



SİVİL HAVACILIK
GENEL MÜDÜRLÜĞÜ



Sektörel Düzenleme ve Eğitim Daire Başkanlığı

EMNİYET YÖNETİM SİSTEMİ UYGULAMALARINA İLİŞKİN KILAVUZ BİLGİLER



T.C.
Ulaştırma Denizcilik ve
Haberleşme Bakanlığı
bağlı kuruluştur.

YAYIN NO: SDED/T-01

EMNİYET YÖNETİM SİSTEMİ UYGULAMALARINA İLİŞKİN KILAVUZ BİLGİLER

SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ YAYINLARI

Yayın No: SDED/T-01

Yayın Türü: Çeviri

Konu: Emniyet Yönetimi Uluslararası İşbirliği Grubu (SMICG) tarafından yayımlanan “1774-1780-2077-2395-3117-3426” nolu dokümanların Türkçe'ye tercüme edilmiş halidir.

İlgili Birim: Sektörel Düzenleme ve Eğitim Daire Başkanlığı

1. Basım Tarihi Ekim 2017, Ankara

© 2017 Sivil Havacılık Genel Müdürlüğü

Telif Hakları Sivil Havacılık Genel Müdürlüğü'ne aittir.

Her hakkı saklıdır. Sivil Havacılık Genel Müdürlüğü tarafından özel olarak izin verilmedikçe bu yayının kopyalanarak çoğaltılması, dağıtılması ve kullanılması yasaktır.

İlk yayımlanma tarihi Ekim 2017'dir.

Bu yayının bilgilendirme amacıyla hazırlanmıştır

www.shgm.gov.tr

Bu yayının basılı hâli Sivil Havacılık Genel Müdürlüğü,
Sektörel Düzenleme ve Eğitim Daire Başkanlığından temin edilebilir.

Sivil Havacılık Genel Müdürlüğü

Gazi Mustafa Kemal Bulvarı No:128/A

06570 Maltepe / ANKARA

Tel: +90 312 203 60 00

Fax: +90 312 212 46 84

www.shgm.gov.tr

İÇİNDEKİLER

BÖLÜM 1

Emniyet Yönetim Sistemi Değerlendirme Aracı _____ 4

BÖLÜM 2

Emniyet Performans Ölçümüne Ortak Yaklaşım _____ 27

BÖLÜM 3

Risk Bazlı Karar Alma İlkeleri _____ 35

BÖLÜM 4

Hizmet Sağlayıcılara Yönelik Olarak

Emniyet Performansının Ölçülmesine İlişkin Kılavuz İlkeler _____ 66

BÖLÜM 5

Emniyet Yönetimi Sistemi (SMS) Entegrasyonu _____ 96

BÖLÜM 6

Emniyet Yönetim Sistemi (SMS) Değerinin Tespit Edilmesi _____ 107

BÖLÜM 1

Emniyet Yönetim Sistemi Değerlendirme Aracı

Emniyet Yönetimi Uluslararası İşbirliği Grubu (SM ICG) Emniyet Yönetim Sistemi (SMS) Değerlendirme Aracı Kılavuz Bilgileri

Geçmiş ve Amaç

Bu Araç, SM ICG tarafından herhangi bir kuruluşun Emniyet Yönetim Sisteminin (SMS) değerlendirilmesi için kullanılmak üzere geliştirilmiştir. İlk değerlendirme veya sürekli denetim ve gözetim için kullanılabilir. Araç, düzenleyici otoriteler tarafından ilgili kuruluşun Emniyet Yönetim Sisteminin (SMS) etkinliğinin değerlendirilmesine yardımcı olan bir dizi göstergeye dayalıdır. Yüz yüze görüşmeler ve değerlendirme kapsamında bireyler ile bir dizi çapraz mülakat da dahil olmak üzere kuruluş ile etkileşimi öngörür. Geleneksel uygunluğa dayalı denetimden, uygunluğun yanı sıra Emniyet Yönetim Sisteminin (SMS) etkinliğini de değerlendiren performansa dayalı denetime kadar olmak üzere denetim metodolojilerindeki farkı ayırt eder.

Herhangi bir kuruluşun Emniyet Yönetim Sisteminin (SMS) düzenlemesine uygunluk ile emniyet riskinin etkin yönetimindeki performansı bakımından beklenen standarda işaret etmek üzere tasarlanmıştır.

Emniyet Yönetim Sistemine (SMS) yönelik olarak global bakımdan muadil bir Emniyet Yönetim Sistemi (SMS) denetim standardı belirleyen bir yaklaşımın uyumlaştırılması için geliştirilmiştir ve bu sebeple, SM ICG üyeleri, kendi sektörlerinde aynı etkinlik standardına ulaşılmasını sağlamaya gayret edeceklerdir. Diğer düzenleyici otoritelerin aynı standardı değerlendirmeleri halinde, bu husus ikili anlaşmalar kapsamında karşılıklı kabule esas teşkil edebilecektir.

