstergeleri (SPI'ler), söz konusu hizmet sağlayıcısının operasyonel emniyet performansını ve Emniyet Yönetimi Sisteminin (SMS) performansını ölçmek için kullanılır. Emniyet Performansı Göstergeleri (SPI'ler), emniyet raporlaması sistemi de dahil olmak üzere, çeşitli kaynaklardan elde edilen verilerin ve bilgilerin izlenmesine dayalıdır. Münferit hizmet sağlayıcısına özgü olmaları ve belirlenmiş bulunan emniyet amaçları ile bağlantılı olmaları gerekir.

9.5.4.14 Emniyet Performansı Göstergeleri (SPI'ler) belirlerken hizmet sağlayıcıları tarafından aşağıdakiler göz önünde bulundurulmalıdır:

a) *Doğru şeylerin ölçülmesi*: Söz konusu organizasyonun emniyet amaçlarına ulaşılmasında doğru yolda olduğunu gösterecek en iyi Emniyet Performansı Göstergelerini (SPI'ler) belirleyin. Aynı zamanda, söz konusu organizasyon tarafından karşılaşılan en büyük emniyet sorunlarının ve emniyet risklerinin neler olduğunu dikkate alın ve bunların etkin kontrolünü gösterecek olan Emniyet Performansı Göstergelerini (SPI'ler) belirleyin.

b) *Verilerin elverişliliği*: Söz konusu organizasyon tarafından ölçülmek istenen ile uyumlu olan veriler mevcut mudur? Mevcut olmaması halinde, ilave veri toplama kaynaklarının tesis edilmesi gerekli olabilecektir. Sınırlı miktarlarda veriye sahip olan küçük organizasyonlar için, veri setlerinin havuzda toplanması da trendlerin belirlenmesine yardımcı olabilecektir. Bu işlem, birden fazla organizasyondan emniyet verilerini harmanlayabilen sektörel birlikler tarafından desteklenebilecektir.

c) *Verilerin güvenilirliği*: Öznelliği veya eksik olması sebebiyle veriler güvenilmez olabilir.

d) *Ortak sektör Emniyet Performansı Göstergeleri (SPI'ler)*: Organizasyonlar arasında karşılaştırmalar yapılabilecek şekilde, benzer organizasyonlarla ortak Emniyet Performansı Göstergelerinin (SPI'ler) kararlaştırılması faydalı olabilir. Bunlara, düzenleyici otorite veya sektörel birlikler tarafından imkan verilebilir.

9.5.4.15 Emniyet Performansı Göstergelerinin (SPI'ler) belirlenmesi sonrasında, hizmet sağlayıcısı tarafından Emniyet Performansı Hedeflerinin (SPT'ler) ve uyarı seviyelerinin belirlenmesinin uygun olup olmadığı değerlendirilmelidir. Emniyet Performansı Hedefleri (SPT'ler) emniyet iyileştirmelerinin yönlendirilmesinde faydalıdır, ancak kötü bir şekilde uygulandıklarında Emniyet Performansı Hedeflerinin (SPT'ler) istenmeyen davranışlara sebebiyet verdiği bilinmektedir ve bu davranışlar, organizasyonel emniyet performansından ziyade, kişilerin ve departmanların söz konusu hedefe ulaşılmasına aşırı derece odaklanması ve belki de söz konusu hedef tarafından ulaşılması amaçlanan şeyin gözden kaçırılmasıdır. Bu gibi hallerde, trendler için Emniyet Performansı Göstergesinin (SPI) izlenmesi daha uygun olabilecektir.

9.5.4.16 Aşağıdaki faaliyetler, emniyet performansının izlenmesine ve ölçülmesine yönelik kaynaklar sağlayabilir:

a) *Emniyet etütleri,* emniyet sorunlarına yönelik daha derin bir anlayışın kazanılmasına ve emniyet performansındaki trendin daha iyi bir şekilde anlaşılmasına yönelik analizlerdir.

b) *Emniyet verileri analizi,* daha fazla soruşturmayı gerektirebilecek ortak sorunları veya trendleri açığa çıkarmak için emniyet raporlaması verilerini kullanır.

c) *Emniyet araştırmaları*, spesifik bir operasyona ilişkin prosedürleri veya süreçleri inceler. Emniyet araştırmaları, kontrol listelerinin, soru formlarının ve gayri resmi gizli mülakatların kullanımını içerebilir. Emniyet araştırmaları genellikle kalitatif bilgiler sunar. Bu da düzeltici faaliyetin gerekli olup olmadığının tespit edilmesi için verilerin toplanması vasıtasıyla doğrulama gerektirebilir. Bununla birlikte, araştırmalar, masrafsız ve değerli emniyet bilgileri kaynağı sağlayabilir.

d) *Emniyet denetimleri,* söz konusu hizmet sağlayıcısının Emniyet Yönetimi Sisteminin (SMS) ve destekleyici sistemlerinin bütünlüğünün değerlendirilmesine odaklanır. Emniyet denetimleri aynı zamanda, kurulu bulunan emniyet riski kontrollerinin etkinliğini değerlendirmek veya emniyet düzenlemelerine uyumu izlemek için de kullanılabilir. Bağımsızlığın ve tarafsızlığın sağlanması, emniyet denetimleri için bir zorluk teşkil etmektedir. Bağımsızlığa ve tarafsızlığa, politikalar, prosedürler, roller, iletişim protokolleri ile uygulanan korumalarla birlikte iç denetimlerle veya harici kuruluşların görevlendirilmesiyle ulaşılabilir.

e) *Emniyet soruşturmalarından* elde edilen *bulgular ve tavsiyeler*, toplanan diğer emniyet verileri karşısında analiz edilebilen faydalı emniyet bilgileri sağlayabilir.

f) FDA, radar bilgileri gibi *operasyonel veri toplama sistemleri*, olaylara ve operasyonel performansa ilişkin faydalı veriler sağlayabilir.

9.5.4.17 Emniyet Performansı Göstergelerinin (SPI'ler) geliştirilmesi, emniyet amaçları ile bağlantılı ve mevcut veya elde edilebilir olan verilerin analizine dayalı olmalıdır. İzleme ve ölçüm süreci, seçilen emniyet performansı göstergelerinin, tekabül eden Emniyet Performansı Hedeflerinin (SPT'ler) ve emniyet tetikleyicilerinin kullanımını içerir.

9.5.4.18 Emniyet performansındaki anormal değişikliklerin belirlenmesi için, organizasyon tarafından, tesis olunan Emniyet Performansı Göstergelerinin (SPI'ler) ve Emniyet Performansı Hedeflerinin (SPT'ler) performansının izlenmesi gerekir. Söz konusu organizasyon ve ilişkili havacılık sektörü için mevcut olan kaynaklar göz önünde bulundurulduğunda, Emniyet Performansı Hedeflerinin (SPT'ler) gerçekçi, bağlama özgü ve ulaşılabilir olması gerekir.

9.5.4.19 Esasen, emniyet performansı izlemesi ve ölçümü, emniyet riski kontrollerinin etkinliğinin doğrulanmasına yönelik bir araç sunar. İlaveten, Emniyet Yönetimi Sistemi (SMS) süreçlerinin ve faaliyetlerinin bütünlüğüne ve etkinliğine ilişkin bir ölçü sunarlar.

9.5.4.20 Söz konusu Devlet, takip edilmesi gerekecek olan Emniyet Performansı Göstergelerinin (SPI'ler) ve Emniyet Performansı Hedeflerinin (SPT'ler) kabulüne yönelik spesifik süreçlere sahip olabilir. Bu sebeple, Emniyet Performansı Göstergelerinin (SPI'ler) ve Emniyet Performansı Hedeflerinin (SPT'ler) geliştirilmesi sırasında, söz konusu hizmet sağlayıcısı tarafından organizasyonun düzenleyici otoritesine veya söz konusu Devlet tarafından yayınlanan ilgili bilgilere danışılmalıdır.

9.5.4.21 Emniyet performansı yönetimi hakkında daha fazla bilgi için bakınız Bölüm 4.

9.5.5 Değişiklik yönetimi

9.5.5.1 Hizmet sağlayıcılarının deneyimi, aşağıdakiler de dahil olmak, ancak bunlarla sınırlı kalmamak üzere, bir dizi faktöre bağlı olarak değişiklik gösterir:

a) organizasyonel genişleme veya daralma;

b) emniyete etki eden iş iyileştirmeleri; bunlar, ürünlerin ve hizmetlerin emniyetli bir şekilde sunumunu destekleyen iç sistemlerde, süreçlerde veya prosedürlerde değişikliklere sonuçlanabilir;

c) organizasyonun çalışma ortamındaki değişiklikler;

d) Emniyet Yönetimi Sisteminin (SMS) harici organizasyonlar ile olan arayüz bağlantılarındaki değişiklikler ve

e) harici mevzuata dayalı değişiklikler, ekonomik değişiklikler ve yükselen riskler.

