SİVİL HAVACILIKTA EMNİYET YÖNETİM SİSTEMİNİN UYGULANMASINA İLİŞKİN TALİMAT
(SHT-SMS)

BİRİNCİ BÖLÜM
Amaç, Kapsam, Dayanak, Tanımlar ve Kısaltmalar

Amaç

MADDE 1 -(1) Bu Talimatın amacı SHY-SMS Yönetmeliğine uygun olarak Emniyet Yönetim Sisteminin (SMS) uygulanmasına ilişkin usul ve esasları belirlemektir.

Kapsam

MADDE 2 -(1) Bu Talimat, 14/10/1983 tarihli ve 2920 sayılı Türk Sivil Havacılık Kanununa göre yetkilendirilen; hava seyrüsefer hizmet sağlayıcıları, havaalanı işletmecileri, terminal işletmecileri, hava taşıyıcılarına en az yolcu trafik (yolcu hizmetleri), yük kontrol ve haberleşme ile ramp hizmeti veren yer hizmetleri kuruluşları, ikram üretim ve servis hizmeti veren yer hizmetleri kuruluşları, hava araçlarına hizmet veren akaryakıt kuruluşları, ticari hava taşıma işletmeleri, ticari özel operasyonları (B2) yetkisine sahip genel havacılık işletmeleri, tip intibak eğitim organizasyonları, uçuş eğitim organizasyonları, onaylı bakım kuruluşları, F bakım kuruluşları, hava aracı bakım eğitimi kuruluşları, onaylı havacılık tıp merkezleri ve tasarım ve üretim kuruluşlarını kapsar.

(2) Bu Talimat Türk Silahlı Kuvvetleri sorumluluğunda yürütülen Hava Seyrüsefer Hizmetlerini kapsamamaktadır.

Dayanak

MADDE 3 -(1) Bu Talimat, 14/10/1983 tarih ve 2920 sayılı Türk Sivil Havacılık Kanununa, 15/07/2018 tarih ve 30479 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren 4 numaralı Bakanlıklara Bağlı, İlgili, İlişkili Kurum ve Kuruluşlar ile Diğer Kurum ve Kuruluşların Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesine ve 13/01/2012 tarih ve 28172 sayılı Sivil Havacılıkta Emniyet Yönetim Sistemi (SHY-SMS) Yönetmeliğine dayanılarak hazırlanmıştır.

(2) Bu Talimat hazırlanırken, Uluslararası Sivil Havacılık Teşkilatının (ICAO) 9859 sayılı rehber dökümanında belirtilen gereklilikler esas alınmıştır.

Tanımlar ve kısaltmalar

MADDE 4 -(1) Bu Talimatta yer alan;

a) ADEP : Acil Durum Eylem Planını,

b) Değişiklik yönetimi : Tehlikelere ve risk azaltma stratejilerine etki edebilecek veya ortaya çıkarabilecek olan değişikliklerin, uygulanması öncesinde, organizasyon içerisinde göz önünde bulundurularak yönetilmesi sürecini,

c) EEG : Emniyet Eylem Grubunu,

ç) EGGK : Emniyet Gözden Geçirme Kurulunu,

d) Emniyet bilgisi : Emniyet yönetimi amaçları için faydalı hale getirilmek üzere belirli bir bağlamda işlenen, düzenlenen veya analiz edilen emniyet verilerini,

e) Emniyet hedefi : SMS tarafından ulaşılacak emniyet başarısına veya arzu edilen sonuca ilişkin kısa, üst seviye bir açıklamayı,

f) Emniyet kültürü : Emniyetin işletmedeki yönetim ve çalışanlar tarafından nasıl algılandığını, değer gördüğünü ve önceliklendirildiğini ve kişilere ve gruplara nasıl yansıtıldığını,

g) Emniyet performansı : Emniyet performansı hedefleri ve emniyet performansı göstergeleriyle tanımlanan emniyet başarısını,

ğ) Emniyet performans göstergesi (SPI) :Emniyet performansının izlenmesi ve değerlendirilmesi için kullanılan veri tabanlı bir parametreyi,

h) Emniyet performans hedefi (SPT) : Emniyet hedefiyle uygun olarak herhangi bir emniyet performansı göstergesine yönelik belirli bir süre için planlanan veya amaçlanan hedefi,

ı) Emniyet riski : Herhangi bir tehlikenin sonuçlarının olasılık ve şiddet olarak tahmin edilmesini,

i) Emniyet verisi : Havacılıkla ilgili çeşitli kaynaklardan toplanan, emniyeti muhafaza etmek veya iyileştirmek üzere kullanılan, tanımlanmış gerçekler veya emniyet değerleri dizisini,

j) Emniyet Yöneticisi: İşletmenin insan faktörleri ve organizasyonel yapısı yönünden emniyetin sağlanması amacıyla oluşturulacak olan emniyet yönetim sisteminin etkili bir şekilde yürütülmesi ve geliştirilmesinden sorumlu kişiyi,

k) Emniyet Yönetim Sistemi (SMS) : Gerekli organizasyon yapıları, yükümlülük, sorumluluk, politika ve prosedürler de dahil olmak üzere, emniyetin yönetilmesine yönelik sistematik bir yaklaşımı,

l) FDM : Uçuş Veri İzlemeyi,

m) Form 4: Genel Müdürlüğümüzün internet sayfasında yer alan Yönetici Personel Onay Formunu,

n) GAP analizi : Tamamen işleyen ve etkili bir SMS'in uygulanması için ihtiyaç duyulan tedbirleri tanımlayan bir SMS uygulama planı vasıtasıyla ele alınması gereken uyumluluk veya farklılıkların analizini,

o) Genel Müdür : Sivil Havacılık Genel Müdürünü,

ö) Genel Müdürlük : Sivil Havacılık Genel Müdürlüğünü,

p) ICAO : Uluslararası Sivil Havacılık Örgütünü,

r) İşletme: 14/10/1983 tarih ve 2920 sayılı Türk Sivil Havacılık Kanununa ve 15/07/2018 tarih ve 30479 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren 4 numaralı Bakanlıklara Bağlı, İlgili, İlişkili Kurum ve Kuruluşlar ile Diğer Kurum ve Kuruluşların Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesine göre yetkilendirilen; hava seyrüsefer hizmet sağlayıcıları, havaalanı işletmecileri, terminal işletmecileri, hava taşıyıcılarına en az yolcu trafik (yolcu hizmetleri), yük kontrol ve haberleşme ile ramp hizmeti veren yer hizmetleri kuruluşları, ikram üretim ve servis hizmeti veren yer hizmetleri kuruluşları, hava araçlarına hizmet veren akaryakıt kuruluşları, ticari hava taşıma işletmeleri, ticari özel operasyonları (B2) yetkisine sahip genel havacılık işletmeleri, tip intibak eğitim organizasyonları, uçuş eğitim organizasyonları, onaylı bakım kuruluşları, F bakım kuruluşları, hava aracı bakım eğitimi kuruluşları, onaylı havacılık tıp merkezleri ve tasarım ve üretim kuruluşları

s) Kalitatif : Nitelik; bir şeyin nasıl olduğunu, özelliğini, değerlendirmeye dayalı ölçümünü;

ş) Kantitatif : Nicelik; bir şeyin sayılabilen, artıp azalabilen ölçümünü,

t) LOSA : Hat Operasyon Emniyet Denetimini,

u) Proaktif yaklaşım: Tehlikenin herhangi bir kazaya veya olaya sebebiyet verip vermeyeceğini tespit etmek üzere, düşük sonuçlu olaylara veya süreç performansına ilişkin emniyet verilerinin toplanması ve emniyet bilgilerinin veya olay sıklığının analiz edilmesi yaklaşımını,

ü) Reaktif yaklaşım : Geçmişteki olayların ve sonuçların analizini içeren, emniyet olaylarının soruşturulmasıyla tehlikenin tanımlanması yaklaşımını,

v) Risk : İnsanların, donanımın ya da yapıların zarar görmesi, kaynakların kaybedilmesine neden olma ya da daha önceden tanımlanmış bir işlevin yerine getirilmesini engelleme ihtimalinin olasılık ve etkinin derecesi olarak ölçülmesini

y) SHY-13 Yönetmeliği: Sivil Hava-Araç Kazaları Soruşturma Yönetmeliğini,

z) Sorumlu Müdür : İşletmede SMS'in etkin ve verimli performansından sorumlu olarak

belirlenen tek kişiyi,

aa) Tehlike : Herhangi bir hava aracı olayına veya kazasına sebebiyet verme ya da tetikleyici olma potansiyeline sahip olan herhangi bir durum veya nesneyi,

ab) Tetikleyici : Belirli bir emniyet performansı göstergesine ilişkin herhangi bir değerlendirme, düzeltme veya iyileştirici faaliyet gibi gerekli görülen eylemin başlatılmasına hizmet eden belirlenmiş seviye veya kriter değerini ifade eder.

İKİNCİ BÖLÜM
Genel Hususlar, Uygulama esasları, Son hükümler

Emniyet Yönetim Sistemi (SMS)

MADDE 5 -(1) İşletme, yayımlamış olduğu emniyet politikası doğrultusunda ve bu Talimat kapsamında SMS oluşturmaktan sorumludur.

(2) Birden fazla havaalanında faaliyet gösteren işletmeciler, tüm havaalanlarındaki faaliyetlerini içerecek şekilde yalnızca bir SMS kurmalıdır.

(3) SMS, işletmelere faaliyetlerini, emniyet performanslarını ve kaynaklarını etkin bir şekilde yönetme imkanı sağlarken, havacılık emniyetine sağladıkları katkıya dair daha iyi bir anlayış kazandırır.

(4) Tehlikelerin tanımlanması, emniyet verilerinin ve emniyet bilgilerinin toplanması ve de analiz edilmesi ile emniyet risklerinin sürekli olarak değerlendirilmesi vasıtasıyla emniyet performansının sürekli olarak iyileştirilmesi sağlanır.

(5) SMS'in amacı, işletmelere emniyetin yönetilmesine yönelik sistematik bir yaklaşımın sağlanmasıdır.

(6) SMS, havacılık olay ve kazaları meydana gelmeden emniyet risklerini proaktif bir şekilde azaltmayı amaçlar.

SMS çerçevesi

MADDE 6 -(1) SMS çerçevesinin tüm unsurları, işletmenin boyutu ve karmaşıklığına bakılmaksızın uygulanmalıdır.

(2) Emniyet Yönetim Sistemi çerçevesi 4 bileşen ve 12 unsurdan oluşur.

a) Emniyet politikası ve hedefleri

1) Yönetim taahhüdü

2) Emniyet yükümlülük ve sorumlulukları

3) Kilit emniyet personelinin atanması

4) Acil durum eylem planı kordinasyonu

5) SMS dökümantasyonu

b) Emniyet risk yönetimi

1) Tehlike tanımlama

2) Emniyet risk değerlendirme ve azaltma

c) Emniyet güvencesi

1) Emniyet performansının izlemesi ve ölçümü

2) Değişikliğin yönetimi

3) SMS'in sürekli iyileştirilmesi

ç) Emniyet teşviki

1) Eğitim ve öğretim

2) Emniyet iletişimi

Emniyet politikası ve hedefleri

MADDE 7 -(1) Emniyet politikası ve hedefleri, emniyet yönetiminin etkin olabileceği bir ortamın oluşmasını sağlar. Bu kapsamda üst yönetimin emniyete yönelik taahhüdü, amaçları ve destekleyici organizasyon yapısı ortaya konulur.

(2) SMS'in uygulanması bakımından, yönetimin taahhüdü ve emniyet liderliği kilit öneme sahiptir. Yönetim kararları ve yapılan kaynak tahsisatıyla emniyete yönelik yönetimin taahhüdü kanıtlanmalı ve bu kararlar daima emniyet politika ve hedefleriyle tutarlı olmalıdır.

(3) Emniyet politikası üst yönetim tarafından geliştirilmeli ve onaylanmalı ve sorumlu müdür tarafından imzalanmalıdır. Emniyet politikası ve hedeflerinin geliştirilmesinde kilit emniyet personeline ve mümkünse personeli temsil eden organlara (çalışan forumları, işçi sendikaları) danışılarak ortak sorumluluk hissinin teşvik edilmesi sağlanmalıdır.

Yönetim taahhüdü

MADDE 8 -(1) Emniyet politikası üst yönetim ve sorumlu müdür tarafından görülür bir şekilde onaylanmalıdır. Görülür onaydan kasıt, yönetimin emniyet politikasına verdiği aktif desteğin işletmenin geri kalanı tarafından görülebilmesini sağlayacak şekilde işletme içerisinde duyurulmasıdır. Bu herhangi bir iletişim yöntemi ile veya faaliyetlerin emniyet politikasıyla uygun hale getirilmesi ile sağlanabilir.

(2) Tüm personelin emniyet politikasını anlaması ve politikaya uygun olarak çalışmasını sağlamak amacıyla emniyet politikasının uygulanması, yönetimin sorumluluğundadır.

(3) İşletmenin emniyete yönelik taahhüdünü yansıtmak üzere, emniyet politikasında şunlara yer verilmelidir:

a) Emniyet performansı seviyesinin sürekli olarak iyileştirilmesi,

b) İşletme içerisinde pozitif emniyet kültürünün teşvik edilmesi ve sürdürülmesi,

c) Geçerli tüm düzenleyici gerekliliklere uyumun sağlanması,

ç) Emniyetli bir ürün ve hizmet sunulması için gerekli kaynakların sağlanması,

d) Emniyetin tüm yöneticilerin birincil sorumluluğu olmasının sağlanması,

e) Emniyetin her seviyede anlaşılmasının, uygulanmasının ve sürdürülmesinin sağlanması.

(4) Emniyet politikası, emniyet sorunlarının rapor edilmesini teşvik etmek için emniyet raporlama sistemine atıfta bulunmalı ve bildirilen emniyet olayları veya emniyet sorunları durumunda uygulanan disiplin politikası hakkında personeli bilgilendirmelidir.

(5) Disiplin politikası, herhangi bir hata veya kural ihlalinin gerçekleşip gerçekleşmediğini tespit ederek işletme tarafından disiplin uygulamasının gerekli olup olmadığının belirlenmesi için kullanılır. Adil muamelede bulunmak için kararı verecek olan sorumlu personelin, söz konusu olayı tümüyle değerlendirecek gerekli teknik uzmanlığa sahip olması gerekmektedir.

(6) Emniyet verilerinin ve emniyet bilgilerinin yanı sıra raporlamada bulunanların korunmasına yönelik bir politika, raporlama kültürü üzerinde pozitif bir etkiye sahip olabilir. İşletme, personeli ve spesifik hizmet sağlayıcıyı belirtmek zorunda kalmadan anlamlı emniyet analizlerinin gerçekleştirilmesi için raporların kimlik bilgisinden arındırılmasını ve toplanmasını sağlamalıdır. Raporların uygun bir şekilde kimlik bilgisinden arındırılmasına imkan veren bir politika, toplanan verilerin niteliğini artırabilir. SMS'in işlem ve süreçleri dışında kalan büyük çaplı olaylarda, işletme tarafından raporların önceden kimlik bilgisinden arındırılmasına izin verilmemelidir.

Emniyet hedefleri

MADDE 9 -(1) İşletme emniyet politikasını göz önünde bulundurarak, hangi emniyet sonuçlarına ulaşmayı amaçladığına yönelik emniyet hedeflerini belirlemelidir. Emniyet hedeflerinin, işletmenin emniyet önceliklerine ilişkin kısa ve üst seviye beyanlar olması ve en önemli emniyet risklerine işaret etmeleri gerekir. Emniyet hedefleri, emniyet politikasına dahil edilebilir veya ayrı bir bölümde yer alabilir. Emniyet hedeflerinin başarısının izlenmesi için emniyet performans göstergeleri ve emniyet performans hedeflerine ihtiyaç duyulur.