Buna ilaveten, söz konusu araç aynı zamanda, düzenleyici otoriteler tarafından bu aracın kendi amaçları için (yoktan bir araç yaratmaktan ziyade) kullanılmasına ve uyarlanmasına imkan vermek üzere tasarlanmıştır.

İlk değerlendirme

Düzenleyici Otorite, bu aracı, ilk değerlendirme kapsamında kullanabilecek olup, Onay sertifikasının düzenlenmesi öncesinde münferit göstergelere ilişkin beklentileri tanımlamalıdır.

Örneğin, ilk değerlendirme, uygunluğa ve performansa ilişkin göstergelerin mevcut ve uygun olup olmadığının değerlendirilmesine odaklanan belgelerin masaüstü incelemesine dayalı olabilir. Masaüstü incelemesinin yerine getirilmesi sonrasında, göstergelerin çalışır halde olup olmadığını ve genel etkinliğe ulaşıp ulaşılmadığını değerlendirmek üzere bir yerinde ziyaret gerçekleştirilmelidir.

Yerinde ziyaret, normalde, değerlendirmeyi destekleyecek teknik uzmanlar ile Emniyet Yönetim Sisteminde (SMS) uygun seviyede yetkinliğe sahip olan bir ekip liderini içeren bir ekip tarafından gerçekleştirilmelidir. Değerlendirmenin, kuruluş genelindeki yönlerin ne kadar etkin olduğunu tespit etmek üzere söz konusu kuruluşun farklı seviyelerinden bir dizi birey ile etkileşime imkan verecek şekilde yapılandırılması önem arz etmektedir. Örneğin, emniyet politikasının yürürlüğe konduğu ve kuruluş genelindeki personel tarafından idrak edildiği derecenin tespiti personel ile çapraz etkileşim gerektirecektir.

Küçük kuruluşlar için, Emniyet Yönetim Sistemi (SMS) konusunda uygun eğitim almış ve söz konusu kuruluşu değerlendirmek üzere teknik yetkinliklere sahip olan tek bir değerlendiricinin olması daha pratik olabilir.

Bir diğer yaklaşım ise, düzenlemeye tabi kuruluş için söz konusu aracın "nasıl edinildi" kutucuğu da dahil olmak üzere öz değerlendirme olarak kısmi bir şekilde tamamlanması ve söz konusu aracın, yerinde ziyaretin karşılanması için yeterli bir şekilde işleme tabi tutulup tutulmadığına karar verecek ve akabinde söz konusu kuruluşun öz değerlendirmesini onaylayacak olan düzenleyici otoriteye sunulmasıdır.

Sürekli denetim

Sürekli denetim için düzenleyici otoriteler münferit göstergelere ilişkin beklentileri de tanımlayabilirler. Bununla birlikte, SM ICG, uygunluğa ve performansa ilişkin tüm münferit göstergelerin en azından çalışır halde olmasını ve unsurların tümünde etkinliğin sağlanmasını tavsiye etmektedir.

Yetkinlikler

Araç, aşağıdaki konularda eğitilmiş ve yetkinliğe sahip olan düzenleyici otorite personeli tarafından kullanılmalıdır:

- ICAO SMS Çerçevesine dayalı Emniyet Yönetim Sistemleri
- Kalite Yönetim Sistemlerine, uygunluk ve denetim konularına hakimiyet
- Mülakat teknikleri
- Risk yönetimine hakimiyet
- Uygunluk ve performans arasındaki farkın bilinmesi
- Değerlendirmenin özetlenmesi için kullanılacak öykülemeye imkan verecek rapor yazma teknikleri.

Söz konusu aracın sınıf ortamında kullanılmasına yönelik eğitim almalarının yanında, personele, araca ve aracın pratik kullanımına alışmaları için canlı değerlendirme sırasında ek eğitim verilmesi tavsiye edilmektedir.

Aracın kullanımı (Talimatlar)

Bu Araç, bir dizi gösterge vasıtasıyla Emniyet Yönetim Sisteminin (SMS) uygunluğunu ve etkinliğini değerlendirir. O unsura ilişkin etkinlik beyanının izlediği Çerçeve tanımıyla ICAO SMS Çerçevesinin 12 unsuru kullanılarak düzenlenir. Her bir unsur için, bir dizi "uygunluk ve performans göstergesi" listelenir ve bunları bir dizi "en iyi uygulama göstergesi" izler. Her bir gösterge, söz konusu unsurun genel etkinliği doğrulanabilecek ve desteklenebilecek şekilde, aşağıda ortaya konan tanımlar ve kılavuz bilgiler kullanılarak göstergenin mevcut, uygun ve çalışır halde ve etkin olup olmadığını tespit etmek üzere incelenmelidir.