9.5.5.2 Değişiklik, mevcut emniyet riski kontrollerinin etkinliğine etki edebilecektir. İlaveten, değişiklik ortaya çıktığında herhangi bir operasyona yeni tehlikeler ve ilgili emniyet riskleri kasıtsız olarak getirilebilecektir. Tehlikeler tanımlanmalı ve söz konusu organizasyonun mevcut tehlike tanımlama veya Emniyet Riski Yönetimi (SRM) prosedürlerinde tanımlandığı şekilde ilgili emniyet riskleri değerlendirilmeli ve kontrol edilmelidir.

9.5.5.3 Söz konusu organizasyonun değişiklik yönetimi sürecinde aşağıdaki hususların dikkate alınması gerekir:

a) Kritiklik. Söz konusu değişiklik ne kadar kritiktir? Hizmet sağlayıcısı tarafından organizasyonun faaliyetleri üzerindeki etki ile diğer organizasyonlar ve havacılık sistemi üzerindeki etki göz önünde bulundurulmalıdır.

b) Konu uzmanlarının mevcut olması. Havacılık topluluğunun önemli üyelerinin değişiklik yönetimine dahil edilmesi önemlidir; bu husus, harici organizasyonlardan kişileri içerebilir.

c) Emniyet performansı verilerinin ve bilgilerinin elverişliliği. Duruma ilişkin bilgi vermek ve değişikliğe yönelik analizi mümkün kılmak için kullanılabilen hangi veriler ve bilgiler mevcuttur?

9.5.5.4 Küçük artımlı değişiklikler genellikle fark edilmez, ancak kümülatif etki kayda değer olabilir. İster büyük ister küçük olsun, değişiklikler, söz konusu organizasyonun sistem tanımına etki edebilecek ve revizyonuna yönelik ihtiyaca yol açabilecektir. Bu sebeple, çoğu hizmet sağlayıcısı tarafından düzenli ve hatta sürekli olarak değişiklik yaşandığı göz önünde bulundurulduğunda, sürekli geçerliliğini tespit etmek için sistem tanımının düzenli olarak gözden geçirilmesi gerekir.

9.5.5.5 Hizmet sağlayıcısı tarafından resmi değişiklik sürecine yönelik tetikleyicinin tanımlanması gerekir. Resmi değişiklik yönetimini tetiklemesi muhtemel olan değişiklikler şunları içerir:

a) yeni teknolojinin veya ekipmanların getirilmesi;

b) çalışma ortamındaki değişiklikler;

c) kilit öneme sahip olan personeldeki değişiklikler;

d) kadro seviyelerindeki önemli değişiklikler;

e) emniyete ilişkin mevzuat gerekliliklerindeki değişiklikler;

f) söz konusu organizasyonun önemli düzeyde yeniden yapılanması ve

g) fiziki değişiklikler (yeni tesis veya üs, havaalanı yerleşimi değişiklikleri vb.).

9.5.5.6 Hizmet sağlayıcısı tarafından aynı zamanda söz konusu değişikliğin personel üzerindeki etkisi de göz önünde bulundurulmalıdır. Bu husus, söz konusu değişikliğin tesir görenler tarafından kabul edilme şekline etki edebilir. Erken iletişim ve angajman normalde söz konusu değişikliğin algılanma ve uygulanma şeklini iyileştirecektir.

9.5.5.7 Değişiklik yönetimi süreci aşağıdaki faaliyetleri içermelidir:

a) *değişikliği anlayın ve tanımlayın;* söz konusu değişikliğe ve söz konusu değişikliğin neden uygulanmakta olduğuna dair açıklamayı içermelidir;

b) *kimleri ve neleri etkileyeceğini anlayın ve tanımlayın;* bunlar, söz konusu organizasyon dahilindeki kişiler, diğer departmanlar veya harici kişiler veya organizasyonlar olabilecektir. Ekipmanlar, sistemler ve süreçler de etkilenebilecektir. Sistem tanımının ve organizasyonun arayüz bağlantılarının gözden geçirilmesine ihtiyaç duyulabilecektir. Bu, söz konusu değişikliğe kimlerin dahil edilmesi gerektiğinin tespit edilmesine yönelik bir fırsattır. Değişiklikler, diğer risklerin hafifletilmesi için halihazırda uygulanmakta olan risk kontrollerine etki edebilecektir ve bu sebeple, değişiklik hemen görülebilir nitelikte olmayan alanlardaki riskleri arttırabilecektir;

c) *değişikliğe ilişkin tehlikeleri tanımlayın ve emniyet riski değerlendirmesi gerçekleştirin;* söz konusu değişiklik ile doğrudan ilgili olan tehlikeleri tanımlamalıdır. Söz konusu değişiklikten tesir görebilecek olan emniyet riski kontrolleri ve mevcut tehlikeler üzerindeki etkinin de gözden geçirilmesi gerekir. Bu adımda, mevcut organizasyonun Emniyet Riski Yönetimi (SRM) süreçleri kullanılmalıdır;

d) *eylem planı geliştirin;* burada neyin kim tarafından ne zaman yapılması gerektiği tanımlanmalıdır. Söz konusu değişikliğin nasıl uygulanacağını ve hangi tedbirlerden kimin sorumlu olacağını ve her bir görevin sıralamasını ve planlamasını açıklayan açık bir plan olmalıdır.

e) *değişikliği resmi olarak onaylayın;* söz konusu değişikliğin uygulanmak için emniyetli olduğunun teyit edilmesi içindir. Söz konusu değişikliğin uygulanmasına yönelik genel sorumluluğa ve yetkiye sahip olan kişi tarafından değişiklik planının onaylanması gerekir ve

f) *güvence planı;* hangi takip tedbirinin gerekli olduğunun tespit edilmesine yöneliktir. Söz konusu değişikliğin nasıl bildirileceğini ve değişiklik sırasında veya sonrasında ilave faaliyetlere (denetimler gibi) ihtiyaç duyulup duyulmadığını göz önünde bulundurun. Yapılan varsayımların test edilmesi gerekir.

9.5.6 Emniyet Yönetimi Sisteminin (SMS) sürekli iyileştirilmesi

9.5.6.1 Annex 19, Ek 2, 3.3 kapsamında ..."hizmet sağlayıcısı, Emniyet Yönetimi Sisteminin (SMS) genel etkinliğini sürdürmek veya sürekli olarak iyileştirmek için kendi Emniyet Yönetimi Sistemi (SMS) süreçlerini izler ve değerlendirir" şeklinde öngörülmektedir. Hizmet sağlayıcısının Emniyet Yönetimi Sisteminin (SMS) etkinliğinin sürdürülmesi ve sürekli iyileştirilmesi, doğrulama ve takip tedbirlerini ve iç denetim süreçlerini içeren emniyet güvencesi faaliyetleri tarafından desteklenir. Organizasyonun kendisinin ve çalışma ortamının sürekli olarak değişecek olmasına bağlı olarak Emniyet Yönetimi Sisteminin (SMS) sürdürülmesinin ve sürekli olarak iyileştirilmesinin süreklilik arz eden bir yolculuk olduğu kabul edilmelidir.

9.5.6.2 İç denetimler, söz konusu hizmet sağlayıcısının, organizasyonun karar alma süreçlerine faydalı olan bilgileri sunabilen havacılık faaliyetlerinin değerlendirilmesini kapsar. İç denetim işlevinde, organizasyon genelindeki emniyet yönetimi işlevlerinin tümüne yönelik değerlendirmeye yer verilir.