(2) Emniyet politikası ve emniyet hedeflerinin güncelliğinin sağlanması için periyodik olarak

gözden geçirilmesi gerekir.

Emniyet yükümlülük ve sorumlulukları

MADDE 10 -(1) Sorumlu müdür, söz konusu işletmenin emniyetli operasyonu üzerinde nihai yetkiye sahip kişidir. Sorumlu müdür, emniyeti işletmenin esas değeri olarak aşılayan emniyet politikası ve emniyet hedeflerini belirlemeli ve teşvik etmelidir. Sorumlu müdürün, işletme adına karar alma yetkisine ve mali ve insan kaynaklarının kontrolüne sahip olması gerekir. Ayrıca emniyet konuları ve emniyet risklerine ilişkin uygun tedbirlerin alınmasının sağlanması ile kaza ve olaylara müdahale edilmesi sorumluluğunu da alması gerekir.

(2) Birden fazla kuruluşa ve birden fazla sertifikaya, yetkilendirmeye ve onaya sahip olan büyük çaplı işletmelerde sorumlu müdür olmaya uygun kişinin belirlenmesi zor olabilir. Seçilen kişinin organizasyonun en üst seviyesinde konumlandırılması ve bu sayede doğru stratejik emniyet kararlarının alınmasının sağlanması önemlidir.

(3) Sorumlu müdürün işletmenin belirli bir seviyede olan bütün emniyet performansının sorumluluğunu üstlenecek ve SMS'in etkin olmasına yönelik işlem yapma yetkisine sahip olacak şekilde tanımlanması gerekmektedir. Yönetimin tüm üyelerinin belirli emniyet sorumlulukları tanımlanmalı ve üyelerin SMS'e ilişkin rollerinin pozitif emniyet kültürüne nasıl katkı yapacağı belirtilmelidir. Yönetimin tüm üyelerinin emniyet sorumlulukları, yükümlülükleri ve yetkileri işletmenin genelinde belgelenmeli ve işletmeye tebliğ edilmelidir. Yönetimin tüm üyelerinin emniyet sorumlulukları SMS'in etkin ve verimli performansı için gerekli olan insan, teknik, mali ve diğer kaynakların tahsis edilmesini kapsamalıdır.

(4) Tümü aynı tüzel kişilik kapsamında olan birden fazla farklı sertifika, yetkilendirme ve onaya, SMS'in uygulandığı durumda, mümkünse tek bir sorumlu müdür belirlenmelidir. Bu durum mümkün değilse, her bir organizasyonel sertifika, yetkilendirme ve onay kapsamındaki sorumluluklar için münferit bir sorumlu müdür belirlenmeli ve yöneticilerin yükümlülükleri açık şekilde tanımlanmalıdır. Bu kişilerin emniyet yükümlülüklerinin nasıl koordine edileceğinin belirlenmesi önemlidir.

(5) Emniyet yükümlülükleri ve sorumlulukları bakımından sorumlu müdürün görünür olabileceği en etkin yollardan biri, düzenli olarak yapılan yönetim emniyet toplantılarına liderlik etmesidir. Sorumlu müdür işletmenin emniyetinden nihai olarak sorumlu olduğundan, bu toplantılara aktif olarak katılması, ona şunları yapmasına olanak tanır:

a) Emniyet hedeflerinin gözden geçirilmesi,

b) Emniyet performansının ve emniyet hedeflerine ulaşılmasının izlenmesi,

c) Zamanında emniyet kararlarının alınması,

ç) Uygun kaynakların tahsis edilmesi,

d) Yöneticilerin emniyet sorumlulukları, performansı ve uygulama zamanlaması bakımından yükümlü tutulması ve,

e) Tüm personel tarafından emniyetle ilgili ve emniyetten sorumlu üst düzey yönetici olarak görülmesine.

(6) Sorumlu müdür işletmenin günlük faaliyetlerine ve işyerinde karşılaşılan sorunlara genellikle dahil olmaz. Sorumlu müdür SMS'i yönetmek ve sürdürmek için uygun bir organizasyonel yapının olmasını sağlamalıdır. Emniyet yönetim sorumluluğu genellikle üst yönetim ekibine ve diğer kilit emniyet personeline delege edilir. SMS'in günlük işletilmesine ilişkin olarak sorumlu müdür sorumluluğu delege edilebilmesine karşın, sisteme ilişkin yükümlülük ve emniyet risklerine ilişkin kararlar delege edilemez. Örneğin; aşağıdaki emniyet yükümlülükleri delege edilemez:

a) Emniyet politikalarının uygun olduğundan ve iletildiğinden emin olunması,

b) Kaynakların (finansman, personel, eğitim, tedarik) gerekli şekilde tahsis edilmesinin sağlanması,

c) Kabul edilebilir emniyet riski seviyelerinin belirlenmesi ve gerekli kontrollere kaynak

sağlanması.

(7) Sorumlu müdürün aşağıdaki yükümlülüklere sahip olması gerekmektedir:

a) SMS'in etkin bir şekilde uygulanması için yeterli mali ve insan kaynağının sağlanması,

b) Pozitif emniyet kültürünün teşvik edilmesi,

c) Emniyet politikasının belirlenmesi ve teşvik edilmesi,

ç) İşletmenin emniyet hedeflerinin belirlenmesi,

d) SMS'in gereği gibi uygulanması ve gerekliliklere uygun şekilde sürdürülmesinin sağlanması,

e) SMS'in sürekli iyileştirilmesinin sağlanması.

(8) Sorumlu müdürün yetkileri, bunlarla sınırlı kalmamakla birlikte, aşağıdakilere ilişkin nihai yetkiyi içerir:

a) Tüm emniyet konularının çözüme kavuşturulması ve

b) Söz konusu operasyonu veya faaliyeti durdurma yetkisi de dahil olmak üzere, işletmenin sertifikası, yetkilendirmesi ve onayı kapsamındaki tüm işlemler.

(9) Emniyet riskinin tolere edilebilirliğine ilişkin karar alma yetkisi tanımlanmalıdır. Risklerin kabul edilebilirliğine ilişkin kararların kimin tarafından alınacağı ve herhangi bir değişikliğin uygulanmasının kabulü bunun içerisinde yer almalıdır. Söz konusu yetki herhangi bir kişiye, yönetim pozisyonuna veya komiteye verilebilir.

(10) Emniyet riski tolere edilebilirliğine ilişkin karar alma yetkisinin, yöneticinin genel karar alma ve kaynak tahsisi yetkisiyle örtüşmesi gerekmektedir. Daha düşük seviyede bir yönetici (veya yönetim grubu), belirli bir seviyeye kadar olan tolere edilebilirlik kararlarını almak üzere yetkilendirilebilir. Söz konusu yöneticinin yetkisini aşan risk seviyeleri, değerlendirilmek üzere daha fazla yetkiye sahip olan bir üst yönetime intikal ettirilmelidir.

(11) Emniyetli ürün ve operasyonların sunulmasını destekleyen emniyet ile ilgili görevlere dahil olan tüm personelin ve yönetimin yükümlülük ve sorumlulukları açık bir şekilde tanımlanmalıdır. Emniyet sorumlulukları, çalışanın işletmedeki emniyet performansına (organizasyonel emniyet sonuçları) yönelik katkısına odaklanmalıdır. Emniyetin yönetimi ana bir işlev olduğundan, her bir üst düzey yöneticinin SMS'in işletilmesine belirli bir derece katkı sağlaması gerekmektedir.

(12) İşletme içerisinde tanımlanan bütün yükümlülük, sorumluluk ve yetkiler, SMS dökümantasyonunda belirtilmeli ve işletme geneline bildirilmelidir. Her bir üst düzey yöneticinin, emniyet yükümlülük ve sorumlulukları kendi görev tanımının ayrılmaz bir parçasıdır. Birim yöneticileri ve emniyet yöneticisi arasındaki farklı emniyet yönetimi işlevleri de bu kapsamda yer almalıdır.

(13) İşletme genelindeki emniyet yükümlülüklerine ilişkin sınırlar ile bunların nasıl tanımlanacağı, söz konusu işletmenin türüne ve karmaşıklığına ve de tercih edilen iletişim yöntemlerine bağlı olacaktır. Emniyet yükümlülük ve sorumlulukları, mümkün olduğunca organizasyon şemalarında ve departman sorumluluklarının, personel iş veya görev tanımlarının yer aldığı dökümanlarda bulunmalıdır.

(14) İşletme tarafından, çalışanların emniyet sorumlulukları ile iş tanımındaki sorumlulukları arasındaki çıkar çatışmasının önlenmesi amaçlanmalıdır. SMS yükümlük ve sorumlulukları, çakışmaları ve/veya boşlukları en aza indirecek şekilde tahsis edilmelidir.

(15) İşletme, bir SMS arayüzünün bulunduğu harici kuruluşların emniyet performansından sorumludur. Harici kuruluşlarda Emniyet Yönetim Sistemi gerekli olmasa bile, bu kuruluşlar tarafından sunulan ürün ve hizmetlerin emniyet performansından işletme sorumlu tutulabilir. Emniyetli ürün ve hizmetin sunulmasına katkısı olduğu için, işletmenin SMS'inin dış kuruluşun emniyet yönetimi ile arayüzünün olması gerekmektedir.

(16) Görevlendirilecek sorumlu müdür, işletmenin Genel Müdürü/CEO'su, Yönetim Kurulu Başkanı, ortağı ya da mal sahibinden biri olabilir. Farklı bir unvanda bulunan personelin sorumlu

müdür olarak atanmasının istenilmesi durumunda, sorumlu müdür olarak atanması istenen personelin, Genel Müdürlük tarafından gerekli kılınan standartları ve işletme tarafından tanımlanan ilave şartları yerine getirmek üzere finanse edebilecek ve yürütebilecek, ayrıca sorumlu olduğu işletmenin insan kaynakları, mali konuları, işletmenin faaliyetleri ve emniyet ile ilgili tüm konularda nihai yetkiye sahip olduğunu belirten bir Yönetim Kurulu Kararı alınması gerekir.

(17) İşletmenin sahip olduğu, sertifika, yetki veya onay kapsamındaki iş ve işlemlerin emniyetinden sörumlu, Sorumlu Müdürün eğitim ve tecrübe gereklilikleri, Genel Müdürlük tarafından belirlenir.

(18) Sorumlu Müdür Genel Müdürlük tarafından Form-4 belgesinin onaylanmasını müteakip yetkilendirilir.

Kilit emniyet personelinin atanması

MADDE 11 -(1) SMS'i etkin bir şekilde uygulamak ve işletmek için yetkin bir kişinin ve kişilerin emniyet yöneticisi olarak atanması gerekmektedir. Emniyet yöneticisi genel bir terim olup kişiden çok görev için kullanılır ve farklı unvanlarla belirlenebilir. Emniyet yöneticisi görevini yürüten kişi, SMS'in uygulanması ve işletmedeki diğer birimlere emniyet hizmetlerinin sunulması konusunda sorumlu müdüre karşı sorumludur.

(2) Emniyet yöneticisi, etkin bir emniyet yönetim sisteminin geliştirilmesi ve sürdürülmesinden sorumludur ve sistemin odak noktası olarak görev yapar. Emniyet yöneticisi ayrıca, emniyet yönetimi ile ilgili konularda sorumlu müdür ve yöneticilere tavsiyelerde bulunur. Emniyet yöneticisi, emniyet ile ilgili konuların paydaşlarla koordinasyonundan ve iletişiminden sorumludur. Emniyet yöneticisinin görevleri bunlarla sınırlı kalmamak üzere aşağıdakileri içerir:

a) Sorumlu müdür adına SMS uygulama planının yönetilmesi (ilk uygulamaya müteakiben),

b) Tehlikelerin belirlenmesi ve operasyonel emniyet risk analizlerinin yapılması veya yaptırılması,

c) Düzeltici faaliyetlerin izlenmesi ve sonuçlarının değerlendirilmesi,

ç) İşletmenin emniyet performansına yönelik periyodik raporların sunulması,

d) SMS dökümantasyonu ve kayıtlarının muhafaza edilmesi,

e) Personele emniyet eğitiminin planlanması ve eğitimine olanak sağlanması,

f) Emniyet ile ilgili konularda bağımsız tavsiyelerde bulunulması,

g) Havacılık sektöründeki emniyet konularını gözlemleyerek, bu konuların işletmenin operasyonları üzerindeki etkilerinin takibinin yapılması,

ğ) Emniyet konularında Genel Müdürlük ve gerektiğinde diğer devlet kurumlarıyla koordinasyonun ve iletişimin sağlanması.

(3) İlgili ulusal mevzuat hükümleri saklı kalmak kaydıyla emniyet yöneticisi olarak bir kişi atanır. Organizasyonun boyutuna, yapısına ve karmaşıklığına bağlı olarak, emniyet yöneticisi rolü özel bir görev olabilir veya diğer görevlerle birleştirilebilir. Ayrıca, bazı işletmelerin bu görev için bir grup tahsis etmesi gerekli olabilir. Bu görevlendirmelerin herhangi bir çıkar çatışması oluşturmayacağından emin olunmalıdır. Mümkün olduğunca, emniyet yöneticisi ürün ve hizmetlerin sunumuna doğrudan dahil olmamalı, ancak bunların nasıl yapıldığı bilgisine sahip olmalıdır. Atama yapılırken diğer görev ve işlevler arasındaki olası çıkar çatışmaları da göz önünde bulundurulmalıdır. Bu çıkar çatışmaları aşağıdakileri içerebilir:

a) Finansman rekabeti (örneğin finans yöneticisinin emniyet yöneticisi olması),

b) Kaynaklara ilişkin çatışan öncelikler,

c) Emniyet yöneticisinin operasyonel role sahip olduğu durumlarda, dahil olduğu operasyonel faaliyetlerin SMS etkinliğini değerlendireceği durumlar,

(4) Emniyet görevinin bir gruba tahsis edildiği durumlarda (örneğin işletme tarafından SMS faaliyeti birden fazla alana genişletildiğinde), sorumlu müdüre doğrudan ve açık bir raporlama işleminin sürdürülebilmesi için bir kişinin "baş" emniyet yöneticisi olarak görevlendirilmesi gerekir.

(5) Emniyet yöneticisinin yetkinlikleri bunlarla sınırlı kalmamak üzere aşağıdakileri

içermelidir:

a) Emniyet/kalite yönetimi deneyimi,

b) İşletme tarafından sunulan ürün ve hizmete yönelik deneyim,

c) Operasyonları veya sunulan ürün/hizmeti destekleyen sistemin kavranmasına yönelik teknik alt yapı,

ç) Çevresiyle uyum becerisi,

d) Analitik ve problem çözme becerisi,

e) Proje yönetim becerileri,

f) Sözlü ve yazılı iletişim becerileri,

g) İnsan faktörlerinin kavranması.

(6) İşletmenin boyutu, doğası ve karmaşıklığına bağlı olarak emniyet yöneticisine ilave personel tarafından destek verilebilir. Emniyet yöneticisi ve destek personeli , emniyet verilerinin hızlıca toplanması ve analiz edilmesinden, emniyet riski kararları ve kontrolleri gibi emniyet bilgilerinin işletme bünyesinde uygun şekilde dağıtımının sağlanmasından sorumludur.

(7) İşletme tarafından, işletme genelinde SMS işlevlerini destekleyen uygun emniyet komiteleri tesis edilmeli ve emniyet komitelerinde kimlere yer verilmesinin gerektiği ve toplantıların hangi sıklıkta yapılacağı belirlenmelidir.