Araç genel olarak düzenleyici otorite tarafından değerlendirilmenin kayıt altına alınması ve belgelenmesi için kullanılacaktır. Alternatif olarak araç, ilgili kuruluş tarafından kendisini değerlendirmek ("Nasıl Edinildi" sütunu) ve düzenleyici otorite tarafından söz konusu kuruluşun değerlendirmesini doğrulamak ve onaylamak ("Doğrulama" sütunu) ve "Özet açıklamalar" kutucuğu üzere kısmi olarak tamamlanabilir.

Uygulanabilirlik

Değerlendirme aracı, düzenlemeye tabi olan kuruluşları değerlendirmek üzere kullanılabilir. Bununla birlikte, değerlendirmenin yapılmasında kuruluşun boyutuna, mahiyetine ve karmaşıklığına ve daha küçük ölçekli kuruluşlar için düzenleyici otorite tarafından tanımlanan daha az sayıda göstergenin kullanılabilmesine gereken dikkat gösterilmelidir.

ARAÇTA KULLANILAN TANIMLAR

Mevcut

"Göstergenin" açık bir şekilde görünür olduğuna ve kuruluşun Emniyet Yönetim Sistemi (SMS) Dokümantasyonu kapsamında belgelendiğine dair kanıt mevcuttur.

Uygun

Gösterge, kuruluşun boyutuna, mahiyetine, karmaşıklığına ve endüstri sektörünün göz önünde bulundurulması da dahil olmak üzere, söz konusu faaliyetteki içsel riske dayalı olarak uygundur.

Çalışır Halde

Göstergenin kullanımda olduğuna ve çıktı üretildiğine dair kanıt mevcuttur.

Etkin

Göstergenin etkin olduğuna ve istenilen sonuca ulaştığına dair kanıt mevcuttur.

Kanıt

Kanıt, dokümantasyonu, raporları, mülakat ve görüşme kayıtlarını kapsar ve gösterge değerlendirmesine ilişkin farklı seviyeler için kanıtın değişkenlik arz etmesi muhtemeldir. Örneğin, herhangi bir göstergenin mevcut olması için kanıtın sadece belgelenmiş olması muhtemel olmakla, çalışır halde olup olmadığının değerlendirilmesi içinse kanıt, kuruluş bünyesindeki personel ile yüz yüze görüşmelerin yanı sıra kayıtların değerlendirilmesini içerebilir. "Nasıl edinildi" sorusu kapsamında özet beyanlar ile dokümantasyona ve kayıtlara atıflar yer almalıdır.

Doğrulama

Doğrulama Sütunu, düzenleyici otorite tarafından gözlemlerin, görüşmelerin, kayıtların ve örneklendirilmiş dokümanların kayıt altına alınması için kullanılmalıdır.

Özet açıklamalar

Düzenleyici otorite tarafından tüm göstergelerin değerlendirmeye tabi tutulması sonrasında, ICAO unsurunun tüm etkinliğine ulaşıp ulaşılmadığına dair bir hükümde bulunulabilir; bu hususa özet açıklamalar kutucuğunda yer verilmelidir.

Aracın Değiştirilmesi

Herhangi bir düzenleyici otorite, terminolojiyi ve aracı kendi ulusal gerekliliklerini karşılamak üzere uyarlayabilecek olmakla birlikte, SM ICG versiyonuna uygunluk Devletler genelinde karşılıklı tanımaya imkan verebilecektir.

Prosedürlerin Geliştirilmesi

Her bir düzenleyici otorite, aracın kullanımına ilişkin, kendi organizasyon yapısına ve Emniyet Yönetim Sistemi (SMS) gözetim faaliyetine uyarlanmış prosedürler tanımlamak zorunda olacaktır.

Tamamlayıcı SM ICG ürünleri

Araç, diğer SM ICG ürünleri ile bağlantılı olarak kullanılmalıdır.

Emniyet Yönetim Sistemi (SMS) Yolculuğu

Çoğu kuruluş için Emniyet Yönetim Sistemi (SMS) uygulamada zaman ve etkin olacağı seviyeye olgunlaşması için birkaç yıl alacaktır. Aşağıdaki şemada, herhangi bir kuruluş kendi Emniyet Yönetim Sistemini (SMS) uyguladıkça ve geliştirdikçe ulaşılan Emniyet Yönetim Sisteminin (SMS) farklı seviyeleri ile hizmet sağlayıcısının Emniyet Yönetim Sistemi (SMS) olgunluğu karşısında göstergelerin değerlendirmeye tabi tutulması için aracın nasıl kullanıldığı gösterilmektedir.

Değerlendirme aracı, başlangıçta Emniyet Yönetim Sisteminin (SMS) temel unsurlarının mevcut ve uygun olup olmadığına bakan aşamalar halinde kullanılabilir. İleri bir aşamada, Emniyet Yönetim Sisteminin (SMS), ne kadar iyi çalışır ve etkin olduğunun yanı sıra en iyi uygulamayı benimseyip benimsemediği de değerlendirilebilir. Hizmet Sağlayıcıları, sürekli gelişim programları kapsamında daima mükemmeliyete ve değerlendirmeye tabi tutulacak en iyi uygulamaya imkan veren araca ulaşmaya gayret edebilirler. En iyi uygulama göstergeleri, SM ICG üyelerinin hizmet sağlayıcılarından edindikleri deneyimler ile belirlenmiştir.