9.5.6.3 Emniyet Yönetimi Sistemi (SMS) etkinliği sadece Emniyet Performansı Göstergelerine (SPI'ler) dayalı olmamalıdır; hizmet sağlayıcıları tarafından, etkinliğinin tespit edilmesine, çıktıların yanı sıra süreçlerin sonuçlarının ölçülmesine ve bu faaliyetler vasıtasıyla elde edilen bilgilerin değerlendirilmesine yönelik çeşitli yöntemlerin uygulanması amaçlanmalıdır. Bu yöntemler aşağıdakileri içerebilir:

a) *Denetimler*; iç denetimleri ve diğer organizasyonlar tarafından yürütülen denetimleri içerir.

b) *Değerlendirmeler*; emniyet kültürüne ve Emniyet Yönetimi Sistemi (SMS) etkinliğine yönelik değerlendirmeleri içerir.

c) *Olayların izlenmesi*: hataların ve kural ihlali durumlarının yanı sıra kazalar ve olaylar da dahil olmak üzere, emniyet olaylarının tekrarını izleyin.

d) *Emniyet araştırmaları*; personel tarafından Emniyet Yönetimi Sistemine (SMS) angaje olunmasına ilişkin faydalı geri bildirim sağlayan kültürel araştırmalar da dahil. Aynı zamanda, söz konusu organizasyonun emniyet kültürüne ilişkin bir gösterge de sunabilir.

e) *Yönetim gözden geçirmeleri*; söz konusu organizasyon tarafından emniyet amaçlarına ulaşılıp ulaşılmadığını ve emniyet amaçlarının, genel trendlerin belirlenmesi için mevcut emniyet performansı bilgilerine bakılmasına yönelik bir fırsat olup olmadığını inceleyin. Emniyet Yönetimi Sisteminin (SMS) etkinliğinin üst yönetim tarafından gözden geçirilmesi önemlidir. Bu gözden geçirme, en üst düzey emniyet komitesinin işlevlerinden biri olarak gerçekleştirilebilir.

f) *Emniyet Performansı Göstergelerinin (SPI'ler) ve Emniyet Performansı Hedeflerinin (SPT'ler) değerlendirilmesi*; muhtemelen yönetim gözden geçirmesi kapsamında. Trendleri dikkate alır ve uygun veriler mevcut olduğunda, diğer hizmet sağlayıcılarının veya Devletin verileri veya global verilerle karşılaştırılabilir.

g) *Öğrenilen derslerin işlenmesi*; emniyet raporlaması sistemlerinden ve hizmet sağlayıcısı emniyet soruşturmalarından öğrenilen derslerin işlenmesi. Bunların, uygulanmakta olan emniyet iyileştirmelerini beraberinde getirmesi gerekir.

9.5.6.4 Özet olarak, emniyet performansı ve iç denetim süreçlerinin izlenmesi, hizmet sağlayıcısının kendi emniyet performansını sürekli olarak iyileştirme becerisine katkı sağlar. Emniyet Yönetimi Sisteminin (SMS); ilgili emniyet riski kontrollerinin ve destek sistemlerinin kesintisiz olarak izlenmesi, söz konusu hizmet sağlayıcısına ve Devlete emniyet yönetimi süreçlerinin arzu edilen emniyet performansı amaçlarına ulaştığı hususunda güvence teşkil eder.

9.6 4. BİLEŞEN: EMNİYET TEŞVİKİ

9.6.1 Emniyetin teşvik edilmesi, pozitif emniyet kültürünü teşvik eder ve eğitim ve öğretim, etkili iletişim ve bilgi paylaşımı vasıtasıyla sürekli olarak iyileştirilen teknik yetkinlik kombinasyonuyla hizmet sağlayıcısının emniyet amaçlarına ulaşılmasına yardımcı olur. Üst yönetim tarafından organizasyon genelinde emniyet kültürünün teşvik edilmesine liderlik edilir.

9.6.2 Etkin emniyet yönetimine sadece zorlama veya politikalara ve prosedürlere sıkı riayetle ulaşılamaz. Emniyetin teşvik edilmesi hem bireysel hem de organizasyonel davranışa etki eder ve emniyet çalışmalarını destekleyen bir değer sistemi sunarak söz konusu organizasyonun politikalarını, prosedürlerini ve süreçlerini tamamlar.

9.6.3 Söz konusu hizmet sağlayıcısı tarafından, organizasyonun tüm seviyeleri genelinde etkin iki yönlü iletişimi kolaylaştıran süreçlerin ve prosedürlerin tesis edilmesi ve uygulanması gerekir. Burada, organizasyonun en üstünden itibaren açık bir stratejik yönlendirmeye ve tüm personelden açık ve yapıcı geri bildirimi teşvik eden "alttan üste" iletişimin mümkün kılınmasına yer verilmelidir.

9.6.4 Eğitim ve öğretim

9.6.4.1 Annex 19 kapsamında, "hizmet sağlayıcısı tarafından, personelin eğitilmesini ve Emniyet Yönetimi Sistemi (SMS) görevlerini ifa etmeye yetkin olmasını sağlayan bir emniyet eğitimi programı geliştirilecek ve sürdürülecektir" şeklinde öngörülmektedir. Ayrıca, "emniyet eğitimi programının kapsamının her bir bireyin Emniyet Yönetimi Sistemine (SMS) dahline uygun olması" öngörülmektedir. Uygun bir emniyet eğitimi programının uygulanmasının sağlanmasından emniyet yöneticisi sorumludur. Söz konusu organizasyon tarafından karşılanan spesifik emniyet sorunlarına ilişkin uygun emniyet bilgilerinin sunulması buna dahildir. Söz konusu organizasyondaki seviyelerine bakılmaksızın, Emniyet Yönetimi Sistemi (SMS) görevlerini ifa etmek üzere eğitimli ve yetkin olan personel, yönetimin etkin bir Emniyet Yönetimi Sistemine (SMS) yönelik taahhüdünün bir göstergesidir. Eğitim programında, başlangıç ve yetkinliklerin sürdürülmesine yönelik tazeleme eğitimi gerekliliklerine yer verilmelidir. Başlangıç emniyet eğitimi kapsamında, asgari olarak, aşağıdakiler göz önünde bulundurulmalıdır:

a) organizasyonel emniyet politikaları ve emniyet amaçları;

b) emniyete ilişkin organizasyonel görevler ve sorumluluklar;

c) temel Emniyet Riski Yönetimi (SRM) prensipleri;

d) emniyet raporlaması sistemleri;

e) söz konusu organizasyonun Emniyet Yönetimi Sistemi (SMS) süreçleri ve prosedürleri ve

f) insan faktörleri.

9.6.4.2 Tazeleme emniyet eğitimi, Emniyet Yönetimi Sistemi (SMS) politikalarındaki, süreçlerindeki ve prosedürlerindeki değişikliklere odaklanmalı ve söz konusu organizasyona veya öğrenilen derslere ilişkin spesifik emniyet sorunlarını vurgulamalıdır.

9.6.4.3 Eğitim programı, söz konusu kişinin Emniyet Yönetimi Sistemi (SMS) dahilindeki ihtiyaçlarına uyarlanmalıdır. Örneğin, söz konusu organizasyonun emniyet komitelerinde yer alan yöneticilerine yönelik eğitim seviyesi ve derinliği, organizasyonun ürün veya hizmetlerinin sunulmasına doğrudan dahil olan personele yönelik olandan daha kapsamlı olacaktır. Operasyonlara doğrudan dahil olmayan personel, sadece söz konusu organizasyona ilişkin üst seviyede genel bilgiye ihtiyaç duyabilir.

Eğitim ihtiyaçları analizi

9.6.4.4 Çoğu organizasyon için, operasyona, personelin emniyet görevlerine ve mevcut eğitime yönelik açık bir anlayışın olmasını sağlamak için resmi bir eğitim ihtiyaçları analizi (TNA) gereklidir. Tipik Eğitim İhtiyaçları Analizi (TNA) normalde, genellikle aşağıdaki adımları içeren bir hedef kitle analizinin gerçekleştirilmesiyle başlar:

a) Söz konusu hizmet sağlayıcısının her bir personeli, aynı yollarda veya aynı derecede olmamak üzere, Emniyet Yönetimi Sisteminin (SMS) uygulanmasından tesir görecektir. Her bir personel gruplamasını ve bu grupların, bilhassa emniyet görevlerine ilişkin olmak üzere, emniyet yönetimi süreçleriyle, girdileriyle ve çıktılarıyla hangi yollarla etkileşim halinde olacaklarını belirleyin. Bu bilgilerin pozisyon/görev tanımlarından elde edilmesi gerekir. Normalde, kişilerin gruplandırılması benzer eğitim ihtiyaçlarına sahip olunduğunu ortaya çıkaracaktır. Hizmet sağlayıcısı tarafından analizin bağlantılı olunan harici organizasyonlardaki personele genişletilmesinin değerli olup olmadığını göz önünde bulundurulması gerekir.

b) Her bir emniyet görevini ifa etmek için gereken ve her bir personel grubu tarafından ihtiyaç duyulan bilgiyi ve yetkinlikleri belirleyin.

c) İş gücü genelindeki halihazırdaki emniyet becerisi ve bilgisi ile tahsis edilen emniyet görevlerinin etkili bir şekilde ifa edilmesi için ihtiyaç duyulan beceri ve bilgi arasındaki boşluğu belirlemek için analiz gerçekleştirin.

d) Her bir kişinin veya grubun emniyet yönetimine dahil olması için uygun olan bir eğitim programı geliştirmek amacıyla, her bir grup için en uygun becerileri ve bilgi geliştirme yaklaşımını belirleyin. Eğitim programında, personelin sürekli emniyet bilgisi ve yetkinliği ihtiyaçları da göz önünde bulundurulmalıdır; bu ihtiyaçlar tipik olarak bir tazeleme eğitimi programıyla karşılanacaktır.