(8) Emniyet Gözden Geçirme Kurulu (EGGK) sorumlu müdür ve üst düzey yöneticileri içeren üst düzey bir emniyet kuruludur, emniyet yöneticisi bu kurula danışman olarak katılır. EGGK stratejiktir ve emniyet politikalarına, kaynak tahsisatına ve işletmenin performansına yönelik üst seviye konularla ilgilenir. EGGK tarafından aşağıdaki konular izlenir:

a) SMS'in etkinliği,

b) Gerekli emniyet riski kontrol tedbirlerinin zamanında uygulanma tepkisi,

c) İşletmenin emniyet politikası ve hedefleri karşısındaki emniyet performansı,

ç) Emniyet riski azaltma stratejilerinin genel etkinliği,

d) İşletmenin aşağıdakileri destekleyen emniyet yönetim süreçlerinin etkinliği:

1) Emniyet yönetiminin önceliğinin işletme tarafından ilan edilmesi ve

2) İşletme genelinde emniyetin teşvik edilmesi.

(9) EGGK tarafından stratejik bir yönlendirme oluşturulması sonrasında, emniyet stratejilerinin uygulamalarının işletme genelinde koordine edilmesi gerekir. Daha çok operasyonel olarak odaklanmış olan Emniyet Eylem Gruplarının (EEG) oluşturulmasıyla bu koordinasyon sağlanabilir. EEG, yöneticilerden ve ön saftaki personellerden oluşur ve bu gruplara atanan bir yönetici başkanlık eder. EEG, EGGK tarafından geliştirilen stratejilere uygun olarak spesifik uygulama sorunlarıyla ilgilenen kurullardır. Emniyet Eylem Grubu:

a) İşletmenin kendi görev alanları dahilindeki operasyonel emniyet performansını izler ve uygun emniyet risk yönetimi faaliyetlerinin yürütülmesini sağlar,

b) Mevcut emniyet verilerini gözden geçirir ve uygun emniyet risk kontrolü stratejilerinin uygulanmasını belirler ve çalışanların geri bildirim yapmasını sağlar,

c) Operasyonel değişikliklerin veya yeni teknolojilerin uygulamaya koyulmasına ilişkin emniyet etkisini değerlendirir,

ç) Emniyet riski kontrollerine ilişkin tedbirlerin uygulanmasını koordine eder ve söz konusu tedbirlerin hızlı bir şekilde alınmasını sağlar,

d) Spesifik emniyet riski kontrollerinin etkinliğini gözden geçirir.

e) Düzeltici faaliyetlerin zamanında yerine getirilmesini sağlamak,

(10) Emniyet Yöneticilerinin eğitim ve tecrübe gereklilikleri, Genel Müdürlük tarafından belirlenir.

(11) Emniyet Yöneticileri ve Baş Emniyet Yöneticileri Genel Müdürlük Tarafından yayımlanan ilgili mevzuata göre Form-4 belgesinin onaylanmasını müteakip yetkilendirilir.

Acil Durum Eylem Planı Koordinasyonu

MADDE 12 -(1) Acil durum tanım gereği derhal eylem gerektiren, ani, planlanmamış bir durum veya olaydır. Acil Durum Eylem Planı'nın (ADEP) koordinasyonu, işletmenin operasyonunu, bir acil durum sırasında sınırlı bir zaman dilimi içerisinde gerçekleşen faaliyetlere yönelik planlama anlamına gelmektedir. ADEP, havacılık ile ilgili acil durum, kriz ve olayların ele alındığı Emniyet Risk Yönetimi sürecinin ayrılmaz bir parçasıdır. İşletmenin havacılık ile ilgili operasyonlarının veya faaliyetlerinin, kamu sağlığı acil durumu/pandemi gibi acil durumlar sebebiyle tehlikeye düşmesi olasılığına yönelik senaryoların da mümkünse ADEP içerisinde ele alınması gerekmektedir. ADEP, SMS yoluyla tanımlanan öngörülebilir acil durumları ele almalı ve havacılıkla ilgili acil durumları etkin bir şekilde yönetmek için hafifletici eylemleri, süreçleri ve kontrolleri içermelidir.

(2) ADEP'in amacı, operasyonların emniyetli bir şekilde devam etmesi ve mümkün olan en kısa süre içerisinde normal operasyonlara geri dönülmesinin sağlanmasıdır. Bu sayede acil durum sorumluluklarının tayini ve yetki devri de dahil olmak üzere, normalden acil durum operasyonlarına düzenli ve etkin bir geçiş sağlanmalıdır. Acil durum sonrasında "normal" operasyonların yeniden tesis edilmesi için gereken süre de buna dahildir. ADEP'te sorumlu personel tarafından herhangi bir acil durum sırasında alınması gereken tedbirler belirlenir. Çoğu acil durum, havacılık dışı ilgili acil durum hizmetleri gibi ve diğer hizmet sağlayıcıları gibi farklı işletmeler arasında koordineli eylem gerektirebilir. ADEP'in, uygun kilit personelin yanı sıra koordinasyon yapılan harici işletmeler tarafından da kolaylıkla erişebilir olması gerekmektedir.

(3) ADEP koordinasyonun test edilebilmesi için periyodik olarak ADEP tatbikatı yapılması gerekmektedir.

SMS Dökümantasyonu

MADDE 13 -(1) SMS dokümantasyonu, işletmenin SMS politikalarını, süreçlerini ve işletmenin iç yönetimini, SMS'in iletişimini ve bakımını kolaylaştırmak için prosedürlerini açıklayan üst seviye bir SMS el kitabı yer almalıdır.SMS el kitabı, personelin kuruluşun SMS'sinin nasıl işlediğini ve emniyet politikası ve hedeflerine nasıl ulaşılacağını anlamasına yardımcı olmalıdır. Belgeler, SMS'nin sınırlarını anlatan bir sistem açıklamasını içermelidir. Ayrıca çeşitli politikalar, süreçler, prosedürler ve uygulamalar arasındaki ilişkiyi netleştirmeye yardımcı olmalı ve bunların işletmenin emniyet politikası ve hedefleriyle nasıl bağlantılı olduğunu tanımlamalıdır. Dokümantasyon, işletmede çalışan personel tarafından kolayca anlaşılabilecek günlük emniyet yönetimi faaliyetlerini ele alacak şekilde uyarlanmalı ve yazılmalıdır.

(2) SMS el kitabı, işletici ve Genel Müdürlük başta olmak üzere kilit emniyet paydaşları arasında birincil emniyet iletişim aracı işlevini görür. SMS el kitabı ayrı bir döküman olarak hazırlanacağı gibi işletme el kitabının bir parçası olarak da hazırlanabilir. El kitabı güncel tutulmalı ve değişiklik yapılan el kitabı Genel Müdürlük onayına sunulmalıdır. SMS süreçlerine ilişkin detayların ayrı prosedür olarak hazırlanması durumunda, SMS el kitabına çapraz referans verilmesi yeterlidir.

(3) SMS el kitabı, işletmenin aşağıdakilerini içeren politikaları, süreçleri ve prosedürlerinin ayrıntılı bir tanımını içermelidir:

a) Emniyet politikası ve emniyet hedefleri,

b) Geçerli mevzuata dayalı SMS gerekliliklerine atıf,

c) Sistemin tanımı,

ç) Emniyet yükümlülükleri ve kilit emniyet personeli,

d) Gönüllü ve zorunlu emniyet raporlaması sistemi süreçleri ve prosedürleri,

e) Tehlike tanımlama ve emniyet risk değerlendirme süreçleri ve prosedürleri,

f) Emniyet soruşturma prosedürleri,

g) Emniyet performans göstergelerinin belirlenmesi ve izlenmesine yönelik prosedürler,

ğ) SMS eğitim süreçleri, prosedürleri ve iletişimi,

h) Emniyet iletişimi süreçleri ve prosedürleri,

ı) İç denetim prosedürleri,

i) Değişiklik yönetimi prosedürleri,

j) SMS dökümantasyon yönetimi ve prosedürleri,

k) Uygulanabildiği hallerde, acil durum eylem planı koordinasyonu.

(4) SMS dökümantasyonu, SMS'in varlığını ve devam eden işleyişini doğrulayan, operasyonel kayıtların, tutulmasını ve muhafaza edilmesini de kapsar. Operasyonel kayıtlar, emniyet risk yönetimi ve emniyet güvencesi gibi SMS süreçlerinin ve prosedürlerinin çıktılarıdır. SMS operasyonel kayıtlarının belirlenen saklama sürelerine uygun olarak saklanması ve muhafaza edilmesi gerekir. SMS operasyonel kayıtları şunları içermelidir.

a) Tehlike kayıt tablosu ve tehlike/emniyet raporlarını,

b) Emniyet performans göstergeleri ve ilgili çizelgelerini,

c) Tamamlanan emniyet risk değerlendirmelerine ilişkin kayıtlarını,

ç) SMS iç gözden geçirme ve iç denetim kayıtlarını,

d) İç denetim kayıtlarını,

e) SMS/emniyet eğitim kayıtlarını,

f) SMS/emniyet komitesi toplantı tutanaklarını,

g) SMS uygulama planını (ilk kurulum sırasında) ve;

ğ) Uygulama planının desteklenmesine yönelik GAP analizini.

Emniyet Risk Yönetimi

MADDE 14 -(1) İşletme emniyet risklerinin yönetildiğinden emin olmalıdır. Emniyet risk yönetimi; tehlike tanımlama, emniyet risk değerlendirme ve emniyet risk azaltma süreçlerini içerir.

(2) Emniyet risk yönetimi sistematik olarak işletmenin ürün ve hizmetlerinin sunumunda ortaya çıkan tehlikeleri tanımlar. Tasarım, teknik işlev, insan arayüzü veya diğer süreç ve sistemlerin etkileşimlerinin yetersiz olduğu durumlarda tehlikeler ortaya çıkabilir. İşletme çalışma ortamındaki değişikliklere uyum sağlamaya çalışırken, mevcut süreç ve sistemlerin aksaklığından da tehlikeler ortaya çıkabilir. Bu etkenlerin dikkatli bir şekilde analiz edilmesi, operasyon veya faaliyet yaşam döngüsünün herhangi bir noktasındaki potansiyel tehlikeleri belirleyebilir.

(3) Sistemi ve çalışma ortamını anlamak, yüksek emniyet performansının elde edilmesi için gereklidir. Sistemi ve sistem arayüzlerinin detaylı bir şekilde tanımlanması da önemlidir. Tehlikeler, iç ve dış kaynaklardan operasyonel yaşam döngüsü boyunca tanımlanabilir. Emniyet riski değerlendirmenin ve emniyet riski azaltımlarının etkin olduğundan emin olmak için sürekli olarak gözden geçirilmesi gerekmektedir.

Tehlike Tanımlama

MADDE 15 -(1) Tehlike tanımlama, emniyet risk yönetimi sürecinde birinci adımdır. İşletme tüm operasyon ve faaliyet alanlarında, havacılık emniyetine etki edebilecek olan tehlikelerin tanımlanmasına yönelik resmi bir süreç geliştirmeli ve sürdürmelidir. Ekipman, sistem ve tesisler buna dahildir. Harici organizasyonlar ile SMS arayüz bağlantıları sonucunda oluşabilecek tehlikelerin de göz önünde bulundurulması gerekmektedir.

(2) Tehlike tanımlaması için işletme içinde veya dışında çeşitli kaynaklar vardır. Tehlike tanımlaması için işletme içindeki kaynaklardan bazıları şunları içerir:

a) LOSA gibi günlük operasyon ve faaliyetlerin, gözlemsel teknikler kullanılarak yapıldığı normal operasyon izlemesidir.

b) FDM gibi analiz edilebilen parametreleri kullanarak yapılan otomasyonlu izleme sistemleridir.

c) Operasyonla ilişkili başka bir işletmede çalışanlar da dahil olmak üzere herkesin, tehlikeleri ve diğer emniyet sorunlarını işletmeye rapor etme imkanı sağlayan gönüllü ve zorunlu emniyet raporlama sistemidir.

ç) Görev ve süreçlerin denetiminde tehlike belirlenmesidir. Değişikliğin uygulanmasında ortaya çıkabilecek tehlikeleri tanımlamak için bunların organizasyonel değişiklikler ile koordine edilmesi gerekir.

d) İnteraktif eğitim yoluyla katılımcılardan gelen geri bildirim, yeni tehlikelerin tanımlanmasını kolaylaştırabilir.

e) Dahili emniyet soruşturmasında ve kaza/olaylara ilişkin takip raporlarında tanımlanan tehlikelerdir.

(3) Tehlike tanımlamaya ilişkin işletme dışındaki kaynaklara ilişkin örnekler şunlardır:

a) Benzer uçak tipine, bölgeye veya çalışma ortamına ilişkin havacılık kazası raporlarıdır.

b) Genel Müdürlüğe işletmelerden gelen zorunlu ve gönüllü emniyet raporlarıdır.

c) Genel Müdürlük gözetim denetimleri ve üçüncü taraf denetimleridir.

ç) Ticari birlik ve sektör gruplarının emniyet verilerini paylaştığı bilgi değişimi sistemleridir. Birçok ticaret birliği ve endüstri grubu, tanımlanmış tehlikeleri içerebilecek emniyet verilerini paylaşabilir.

Emniyet Raporlama Sistemi

MADDE 16 -(1) Tehlikeleri tanımlamanın ana kaynaklarından biri, emniyet raporlama sistemi, özellikle gönüllü emniyet raporlama sistemidir. Zorunlu raporlama, normalde meydana gelen olaylar için kullanılırken, gönüllü raporlama tehlikeler, ramak kalalar veya hatalar gibi potansiyel emniyet sorunları için ek bir raporlama kanalı sağlar.

(2) İşletmelerin, çalışanları gördüklerini veya deneyimlediklerini bildirmeye teşvik etmek için uygun korumaları sağlaması önemlidir. Örneğin, işletme, hata bildirimleri veya bazı durumlarda kural ihlali nedeniyle yaptırımdan feragat edebilir. Bildirilen bilgilerin yalnızca emniyetin artırılmasını desteklemek için kullanılacağı açıkça belirtilmelidir. Amaç, etkili bir raporlama kültürünü ve potansiyel emniyet açıklarının proaktif olarak tanımlanmasını teşvik etmektir.

(3) Rapor takibi sürecinin yapılabilmesi adına raporlayan kişinin tanımlayıcı bilgileri, sadece emniyet yöneticisi ve emniyet soruşturmasına katılan sorumlu personel tarafından bilinmeli ve gönüllü emniyet raporlama sistemi gizli olmalıdır. Gizlilik, cezalandırma ve mahcubiyet korkusu olmadan insan hatasına yol açan tehlikelerin belirlenmesinde kolaylık sağlar. Gerekli takip işlemleri yapıldıktan sonra gönüllü emniyet raporları kimlik bilgisinden arındırılabilir ve arşivlenebilir. Kimlik bilgisinden arındırılmış raporlar, risk azaltıcı işlemlerinin etkinliğini izlemek ve ortaya çıkan tehlikeleri tanımlamak üzere gelecekteki trend analizlerini destekleyebilir.

(4) İşletmedeki tüm personel, emniyet raporlama sistemiyle tehlikeleri tanımlamaya ve diğer emniyet sorunlarını raporlamaya teşvik edilmelidir. Emniyet raporlama sistemlerinin etkin olması için tüm personel tarafından kolay ulaşılabilir olması gerekmektedir. Basılı form, web tabanlı veya masaüstü form, duruma göre kullanılabilir. Birden fazla raporlama yönteminin kullanılması, personelin katılım oranını daha üst düzeye çıkartır. Emniyet raporlamasının faydalarından ve nelerin rapor edilmesi gerektiğinden herkes haberdar edilmelidir.