Emniyet Yönetim Sistemi (SMS) Yolculuğu



1. EMNİYET POLİTİKASI VE HEDEFLERİ

1.1. YÖNETİMİN TAAHHÜDÜ VE SORUMLULUĞU

Kuruluş, ulusal ve uluslararası gereklilikler doğrultusunda olması gereken ve kuruluşun Sorumlu Yöneticisi tarafından imzalanacak emniyet politikasını belirleyecektir. Emniyet politikası, uygulanmasına yönelik gerekli insan kaynağının ve mali kaynakların sunumuna ilişkin açık bir beyanı da içerecek şekilde emniyete ilişkin olarak kuruluşun taahhütlerini yansıtacak ve görülür bir destek ile kuruluş genelinde duyurulacaktır. Emniyet politikası, emniyet raporlama prosedürlerini içerecek ve kabul edilemez davranış tiplerini açık bir şekilde belirtecek ve disiplin tedbirlerinin geçerli olmayacağı durumlara yer verecektir. Emniyet politikası, kuruluş ile ilgili ve kuruluşa uygun olmasının sağlanması amacıyla periyodik olarak gözden geçirilecektir.

ETKİNLİK, kuruluş tarafından kuruluşun amaçlarının, emniyet hedeflerinin ve felsefelerinin açıkça belirtildiği emniyet politikası tanımlandığında ve "teorinin pratiğe döküldüğü" ve örnek yoluyla ispatlanan emniyet liderliğine ve yönetimine dair görünür kanıt mevcut olduğunda edinilir.

UYUMLULUK + PERFORMANS GÖSTERGELERİ		P	S	O	E	Nasıl edinildi	Doğrulama
1.1.1	Sorumlu Yönetici tarafından imzalanmış, en yüksek emniyet standartlarına ulaşılmasına yönelik taahhüdü içeren bir emniyet politikası mevcuttur.						
1.1.2	Kuruluş, emniyet yönetim sistemini emniyet politikasına dayandırmıştır.						
1.1.3	Sorumlu Yönetici ile üst yönetim ekibi, emniyet yönetim sistemine faal ve görünür katılımı Emniyet Politikasına olan bağlılıklarını sergilemekte ve teşvik etmektedirler.						
1.1.4	Emniyete ilişkin bireysel katkılarının ve yükümlülüklerinin bilincinde olmalarını sağlamak amacıyla emniyet politikası tüm personele bildirilmektedir.						
1.1.5	Emniyet politikası, uygun kaynakları sunan ve emniyeti tüm Yöneticilerin birincil sorumluluk olarak tanımlayan tüm geçerli yasal şartlara, standartlara ve en iyi uygulamaya riayet edileceğine dair bir taahhüt içermektedir.						
1.1.6	Emniyet politikası emniyet raporlamasını faal bir şekilde teşvil etmektedir.						
1.1.7	Emniyet politikası, kuruluşun amaçlarını, emniyet prensiplerini ve emniyet seviyesinde sürekli gelişim taahhüdünü belirtmektedir.						
1.1.8	Güncel olduğundan emin olmak üzere emniyet politikası periyodik olarak gözden geçirilmektedir.						

1.1.9	Kuruluşun üst yönetiminin emniyet yönetim sisteminin geliştirilmesi ve sürekli iyileştirilmesi hususunda taahhüdü mevcuttur.						
1.1.10	Cezalandırmanın değerlendirilebileceği halleri (örneğin, yasadışı faaliyet, ihmal veya kasti suistimal) açık bir şekilde tanımlayan bir disiplin politikası tanımlanmıştır.						
1.1.11	Pozitif emniyet kültürünü yansıtan karar vermeye, eylemlere ve davranışlara dair kanıt mevcuttur.						
EN İYİ UYGULAMA GÖSTERGELERİ		P	S	O	E	Nasıl edinildi	Doğrulama
1.1.12	Tüm seviyelerdeki personel emniyet yönetim sisteminin oluşturulmasına ve sürdürülmesine müdahil olmaktadır.						
1.1.13	Kuruluş genelinde kullanılan tek bir havacılık emniyeti politikası mevcuttur ve bu politika, kuruluşun tüm seviyelerinde yürütülmektedir.						
1.1.14	Emniyet politikası tüm personel için açık bir şekilde görünür veya mevcut olup, temel dokümantasyon ve haberleşme ortamında emniyet politikasına yer verilmiştir.						
1.1.15	Emniyet politikası hedefleri, kuruluşun amaç ve misyon beyanlarını yönlendirmektedir.						
1.1.16	Kuruluş, kuruluş genelindeki personelin söz konusu politikayı ve mesajını bildiklerini ve anlamış olduklarını düzenli olarak doğrulamaktadır.						
1.1.17	Sorumlu Yönetici, eğitimlere ve/veya emniyet konferanslarına katılarak taahhüdünü kanıtlamaktadır.						
1.1.18	Üst yönetim, yayınlanmış ve ölçülebilir emniyet hedefleri ve amaçlarıyla entegre bir emniyet planlama süreci benimsemiştir.						
1.1. ÖZET AÇIKLAMALAR							