9.6.4.5 Aynı zamanda, eğitim sunumuna yönelik uygun yöntemin belirlenmesi de önemlidir. Ana amaç, eğitimin tamamlanması sonrasında personelin kendi Emniyet Yönetimi Sistemi (SMS) görevlerini ifa etmeye yetkin olmasıdır. Yetkin eğitmenler genellikle dikkate alınması gereken en önemli husustur; bu kişilerin bağlılığı, öğretme becerileri ve emniyet yönetimi uzmanlığı, verilen eğitimin etkinliği üzerinde belirgin bir etkiye sahip olacaktır. Emniyet eğitimi programında aynı zamanda eğitim içeriğinin ve planlamasının geliştirilmesine ve eğitim ve yetkinlik kayıtlarının yönetimine yönelik sorumluluklar da belirtilmelidir.

9.6.4.6 Organizasyon tarafından, kimlerin ne derinlikte eğitime tabi tutulması gerektiği tespit edilmelidir ve bu husus, ilgili kişilerin Emniyet Yönetimi Sistemine (SMS) dahil olmalarına bağlı olacaktır. Söz konusu organizasyonda çalışan çoğu kişi havacılık emniyeti ile bir takım doğrudan veya dolaylı ilişkiye, dolayısıyla da bir takım Emniyet Yönetimi Sistemi (SMS) görevlerine sahiptir. Bu husus, ürünlerin ve hizmetlerin sunumuna doğrudan dahil olan tüm personel ile söz konusu organizasyon emniyet komitelerinde yer alan personel için geçerlidir. Bazı idari personel ve destek personeli sınırlı Emniyet Yönetimi Sistemi (SMS) görevlerine sahip olacak ve işlerinin havacılık emniyetinde yine de dolaylı etkiye sahip olabilecek olmasına bağlı olarak bir takım Emniyet Yönetimi Sistemi (SMS) eğitimine ihtiyaç duyacaktır.

9.6.4.7 Hizmet sağlayıcısı tarafından personelin Emniyet Yönetimi Sistemi (SMS) görevleri belirlenmeli ve söz konusu bilgiler, emniyet eğitimi programını incelemek üzere kullanılmalı ve her bir birey tarafından söz konusu bireyin Emniyet Yönetimi Sistemine (SMS) dahli ile uyumlu eğitim alması sağlanmalıdır. Emniyet eğitimi programında, destek personeline, operasyon personeline, yöneticilere ve amirlere, üst düzey yöneticilere ve sorumlu yöneticiye yönelik emniyet eğitiminin içeriği belirtilmelidir.

9.6.4.8 Sorumlu yöneticiye ve üst düzey yöneticilere yönelik olarak aşağıdaki konu başlıklarını içeren spesifik emniyet eğitimi olmalıdır:

a) yeni sorumlu yöneticilere ve post holder'lara yönelik, kendi Emniyet Yönetimi Sistemi (SMS) mesuliyetlerine ve sorumluluklarına ilişkin spesifik farkındalık eğitimi;

b) ulusal ve organizasyonel emniyet gerekliliklerine uyumun önemi;

c) yönetim taahhüdü;

d) kaynakların tahsis edilmesi;

e) emniyet politikasının ve Emniyet Yönetimi Sisteminin (SMS) teşvik edilmesi;

f) pozitif emniyet kültürünün teşvik edilmesi;

g) departmanlar arası etkin emniyet iletişimi;

h) emniyet amacı, Emniyet Performansı Hedefleri (SPT'ler) ve uyarı seviyeleri ve

i) disiplin politikası.

9.6.4.9 Emniyet eğitimi programının ana amacı, organizasyonun tüm seviyelerindeki personel tarafından emniyet görevlerinin yerine getirilmesi için yetkinliğin sürdürülmesinin sağlanmasıdır; bu sebeple personelin yetkinlikleri düzenli olarak gözden geçirilmelidir.

9.6.5 Emniyet iletişimi

9.6.5.1 Söz konusu organizasyonun Emniyet Yönetimi Sistemi (SMS) amaçları ve prosedürleri, hizmet sağlayıcısı tarafından tüm uygun personele bildirilmelidir. Emniyet iletişiminin, kişinin rolüne ve emniyet ile ilgili bilgileri alma ihtiyacına dayalı en uygun yöntemle verilmesini mümkün kılan bir iletişim stratejisi olmalıdır. Bu, haber bültenleri, bildirimler, bültenler, brifingler veya eğitim kurslarıyla yapılabilir. Emniyet yöneticisi tarafından aynı zamanda, gerek dahili olarak gerekse de diğer organizasyonlardan olmak üzere, soruşturmalardan ve vaka geçmişlerinden veya deneyimlerden öğrenilen derslerin geniş çaplı olarak dağıtılması sağlanmalıdır. Bu sebeple, emniyet iletişiminin amaçları şunlardır;

a) *personelin Emniyet Yönetimi Sisteminden (SMS) tümüyle haberdar olmasının sağlanması;* bu, organizasyonun emniyet politikasının ve emniyet amaçlarının teşvik edilmesine yönelik iyi bir yoldur.

b) *emniyet bakımından kritik bilgilerin aktarılması;* Emniyet bakımından kritik bilgiler, söz konusu organizasyonu emniyet riskine maruz bırakabilecek emniyet risklerine ve emniyet sorunlarına ilişkin spesifik bilgilerdir. Bu bilgiler, öğrenilen dersler veya emniyet riski kontrollerine ilişkin olanlar gibi dahili veya harici kaynaklardan elde edilen emniyet bilgilerinden sağlanabilir. Hizmet sağlayıcısı tarafından hangi bilgilerin emniyet bakımından kritik sayıldığı ve bu bilgilerin iletişiminin zamanı tespit edilir.

c) *yeni emniyet riski kontrollerine ve düzeltici faaliyetlere yönelik farkındalığın arttırılması;* Hizmet sağlayıcısı tarafından karşı karşıya kalınan emniyet riskleri zamanla değişecektir ve ister tanımlanmış yeni bir emniyet riski, ister emniyet riski kontrollerindeki değişiklikler olsun, bu değişikliklerin uygun personele bildirilmesi gerekecektir.

d) *yeni veya değiştirilen emniyet prosedürlerine ilişkin bilgi sağlanması;* emniyet prosedürleri güncellendiğinde, uygun kişilerin bu değişikliklerden haberdar edilmeleri önemlidir.

e) *pozitif emniyet kültürünün teşvik edilmesi ve personelin tehlikeleri tanımlamaya ve rapor etmeye cesaretlendirilmesi;* emniyet iletişimi iki yönlüdür. Tüm personel tarafından emniyet sorunlarının emniyet raporlaması sistemi vasıtasıyla organizasyona bildirilmesi önemlidir.

f) *geri bildirimin sağlanması;* emniyet raporları sunan personele, belirlenen kaygıların ele alınması için hangi tedbirlerin alınmış olduğuna dair geri bildirimde bulunun.

9.6.5.2 Hizmet sağlayıcıları tarafından, yukarıda listelenmekte olan emniyet bilgilerinden herhangi birinin harici organizasyonlara bildirilmesinin gerekli olup olmadığı değerlendirilmelidir.

9.6.5.3 Hizmet sağlayıcıları tarafından, kendi emniyet iletişimlerinin etkinliği, dağıtılan emniyet bakımından kritik bilgilerin personel tarafından alınmış ve anlaşılmış olduğu kontrol edilerek değerlendirilmelidir. Bu değerlendirme, iç denetim faaliyetleri kapsamında veya Emniyet Yönetimi Sistemi (SMS) etkinliği değerlendirilirken yapılabilir.

9.6.5.4 Emniyet teşviki faaliyetleri, sadece başlangıçta değil, Emniyet Yönetimi Sisteminin (SMS) yaşam döngüsü genelinde yürütülmelidir.

9.7 UYGULAMANIN PLANLANMASI

9.7.1 Sistem tanımı

9.7.1.1 Sistem tanımı, Emniyet Yönetimi Sisteminin (SMS) kapsamını tanımlamak üzere, arayüz bağlantıları da dahil olmak üzere organizasyonel süreçlerin tanımlanmasına yardımcı olur. Bu, söz konusu hizmet sağlayıcısının Emniyet Yönetimi Sistemi (SMS) bileşenlerine ve unsurlarına ilişkin boşlukların saptanmasına imkan verir ve organizasyonel ve operasyonel tehlikelerin tanımlanmasına yönelik bir başlangıç noktası işlevi görebilir. Sistem tanımı, Emniyet Riski Yönetiminin (SRM) ve emniyet güvencesinin etkin olması için söz konusu ürünün, hizmetin veya faaliyetin özelliklerinin belirlenmesine hizmet eder.