(5) Emniyet raporu sunan herkes, alınan kararlar veya eylemler hakkında geri bildirim almalıdır. Raporlama sistemi gerekliliklerinin, analiz araçlarının ve yöntemlerinin uyumlu hale getirilmesi, emniyet bilgilerinin değişiminin yanı sıra belirli emniyet performansı göstergelerine ilişkin kıyaslamaları kolaylaştırabilir. Gönüllü raporlamada rapor eden kişilere sağlanan geri bildirim aynı zamanda söz konusu raporların ciddiye alındığını göstermektedir. Bu da pozitif emniyet kültürünün desteklenmesine ve gelecekteki raporlamanın teşvik edilmesine yardım eder.

(6) Emniyet raporlamalarının sayısı fazla olduğunda raporların filtrelenmesine ihtiyaç duyulabilir. Bu filtreleme, daha fazla araştırmanın gerekli olup olmadığının ve hangi seviyede araştırmanın gerekli olduğunun tespit edilmesine yönelik olarak başlangıç emniyet risk değerlendirmesini içerebilir.

(7) Emniyet raporları genellikle bir sınıflandırma veya taksonomi sistemi kullanılarak filtrelenir. Sınıflandırma kullanılarak bilgilerin filtrelenmesi yaygın sorunların ve trendlerin

belirlenmesini kolaylaştırabilir. İşletmeler tarafından kendi operasyon türünü veya türlerini kapsayan sınıflandırmalar geliştirilmelidir. Bazı durumlarda tanımlanan tehlike, belirlenen kategorilerden herhangi birine tam olarak uymayabilir. Tehlikelerin kolaylıkla ayrılmasını sağlayacak, analiz için ise değerli olacak bilgileri içerecek genel sınıflandırmalar kullanılmalıdır. ICAO tarafından hazırlanan 9859 numaralı rehber dökümanın 5 inci bölümünde taksonomi ile ilgili bilgiler yer almaktadır.

(8) Tehlike tanımlaması için konusunda uzman kişiler tarafından detaylı analiz senaryolarının yürütüldüğü çalıştay veya toplantılar da gerçekleştirilmelidir. Bunun için deneyimli operasyon ve teknik personellerin sağladığı katkılardan faydalanılmalıdır. Bu tür faaliyetler ve ilişkili emniyet risklerinin değerlendirilmesi için emniyet kurulu toplantıları (EGGK, EEG) kullanılabilir.

(9) Tanımlanan tehlikelerin ve olası sonuçlarının, emniyet risk değerlendirmesi süreçlerinde kullanılması için belgelenmesi gerekmektedir.

(10) Tehlike tanımlama süreci kapsamında işletme dahilinde ve işletme haricinde ve diğer sistemlerle olan arayüz bağlantıları da dahil olmak üzere, havacılık faaliyetleri kapsamında, işletmenin mevcut olabilecek tüm tehlikeleri göz önünde bulundurulmalıdır. Tehlikelerin tanımlanması sonrasında, sonuçları da belirlenmelidir.

Tehlikelerin Soruşturulması

MADDE 17 -(1) Tehlike tanımlama, işletmenin devam eden faaliyetleri kapsamında ve sürekli olmalıdır. Bazı koşullar için daha detaylı soruşturma gerekebilir ve bunlar aşağıdakileri içerebilir;

a) İşletmede, havacılık emniyeti ile ilgili olaylarda veya mevzuata uyumsuzluklarda açıklanamayan bir artışın yaşandığı haller veya

b) İşletmenin organizasyonunda veya faaliyetlerinde önemli değişiklikler.

(2) Etkin emniyet yönetimi, emniyet olaylarının ve emniyet tehlikelerinin analiz edilmesine ve çalışma ortamındaki emniyetin iyileştirilmesine ilişkin tavsiyelerin ve bulguların rapor edilmesine yönelik kaliteli araştırmalara bağlıdır.

(3) SHY-13 kapsamındaki kaza ve olay soruşturmaları ile işletmelerin soruşturmaları arasında ayrım, SHY-13 kapsamındaki kazalara ve ciddi olaylara ilişkin soruşturmadan Devlet'in sorumlu olmasıdır. Bu tür bilgiler, kaza ve olaylardan öğrenilen derslerin yayılması bakımından önemlidir. İşletmenin emniyet soruşturmaları kendi SMS'i kapsamında, tehlike tanımlama ve risk değerlendirme süreçlerini desteklemek üzere kendisi tarafından yürütülür. SHY-13 kapsamı dışında kalan, tehlike tanımlamasına yönelik değerli kaynak olabilecek veya risk kontrollerindeki zayıflıkları belirleyebilecek birçok emniyet olayı söz konusudur. Bu problemler, işletmenin emniyet soruşturmasıyla ortaya çıkarılabilir ve çözüme kavuşturulabilir.

(4) Emniyet soruşturmasının işletmedeki asıl amacı, neyin gerçekleştiğini ve emniyet eksikliklerinin ortadan kaldırılmasını veya hafifletilmesini sağlayarak benzer durumların gelecekte meydana gelmesinin nasıl engelleneceğinin anlaşılmasıdır. Olay dikkatli ve metotlu bir şekilde incelenmeli ve olayın gelecekteki tekrar etme ihtimalinin ve/veya sonucunun azaltılması için dersler çıkarılmalıdır. İşletmenin emniyet soruşturmaları, kendi SMS'inin ayrılmaz bir parçasıdır.

(5) İşletmenin emniyet olayları ve tehlikelere ilişkin araştırmaları, havacılıktaki genel risk yönetimi sürecinin önemli bir faaliyetidir. Bir emniyet soruşturması yapmanın faydaları şunları içerir:

a) Meydana gelen olayların daha iyi anlaşılması,

b) Olayın meydana gelmesine katkıda bulunan insani, teknik ve organizasyonel faktörlerin belirlenmesi,

c) Tehlikelerin tanımlanması ve risk değerlendirmelerinin gerçekleştirilmesi,

ç) Kabul edilemez risklerin azaltılması veya giderilmesi için tavsiyelerde bulunulması ve

d) Havacılıkla ilgili işletmelerin uygun üyeleri ile paylaşılması ve çıkarılacak derslerin belirlenmesi,

(6) İşletmenin emniyet soruşturması, genellikle emniyet raporlaması sistemi vasıtasıyla

sunulan bir bildirim (rapor) ile tetiklenir. EK-2' de emniyet soruşturması kararı süreci ve işletme emniyet soruşturması ile SHY-13 hükümleri kapsamındaki soruşturmanın ne zaman gerçekleştirilmesi gerektiği arasındaki ayrım ortaya konmaktadır.

(7) Tüm olaylar veya tehlikeler soruşturulmayabilir veya soruşturulması gerekli değildir; soruşturma yürütülmesine ve soruşturmanın derinliğine yönelik karar, söz konusu olayın veya tehlikenin gerçekleşmesine veya olası sonuçlarına bağlı olmalıdır. Yüksek risk potansiyeline sahip olduğu değerlendirilen olay ve tehlikelerin soruşturulması daha olasıdır ve bunların düşük risk potansiyeline sahip olanlardan daha derinlemesine soruşturulması gerekmektedir. İşletme tarafından tanımlanmış tetikleme noktalarına sahip olan yapılandırılmış bir karar alma yaklaşımı kullanılmalıdır. Bu sayede emniyet soruşturması kararları, neyin soruşturulması gerektiğini ve soruşturmanın kapsamını yönlendirilecektir. Aşağıdakiler bunu belirlemede yardımcı olacaktır:

a) Sonucun şiddeti veya olası şiddeti,

b) Soruşturmanın yürütülmesine yönelik mevzuata dayalı veya organizasyonel gereklilikler,

c) Elde edilecek emniyet değeri,

ç) Alınacak emniyet tedbirine yönelik imkan,

d) Soruşturma yapılmaması durumunda riskler,

e) Hedeflenen emniyet programlarına katkı,

f) Belirlenen trendler,

g) Eğitim faydası ve

ğ) Kaynak elverişliliği.

(8) Soruşturma başlatılması durumunda ilk işlem, gerekli becerilere ve uzmanlığa sahip olan bir soruşturmacının veya mümkün olması durumunda bir soruşturma ekibinin tayin edilmesi olmalıdır. Söz konusu ekibin boyutu ve üyelerinin uzmanlık profili, soruşturulmakta olan olayın mahiyetine ve önem derecesine bağlıdır. Soruşturma ekibi tarafından diğer uzmanların yardımı gerekli görülebilir. Çoğunlukla iç soruşturmalar operasyon ve emniyet birimi uzmanlarından destek alınarak, tek bir kişi tarafından yürütülür.

(9) İşletmenin emniyet soruşturmacılarının söz konusu olay veya tanımlanan tehlike ile ilişkili alandan organizasyonel bakımdan bağımsız olması daha uygundur. Soruşturmacının bilgi sahibi, eğitimli ve tecrübeli olması; işletmenin emniyet soruşturmalarında daha iyi sonuçlar elde edilmesini sağlar. Soruşturmacının sahip olduğu bilgi, beceri, dürüstlük, tarafsızlık, mantıklı düşünme, faydacılık ve etraflıca düşünme gibi özelliklere göre seçilmesi daha uygundur.

(10) Soruşturmada neyin gerçekleştiği ve neden gerçekleştiği belirlenmelidir. Bunun için soruşturma kapsamında uygulanmak üzere kök neden analizi gerekebilir. Mümkün olan en kısa süre içerisinde söz konusu olaya dahil olan kişiler ile görüşme yapılması en uygunudur. Soruşturma aşağıdakileri içermelidir:

a) Dahil olan kişilerin eylemlerini de içerecek şekilde, önemli olaylara ilişkin zaman çizelgelerinin belirlenmesi,

b) Faaliyetlere ilişkin politikaların ve prosedürlerin gözden geçirilmesi,

c) Olaya ilişkin alınan kararların gözden geçirilmesi,

ç) Olayın meydana gelmesini önlemesi beklenen mevcut risk kontrollerinin belirlenmesi, ve

d) Önceki veya benzer olaylara ilişkin emniyet verilerinin gözden geçirilmesi.

(11) Emniyet soruşturması, suçlama veya cezalandırmaya değil, tanımlanan tehlikelere, emniyet risklerine ve iyileştirme imkanlarına odaklanmalıdır. Soruşturmanın yürütülme şekli ve en önemlisi raporun nasıl yazıldığı; olası emniyet etkisine, organizasyonun gelecekteki emniyet kültürüne ve gelecekteki emniyet girişimlerinin etkinliğine tesir edecektir.

(12) Soruşturma, emniyet eksikliklerini gideren veya azaltan açık bir şekilde tanımlanmış bulgular ve tavsiyeler ile sonuçlanmalıdır.

Emniyet risk değerlendirme ve azaltma

MADDE 18 -(1) İşletme tarafından emniyet risklerinin değerlendirilmesine yönelik tutarlı ve

sistematik yaklaşıma imkan verecek bir model geliştirilmelidir. Bu model hangi emniyet risklerinin kabul edilebilir, hangilerinin kabul edilemez olduğunun belirlenmesine ve tedbirlerin önceliklendirilmesine yardımcı olacak bir yöntem içermelidir.

(2) İşletmenin çalışma ortamına uygunluğunun sağlanması için emniyet risk yönetimi araçlarının periyodik olarak gözden geçirilmesi ve uyarlanması gerekebilir. İşletmenin, Emniyet Yönetimi Sistemi olgunlaştıkça, operasyonunun ihtiyaçlarını daha iyi bir şekilde yansıtan daha sofistike yaklaşımlar bulunabilir. İşletme ile Genel Müdürlük tarafından bir metodoloji kararlaştırılmalıdır.

(3) Emniyet risk sınıflandırmasına yönelik daha sofistike yaklaşımlar mevcuttur. İşletme emniyet yönetimi konusunda deneyimliyse veya yüksek riskli bir ortamda faaliyet gösteriyorsa bu yaklaşımlar daha uygun olabilir.

(4) Emniyet risk değerlendirmesi sürecinde mevcut olan her türlü emniyet verileri ve emniyet bilgileri kullanılmalıdır. Emniyet riskleri değerlendirildikten sonra, işletme hangi emniyet riski kontrollerinin gerekli olduğunu belirlemek için veriye dayalı karar alma sürecine geçmelidir.

(5) Emniyet risk değerlendirmelerinde bazı durumlarda verilerin elverişsizliğine bağlı olarak nicel verilerden ziyade uzman değerlendirmesine dayalı bilgilerin kullanılması gerekebilir. Emniyet risk matrisinin kullanılması, tanımlanan tehlikeye ilişkin emniyet risklerini nicel bir formatta ifade etme imkanı verir. Böylelikle, tanımlanan emniyet riskleri arasında doğrudan büyüklük karşılaştırmasına imkan verilir. Nicel veriler mevcut olmadığında, tanımlanan her bir emniyet riskine "oluşması muhtemel" veya "ihtimal dışı" gibi nitel bir emniyet riski kriteri belirlenebilir.

(6) Spesifik çalışma ortamlarına sahip, birden fazla yerde operasyonları olan işletmeler için, emniyet risk değerlendirme ve emniyet risk kontrolü tanımlamasının gerçekleştirilmesi için lokal emniyet komitelerinin oluşturulması daha etkili olabilir. Genellikle işletmenin bünyesindeki veya dışındaki, operasyon alanındaki bir uzmandan görüş talep edilir. Uygun kaynakların sağlanması için daha üst mercilerden nihai kararlar veya kontrol kabulü istenebilir.

(7) Emniyet risk değerlendirmelerinin önceliklendirilmesi ve emniyet risk kontrollerinin benimsenmesi durumuna işletme tarafından karar verilmelidir. İşletme tarafından aşağıdaki belirtilen önceliklendirme süreci rehber olarak göz önüne alınmalıdır.

a) En yüksek emniyet riskini değerlendiren ve kontrol eden,

b) Kaynakları en yüksek emniyet risklerine tahsis eden,

c) Emniyeti etkin bir şekilde sağlayan veya iyileştiren,

ç) Belirtilen ve kararlaştırılan emniyet hedeflerine ve Emniyet Performans Hedeflerine (SPT) ulaşan ve

d) Emniyet risklerinin kontrolüne ilişkin ulusal ve uluslararası mevzuatlar kapsamındaki gereklilikleri karşılayan.

(8) Emniyet risklerinin değerlendirilmesi sonrasında uygun emniyet risk kontrolleri uygulanabilir. Uygun emniyet risk kontrollerinin belirlenmesine son kullanıcıların ve konu uzmanlarının dahil edilmesi önemlidir. Doğru kişilerin dahil edilmesini sağlamak, seçilen emniyet risk azaltmalarının uygulanabilirliğini en üst düzeye çıkaracaktır. Emniyet risk kontrollerinin uygulanması öncesinde, özellikle yeni tehlikelerin ortaya çıkması olmak üzere, istenmeyen sonuçlara yönelik bir tespitte bulunulmalıdır.

(9) Emniyet risk kontrolünün kararlaştırılması ve uygulanması sonrasında, emniyet performansı izlenerek risk kontrolünün etkinliği güvence altına alınmalıdır. Bu, operasyonel koşullar altında yeni emniyet riski kontrollerinin bütünlüğünü, verimliliğini ve etkinliğini doğrulamak için gereklidir.

(10) Emniyet risk yönetimi çıktıları belgelenmelidir. Bu, tehlikeyi ve her türlü sonucu, emniyet riski değerlendirmesini ve gerçekleştirilen herhangi bir emniyet riski kontrol eylemini içermelidir. Bunların takip edilebilmesi ve izlenebilmesi için bir kayıt olarak tutulmalıdır. Emniyet risk yönetimi dokümantasyonu, emniyet kararları alınırken referans olarak kullanılabilen, işletmenin

emniyet tecrübesi ve emniyet bilgilerinin değişimi için geçmişe yönelik bir kaynak haline gelir. Bu, emniyet tecrübesi, emniyet trendi analizleri ile emniyet eğitim ve iletişimine yönelik materyal sunar. Emniyet riski kontrollerinin ve eylemlerinin uygulanıp uygulanmadığını ve etkili olup olmadığını değerlendirmek, iç denetimler için de yararlıdır.