1.2. EMNİYET SORUMLULUKLARI

Kuruluş, diğer görevlerine bakılmaksızın, Emniyet Yönetim Sisteminin (SMS) uygulanması ve sürdürülmesi için kuruluş hesabına nihai sorumluluğa ve mesuliyyete sahip olacak Sorumlu Yöneticiyi belirleyecektir. Kuruluş ayrıca, diğer görevlerine bakılmaksızın tüm üst yönetim üyelerinin ve personelin Emniyet Yönetim Sisteminin (SMS) emniyet performansına ilişkin emniyet mesuliyetlerini belirleyecektir. Emniyet sorumlulukları, mesuliyetleri ve yetkileri dokümente edilecek ve kuruluş genelinde bildirilecek ve emniyet riski tolere edilebilirliğine ilişkin olarak karar verme yetkisine sahip olan yönetim seviyelerinin bir tanımını içerecektir.

ETKİNLİK, Emniyet Yönetim Sistemine (SMS) ilişkin nihai mesuliyyete sahip olan sorumlu şahıs da dahil olmak üzere kuruluş genelinde emniyet mesuliyetlerine ilişkin açık hatlar mevcut olduğunda ve kuruluşun karşılaştığı riskler Sorumlu Yönetici ile yönetim ekibi tarafından tamamen idrak edildiğinde edinilir.

UYUMLULUK GÖSTERGELERİ	PERFORMANS	P	S	O	E	Nasıl edinildi	Doğrulama
1.2.1	Düzgün bir şekilde uygulandığından ve etkin bir performans sergilediğinden emin olmak üzere, Emniyet Yönetim Sistemine (SMS) ilişkin tam sorumluluğa ve nihai mesuliyyete sahip olan bir Sorumlu Yönetici tayin edilmiştir.						
1.2.2	Sorumlu Yönetici, etkin bir Emniyet Yönetim Sisteminin (SMS) düzgün bir şekilde uygulanması için gerekli olan mali kaynakların ve insan kaynaklarının kontrolüne sahiptir.						
1.2.3	Sorumlu Yönetici, kuruluşun emniyet politikasına, emniyet standartlarına ve emniyet kültürüne ilişkin Emniyet Yönetim Sistemi (SMS) görev ve sorumluluklarının bütünüyle bilincindedir.						
1.2.4	Emniyet mesuliyetleri, yetkileri ve sorumlulukları kuruluş genelinde tanımlanmış ve dokümente edilmiştir.						
1.2.5	Tüm seviyelerdeki personel, tüm emniyet yönetimi süreçlerine, kararlarına ve eylemlerine ilişkin emniyet mesuliyetlerini, yetkilerini ve sorumluluklarını bilmekte ve idrak etmektedir.						
1.2.6	Emniyet yönetimi kuruluş genelinde paylaşılmaktadır (ve sadece Emniyet Yöneticisi ile ekibinin sorumluluğu değildir).						
1.2.7	Tüm personel için görev tanımları ile dokümente edilmiş yönetim organizasyon şemaları mevcuttur.						

EN İYİ UYGULAMA GÖSTERGELERİ		P	S	O	E	Nasıl edinildi	Doğrulama
1.2.8	Emniyet Yönetim Sisteminin (SMS) oluşturulmasına ve işletilmesine personelin katıldığına ve bu hususta personel ile istişare edildiğine dair kanıt mevcuttur.						
1.2.9	Emniyet yönetim sistemi prensiplerinin kuruluşun tüm seviyelerine nüfuz ettiğine ve emniyetin günlük lisanın bir parçası olduğuna dair kanıt mevcuttur.						
1.2.10	Kuruluş bünyesindeki emniyet mesuliyetleri açık bir şekilde dokümente edilmiştir ve bireyler kendi mesuliyetlerini imzalamaktadırlar.						
1.2.11	Temel emniyet işlemleri üst yönetim görevlerinde ve sorumluluklarında açık bir şekilde tarif edilmiş ve personel performans hedeflerine dahil edilmiştir.						
1.2.12	Üst yönetimin kuruluşun tüm seviyelerinden katkıların önemini bildiğine ve bu katkıların kabulüne yönelik bir mekanizmaya sahip olduğuna dair kanıt mevcuttur.						
1.2. ÖZET AÇIKLAMALAR							

1.3. KİLİT PERSONEL TAYİNİ

Kuruluş, etkin bir Emniyet Yönetim Sisteminin (SMS) uygulanması ve sürdürülmesi için sorumlu kişi ve merkez noktası olacak olan bir Emniyet Yöneticisi belirleyecektir.