9.7.1.2 Çoğu organizasyon, farklı departmanların yanı sıra tümü söz konusu organizasyonun emniyetli operasyonuna katkı sağlayan farklı harici organizasyonları içeren karmaşık bir arayüz bağlantıları ve etkileşimler ağından oluşur. Sistem tanımının kullanılması, söz konusu organizasyona, bir çok etkileşiminin ve arayüz bağlantısının daha belirgin bir resmine sahip olma imkanı verir. Bu sayede emniyet riski ve tanımlanmaları halinde emniyet riski kontrollerinin daha iyi bir şekilde yönetilmesi sağlanacak ve Emniyet Yönetimi Sistemi (SMS) süreçlerindeki ve prosedürlerindeki değişikliklerin etkisinin anlaşılmasına yardımcı olunacaktır.

9.7.1.3 Herhangi bir sistem tanımı değerlendirilirken, "sistemin", birbirine bağlı bir ağın parçaları olarak birlikte çalışan unsurlar seti olduğunun kavranılması önemlidir. Emniyet Yönetimi Sisteminde (SMS), söz konusu organizasyonun havacılık emniyeti faaliyetlerine ilişkin olan ve söz konusu organizasyonun havacılık emniyeti faaliyetlerine etki edebilecek unsurlar organizasyonun ürünleri, kişileri, süreçleri, prosedürleri, tesisleri, hizmetleri ve (dış etkenler de dahil olmak üzere) diğer unsurlardır. Genellikle, "sistem", alt sistemlere sahip olan sistem olarak da görülebilecek olan sistemler koleksiyonudur. Bu sistemler ve bunların birbirleriyle olan etkileşimleri tehlikelerin kaynaklarını oluşturur ve emniyet risklerinin kontrolüne katkı sağlar. Önemli sistemler, hem havacılık emniyetine doğrudan etki edebilecek olanları hem de organizasyonun etkin emniyet yönetimini yürütme becerisine veya kapasitesine etki edenleri içerir.

9.7.1.4 Emniyet Yönetimi Sistemi (SMS) dokümantasyonunda sistem tanımına ve Emniyet Yönetimi Sistemi (SMS) arayüz bağlantılarına ilişkin genel bilgilere yer verilmelidir. Sistem tanımı, politikalara ve prosedürlere atıfların yapıldığı bir madde imli listeyi içerebilir. Süreç akışı veya ek açıklamalara sahip olan organizasyon şeması gibi grafiksel bir gösterim bazı organizasyonlar için yeterli olabilir. Organizasyon tarafından, söz konusu organizasyon için işe yarayan bir yöntem ve format kullanılmalıdır.

9.7.1.5 Her organizasyonun kendine mahsus olması sebebiyle, Emniyet Yönetimi Sistemi (SMS) uygulamasına yönelik "her soruna uygun tek çözüm" yöntem mevcut değildir. Her organizasyon tarafından kendine mahsus duruma yönelik olarak işe yarayan bir Emniyet Yönetimi Sisteminin (SMS) uygulanması beklenir. Her organizasyon, temel gerekliliklerin karşılanmasını nasıl amaçladığını kendisi için tanımlamalıdır. Bunu başarmak için, her bir organizasyon tarafından söz konusu organizasyonun organizasyon yapısını, süreçlerini ve emniyet yönetimi işlevleri bakımından önemli olarak değerlendirdiği iş düzenlemelerini tanımlayan bir sistem tanımının hazırlanması önemlidir. Sistem tanımına dayalı olarak, söz konusu organizasyon tarafından kendi emniyet yönetimi gerekliliklerini tesis eden politikanın, süreçlerin ve prosedürlerin tanımlanması veya geliştirilmesi gerekir.

9.7.1.6 Herhangi bir organizasyon tarafından sistem tanımında tanımlanan süreçlerde belirgin veya maddi değişikliklerin yapılması tercih edildiğinde, söz konusu değişikliklerin, temel emniyet riski değerlendirmesine potansiyel olarak etki eder şekilde görülmesi gerekir. Dolayısıyla, sistem tanımının değişiklik yönetimi süreçleri kapsamında gözden geçirilmesi gerekir.

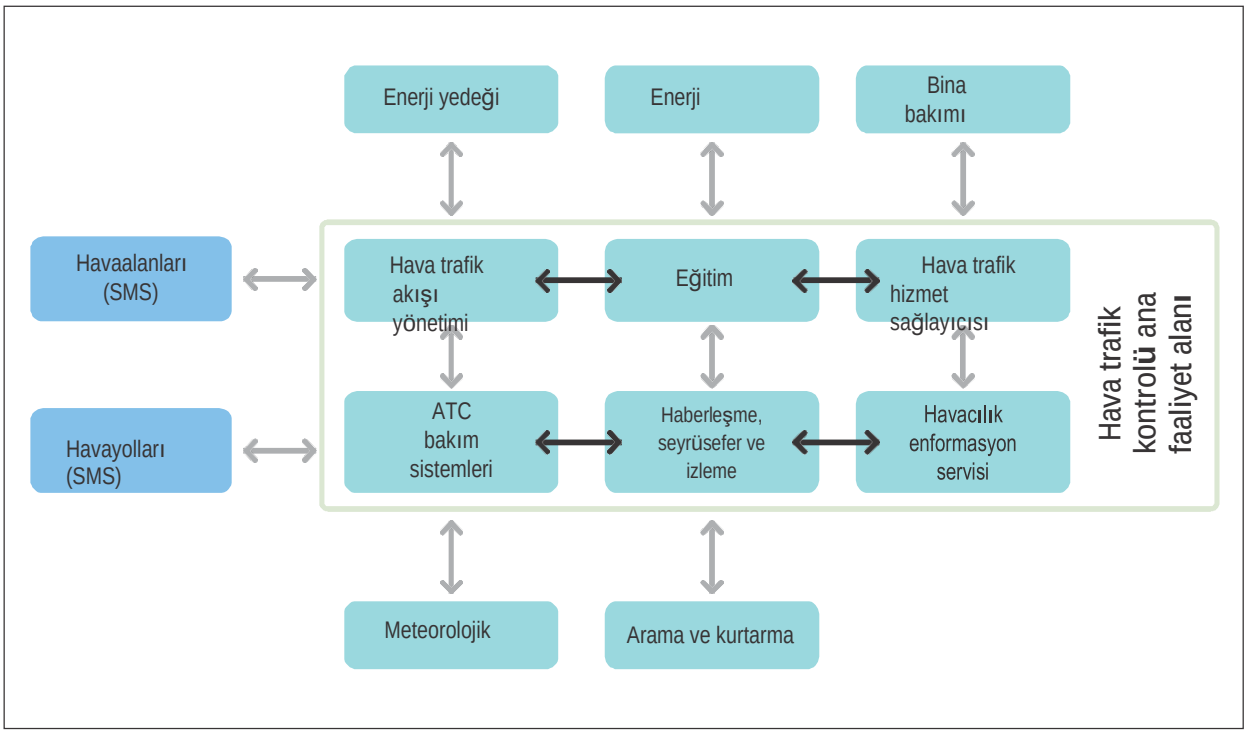
9.7.2 Arayüz yönetimi

Hizmet sağlayıcıları tarafından karşı karşıya kalınan emniyet riskleri arayüzlerden etkilenir. Arayüzler dahili (örneğin, departmanlar arasında) veya harici (örneğin, diğer hizmet sağlayıcıları veya sözleşmeye dayalı hizmetler) olabilir. Bu arayüzleri belirlemek ve yönetmek suretiyle, söz konusu hizmet sağlayıcısı, arayüzlere ilişkin emniyet risklerinin üzerinde daha fazla kontrole sahip olacaktır. Bu arayüzlerin sistem tanımı dahilinde tanımlanması gerekir.

9.7.3 Emniyet Yönetimi Sistemi (SMS) arayüzlerinin belirlenmesi

9.7.3.1 Başlangıçta, hizmet sağlayıcıları tarafından kendi iş faaliyetlerine ilişkin arayüz bağlantılarına yoğunlaşılmalıdır. Bu arayüzlerin tanımlanması, Emniyet Yönetimi Sisteminin (SMS) kapsamını ortaya koyan sistem tanımında detaylandırılmalı ve dahili ve harici arayüz bağlantılarını içermelidir.