Emniyet Güvencesi

MADDE 19 -(1) İşletmenin emniyet performansının doğrulanmasına ve emniyet risk kontrollerinin etkinliğinin onaylanmasına yönelik araçların geliştirilmesi ve muhafaza edilmesi, SMS'in emniyet güvencesi bileşeni tarafından sağlanır.

(2) Emniyet güvencesi, SMS'in beklentilere ve gerekliliklere uygun bir şekilde işleyip işlemediğinin tespit edilmesi için gerçekleştirilen süreçlerden ve faaliyetlerden oluşur. Değişikliklerin veya sapmaların meydana getireceği emniyet risklerinin veya mevcut emniyet risk kontrollerinin bozulmasının tespit edilmesi için süreçlerin yanı sıra çalışma ortamının sürekli olarak izlenmesi gerekir. Bu sayede emniyet risk yönetimi süreci vasıtasıyla bu tür değişiklikler veya sapmalar ele alınabilir.

(3) Emniyet güvencesi faaliyetleri, potansiyel bir emniyet etkisi olan, belirlenmiş sorunlar karşısında, alınan tedbirlerin geliştirilmesini ve uygulanmasını içermelidir. Bu tedbirler işletmenin SMS performansını sürekli olarak iyileştirir.

Emniyet Performansının İzlenmesi ve Ölçülmesi

MADDE 20 -(1) Emniyet performansının doğrulanması ve emniyet risk kontrollerinin etkinliğinin onaylanması için, iç denetimlerin bir kombinasyonunun kullanılması ve Emniyet performansı göstergelerinin (SPI) oluşturulması ve izlenmesi gerekir. Emniyet riski kontrollerinin etkinliğinin değerlendirilmesi önemlidir, çünkü bunların uygulanması her zaman amaçlanan sonuçlara ulaşmaz. Bu değerlendirme doğru emniyet riski kontrolünün seçilip seçilmediğinin belirlenmesine yardımcı olur ve farklı bir emniyet riski kontrolü stratejisinin uygulanmasıyla sonuçlanabilir.

(2) İç denetimler SMS'in etkinliğini değerlendirmek ve potansiyel iyileştirme alanlarını belirlemek üzere gerçekleştirilir. Genel Müdürlük tarafından hazırlanan çoğu havacılık emniyeti düzenlemesi, tesis edilmiş olan bir genel emniyet risk kontrolüdür. İç denetim vasıtasıyla söz konusu düzenlemelere uyumun sağlanması, emniyet güvencesinin başlıca unsurudur.

(3) Emniyet riski kontrollerinin etkin bir şekilde uygulanmasını ve izlenmesini sağlamak da gereklidir. Uygunsuzluklar ve diğer sorunlar belirlendiğinde, sebepler ve sebep olan etkenler araştırılmalı ve analiz edilmelidir. İç denetimin ana odak noktası, emniyet riski kontrollerini sağlayan politikalar, süreçler ve prosedürlerdir.

(4) İç denetimler denetlenen birimden bağımsız olan kişi veya departman tarafından gerçekleştirildiğinde daha etkili olur. Bu tür denetimler, sorumlu müdüre ve üst yönetime aşağıdakilerin durumuna yönelik geri bildirim sağlamalıdır:

a) Mevzuatlara uyum,

b) Politika, süreç ve prosedürlere uyum,

c) Emniyet risk kontrollerinin etkinliği,

ç) Düzeltici faaliyetlerin etkinliği ve

d) SMS'in etkinliği.

(5) Bazı işletmeler tarafından iç denetimlerin uygun derecede bağımsızlığı sağlanamayabilir. Bu gibi durumlarda işletme tarafından bağımsız denetçiler veya başka bir işletmenin denetçileri gibi dış denetçilerin görevlendirilmesi değerlendirilmelidir.

(6) İç denetimlerin planlanmasında söz konusu süreçlerin emniyet bakımından kritikliği, önceki denetimlerin ve değerlendirmelerin sonuçları ile uygulanan emniyet risk kontrolleri dikkate alınmalıdır. İç denetimlerde, düzenlemelere, politikalara, süreçlere ve prosedürlere uyumsuzluk belirlenmelidir. İç denetimler aynı zamanda, sistem eksikliklerini, emniyet risk kontrollerinin etkinliğinin eksikliğini ve iyileştirme imkanlarını da belirlemelidir.

(7) Uyum ve etkinliğin değerlendirilmesi, emniyet performansına ulaşılması için çok önemlidir. İç denetim süreci, hem uyumu hem de etkinliği belirlemek için kullanılabilir. Her bir süreç veya prosedürün uygunluğunu ve etkinliğini değerlendirmek için aşağıdaki sorular sorulabilir:

a) Uyumluluğun tespit edilmesi;

1) Öngörülen süreç veya prosedür mevcut mudur?

2) Söz konusu süreç veya prosedür girdiler, faaliyetler, arayüzler ve çıktılar olarak belgelenmiş midir tanımlanmış mıdır?

3) Söz konusu süreç veya prosedür kriterleri veya gereklilikleri 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 çıktılar 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 tutarlı bir şekilde ulaşılıyor mu? ?

3) Söz konusu sürecin veya prosedürün sonuçları, "müşteri" tarafından talep edilen sonuçlar mıdır?

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?

(8) İç denetimlerin daha önceden tespit edilen uyumsuzlukların kapatılma durumunu da izlemesi gerekir. Bunlar, kök neden analizi ve düzeltici ve önleyici eylem planlarının geliştirilmesi ve uygulanması yoluyla ele alınmalıdır.Herhangi bir uyumsuzluğa ilişkin nedenlerin ve katkıda bulunan etkenlerin analizinden elde edilen sonuçların, söz konusu işletmenin emniyet risk yönetimi süreçlerini beslemesi gerekir.

(9) İç denetim sürecinin sonuçları, emniyet riski yönetimi ve emniyet güvencesi işlevlerinin çeşitli girdilerinden biri haline gelir. İç denetimler, işletme yönetiminin organizasyon dahilindeki uyumluluk seviyesi, emniyet riski kontrollerinin etkinlik derecesi ve nerelerde düzeltici veya önleyici faaliyetin gerekli olduğu hakkında bilgi verir.

(10) Mevzuatlara uyum durumuna, SMS'in etkinliğine ve işletmenin kendi organizasyon ve süreçlerini denetlemesi için seçtiği sektörel birliklerin veya diğer üçüncü tarafların etkinliğine ilişkin, Genel Müdürlük ilave geri bildirim sağlayabilir. Bu tür ikinci ve üçüncü taraf denetimlerinin sonuçları, işletmenin SMS'inin iyileştirilmesine yönelik imkan sağlayan ve kendi iç denetim süreçlerinin etkinliğine dair göstergeler sunan emniyet güvencesi girdileridir.

(11) Emniyet performansı izlemesi, bir işletme için mevcut olan çeşitli kaynaklardan emniyet verilerinin ve emniyet bilgilerinin toplanması vasıtasıyla gerçekleştirilir. Bilgiye dayalı karar almayı destekleyen veri kullanımı, SMS' in en önemli unsurlarından biridir. Bu verilerin emniyet performansının izlenmesi ve ölçülmesi için kullanılması, emniyet riskine yönelik karar alma sürecinde gerekli bilgileri üretmek için faydalıdır.

(12) Emniyet performansının izlenmesi ve ölçülmesi bazı temel ilkeler gözetilerek gerçekleştirilmelidir. Ulaşılan emniyet performansı, hem kurumsal davranışın bir göstergesi, hem de SMS'in etkinliğinin bir ölçüsüdür. Bunun için işletme tarafından aşağıdakilerin tanımlanması gerekir:

a) Öncelikle işletmenin operasyonel yapısına özgü, emniyetle ilgili stratejik kazanımlarını veya arzu edilen sonuçlarını yansıtmak üzere tesis edilmesi gereken emniyet hedefleri,

b) Emniyet hedeflerine ilişkin taktik parametreler olan ve dolayısıyla da verilerin toplanmasına yönelik kaynak olan emniyet performans göstergeleri,

c) Emniyet hedeflerine ulaşılmasına yönelik gelişmenin izlenmesi için kullanılan emniyet

performansı hedefleri taktik parametreleri.

(13) Emniyet performansı göstergelerinin geniş bir gösterge yelpazesini kapsaması halinde, işletmenin emniyet performansının daha eksiksiz ve gerçekçi bir resmi elde edilecektir. Burada gösterge olarak aşağıdakiler kapsanmalıdır:

a) Kaza ve ciddi olay gibi düşük olasılıklı/yüksek önem derecesine sahip olan olaylar,

b) Sorunsuz operasyonel olaylar, uygunsuzluk raporları ve sapmalar gibi yüksek olasılıklı/düşük önem derecesine sahip olaylar,

c) Eğitim, sistem iyileştirmeleri ve raporların işlemesi gibi süreç performansları.

(14) Emniyet performansı göstergeleri işletmenin operasyonel emniyet performansını ve SMS performansını ölçmek için kullanılır. Emniyet performansı göstergeleri emniyet raporlama sistemi de dahil olmak üzere, çeşitli kaynaklardan elde edilen verilerin ve bilgilerin izlenmesine dayalıdır. İşletmeye özgü olmaları ve belirlenmiş olan emniyet hedefleri ile bağlantılı olmaları gerekir.

(15) Emniyet performansı göstergeleri belirlerken işletmeler tarafından aşağıdakiler göz önünde bulundurulmalıdır:

a) Doğru şeylerin ölçülmesi: İşletmenin emniyet hedeflerine ulaşmasında doğru yolda olduğunu gösterecek en iyi emniyet performansı göstergeleri belirlenmelidir. Aynı zamanda, işletme tarafından karşılaşılan en büyük emniyet sorunlarının ve emniyet risklerinin neler olduğu dikkate alınmalıdır ve bunların etkin kontrolünü gösterecek olan emniyet performansı göstergeleri belirlenmelidir.

b) Verilerin elverişliliği: İşletme tarafından ölçülmek istenen ile uyumlu olan verilerin ortaya çıkması beklenir. Eğer ortaya çıkmıyorsa, ilave veri toplama kaynaklarının tesis edilmesi gerekli olabilir. Sınırlı miktarda veriye sahip olan küçük işletmeler için, veri setlerinin havuzda toplanması trendlerin belirlenmesine yardımcı olabilir. Bu işlem, birden fazla işletmede emniyet verilerini harmanlayabilen sektörel birlikler tarafından desteklenebilir.

c) Verilerin güvenilirliği: Subjektifliği veya eksik olması sebebiyle veriler güvenilmez olabilir. Bu sebeple veri güvenirliliği göz önünde bulundurulmalıdır.

ç) Ortak sektör emniyet performansı göstergeleri : İşletmeler arasında karşılaştırmalar yapabilmek için benzer işletmelerle ortak emniyet performansı göstergelerinin kararlaştırılması faydalı olabilir. Genel Müdürlük veya sektörel birlikler buna imkan veren düzenlemeler yapabilir.

(16) Emniyet performans göstergeleri belirlendikten sonra, emniyet performans hedeflerinin ve belirlenen alarm seviyelerinin uygun olup olmadığı işletme tarafından değerlendirilmelidir. Emniyet performans hedefleri, emniyet iyileştirmelerinin sağlanmasında faydalıdır ancak iyi uygulanmadığında, işletmenin emniyet performansından ziyade, kişilerin ve birimlerin söz konusu hedefe ulaşılmasına aşırı derece odaklanması ve belki de amaçlanan şeyin gözden kaçırılması gibi istenmeyen durumlara sebep olur. Bu gibi hallerde, trendler için emniyet performans göstergesinin izlenmesi daha uygun olabilir.

(17) Aşağıdaki faaliyetler, emniyet performansının izlenmesine ve ölçülmesine yönelik kaynaklar sağlayabilir:

a) Emniyet çalışmaları, emniyet sorunlarına yönelik daha derin bir anlayışın kazanılması ve emniyet performansındaki trendin daha iyi bir şekilde anlaşılmasına yönelik analizlerdir.

b) Emniyet verileri analizinde, daha fazla soruşturmayı gerektirebilecek ortak sorunları veya trendleri açığa çıkarmak için emniyet raporlaması verileri kullanılabilinir.

c) Emniyet anketleri, spesifik bir operasyona ilişkin prosedürleri veya süreçleri inceler. Kontrol listeleri, soru formları ve gayri resmi gizli mülakatların kullanımını içerebilir. Genellikle niteliksel bilgiler sunduğundan, düzeltici faaliyetin gerekli olup olmadığının tespit edilmesi için verilerin toplanması vasıtasıyla doğrulama gerektirebilir. Anketler, ucuz ve değerli bir emniyet bilgi kaynağı sağlayabilir.

ç) Emniyet denetimleri, işletmenin SMS'inin ve destekleyici sistemlerinin bütünlüğünün değerlendirilmesine odaklanır. Emniyet denetimleri aynı zamanda, kurulu bulunan emniyet risk

kontrollerinin etkinliğini değerlendirmek veya emniyet düzenlemelerine uyumu izlemek için de kullanılabilir. Bağımsızlığın ve tarafsızlığın sağlanması, emniyet denetimleri için bir zorluk teşkil etmektedir. Politika, prosedür, rol ve iletişim protokolü korunarak uygulanan iç denetimlerle veya harici kuruluşların görevlendirilmesiyle bağımsızlık ve tarafsızlığa ulaşılabilir.

d) Emniyet soruşturmalarından elde edilen bulgular ve tavsiyeler, toplanan diğer emniyet verilerine kıyasla analiz edilebilen faydalı emniyet bilgileri sağlayabilir.

e) Uçuş veri analizi, radar bilgileri gibi operasyonel veri toplama sistemleri, olaylara ve operasyonel performansa ilişkin faydalı veriler sağlayabilir.

(18) Mevcut veya elde edilebilir olan verilerin analizine dayalı ve emniyet hedefleri ile bağlantılı olarak emniyet performans göstergeleri geliştirilmelidir. İzleme ve ölçüm süreci, seçilen emniyet performansı göstergelerinin, ilgili emniyet performans hedefleri ve emniyet tetikleyicilerinin kullanımını içerir.

(19) Emniyet performans göstergeleri ve emniyet performans hedefleri izlenerek emniyet performansındaki anormal değişiklikler belirlenir. Emniyet performans hedefleri, işletme ve ilgili havacılık sektörü için mevcut kaynaklar dikkate alındığında gerçekçi ve ulaşılabilir olmalıdır.

(20) Emniyet performansı izlemesi ve ölçümü, emniyet risk kontrollerinin etkinliğinin doğrulanmasına yönelik bir araç sunar, ayrıca SMS süreçlerinin ve faaliyetlerinin bütünlüğüne ve etkinliğine ilişkin bir ölçü sunar.

(21) Genel Müdürlük takip edilmesi gereken emniyet performans göstergelerinin ve emniyet performans hedeflerinin kabulüne yönelik spesifik süreçler oluşturabilir. Emniyet performans göstergelerinin ve emniyet performans hedeflerinin geliştirilmesi sırasında, Genel Müdürlük tarafından yapılan düzenlemelere uyulmalıdır.

Değişiklik Yönetimi

MADDE 21 -(1) İşletmeler, aşağıda belirtilen bir dizi faktöre bağlı olarak değişiklik gösterebilir , ancak bunlarla sınırlı değildir:

a) Organizasyonel büyüme veya küçülme,

b) Emniyete etki eden, ürünlerin ve hizmetlerin emniyetli bir şekilde sunulmasını destekleyen; iç sistemlerde, süreçlerde veya prosedürlerde değişikliklerle sonuçlanabilen iş iyileştirmeleri,

c) İşletmenin çalışma ortamındaki değişiklikler,

ç) Harici işletmelerle olan SMS arayüz bağlantılarındaki değişiklikler

d) Dış mevzuata dayalı değişiklikler, ekonomik değişiklikler ve yükselen riskler.