ETKİNLİK, Emniyet Yönetim Sistemi (SMS) sorumlu kişi tarafından kolaylaştırıldığında ve kuruluşun çeşitli operasyon sahalarından kilit personelin emniyet yapısı mevcut olduğunda edinilir. İş sahası yöneticileri emniyet yönetim sistemine faal bir şekilde katılırlar.

UYUMLULUK + PERFORMANS GÖSTERGELERİ		P	S	O	E	Nasıl edinildi	Doğrulama
1.3.1	Emniyet Yönetim Sisteminin (SMS) işleyişini yönetmek üzere uygun bilgiye, becerilere ve tecrübeye sahip olan yetkin bir kişi tayin edilmiştir.						
1.3.2	Emniyet Yönetim Sisteminin (SMS) işleyişini yöneten kişi gerekli iş görevlerini ve sorumluluklarını yerine getirmektedir.						
1.3.3	Emniyet Yöneticisi ile Sorumlu Yönetici arasında doğrudan raporlama hattı mevcuttur.						
1.3.4	Kuruluş tarafından, emniyet soruşturmasına, analizine, denetimine ve teşvikine yönelik iş gücü de dahil olmak üzere, Emniyet Yönetim Sistemini (SMS) yönetmeye yeterli kaynak tahsis edilmiştir.						
1.3.5	Önemli emniyet görevlerindeki personel, ilave eğitim ve konferans ve seminerlere katılımla güncel tutulmaktadır.						
EN İYİ UYGULAMA GÖSTERGELERİ		P	S	O	E	Nasıl edinildi	Doğrulama
1.3.6	Kuruluş, tüm üst yönetim temsilcileri de dahil olmak üzere, söz konusu kuruluşun boyutuna ve karmaşıklığına uygun olan yapılandırılmış bir emniyet kurulu veya böyle bir kurulun muadilini tesis etmiştir.						
1.3.7	Emniyet Kurulu veya muadili, operasyonların emniyet performansını ve Emniyet Yönetim Sisteminin (SMS) etkinliğini izler ve bu kurula genellikle Sorumlu Yönetici başkanlık eder.						
1.3.8	Emniyet Yönetim Sisteminin yönetilmesinden ve sürdürülmesinden sorumlu olan kişiye/kişilere kuruluştaki kuruluş bünyesinde emniyet görevinin önemini yansıtan uygun bir statü verilir.						
1.3.9	Emniyet kuralları, paydaşları ve önemli anlaşmalı kuruluşları da kapsar.						
1.3.10	Emniyet kuralları emniyet konularına odaklanır ve tüm katılımcılar eksiksiz olarak katılım sağlar.						
1.3. ÖZET AÇIKLAMALAR							

1.4. ACİL DURUM EYLEM PLANLAMASININ KOORDİNASYONU

Kuruluş, normal operasyonlardan acil durum operasyonlarına düzenli ve etkin bir şekilde geçilmesini ve normal operasyonlara dönüşün hizmetlerin sunulması sırasında etkileşim içerisinde olması gereken diğer kuruluşların acil durum eylem planları ile koordinasyon içerisinde yürütülmesini sağlayan bir acil durum eylem planı oluşturacaktır.

ETKİNLİK, söz konusu kuruluş kendisine uygun olan ve icabında diğer kuruluşlar ile koordinasyon da dahil olmak üzere düzenli bir şekilde teste tabi tutulan ve güncellenen bir acil durum eylem planına sahip olduğunda edinilir.

UYUMLULUK + PERFORMANS GÖSTERGELERİ		P	S	O	E	Nasıl edinildi	Doğrulama
1.4.1	Operasyonun boyutunu, mahiyetini ve karmaşıklığını yansıtan bir acil durum eylem planı (ERP) oluşturulmuştur ve çeşitli kuruluşların ve kilit personelin prosedürlerini, görevlerini, sorumluluklarını ve eylemlerini tanımlamaktadır.						
1.4.2	Kilit personel herhangi bir acil durum halinde Acil Durum Eylem Planına (ERP) daima kolaylıkla erişim imkanına sahiptir.						
1.4.3	Kuruluş, Acil Durum Eylem Planı (ERP) prosedürlerinin dağıtılmasına ve içeriğin tüm personele iletilmesine yönelik bir süreçte sahiptir.						
1.4.4	Acil Durum Eylem Planı (ERP) planının yeterliliği bakımından periyodik olarak teste tabi tutulur ve etkinliğin geliştirilmesi için sonuçlar gözden geçirilir.						
EN İYİ UYGULAMA GÖSTERGELERİ		P	S	O	E	Nasıl edinildi	Doğrulama
1.4.5	Kuruluş, karşılıklı yardım ve acil durum hizmetlerinin sunulması için diğer kuruluşlarla Mutabakat Anlaşmalarına (MoU'lar) veya anlaşmalara sahiptir.						
1.4.6	Kuruluş, kendi personeli için Kritik Olay Stres Yönetimi uygulamıştır.						
1.4. ÖZET AÇIKLAMALAR							