9.7.3.2 Şekil 9-3, Emniyet Yönetimi Sistemi (SMS) arayüzlerini tanımlamak için etkileşimde bulunduğu farklı organizasyonların hizmet sağlayıcısı tarafından nasıl detaylarıyla gösterilebileceğine dair bir örnektir. Bu gözden geçirmenin amacı, tüm arayüz bağlantılarına ilişkin kapsamlı bir liste oluşturmaktır. Organizasyon tarafından mutlaka tamamen haberdar olunması gerekmeyen Emniyet Yönetimi Sistemi (SMS) arayüz bağlantılarının olabilecek olması, bu uygulamanın gerekçesini teşkil etmektedir. Enerji veya bina bakımı şirketlerinde olduğu gibi, resmi sözleşmelerin uygulamada olmadığı arayüz bağlantıları söz konusu olabilecektir.



Şekil 9-3. Hava trafik hizmet sağlayıcısı Emniyet Yönetimi Sistemi (SMS) arayüzlerine ilişkin örnek

9.7.3.3 Dahili arayüzlerden bazıları, pazarlama, finans, hukuk ve insan kaynakları gibi, emniyet ile doğrudan ilişkili olmayan iş alanlarına ilişkin olabilir. Bu alanlar, iç kaynaklara ve yatırıma etki eden kararların yanı sıra harici organizasyonlarla olan anlaşmalar ve sözleşmeler vasıtasıyla emniyete etki edebilir ve bunların mutlaka emniyetine yönelik olmasına gerek bulunmayabilir.

9.7.3.4 Emniyet Yönetimi Sistemi (SMS) arayüzlerinin belirlenmesi sonrasında, söz konusu hizmet sağlayıcısı tarafından bunların nispi kritikliğinin dikkate alınması gerekir. Bu sayede, söz konusu hizmet sağlayıcısı tarafından daha kritik arayüzlerin ve bunların potansiyel emniyet risklerinin yönetilmesine öncelik verilmesine imkan verilir. Dikkate alınması gereken hususlar şunlardır:

a) neyin sağlanmakta olduğu;

b) buna neden ihtiyaç duyulduğu;

c) dahil olan organizasyonların uygulamada olan bir Emniyet Yönetimi Sistemine (SMS) veya başka bir yönetim sistemine sahip olup olmadığı ve

d) söz konusu arayüzün emniyet verilerinin / bilgilerinin paylaşılmasını kapsayıp kapsamadığı.

Arayüzlerin emniyet etkisinin değerlendirilmesi

9.7.3.5 Söz konusu hizmet sağlayıcısı tarafından bunun akabinde arayüzlere ilişkin tehlikelerin tanımlanmalı ve mevcut risk tanımlama ve emniyet riski değerlendirmesi süreçleri kullanılarak emniyet riski değerlendirmesi gerçekleştirilmelidir.

9.7.3.6 Tanımlanan risklere dayalı olarak, söz konusu hizmet sağlayıcısı tarafından, uygun bir emniyet riski kontrolü stratejisinin belirlenmesi ve tanımlanması için diğer organizasyon ile çalışılması değerlendirilebilir. Diğer organizasyonu dahil etmekle, tehlikelerin tanımlanmasına, emniyet riskinin değerlendirilmesine ve uygun emniyet riski kontrolünün belirlenmesine katkıda bulunulabilir. Emniyet risklerinin algılanmasının her bir organizasyon için aynı olmayabilecek olmasına bağlı olarak bu ortak çalışmaya ihtiyaç duyulur. Risk kontrolü, hizmet sağlayıcısı veya harici organizasyon tarafından yürütülebilecektir.

9.7.3.7 Dahil olan her bir organizasyonun kendi organizasyonuna etki eden tehlikeleri tanımlama ve yönetme sorumluluğuna sahip olduğunun kabulü de önemlidir. Bu husus, farklı emniyet riski sınıflandırmaları uygulamaları ve farklı emniyet riski önceliklerine (emniyet performansı, kaynaklar, zaman, vb. bakımından) sahip olmaları sebebiyle, söz konusu arayüzün kritik mahiyetinin her bir organizasyon için farklı olması anlamına gelebilir.

Arayüzlerin yönetilmesi ve izlenmesi

9.7.3.8 Hizmetlerinin ve ürünlerinin emniyetli bir şekilde sunulmasını sağlamak üzere, arayüzlerin yönetilmesinden ve izlenmesinden hizmet sağlayıcısı sorumludur. Bu sayede, söz konusu arayüzlerin etkin bir şekilde yönetilmesi ve güncel ve ilgili kalması sağlanacaktır. Arayüzlerin ve ilişkili sorumlulukların açık bir şekilde tanımlanabilmesine bağlı olarak, resmi sözleşmeler buna ulaşılmasına yönelik etkin bir yoldur. Arayüzlerdeki ve ilişkili etkilerdeki değişikliklerin ilgili organizasyonlara bildirilmesi gerekir.

9.7.3.9 Hizmet sağlayıcısının arayüz emniyet risklerini yönetme becerisi ile ilişkili zorluklar aşağıdakileri içerir:

a) tek bir organizasyonun emniyet riski kontrollerinin diğer organizasyonların emniyet riski kontrolleri ile uyumlu olmaması;

b) her iki organizasyonun kendi süreçlerindeki ve prosedürlerindeki değişiklikleri kabul etme istekliliği;

c) arayüzün yönetilmesi ve izlenmesi için yetersiz kaynakların veya teknik uzmanlığın mevcut olması ve

d) arayüzlerin sayısı ve konumu.

9.7.3.10 Arayüze dahil olan organizasyonlar arasındaki koordinasyon ihtiyacının kabulü önemlidir. Etkin koordinasyon aşağıdakileri içermelidir:

a) her bir organizasyonun görevlerinin ve sorumluluklarının açıklığa kavuşturulması;

b) alınacak tedbirlere (örneğin, emniyet riski kontrol tedbirleri ve zaman ölçekleri) ilişkin kararlara yönelik mutabakat;

c) hangi emniyet bilgilerinin paylaşılması ve bildirilmesi gerektiğinin belirlenmesi;

d) koordinasyonun nasıl ve ne zaman gerçekleşmesi gerektiği (görev gücü, düzenli toplantılar, özel amaçlı veya tahsisli toplantılar) ve

e) her iki organizasyona da fayda sağlayan ancak Emniyet Yönetimi Sisteminin etkinliğine zarar vermeyen çözümler üzerinde mutabakata varılması.

9.7.3.11 Arayüzlere ilişkin tüm emniyet sorunları veya emniyet riskleri belgelenmeli ve paylaşım ve gözden geçirme için her bir organizasyon tarafından ulaşılabilir kılınmalıdır. Bu sayede, öğrenilen derslerin paylaşılmasına ve her iki organizasyon için değerli olacak olan emniyet verilerinin bir havuzda toplanılmasına imkan verilecektir. Operasyonel emniyet faydalarına, emniyet risklerinin ve sorumluluğun mülkiyetinin paylaşılması sonucunda her bir organizasyon tarafından ulaşılan emniyetin iyileştirilmesi vasıtasıyla ulaşılabilecektir.

9.7.4 Emniyet Yönetimi Sistemi (SMS) Ölçeklendirilebilirliği

9.7.4.1 Politikalar, süreçler ve prosedürler de dahil olmak üzere, organizasyonun Emniyet Yönetimi Sistemi (SMS), söz konusu organizasyonun ve faaliyetlerinin boyutunu ve karmaşıklığını yansıtmalıdır. Aşağıdakileri dikkate almalıdır:

a) organizasyon yapısı ve kaynakların elverişliliği;

b) organizasyonun boyutu ve karmaşıklığı (birden fazla iş yeri ve üs dahil) ve

c) faaliyetlerin karmaşıklığı ve harici organizasyonlar ile olan arayüz bağlantıları.

9.7.4.2 Hizmet sağlayıcısı tarafından, Emniyet Yönetimi Sisteminin (SMS) yönetilmesi için doğru kaynak seviyesinin belirlenmesi için kendi faaliyetlerine yönelik bir analiz gerçekleştirilmelidir. Emniyet Yönetimi Sisteminin (SMS) yönetilmesi için ihtiyaç duyulan organizasyon yapısının belirlenmesi buna dahil olmalıdır. Emniyet Yönetimi Sisteminin (SMS) yönetilmesinden ve sürdürülmesinden kimin sorumlu olacağına, mevcut olması halinde hangi emniyet komitelerine ihtiyaç duyulacağına ve spesifik emniyet uzmanlarına yönelik ihtiyaca yönelik olarak dikkate alınması gereken hususlar buna dahil olacaktır.