(2) Değişiklik mevcut emniyet risk kontrollerinin etkinliğine etki edebilir. Ayrıca yapılan değişiklik, herhangi bir operasyona yanlışlıkla, yeni tehlikeler ve ilişkili emniyet riskleri oluşturabilir. İşletmenin tehlike tanımlama veya emniyet risk yönetimi prosedürlerinde tanımlandığı şekilde tehlikeler tanımlanmalı ve ilişkili emniyet riskleri değerlendirilmeli ve kontrol edilmelidir.

(3) Değişikliğin yönetimi sürecinde aşağıdaki hususların dikkate alınması gerekir:

a) Söz konusu değişiklik ne kadar kritiktir? İşletme tarafından, değişikliğin işletmenin faaliyetleri üzerindeki ve diğer organizasyonlar ve havacılık sistemi üzerindeki etkileri göz önünde bulundurulmalıdır.

b) Havacılık topluluğunun kilit üyelerinin değişiklik yönetimi faaliyetlerine dahil olması önemlidir; bu, harici kuruluşlardan bireyleri içerebilir.

c) Durum hakkında bilgi vermek ve değişikliğin analizini sağlamak için kullanılabilecek hangi veri ve bilgiler mevcut?

(4) Küçük artımlı değişiklikler genellikle fark edilmez, ancak kümülatif etkisinin hesaba katılması önemlidir. Küçük veya büyük değişiklikler, organizasyonun sistem tanımına etki edebilir ve sistemde revizyon gerçekleştirilmesine ihtiyaç duyulabilir. Bu sebeple, işletmelerde düzenli ve hatta sürekli olarak değişiklik yaşandığı göz önünde bulundurulduğunda, sistem tanımının geçerliliğinin devam ettiğini tespit etmek için düzenli olarak gözden geçirilmesi gerekir.

(5) İşletme tarafından resmi değişiklik sürecine yönelik tetikleyicinin tanımlanması gerekir. Resmi değişiklik yönetimini tetiklemesi muhtemel olan değişiklikler şunlardır:

a) Yeni teknoloji veya ekipmanların getirilmesi,

b) Çalışma ortamındaki değişiklikler,

c) Kilit öneme sahip personel değişiklikleri,

ç) İstihdam seviyesinde önemli değişiklikler,

d) Emniyete ilişkin mevzuat gerekliliklerindeki değişiklikler,

e) Organizasyonun önemli düzeyde yeniden yapılanması ve

f) Yeni tesis veya üs, havaalanı yerleşimi değişiklikleri gibi fiziki değişiklikler.

(6) İşletme aynı zamanda değişikliğin personel üzerindeki etkisini de göz önünde bulundurmalıdır. Bu husus söz konusu değişiklikten etkilenenlerin, değişikliği kabul etme şekline etki edebilir. Hızlı iletişim ve anlaşma normalde değişikliğin algılanma ve uygulanma şeklini iyileştirir.

(7) Değişiklik yönetimi süreci aşağıdaki faaliyetleri içermelidir.

a) Değişiklik, değişikliğe ve değişikliğin neden uygulanmakta olduğuna dair açıklamayı içerecek şekilde anlanmalı ve tanımlanmadır.

b) İşletme dahilindeki kişiler, diğer departmanlar, harici kişiler veya diğer işletmelerin yanı sıra ekipmanlar, sistemler ve süreçler değişiklikten etkilenebileceği için değişikliğin kimleri ve neleri etkileyeceği anlaşılabilecek şekilde tanımlanmadır. Bu faaliyet, değişikliğe kimlerin dahil edilmesi gerektiğinin tespit edilmesine yönelik bir fırsattır. Sistem tanımının ve işletmenin arayüz bağlantılarının gözden geçirilmesine ihtiyaç duyulabilir. Değişiklikler diğer risklerin hafifletilmesi için halihazırda uygulanmakta olan risk kontrollerine etki edebilir ve bu sebeple değişiklik, hemen görülebilir nitelikte olmayan alanlardaki riskleri artırabilir.

c) Değişikliğe ilişkin tehlikeler tanımlanmalı ve emniyet risk değerlendirmesi gerçekleştirilmelidir. Söz konusu değişiklik ile doğrudan ilgili olan tehlikeler tanımlanmalıdır. Söz konusu değişiklikten etkilenecek olan emniyet risk kontrollerinin ve mevcut tehlikelerin gözden geçirilmesi gerekir. Bu adımda, işletmenin emniyet risk yönetimi süreçleri kullanılmalıdır.

ç) Değişikliğe yönelik olarak eylem planı geliştirilmelidir. Planda 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 programını tanımlayan açık bir plan olmalıdır.

d) Değişikliği uygulamak için değişikliğin emniyetli olduğu teyit edilerek onaylanmalıdır. Değişiklik planının, değişikliğin uygulanmasına yönelik genel sorumluluğa ve yetkiye sahip olan kişi tarafından onaylanması gerekir.

e) Hangi izleme faaliyetinin gerekli olduğunun tespit edilmesine yönelik güvence planı olmalıdır. Değişikliğin nasıl bildirileceği ve değişiklik sırasında veya sonrasında denetim gibi ilave faaliyetlere ihtiyaç duyulup duyulmadığı düşünülmelidir. Yapılan varsayımların test edilmesi gerekir.

SMS'in sürekli iyileştirilmesi

MADDE 22 -(1) İşletmenin SMS etkinliğinin sürdürülmesi ve sürekli iyileştirilmesi, doğrulama ve izleme faaliyetleri ile iç denetim süreçlerini içeren emniyet güvencesi tarafından desteklenmelidir. İşletmenin kendisinin ve çalışma ortamının sürekli olarak değişecek olmasına bağlı olarak SMS'in sürdürülmesinin ve sürekli olarak iyileştirilmesinin devam eden bir süreç olduğu kabul edilmelidir.

(2) İç denetimler, işletmenin karar alma süreçlerine faydalı olan bilgileri sunabilen havacılık faaliyetlerinin değerlendirilmesini kapsar. İç denetimde işletme genelindeki emniyet yönetimi işlevlerinin tümüne yönelik değerlendirmeye yer verilir.

(3) SMS etkinliği sadece emniyet performans göstergelerine dayalı olmamalıdır. İşletme tarafından, çıktıların yanı sıra süreçlerin sonuçlarının ölçülmesine ve bu faaliyetler vasıtasıyla elde edilen bilgilerin değerlendirilmesine yönelik çeşitli yöntemlerin uygulanması ile etkinliğinin tespit edilmesi amaçlanmalıdır. Bu yöntemler aşağıdakileri içerebilir:

a) İç denetimleri ve diğer işletmeler tarafından yürütülen denetimleri içerir.

b) Emniyet kültürüne ve SMS etkinliğine yönelik değerlendirmeleri içerir.

c) Hata ve kural ihlali durumlarının yanı sıra kaza ve olayların içinde olduğu emniyet olaylarının tekrarının izlenmesidir.

ç) Personelin SMS'e bağlılığını ölçmek için kültürel anketler de yapılabilir bu aynı zamanda işletmenin emniyet kültürüne ilişkin bir gösterge de sunabilir.

d) Emniyet hedeflerine işletme tarafından ulaşılıp ulaşılmadığını ve genel eğilimleri belirlemek için mevcut emniyet performansı bilgileri yönetim tarafından incelenmelidir. SMS etkinliğinin üst yönetim tarafından gözden geçirilmesi önemli olup en üst düzey EGGK'nın işlevlerinden biri olarak gerçekleştirilebilir.

e) Eğilimler dikkate alınarak EGGK tarafından emniyet performans göstergeleri ve emniyet performans hedefleri değerlendirilmelidir. Mümkünse veriler diğer işletmelerin verileri ile veya uluslararası verilerle karşılaştırılabilir.

f) Emniyet raporlama sistemlerinden ve işletmenin emniyet araştırmalarından ders çıkarılmalıdır. Bunun aynı zamanda emniyet iyileştirmelerini beraberinde getirmesi beklenir.

(4) Kısacası emniyet performansının ve iç denetim süreçlerinin izlenmesi, işletmenin kendi emniyet performansını sürekli olarak iyileştirme becerisine katkı sağlar. SMS'in, ilgili emniyet risk kontrollerinin ve destek sistemlerinin kesintisiz olarak izlenmesi, işletmelere ve Genel Müdürlüğe emniyet yönetim süreçlerinin istenen emniyet performansı hedeflerine ulaştığı hususunda güvence teşkil eder.

Emniyet Teşviki

MADDE 23 -(1) Emniyetin teşvik edilmesi, pozitif bir emniyet kültürünü teşvik eder ve eğitim ve öğretim, etkili iletişim ve bilgi paylaşımı yoluyla sürekli olarak geliştirilen teknik yeterlilik kombinasyonu yoluyla hizmet sağlayıcının emniyet hedeflerine ulaşmasına yardımcı olur. Üst yönetim işletme genelinde emniyet kültürünün teşvik edilmesine liderlik etmelidir.

(2) Etkin emniyet yönetimi, yalnızca yetkilendirme veya politika ve prosedürlere sıkı sıkıya bağlı kalma ile elde edilemez. Emniyetin teşviki, hem bireysel hem de kurumsal davranışı etkiler ve emniyet çabalarını destekleyen bir değer sistemi sağlayarak kuruluşun politikalarını, prosedürlerini ve süreçlerini tamamlar.

(3) İşletme tarafından, organizasyonun tüm kademelerinde etkin iki yönlü iletişimi kolaylaştıran süreçlerin ve prosedürlerin tesis edilmesi ve uygulanması gerekir. Bu, kuruluşun tepesinden, net bir stratejik yönlendirmeyi ve tüm personelden açık ve yapıcı geri bildirimi teşvik eden "aşağıdan yukarıya" iletişimin etkinleştirilmesini içermelidir.

Eğitim ve Öğretim

MADDE 24 -(1) İşletme tarafından personelin eğitilmesini ve SMS görevlerini yerine getirmeye yetkin olmasını sağlayan bir emniyet eğitimi programı geliştirilmeli ve uygulanmalıdır. Emniyet eğitim programının kapsamı her bir bireyin SMS'e katılımına uygun olmalıdır. Emniyet eğitim programının uygulanmasının sağlanmasından emniyet yöneticisi sorumludur. Bu programa işletme tarafından karşılaşılan spesifik emniyet sorunlarına ilişkin uygun emniyet bilgileri ilave edilmelidir. İşletmedeki seviyeleri ne olursa olsun, SMS görevlerini yerine getirmek için eğitimli ve yetkin personel, yönetimin etkili bir SMS'ye bağlılığının bir göstergesidir. Eğitim programında yetkinliklerin sürdürülmesine yönelik başlangıç ve tazeleme eğitimi gerekliliklerine yer verilmelidir. Başlangıç emniyet eğitimi kapsamında asgari olarak aşağıdakiler göz önünde bulundurulmalıdır:

a) İşletmenin emniyet politikası ve emniyet hedefleri,

b) Emniyete ilişkin organizasyonel görevler ve sorumluluklar,

c) Temel emniyet risk yönetimi prensipleri,

ç) Emniyet raporlama sistemleri,

d) İşletmenin SMS süreçleri ve prosedürleri ve

e) İnsan faktörleri.

(2) Emniyet tazeleme eğitimi; SMS politikalarındaki, süreçlerindeki ve prosedürlerindeki değişikliklere odaklanmalı ve işletmenin spesifik emniyet sorunlarını veya çıkarılan dersleri vurgulamalıdır.

(3) Eğitim programı kişinin SMS dahilindeki ihtiyaçlarına uyarlanmalıdır. Örneğin; organizasyonun emniyet komitelerinde yer alan yöneticilere yönelik eğitim seviyesi ve derinliği, organizasyonun ürün veya hizmetlerinin sunulmasına doğrudan dahil olan personele yönelik olandan daha kapsamlı olur. Operasyonlara doğrudan dahil olmayan personel, sadece organizasyona ilişkin üst seviyede genel bilgiye ihtiyaç duyabilir.

(4) Çoğu işletme için, operasyonun, personelin emniyet görevlerinin ve mevcut eğitimin net bir şekilde anlaşılmasını sağlamak için resmi bir eğitim ihtiyaç analizi gereklidir. Tipik eğitim ihtiyaçları analizi genellikle aşağıdaki adımları içeren bir hedef kitle analizinin gerçekleştirilmesiyle başlar:

a) İşletmenin her bir personeli aynı yöntem veya aynı derecede olmamak üzere SMS'in uygulanmasından etkilenir. Her bir personel grubunun bilhassa emniyet görevlerine ilişkin olmak üzere emniyet yönetimi süreçleriyle, girdileriyle ve çıktılarıyla hangi şekilde etkileşim halinde olacakları belirlenmelidir. Bu bilgilerin pozisyon/görev tanımlarından elde edilmesi gerekir. Kişilerin gruplandırılması benzer eğitim ihtiyaçları olduğunu ortaya çıkarır. İşletme tarafından bağlantılı olunan harici organizasyonlardaki personel için analizin genişletilmesinin gerekip gerekmediği göz önünde bulundurulmalıdır.

b) Her bir emniyet görevini yerine getirmek için gereken ve her bir personel grubu tarafından ihtiyaç duyulan bilgi ve yetkinlikler belirlenmelidir.

c) İş gücü genelindeki mevcut emniyet bilgi ve becerisi ile emniyet görevlerinin etkili bir şekilde yapılması için ihtiyaç duyulan bilgi ve beceri arasındaki boşluğu belirlemek için analiz gerçekleştirilmelidir.

ç) Her bir kişinin veya grubun emniyet yönetimine dahil olması için uygun bir bilgi ve beceri geliştirme yaklaşımı belirlenerek uygun bir eğitim programı geliştirilmelidir. Eğitim programında personelin devam eden emniyet bilgisi ve yetkinlik ihtiyaçları da göz önünde bulundurulmalı, bu ihtiyaç genel anlamda bir tazeleme eğitimi programıyla karşılanmalıdır.

(5) Eğitimin verilmesine yönelik en uygun yöntemin belirlenmesi önemlidir. Eğitimin verilmesinde temel amaç, eğitimin tamamlanmasıyla personelin SMS görevlerini yerine getirebilecek yetkinliğe sahip olmasıdır. Eğitmen yetkinliği de genellikle dikkate alınması gereken önemli bir husustur. Bu kişilerin taahhüdü, öğretme becerileri ve emniyet yönetimi uzmanlığı verilen eğitimin etkinliği üzerinde belirgin bir etkiye sahip olur. Emniyet eğitimi programı aynı zamanda eğitim içeriği ve zamanlamasının yanı sıra eğitim ve yetkinlik kayıtlarının yönetimine ilişkin sorumlulukları da belirtmelidir.

(6) İşletme SMS'e katılımlarına bağlı olmak üzere, kimin ve hangi kapsamda eğitileceğini belirlemelidir. İşletmede çalışanların çoğu, havacılık emniyeti ile doğrudan veya dolaylı ilişkisi olması dolayısıyla bir takım SMS görevlerine de sahiptir. SMS görevi ürünlerin ve hizmetlerin sunumuna doğrudan dahil olan tüm personel ile işletmenin emniyet komitelerinde yer alan personel için geçerlidir. Sınırlı SMS görevlerine sahip olsa da, bazı idari personel ve destek personeli işlerinin havacılık emniyetinde dolaylı etkiye sahip olmasına bağlı olarak SMS eğitiminin birazına ihtiyaç duyar.