1.5. SMS DOKÜMANTASYONU

Kuruluş, emniyet politikasını ve hedeflerini, SMS gerekliliklerini, SMS süreçlerini ve prosedürlerini, bu süreçlere ve prosedürlere ilişkin mesuliyetleri, sorumlulukları ve yetkileri ve SMS çıktılarını tanımlayan SMS dokümantasyonunu oluşturacak ve muhafaza edecektir. Kuruluş, SMS dokümantasyonu mevcut kuruluş dokümantasyonunun bünyesine dahil edebilir veya kuruluş genelinde emniyet yönetimine yönelik yaklaşımını duyurmak için bir emniyet yönetim sistemi el kitabı (SMSM) oluşturabilir ve muhafaza edebilir.

ETKİNLİK, söz konusu kuruluş, kuruluş genelinde kullanılan ve düzenli olarak gözden geçirilerek güncellenen, emniyet yönetimine yönelik yaklaşımını tanımlayan SMS dokümantasyonuna sahip olduğunda edinilir. Dokümantasyon, kuruluşun emniyet hedeflerini karşılar.

UYUMLULUK + PERFORMANS GÖSTERGELERİ		P	S	O	E	Nasıl edinildi	Doğrulama
1.5.1	Emniyet yönetim sistemini ve tüm unsurları arasındaki karşılıklı ilişkileri tanımlayan dokümantasyon mevcuttur.						
1.5.2	SMS dokümantasyonu, uygulanan uygun versiyon kontrolü ile düzenli olarak gözden geçirilerek güncellenir.						
1.5.3	SMS dokümantasyonu halihazırda tüm personele temin edilmiştir.						
1.5.4	SMS dokümantasyonu, SMS ile ilgili diğer kayıtların saklanmasıyla ilişkin yöntemleri detaylandırır ve referans verir.						
EN İYİ UYGULAMA GÖSTERGELERİ		P	S	O	E	Nasıl edinildi	Doğrulama
1.5.6	Emniyet yönetim süreçleri mevcut organizasyonel el kitaplarına entegre edilir.						
1.5.7	Kuruluş, gerek kurumsal gerekse de operasyonel seviyede dokümantasyonun teslimatı için en uygun ortamı analiz etmiştir ve kullanmaktadır.						
1.5. ÖZET AÇIKLAMALAR							

2. EMNİYET RİSKİ YÖNETİMİ

2.1. TEHLİKE TANIMLAMA

Kuruluş, havacılık emniyeti tehlikelerinin tanımlanmasını sağlayan resmi bir süreç geliştirecek ve muhafaza edecektir. Potansiyel tehlikelerin saptanması için olay ve kazaların soruşturulması buna dahil olmalıdır. Tehlike tanımlama, reaktif, proaktif ve kestirimci emniyet verileri toplama yöntemlerinin kombinasyonuna dayalı olacaktır.

ETKİNLİK, kuruluş genelinde havacılık emniyeti tehlikeleri saptandığında rapor edildiğinde edinilir. Tehlikeler, tehlike kayıt defterine işlenir ve sistematik ve vakitli bir şekilde değerlendirmeye tabi tutulur.

UYUMLULUK + PERFORMANS GÖSTERGELERİ	P	S	O	E	Nasıl edinildi	Doğrulama
2.1.1						
2.1.2						
2.1.3						
2.1.4						
2.1.5						
2.1.6						
2.1.7						
2.1.8						
2.1.9						
2.1.10						

2.1.11	Kuruluş, sistemde tehlike tanımlama için kaynak olarak olay ve kaza soruşturma sonuçlarından yararlanmaktadır.						
--------	----------------------------------------------------------------------------------------------------------------	--	--	--	--	--	--

EN İYİ UYGULAMA GÖSTERGELERİ		P	S	O	E	Nasıl edinildi	Doğrulama
2.1.12	Ortalama olarak yılda kişi başına 1 raporun üzerinde olan raporlama seviyesiyle gösterilen faal bir raporlama sistemi mevcuttur.						
2.1.13	Emniyet Raporlarında, raporlamada bulunanın kendi hataları ile raporlamada bulunanın normalde raporlama yapmayacağı olaylar (izleyen kimsenin olmadığı olaylar) yer almaktadır.						
2.1.14	Raporlama sistemi, personele, önleyici ve düzeltici faaliyet önerilerinde bulunma yetkisi vermektedir.						
2.1.15	Raporlama sisteminin kuruluşun tümü genelinde (her departmanda ve her lokasyonda) faal bir şekilde kullanılmakta olduğuna dair kanıt mevcuttur.						
2.1.16	Raporlama sistemi, raporlamada bulunmak üzere anlaşmalı kuruluşlara ve müşterilere açıktır.						
2.1.17	Eğilimleri incelemek ve kullanılabilir yönetim bilgileri kazanmak üzere raporların ve tehlike kayıt defterlerinin analizi için uygulanan bir süreç mevcuttur.						