Emniyet riski bakımından dikkate alınması gereken hususlar

9.7.4.3 Hizmet sağlayıcısının boyutuna bakılmaksızın, ölçeklendirilebilirlik, aynı zamanda, söz konusu hizmet sağlayıcısının faaliyetlerinin içsel riskine ilişkin bir işlev olmalıdır. Belirgin havacılık emniyeti risklerini içerebilecek olan faaliyetlere küçük organizasyonlar dahi dahil olabilecektir. Bu sebeple, emniyet yönetimi kabiliyetinin yönetilecek emniyet riski ile oranlı olması gerekir.

Emniyet verileri ve emniyet bilgileri ve analizi

9.7.4.4 Küçük organizasyonlar için, düşük veri hacmi, emniyet performansındaki trendlerin veya değişikliklerin belirlenmesinin daha zor olduğu anlamına gelebilir. Bunun için uygun uzmanlarla emniyet sorunlarının ele alınmasına yönelik görüşmelerin ve toplantıların yapılması gerekebilir. Bu, kantitatiften ziyade çok daha kalitatif olabilir, ancak söz konusu hizmet sağlayıcısı için tehlikelerin ve risklerin belirlenmesine yardımcı olacaktır. Söz konusu hizmet sağlayıcısının sahip olmadığı verilere sahip olabilecek olmaları sebebiyle, diğer hizmet sağlayıcıları veya sektör birlikleri ile işbirliği yapılması faydalı olabilir. Örneğin, emniyet riski bilgilerini paylaşmak ve emniyet performansı trendlerini belirlemek için daha küçük ölçekli hizmet sağlayıcıları tarafından benzer organizasyonlarla/operasyonlarla bilgi paylaşımında bulunulabilir. Hizmet sağlayıcılarının, sınırlı olabilecek olması halinde dahi kendi iç verilerini yeterli bir şekilde analiz etmeleri ve işlemeleri gerekir.

9.7.4.5 Birçok etkileşime ve arayüze sahip olan hizmet sağlayıcıları tarafından, birden fazla organizasyondan emniyet verilerini ve emniyet bilgilerini nasıl topladıklarının değerlendirilmesi gerekli olacaktır. Bu, harmanlanmak ve daha sonradan analiz edilmek üzere toplanmakta olan büyük hacimlerde verilerle sonuçlanabilir. Bu hizmet sağlayıcıları tarafından bu tür verilerin yönetilmesine yönelik uygun bir yöntem kullanılmalıdır. Söz konusu verilerin analizine yardımcı olması için, toplanan verilerin kalitesine ve sınıflandırmaların kullanılmasına da özen gösterilmelidir.

9.7.5 Yönetim sistemlerinin entegrasyonu

9.7.5.1 Emniyet yönetimi sisteminin (ayrı olarak değil) bir emniyet yönetimi sistemi kapsamında değerlendirilmesi gerekir. Bu sebeple, herhangi bir hizmet sağlayıcısı tarafından Emniyet Yönetimi Sistemini (SMS) içeren herhangi bir entegre yönetim sistemi uygulanabilir. Entegre yönetim sistemi, birden fazla sertifikayı, yetkilendirmeyi veya onayı elde etmek, kalite, güvenlik, iş sağlığı ve çevre yönetim sistemleri gibi diğer iş yönetimi sistemlerini kapsamak için kullanılabilir. Bu, tekrarı gidermek ve birden fazla faaliyet genelindeki emniyet risklerini yöneterek sinerjilerden yararlanmak için yapılır. Örneğin, hizmet sağlayıcısı birden fazla sertifikaya sahip olduğunda, faaliyetlerinin tümünü kapsamak üzere tek bir yönetim sistemi uygulamayı seçebilir. Söz konusu hizmet sağlayıcısı tarafından kendi iş ihtiyaçlarına veya organizasyonel ihtiyaçlarına uyarlamak üzere kendi Emniyet Yönetimi Sisteminin entegre edilmesine veya ayrı tutulmasına yönelik en iyi yöntemlere karar verilmesi gerekir.

9.7.5.2 Tipik bir entegre yönetim sistemi aşağıdakileri içerebilir:

a) kalite yönetimi sistemi (KYS);

b) emniyet yönetimi sistemi (SMS);

c) güvenlik yönetimi sistemi (SeMS), *Havacılık Güvenliği El Kitabı* (Doc 8973 - Hizmete Özel) kapsamında daha fazla rehberliğe ulaşılabilir

d) çevre yönetim sistemi (ÇYS);

e) iş sağlığı ve emniyet yönetimi sistemi (OHSMS);

f) finansal yönetim sistemi (FYS);

g) dokümantasyon yönetimi sistemi (DYS) ve

h) yorgunluk riski yönetimi sistemi (FRMS).

9.7.5.3 Hizmet sağlayıcısı tarafından kendine özgü ihtiyaçlarına dayalı olarak bu yönetim sistemlerinin entegre edilmesi seçilebilir. Risk yönetimi süreçleri ve iç denetim süreçleri, bu yönetim sistemlerinin çoğunun önemli özellikleridir. Risklerin ve bu sistemlerin herhangi birinde geliştirilen risk kontrollerinin diğer sistemler üzerinde etkiye sahip olabileceği kabul edilmelidir. İlaveten, tedarikçi yönetimi, tesis yönetimi, vb. gibi, yine entegre edilebilecek iş faaliyetleri ile ilişkili diğer operasyonel sistemler de söz konusu olabilecektir.

9.7.5.4 Hizmet sağlayıcısı tarafından, aynı zamanda, Emniyet Yönetimi Sisteminin (SMS) halihazırda Emniyet Yönetimi Sistemine (SMS) yönelik güncel bir mevzuata dayalı gerekliliğin bulunmadığı diğer alanlara uygulanması da değerlendirilebilir. Hizmet sağlayıcıları tarafından, kendi yönetim sistemlerinin kendi iş modellerine, çalışma ortamlarına, mevzuata dayalı ve yasal gerekliliklere ve havacılık topluluğunun beklentilerine uyumlu hale getirilmesi için entegre edilmesine veya ayrı tutulmasına yönelik en uygun yöntemlerin belirlenmesi gerekir. Hangi opsiyon seçilirse seçilsin, Emniyet Yönetimi Sistemi (SMS) gerekliliklerini karşılandığından yine de emin olunmalıdır.

Yönetim sistemi entegrasyonunun faydaları ve zorlukları

9.7.5.5 Farklı alanların tek bir yönetim sistemi altında entegre edilmesi aşağıdakilerle verimliliği iyileştirecektir:

a) süreçlerin ve kaynakların tekrarını ve örtüşmesini azaltarak;

b) potansiyel olarak çatışan sorumlulukları ve ilişkileri azaltarak;

c) tüm faaliyetler genelindeki risklerin ve fırsatların daha geniş etkilerini dikkate alarak ve

d) tüm faaliyetler genelinde performansın etkin bir şekilde izlenmesine ve yönetilmesine imkan vererek.

9.7.5.6 Emniyet sistemi entegrasyonunun olası zorlukları aşağıdakileri içerir:

a) mevcut sistemler, entegrasyona karşı çıkan farklı birim yöneticilerine sahip olabilecektir; bunun sonucunda çatışma ortaya çıkabilecektir;

b) daha fazla işbirliği ve koordinasyon gerektirecek olmasına bağlı olarak söz konusu entegrasyondan etkilenen personel için değişikliğe karşı direnç olabilecektir;

c) her bir sisteme ilişkin olarak farklı kültürlerin söz konusu olabilecek olmasına bağlı olarak organizasyon dahilindeki genel emniyet kültürü üzerindeki etki; bu etki çatışmalar oluşturabilecektir;

d) böyle bir entegrasyonun düzenlemeler tarafından önlenebilecek olması veya farklı düzenleyici otoritelerin veya standart organlarının kendi gerekliliklerinin nasıl karşılanması gerektiği hususunda ayrılan beklentilere sahip olabilecek olması ve

e) farklı yönetim sistemlerinin (KYS ve SMS gibi) entegre edilmesinin, ayrı gerekliliklerin karşılanmakta olduğunun kanıtlanabilmesine yönelik olarak ek iş oluşturabilecek olması.

9.7.5.7 Entegrasyonun faydalarını azami düzeye getirmek ve ilgili zorluklara işaret etmek için, söz konusu değişikliğin etkin bir şekilde yönetilmesi için üst yönetim taahhüdü ve liderliği elzemdir. Entegre yönetim sistemine ilişkin genel sorumluluğa sahip olan kişinin belirlenmesi önemlidir.