(7) İşletme tarafından personelin SMS görevleri belirlenmelidir. Bu bilgiler emniyet eğitimi programının kontrolü için kullanılmalı ve her bir bireyin SMS'e katılımıyla uyumlu eğitim alması sağlanmalıdır. Emniyet eğitimi programında destek personeline, operasyon personeline, yöneticilere ve amirlere, üst düzey yöneticilere ve sorumlu müdüre yönelik emniyet eğitiminin içeriği belirtilmelidir.

(8) Sorumlu müdüre ve üst düzey yöneticilere yönelik olarak hazırlanacak emniyet eğitimi aşağıdaki konu başlıklarını içermelidir:

a) Yeni sorumlu müdürlere ve yönetici personellere yönelik, kendi SMS yükümlülük ve sorumluluklarına ilişkin spesifik farkındalık eğitimi,

b) Ulusal ve organizasyonel emniyet gerekliliklerine uyumun önemi,

c) Yönetim taahhüdü,

ç) Kaynakların tahsis edilmesi,

d) Emniyet politikasının ve SMS'in teşvik edilmesi,

e) Pozitif emniyet kültürünün teşvik edilmesi,

f) Birimler arası etkin emniyet iletişimi,

g) Emniyet hedefi, emniyet performansı hedefleri ve uyarı seviyeleri ve

ğ) Disiplin politikası.

(9) Emniyet eğitimi programının ana amacı işletmenin tüm seviyelerindeki personelinin emniyet görevlerini yerine getirebilmesi için yetkinliğinin sürdürülmesinin sağlanmasıdır. Bu sebeple personelin yetkinlikleri düzenli olarak gözden geçirilmelidir.

Emniyet İletişimi

MADDE 25 -(1) İşletme, SMS amaçlarını ve prosedürlerini tüm uygun personele iletmelidir. Kişinin rolüne ve emniyet ile ilgili bilgileri alma ihtiyacına bağlı olarak en uygun yöntemle emniyet iletişimi sağlanmasına yönelik bir iletişim stratejisi olmalıdır. İletişim, haber bültenleri, bildirimler, bültenler, brifingler veya eğitim kurslarıyla yapılabilir. Aynı zamanda emniyet yöneticisi tarafından gerek dahili gerek diğer işletmelerden olmak üzere, soruşturmalardan ve olay geçmişlerinden veya deneyimlerden öğrenilen derslerin geniş çaplı olarak dağıtılması sağlanmalıdır. Emniyet iletişiminin amaçları şunlardır;

a) Personelin SMS'den tamamen haberdar olmasını sağlamak; bu, organizasyonun emniyet politikasını ve emniyet hedeflerini geliştirmenin iyi bir yoludur.

b) Emniyet açısından kritik bilgileri iletmek; emniyet açısından kritik bilgiler, kuruluşu emniyet riskine maruz bırakabilecek emniyet sorunları ve emniyet riskleriyle ilgili özel bilgilerdir. Bu, öğrenilen dersler veya emniyet riski kontrolleriyle ilgili gibi dahili veya harici kaynaklardan toplanan emniyet bilgilerinden olabilir. Hizmet sağlayıcı, hangi bilgilerin emniyet açısından kritik kabul edildiğini ve iletişiminin güncelliğini belirler.

c) Yeni bir emniyet riski kontrolleri ve düzeltici eylemleri konusunda farkındalığı artırmak; İşletmenin karşılaştığı emniyet riskleri zamanla değişecektir ve bunun tanımlanmış yeni bir emniyet riski veya emniyet riski kontrollerinde değişiklik olup olmadığına bakılmaksızın, bu değişikliklerin uygun personele iletilmesi gerekecektir.

ç) Yeni veya değiştirilmiş emniyet prosedürleri hakkında bilgi sağlamak; emniyet prosedürleri güncellendiğinde, uygun kişilerin bu değişikliklerden haberdar edilmesi önemlidir.

d) Pozitif bir emniyet kültürünü teşvik etmek ve personeli tehlikeleri belirlemeye ve raporlamaya teşvik etmek; emniyet iletişimi iki yönlüdür. Tüm personelin emniyet sorunlarını emniyet raporlama sistemi aracılığıyla kuruluşa iletmesi önemlidir.

e) Geri bildirim sağlamak; belirlenen herhangi bir tehlikeyi gidermek için hangi önlemlerin alındığına ilişkin olarak emniyet raporları gönderen personele geri bildirim sağlamak.

(2) İşletme bir üst maddede listelenmekte olan emniyet bilgilerinden herhangi birinin, harici organizasyonlarla olan iletişim için gerekli olup olmadığı değerlendirmelidir.

(3) İşletme tarafından, emniyet bakımından paylaşılan kritik bilgilerin personel tarafından alınmış ve anlaşılmış olduğu kontrol edilerek, emniyet iletişiminin etkinliği değerlendirilmelidir. Bu değerlendirme, iç denetim faaliyetleri kapsamında veya SMS etkinliği değerlendirilirken yapılabilir.

(4) Emniyet teşviki faaliyetleri SMS'in sadece kurulmasında veya ilk uygulanma döneminde değil, SMS yaşam döngüsü genelinde yürütülmelidir.

ÜÇÜNCÜ BÖLÜM
İdari Yaptırımlar, Çeşitli ve Son Hükümler

Denetleme ve İdari Yaptırımlar

MADDE 26 -(1) Bu Talimat hükümlerine göre SMS kurmaktan sorumlu işletmeler, Genel Müdürlük tarafından Türk Sivil Havacılık Kanunu'nun 27nci maddesine göre bu Talimat kapsamında denetlenir.

(2) Bu Talimatta belirtilen kurallara uymayan işletmelere ve ilgili personele 2920 sayılı Türk Sivil Havacılık Kanunu'nun 27nci, 30uncu ve 143üncü maddelerinde belirtilen hükümler ile SHY-İPC Yönetmeliği hükümleri uygulanır.

Yürürlükten kaldırılan mevzuat

MADDE 27 -(1) Bu Talimat yürürlüğe girdiği tarihten itibaren, 14/11/2011 tarihli Ticari Hava Taşıma İşletmeleri, Uçuş Eğitim ve Bakım, Tasarım ve Üretim Kuruluşlarında Emniyet Yönetim Sisteminin Uygulanmasına İlişkin Talimat (SHT-SMS) yürürlükten kalkar.

(2) Bu talimat yürürlüğe girdiği tarihten itibaren 07/02/2012 tarihli Havaalanlarında Emniyet Yönetim Sisteminin Uygulanmasına İlişkin Talimat (SHT - SMS/HAD) yürürlükten kalkar

(3) Bu talimat yürürlüğe girdiği tarihten itibaren 10/03/2011 tarihli Hava Seyrüsefer Hizmet Sağlayıcıları Tarafından Emniyet Yönetim Sistemlerinin Kullanılmasına İlişkin Talimat (SHT- 65.03) yürürlükten kalkar

Yürürlük

MADDE 28 -(1) Bu Talimat yayımı tarihinde yürürlüğe girer.

Yürütme

MADDE 29 -(1) Bu Talimat hükümlerini Genel Müdür yürütür.

EK-1
UYGULAMANIN PLANLANMASI

1-Sistem Tanımı

1)Sistem tanımı, SMS'in kapsamını tanımlamak üzere, arayüz bağlantıları da dahil olmak üzere organizasyonel süreçlerin tanımlanmasına yardımcı olur. İşletmenin SMS bileşenlerine ve unsurlarına ilişkin boşlukların saptanmasına imkan verir ve organizasyonel ve operasyonel tehlikelerin tanımlanmasına yönelik bir başlangıç noktası işlevi görebilir. Sistem tanımı, emniyet risk yönetimi ve emniyet güvencesinin etkin olması için ürünün, hizmetin veya faaliyetin özelliklerini tanımlamaya hizmet eder.

2)Çoğu işletme, farklı iç birimlerin yanı sıra işletmenin emniyetli operasyonuna katkı sağlayan farklı harici organizasyonları içeren karmaşık bir arayüz bağlantıları ve etkileşimler ağından oluşur. Sistem tanımının kullanılması kuruluşun birçok etkileşimi ve arayüzü hakkında daha net bir resme sahip olmasını sağlar. Emniyet riski ve emniyet risk kontrollerinin tanımlanmaları halinde daha iyi bir şekilde yönetilmesi sağlanacak ve SMS süreçlerindeki ve prosedürlerindeki değişikliklerin etkisinin anlaşılmasına yardımcı olunacaktır.

3)Herhangi bir sistem tanımı değerlendirilirken, "sistemin", birbirine bağlı bir ağın parçaları olarak birlikte çalışan unsurlar seti olduğunun kavranılması önemlidir. Havacılık emniyeti faaliyetlerine ilişkin olan ve havacılık emniyeti faaliyetlerine etki edebilecek işletmenin ürünleri, kişileri, süreçleri, prosedürleri, tesisleri, hizmetleri ve dış etkenler de dahil olmak üzere diğer unsurlar SMS'in içerisindedir. "Sistem" genellikle alt sistemlere sahip olan sistemler bütünüdür. Bu sistemler ve bunların birbirleriyle olan etkileşimleri tehlikelerin kaynaklarını oluşturur ve emniyet risklerinin kontrolüne katkı sağlar. Önemli sistemler havacılık emniyetine doğrudan etki edebilecek olan ve işletmenin etkin emniyet yönetimi becerisine veya kapasitesine etki eden unsurları içerir.

4)SMS dokümantasyonunda, sistem tanımına ve SMS arayüz bağlantılarına ilişkin genel bilgilere yer verilmelidir. Sistem tanımı, politikalara ve prosedürlere atıfların yapıldığı madde işaretli listeyi içerebilir. Süreç akışı veya açıklamalı organizasyon şeması gibi grafiksel bir gösterim bazı organizasyonlar için yeterli olabilir. İşletme tarafından kullanışlı bir yöntem ve format kullanılmalıdır.

5)Her işletmenin kendine özgü yapısı olması sebebiyle, SMS uygulamasına yönelik her şeyi çözebilecek tek bir yöntem mevcut değildir. Her işletmenin kendi yapısına uygun olarak işleyen bir SMS uygulaması beklenir. Temel gerekliliklerin nasıl karşılanmasının amaçladığı her işletme tarafından tanımlanmalıdır. Bunu başarmak için, işletmenin organizasyon yapısı, süreçleri ve emniyet yönetimi işlevleri bakımından önemli olarak değerlendirilen iş düzenlemelerini tanımlayan bir sistem tanımının hazırlanması önemlidir. Sistem tanımına dayalı olarak, işletme tarafından kendi emniyet yönetimi gerekliliklerini tesis eden politikanın, süreçlerin ve prosedürlerin tanımlanması veya geliştirilmesi gerekir.

6)İşletme tarafından sistem tanımında belirtilen süreçlerde önemli veya esas değişikliklerin yapılması durumunda, söz konusu değişikliklerin emniyet risk değerlendirmesi temelinde potansiyel olarak etkilerinin değerlendirilmesi gerekmektedir. Dolayısıyla sistem tanımının değişiklik yönetimi süreçleri kapsamında gözden geçirilmesi gerekir.

2-Arayüz Yönetimi

1)İşletmenin karşı karşıya kaldığı emniyet riskleri arayüzlerden etkilenir. Arayüzler iç birimler gibi dahili veya diğer hizmet sağlayıcıları veya sözleşmeli hizmetler gibi harici olabilir. Bu arayüzleri belirlemek ve yönetmek suretiyle işletmeler arayüzlere ilişkin emniyet riskleri üzerinde daha fazla kontrole sahip olur. Bu arayüzlerin sistem tanımında belirlenmesi gerekir.

3-SMS Arayüzlerinin Belirlenmesi

1)İlk olarak işletme tarafından kendi iş faaliyetlerine ilişkin arayüz bağlantılarına yoğunlaşılmalıdır. Bu arayüzlerin tanımlanması, SMS'in kapsamını ortaya koyan sistem tanımında detaylandırılmalı ve dahili ve harici arayüz bağlantılarını içermelidir.

2)SMS arayüzlerini tanımlamak için işletmenin etkileşimde bulunduğu farklı organizasyonlarla nasıl gösterilebileceğine dair EK-3' te bir örnek yer almaktadır. Bu gözden geçirmenin amacı tüm arayüz bağlantılarına ilişkin kapsamlı bir liste oluşturmaktır. Bu uygulamanın mantığı bir organizasyonun tam olarak farkında olmadığı SMS arayüzlerinin olabileceğidir. Güç kaynağı veya bina bakım şirketleri gibi resmi anlaşmaların olmadığı durumlarda arayüzler olabilir.

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 doğrudan emniyeti göstermesine gerek bulunmayabilir.

4)SMS arayüzlerinin belirlendikten sonra, arayüzlerin göreceli kritikliğinin işletme tarafından dikkate alınması gerekir. Bu sayede işletmenin daha kritik arayüzlerin yönetimine ve bunların potansiyel güvenlik risklerine öncelik vermesi sağlanır. Dikkate alınması gereken hususlar şunlardır:

a)Neyin sağlanmakta olduğu,

b)Buna neden ihtiyaç duyulduğu,

c)Dahil olan organizasyonların uygulamada olan bir SMS'e veya başka bir yönetim sistemine sahip olup olmadığı ve

ç)Söz konusu arayüzün emniyet verilerinin/bilgilerinin paylaşılmasını kapsayıp kapsamadığı.

5)İşletme tarafından mevcut tehlike tanımlama ve risk değerlendirme süreçleri kullanılarak arayüzlere ilişkin tehlikeler tanımlanmalı ve emniyet risk değerlendirmesi gerçekleştirilmelidir.

6)İşletme tarafından tanımlanan risklere dayalı olarak, uygun bir emniyet risk kontrolü stratejisinin belirlenmesi için diğer organizasyon ile çalışılması değerlendirilebilir. Tehlikelerin tanımlanmasına, emniyet riskinin değerlendirilmesine ve uygun emniyet riski kontrolünün belirlenmesine diğer organizasyonu dahil etmekle katkıda bulunulabilir. Emniyet risklerinin her bir organizasyon için farklı algılanabilmesine bağlı olarak bu ortak çalışmaya ihtiyaç duyulur. Risk kontrolü, işletme veya harici organizasyon tarafından yürütülebilir.

7)Dahil olan her bir organizasyonun kendi organizasyonuna etki eden tehlikeleri tanımlama ve yönetme sorumluluğuna sahip olduğu da kabul edilmelidir. Her bir organizasyonun farklı emniyet riski sınıflandırmaları uygulamaları ve emniyet performansı, kaynaklar, zaman, vs. bakımından farklı emniyet risk önceliklerine sahip olması sebebiyle, söz konusu arayüzün kritik mahiyetinin farklı olması anlamına gelebilir.

8)Hizmetlerin ve ürünlerin emniyetli bir şekilde sunulmasını sağlamak üzere, arayüzlerin yönetilmesinden ve izlenmesinden işletme sorumludur. Bu sayede arayüzlerin etkin bir şekilde yönetilmesi ve de güncel ve amaca uygun kalması sağlanır. Arayüzlerin ve ilişkili sorumlulukların açık bir şekilde tanımlanabilmesine yönelik resmi sözleşme yapılması etkili bir yoldur. Arayüzlerdeki ve ilişkili etkilerdeki değişiklikler için ilgili organizasyonlarla iletişim sağlanması gerekmektedir.

9)İşletmenin arayüz emniyet risklerini yönetmesine ilişkin zorluklar aşağıdakileri içerir:

a)Bir organizasyonun emniyet risk kontrollerinin diğer organizasyonların emniyet risk kontrolleri ile uyumlu olmaması,

b)Her iki organizasyonun kendi süreçlerindeki ve prosedürlerindeki değişiklikleri kabul etme eğilimi,

c)Arayüzün yönetilmesi ve izlenmesi için yetersiz kaynakların veya teknik uzmanlığın mevcut olması ve

ç)Arayüzlerin sayısı ve konumu.

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 risk kontrol tedbirleri ve zaman ölçekleri) ilişkin kararlara yönelik mutabakat,

c)Hangi emniyet bilgilerinin paylaşılması ve bildirilmesi gerektiğinin belirlenmesi,

ç)Koordinasyonun nasıl ve ne zaman gerçekleşmesi gerektiği (görev gücü, düzenli toplantılar, özel amaçlı veya ayarlanmış toplantılar) ve

d)Her iki organizasyona da fayda sağlayan ancak SMS'in etkinliğini azaltmayan çözümler üzerinde mutabakata varılması.

11)Arayüzlere ilişkin tüm emniyet sorunları veya emniyet riskleri belgelenmeli ve paylaşım ve gözden geçirme için her bir organizasyon tarafından ulaşılabilir kılınmalıdır. Böylece çıkarılan derslerin paylaşılmasına ve her iki organizasyon için değerli olan emniyet verilerinin bir havuzda toplanılmasına imkan verilir. Emniyet risklerinin ve sorumluluğunun paylaşılması sonucunda her bir organizasyon tarafından emniyetin iyileştirilmesi sağlanır ve operasyonel emniyet faydalarına ulaşılabilir.

4-SMS Ölçeklenebilirliği

1)Politikalar, süreçler ve prosedürler de dahil olmak üzere işletmenin SMS'i, organizasyonun ve faaliyetlerinin boyutunu ve karmaşıklığını yansıtmalıdır. Aşağıdakiler dikkate alınmalıdır:

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.

2)SMS'in yönetilmesine yönelik doğru kaynak seviyesinin belirlenmesi için işletme kendi faaliyetlerine yönelik bir analiz gerçekleştirmelidir. SMS'in yönetilmesi için ihtiyaç duyulan organizasyon yapısının belirlenmesi buna dahil olmalıdır. SMS'in yönetilmesinden ve sürdürülmesinden kimin sorumlu olacağına, mümkünse hangi emniyet komitelerine ihtiyaç duyulacağına ve spesifik emniyet uzmanı ihtiyacına yönelik dikkate alınması gereken hususlar bulunmaktadır.

3)Ölçeklenebilirlik, işletmenin boyutuna bakılmaksızın faaliyetlerinin doğal emniyet riskine ilişkin bir işlev olmalıdır. Önemli havacılık emniyeti risklerini içerebilecek olan faaliyetlere küçük organizasyonlar da dahil olabilir. Bu sebeple, emniyet yönetimi kabiliyetinin yönetilecek emniyet riski ile oranlı olması gerekir.

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. Daha kalitatif olan bu yöntem işletmede tehlikelerin ve risklerin belirlenmesine yardımcı olur. Diğer işletmeler veya sektör birlikleri ile işbirliği yapılması işletmenin daha fazla veriye sahip olması adına faydalı olabilir. Örneğin, emniyet riski bilgilerini paylaşmak ve emniyet performansı trendlerini belirlemek için küçük ölçekli işletmeler tarafından benzer organizasyonlarla/operasyonlarla bilgi paylaşımında bulunulabilir. İşletmelerin sınırlı da olsa kendi verilerini yeterli bir şekilde analiz etmeleri ve işlemeleri gerekir.

5)Birçok etkileşime ve arayüze sahip olan işletmelerin, emniyet verilerini ve emniyet bilgilerini birden fazla organizasyondan nasıl topladıklarını değerlendirmesi gerekir. Ortaya çıkabilecek bu büyük hacimli veriler düzenlenmeli ve sonrasında analiz edilmelidir. İşletmeler tarafından bu tür verilerin yönetilmesine yönelik uygun bir yöntem kullanılmalıdır. Verilerin analizine yardımcı olması için toplanan verilerin kalitesine ve sınıflandırmaların kullanılmasına da özen gösterilmelidir.

5-Yönetim Sistemlerinin Entegrasyonu

1)Emniyet yönetimi ayrı olarak değil bir yönetim sisteminin parçası olarak değerlendirilmelidir. Bu sebeple işletme tarafından SMS'i içeren bir entegre yönetim sistemi uygulanabilir. Entegre yönetim sistemi; birden fazla sertifikayı, yetkilendirmeyi veya onayı elde etmek veya kalite, güvenlik, iş sağlığı ve çevre yönetim sistemleri gibi diğer iş yönetimi sistemlerini kapsamak için kullanılabilir. Bu birden fazla faaliyet genelindeki emniyet risklerini yöneterek sinerjilerden yararlanmak ve tekrarı gidermek için yapılır. Örneğin, işletme birden fazla sertifikaya sahip olduğunda, faaliyetlerinin tümünü kapsamak üzere tek bir yönetim sistemi uygulamayı seçebilir. İşletmenin iş veya organizasyonel ihtiyaçlarına uyarlamak üzere SMS'inin entegre edilmesine veya ayrı tutulmasına yönelik en iyi yönteme karar vermesi gerekir.

2)Tipik bir entegre yönetim sistemi aşağıdakileri içerebilir:

a)Kalite Yönetimi Sistemi (QMS),

b)Emniyet Yönetim Sistemi (SMS),

c)Güvenlik Yönetimi Sistemi (SeMS),

ç)Çevre Yönetimi Sistemi (EMS),

d)İş Sağlığı ve Emniyet Yönetimi Sistemi (OHSMS),

e)Finansal Yönetim Sistemi (FMS),

f)Dokümantasyon Yönetimi Sistemi (DMS),

g)Yorgunluk Riski Yönetimi Sistemi (FRMS).

3)Kendine özgü ihtiyaçlarına dayalı olarak işletme tarafından bu yönetim sistemlerinin entegre edilmesi tercih edilebilir. 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. Ayrıca tedarikçi yönetimi, tesis yönetimi, vb. gibi entegre edilebilecek iş faaliyetleri ile ilişkili diğer operasyonel sistemler de söz konusu olabilir.

4)İşletme, halihazırda SMS'e dayalı bir mevzuata yönelik gerekliliğin bulunmadığı diğer alanlarda SMS'in uygulanmasını değerlendirilebilir. Kendi iş modeline, çalışma ortamına, mevzuata dayalı ve yasal gerekliliklere ve havacılık topluluğunun beklentilerine yönetim sisteminin uyumlu hale getirilmesi için, işletme tarafından yönetim sisteminin entegre edilmesine veya ayrı tutulmasına yönelik en uygun yöntemlerin belirlenmesi gerekir. Her durumda SMS gerekliliklerinin karşılandığından yine de emin olunmalıdır.

5)Farklı alanların tek bir yönetim sistemi altında entegre edilmesi verimliliği aşağıdakiler yoluyla iyileştirecektir:

a)Süreçlerin ve kaynakların tekrarını ve örtüşmesini azaltarak,

b)Potansiyel olarak bağdaşmayan sorumlulukları ve ilişkileri azaltarak,

c)Tüm faaliyetler genelindeki risklerin ve fırsatların daha geniş etkilerini dikkate alarak ve

ç)Tüm faaliyetler genelinde performansın etkin bir şekilde izlenmesine ve yönetilmesine imkan vererek.

6)Emniyet sistemi entegrasyonunun olası zorlukları şunları içerir:

a)Mevcut sistemlerde entegrasyona karşı çıkan farklı birim yöneticileri bulunması uyuşmazlık ortaya çıkabilir,

b)Daha fazla işbirliği ve koordinasyon gerektirmesine bağlı olarak entegrasyondan etkilenecek olan personel, değişikliğe karşı direnç gösterebilir,

c)Her bir sisteme ilişkin farklı kültürlerin olabilme durumu organizasyon dahilindeki genel emniyet kültürü üzerindeki etki edebilir bu da uyuşmazlık oluşturabilir,

ç)Böyle bir entegrasyon yapılan düzenlemelerle engellenebilir veya farklı düzenleyici otorite veya standart yapılar kendi gerekliliklerinin nasıl karşılanması gerektiği hususunda farklı beklentilere sahip olabilir,

d)KYS ve SMS gibi farklı yönetim sistemlerinin entegre edilmesinde, ayrı gerekliliklerin karşılandığının kanıtlanabilmesine yönelik ek iş oluşabilir.

7)Sonuç olarak, birleştirilmiş amaçlara ve karar almaya dayalı olan bir entegre yönetim sisteminde tüm faaliyetler genelindeki daha geniş etkiler dikkate alınır. Kalite yönetimi ve emniyet yönetimi süreçleri ziyadesiyle tamamlayıcı nitelikte olur ve bu da genel emniyet amaçlarına ulaşılmasını destekler.

6-SMS ve Kalite Yönetim Sistemi Entegrasyonu

1)Bazı işletmeler hem SMS'e hem de kalite yönetimi sistemine sahiptir ve bunlar genellikle tek bir yönetim sisteminde entegre edilir. Kalite yönetim sistemi genel olarak gerekli organizasyon yapısı ve bağlı yükümlülük, kaynak, süreç ve prosedürler sağlanarak herhangi bir ürünün veya hizmetin sunumunda sürekli kalite güvencesine ve iyileştirmeye yönelik bir sistemin tesis ve teşvik edilmesidir.

2)Her iki sistem de tamamlayıcı niteliktedir. SMS emniyet risklerinin ve emniyet performansının yönetilmesine odaklanırken, kalite yönetim sistemi müşteri beklentilerinin ve akdi yükümlülüklerin karşılanmasına yönelik gerekliliklere ve yerleşik mevzuatlara uyuma odaklanır. SMS'in hedefleri, tehlikelerin tanımlanması ilişkili emniyet risklerinin değerlendirilmesi ve etkin emniyet risk kontrollerinin uygulanmasıdır. Bunun aksine kalite yönetimi, ilgili spesifikasyonları karşılayan ürünlerin ve hizmetlerin istikrarlı bir şekilde sunulmasına odaklanır. Diğer taraftan SMS ve kalite yönetim sistemi;

a)Planlanmalı ve yönetilmeli,

b)Havacılık ürünlerinin ve hizmetlerinin sunumuna ilişkin tüm organizasyonel işlevleri içermeli,

c)Etkisiz süreçleri ve prosedürleri belirlemeli,

ç)Sürekli iyileştirmeyi amaçlamalı ve

d)Müşterilere, emniyetli ve güvenilir ürün ve hizmetlerin sunulmasına yönelik amaca sahip olmalıdır.

3)SMS aşağıdakilere odaklanır:

a)İşletme tarafından karşı karşıya kalınan emniyet ile ilgili tehlikelerin tanımlanmasına,

b)İlişkili emniyet riskinin değerlendirilmesine,

c)Emniyet risklerinin azaltılmasına yönelik etkin emniyet risk kontrollerinin uygulanmasına,

ç)Emniyet performansının ölçülmesine ve

d)Emniyet performansı gerekliliklerinin karşılanmasına yönelik olarak uygun kaynak tahsisatının sağlanmasına.

4)Kalite yönetim sistemi aşağıdakilere odaklanır:

a)Mevzuatlara ve gerekliliklere uyuma,

b)Ürünlerin ve hizmetlerin sunumundaki tutarlılığa,

c)Belirlenen performans standartlarının karşılanmasına ve

ç)Amaca uygun olarak, kusur ve hatadan arındırılmış olan ürünlerin ve hizmetlerin sunulmasına.

5)Emniyet risk kontrollerinin işletme tarafından etkin bir şekilde uygulandığından ve izlendiğinden emin olunması için mevzuatlara uyumun izlenmesi gereklidir. Uyumsuzlukların sebepleri ve katkıda bulunan faktörleri analiz edilmeli ve ele alınmalıdır.

6)SMS ve kalite yönetim sisteminin tamamlayıcı yönleri göz önünde bulundurulduğunda, herhangi bir işlevden ödün vermeksizin her iki sistemi entegre etmek mümkündür. Bu husus aşağıdaki şekilde özetlenebilir:

a)Denetim, inceleme, soruşturma, kök neden analizi, süreç tasarımı ve önleyici faaliyetler gibi kalite yönetim sistemi süreçleri ile SMS desteklenir,

b)Kalite yönetim sistemi emniyet riski kontrollerindeki zayıflıkları veya emniyet sorunlarını belirleyebilir,

c)Organizasyonun standartlara ve spesifikasyonlara uyumuna karşı mevcut olan emniyet sorunları kalite yönetim sistemi kapsamında önceden görülebilir,

ç)Kalite prensiplerinin, politikalarının ve uygulamalarının emniyet yönetiminin hedefleriyle uyumlu hale getirilmesi gerekir ve

d)Tanımlanan tehlikelerin ve emniyet riski kontrollerinin, kalite faaliyetleri kapsamındaki iç denetimlerin planlanması ve icrası için göz önünde bulundurulması gerekir.

7)Sonuç olarak tüm faaliyet genelindeki 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.

7-SMS GAP Analizi ve Uygulaması

1)SMS uygulanması öncesinde, işletme tarafından bir GAP analizi gerçekleştirilmelidir. İşletmenin mevcut emniyet yönetimi süreçleri ve prosedürleri Genel Müdürlük tarafından belirlenen SMS gerekliliklerıyle karşılaştırılır. SMS işlevlerinden bazılarının işletme tarafından halihazırda uygulanmakta olması muhtemeldir. SMS'in geliştirilmesi mevcut organizasyonel politikalara ve süreçlere dayalı olmalıdır. GAP analizi tamamen işleyen ve etkili bir SMS'in uygulanması için ihtiyaç duyulan tedbirleri tanımlayan bir SMS uygulama planı vasıtasıyla ele alınması gereken boşlukları belirler.

2)SMS uygulama planı, SMS'in uygulanması için gereken kaynakların, görevlerin ve süreçlerin açık bir resmini sunmalıdır. Uygulama planının zamanlaması ve sıralaması her bir organizasyona özgü olan aşağıdakiler gibi çeşitli etkenlere dayalı olabilir:

a)Mevzuata dayalı gereklilikler, müşteri gereklilikleri ve yasal gereklilikler,

b)Muhtemelen farklı mevzuata dayalı uygulama tarihlerine sahip olunan birden fazla sertifika,

c)SMS'in mevcut yapılara ve süreçlere dayalı olabileceği alan,

ç)Kaynakların ve bütçelerin elverişliliği,

d)Farklı adımlar arasındaki karşılıklı bağımlılıklar (veri analizi sisteminin tesis edilmesi öncesinde bir raporlama sistemi uygulanmalıdır) ve

e)Mevcut emniyet kültürü.

3)SMS uygulama planı, sorumlu müdür ve diğer üst düzey yöneticiler ile istişare edilerek geliştirilmeli ve zaman aralıkları ile birlikte ilgili faaliyetlerden kimlerin sorumlu olduğunu içermelidir. Planda mümkünse harici organizasyonlarla veya yüklenicilerle koordinasyona işaret edilmelidir.

4)SMS uygulama planı, basit bir sütunlu tablodan özel üretilmiş proje yönetimi yazılımına kadar farklı şekillerde belgelenebilir. Plan düzenli olarak izlenmeli ve gerektiğinde güncellenmelidir. Herhangi bir spesifik bölümün ne zaman başarılı bir şekilde uygulanmış olarak değerlendirilebildiği de açıklığa kavuşturulmalıdır.

5)Etkin bir SMS'e ulaşılmasının birkaç yıl sürebileceği kabul edilmelidir. Genel Müdürlük SMS'in uygulanmasına ilişkin aşamalı bir yaklaşıma yönelik gereklilikler ortaya koyabilir.

EKLER:
EK-2 - Emniyet Soruşturması Karar Süreci
EK-3 - Hava Trafik Hizmet Sağlayıcısı SMS Arayüzleri Örneği