9.7.6 Emniyet Yönetimi Sistemi (SMS) ve Kalite Yönetimi Sistemi (KYS) entegrasyonu

9.7.6.1 Bazı hizmet sağlayıcıları hem Emniyet Yönetimi Sistemine (SMS) hem de Kalite Yönetimi Sistemine (KYS) sahiptirler. Bunlar kimi zaman tek bir yönetim sisteminde entegre edilirler. KYS genel olarak herhangi bir ürünün veya hizmetin sunumu sırasında sürekli kalite güvencesine ve iyileştirmeye yönelik bir sistemin tesis ve teşvik edilmesi için gerekli organizasyon yapısı ve ilişkili mesuliyetler, kaynaklar, süreçler ve prosedürler olarak tanımlanır.

9.7.6.2 Her iki sistem de tamamlayıcı niteliktedir; Emniyet Yönetimi Sistemi (SMS) emniyet risklerinin ve emniyet performansının yönetilmesine odaklanırken, KYS, müşteri beklentilerinin ve akdi yükümlülüklerin karşılanmasına yönelik gerekliliklere ve kural koyucu düzenlemelere uyuma odaklanır. Emniyet Yönetimi Sisteminin (SMS) amaçları, tehlikelerin tanımlanması, ilişkili emniyet riskinin değerlendirilmesi ve etkin emniyet riski kontrollerinin uygulanmasıdır. Bunun karşısında, KYS, ilgili spesifikasyonları karşılayan ürünlerin ve hizmetlerin istikrarlı bir şekilde sunulmasına odaklanır. Bununla birlikte, gerek Emniyet Yönetimi Sistemi (SMS) gerek KYS;

a) planlanmalı ve yönetilmeli;

b) havacılık ürünlerinin ve hizmetlerinin sunumuna ilişkin tüm organizasyonel işlevleri içermeli;

c) etkisiz süreçleri ve prosedürleri belirlemeli;

d) sürekli iyileştirmeyi amaçlamalı ve

e) müşterilere emniyetli ve güvenilir ürünlerin ve hizmetlerin sunulmasına yönelik aynı amaca sahip olmalıdır.

9.7.6.3 Emniyet Yönetimi Sistemi (SMS) aşağıdakilere odaklanır:

a) söz konusu organizasyon tarafından karşı karşıya kalınan emniyet ile ilgili tehlikelerin tanımlanması;

b) ilişkili emniyet riskinin değerlendirilmesi;

c) emniyet risklerinin hafifletilmesine yönelik etkin emniyet riski kontrollerinin uygulanması;

d) emniyet performansının ölçülmesi ve

e) emniyet performansı gerekliliklerinin karşılanmasına yönelik olarak uygun kaynak tahsisatının sürdürülmesi.

9.7.6.4 KYS aşağıdakilere odaklanır:

a) düzenlemelere ve gerekliliklere uyum;

b) ürünlerin ve hizmetlerin sunumunda tutarlılık;

c) belirlenen performans standartlarının karşılanması ve

d) "amaca uygun" ve kusurlardan veya hatalardan ari olan ürünlerin ve hizmetlerin sunulması.

9.7.6.5 Düzenlemeler şeklinde uygulanan emniyet riski kontrollerinin söz konusu hizmet sağlayıcısı tarafından etkin bir şekilde uygulandığından ve izlendiğinden emin olunması için düzenlemelere uyumun izlenmesi gereklidir. Uyumsuzlukların sebepleri ve katkıda bulunan faktörleri de analiz edilmeli ve ele alınmalıdır.

9.7.6.6 Emniyet Yönetimi Sisteminin (SMS) ve KYS'nin tamamlayıcı yönleri göz önünde bulundurulduğunda, her bir işlevden ödün vermeksizin her iki sistemi entegre etmek mümkündür. Bu husus aşağıdaki şekilde özetlenebilir:

a) Emniyet Yönetimi Sistemi (SMS), denetim, inceleme, soruşturma, kök neden analizi, süreç tasarımı ve önleyici faaliyetler gibi KYS süreçleri tarafından desteklenir;

b) KYS, emniyet riski kontrollerindeki zayıflıkları veya emniyet sorunlarını belirleyebilir;

c) KYS kapsamında, söz konusu organizasyonun standartlara ve spesifikasyonlara uyumuna karşın mevcut olan emniyet sorunları önceden görülebilir;

d) kalite prensiplerinin, politikalarının ve uygulamalarının emniyet yönetiminin amaçlarıyla uyumlu hale getirilmesi gerekir ve

e) KYS faaliyetleri kapsamında, iç denetimlerin planlanması ve icrası için tanımlanan tehlikelerin ve emniyet riski kontrollerinin göz önünde bulundurulması gerekir.

9.7.6.7 Sonuç olarak, tüm faaliyetler genelindeki daha geniş etkileri dikkate alan karar almaya ve birleştirilmiş amaçlara sahip olan bir entegre yönetim sisteminde, kalite yönetimi ve emniyet yönetimi süreçleri ziyadesiyle tamamlayıcı nitelikte olacak ve genel emniyet amaçlarına ulaşılmasını destekleyecektir.

9.7.7 Emniyet Yönetimi Sistemi (SMS) boşluk analizi ve uygulaması

9.7.7.1 Emniyet Yönetimi Sisteminin (SMS) uygulanması öncesinde, hizmet sağlayıcısı tarafından bir boşluk analizi gerçekleştirilmelidir. Burada, söz konusu hizmet sağlayıcısının mevcut emniyet yönetimi süreçleri ve prosedürleri, söz konusu Devlet tarafından belirlenen Emniyet Yönetimi Sistemi (SMS) gerekliliklerıyle karşılaştırılır. Hizmet sağlayıcısının söz konusu Emniyet Yönetimi Sistemi (SMS) işlevlerinden bazılarını halihazırda uygulamakta olması muhtemeldir. Emniyet Yönetimi Sisteminin (SMS) geliştirilmesi, mevcut organizasyonel politikalara ve süreçlere dayalı olmalıdır. Boşluk analizi, tamamen işler ve etkili olan bir Emniyet Yönetimi Sisteminin (SMS) uygulanması için ihtiyaç duyulan tedbirleri tanımlayan bir Emniyet Yönetimi Sistemi (SMS) uygulama planı vasıtasıyla ele alınması gereken boşlukları belirler.

9.7.7.2 Emniyet Yönetimi Sistemi (SMS) uygulama planı, söz konusu Emniyet Yönetimi Sisteminin (SMS) uygulanması için gereken kaynakların, görevlerin ve süreçlerin açık bir resmini sunmalıdır. Uygulama planının zamanlaması ve sıralaması, aşağıdakiler gibi, her bir organizasyona özgü olacak olan çeşitli etkenlere dayalı olabilecektir:

a) mevzuata dayalı gereklilikler, müşteri gereklilikleri ve yasal gereklilikler;

b) (muhtemelen farklı mevzuata dayalı uygulama tarihlerine sahip olmak üzere) sahip olunan birden fazla sertifika;

c) söz konusu Emniyet Yönetimi Sisteminin (SMS) mevcut yapılara ve süreçlere dayalı olabileceği ölçü;

d) kaynakların ve bütçelerin elverişliliği;

e) farklı adımlar arasındaki karşılıklı bağımlılıklar (veri analizi sisteminin tesis edilmesi öncesinde bir raporlama sistemi uygulanmalıdır) ve

f) mevcut emniyet kültürü.

9.7.7.3 Emniyet Yönetimi Sistemi (SMS) uygulama planı, sorumlu yönetici ve diğer üst düzey yöneticiler ile istişare edilerek geliştirilmeli ve zaman aralıkları ile birlikte ilgili tedbirlerden kimlerin sorumlu olduğunu içermelidir. Söz konusu planda, uygulanabildiği hallerde, harici organizasyonlarla veya yüklenicilerle koordinasyona işaret edilmelidir.

9.7.7.4 Emniyet Yönetimi Sistemi (SMS) uygulama planı, basit bir sütunlu tablodan belirli bir amaç için üretilmiş proje yönetimi yazılımına kadar değişiklik gösteren farklı şekillerde belgelenebilecektir. Söz konusu plan düzenli olarak izlenmeli ve gerektiğinde güncellenmelidir. Herhangi bir spesifik unsurun ne zaman başarılı bir şekilde uygulanmış olarak değerlendirilebildiğini de açıklığa kavuşturmalıdır.

9.7.7.5 Gerek söz konusu Devlet gerek söz konusu hizmet sağlayıcısı tarafından, etkin bir Emniyet Yönetimi Sistemine (SMS) ulaşılmasının birkaç yıl sürebileceği kabul edilmelidir. Emniyet Yönetimi Sisteminin (SMS) uygulanmasına ilişkin aşamalı bir yaklaşıma yönelik gerekliliklerin söz konusu olabilecek olmasına bağlı olarak hizmet sağlayıcıları tarafından kendi Devletlerine başvurulması gerekir.

— SON —

ISBN 978-92-9258-552-5