2.1. ÖZET AÇIKLAMALAR

2.2. RİSK DEĞERLENDİRME VE AZALTMA

Kuruluş, operasyonlardaki emniyet risklerinin analizini, değerlendirilmesini ve kabul edilebilir bir seviyede kontrol edilmesini sağlayan resmi bir süreç oluşturacak ve sürdürecektir.

ETKİNLİK, operasyonlardaki emniyet risklerinin analizini, değerlendirilmesini ve kabul edilebilir bir seviyede kontrol edilmesini sağlayan resmi bir süreç mevcut olduğunda edinilir.

UYUMLULUK + PERFORMANS GÖSTERGELERİ		P	S	O	E	Nasıl edinildi	Doğrulama
2.2.1	Etki ve olasılık bakımından ifade edilen, tanımlanan tehlikelere ilişkin riskin değerlendirilmesini içeren risk yönetim sürecine yönelik yapılandırılmış bir süreç mevcuttur.						
2.2.2	Kuruluşun kabul etmeye istekli olduğu risk seviyesinin değerlendirilmesine yönelik kriter mevcuttur.						
2.2.3	Kuruluş, tehlikenin giderilmesini, risk kontrolünü, riskten kaçınmayı, risk kabulünü, risk azaltmayı ve icabında eylem planını içeren risk kontrol stratejilerine sahiptir.						
2.2.4	Vakitlilik ve sorumlulukların dağıtılması dahil olmak üzere, risk değerlendirmesinden kaynaklanan hafifletici tedbirler belgelendirilmektedir.						
2.2.5	Risk yönetimi, karar verme süreçlerinde rutin olarak uygulanmaktadır.						
2.2.6	Etkin ve güçlü hafifletmeler ve kontroller uygulanmaktadır.						
2.2.7	Risk değerlendirmeleri ve risk derecelendirmeleri uygun bir şekilde gerçekleştirilmektedir.						
2.2.8	Üst yönetim orta ve yüksek risk tehlikeleri ile bunların azaltımını ve kontrollerini görmektedir.						

EN İYİ UYGULAMA GÖSTERGELERİ		P	S	O	E	Nasıl edinildi	Doğrulama
2.2.9	Risklerin makul çerçevede pratikte düşük olarak yönetilmekte olduğuna dair kanıt mevcuttur.						
2.2.10	Kuruluş, risk yönetimi sonuçlarını sektör ile paylaştığı en iyi uygulama esaslarını geliştirmek için kullanmaktadır.						

2.2.11	Risk yönetim süreçleri periyodik esasta gözden geçirilir ve iyileştirilir.						
2.2. ÖZET AÇIKLAMALAR							

3. EMNİYET GÜVENCE

3.1. EMNİYET PERFORMANSI TAKİBİ VE ÖLÇÜMÜ

Kuruluş, kuruluşun emniyet performansını doğrulamak ve emniyet riski kontrollerinin etkinliğini onaylamak üzere yöntemler geliştirecek ve muhafaza edecektir. Kuruluşun emniyet performansı, Emniyet Yönetim Sisteminin (SMS) emniyet performansı göstergelerine ve emniyet performansı hedeflerine göre doğrulanacaktır.

ETKİNLİK, kuruluş tarafından operasyon tipine uygun olan bir dizi emniyet performans göstergesi oluşturulduğunda edinilir. Eğilimlerin ölçülmesine ve takip edilmesine ve gerektiğinde uygun tedbirin alınmasına yönelik bir yöntem mevcuttur.

UYGUNLUK + PERFORMANS GÖSTERGELERİ		P	S	O	E	Nasıl edinildi	Doğrulama
3.1.1	Emniyet hedefleri tesis edilmiştir.						
3.1.2	Emniyet performans göstergeleri tanımlanmış, ilan edilmiş olup, eğilimler için takip ve analiz edilmektedir.						
3.1.3	İşler ve etkin olduklarını teyit etmek üzere risk azaltımı ve kontrolleri doğrulanmakta/denetime tabi tutulmaktadır.						
3.1.4	Kuruluşun emniyet performansına ve hizmetlerine odaklanan ve normal operasyonları değerlendirmeye tabi tutan emniyet denetimleri yürütülmektedir.						
3.1.5	Emniyet hedefleri ve performans göstergeleri periyodik olarak gözden geçirilmekte ve güncellenmektedir.						
3.1.6	Emniyet hedefleri ve amaçları spesifik, ölçülebilir, kabul edilmiş, ilgili ve zamana dayalıdır.						
3.1.7	Emniyet güvenceden ve uyum takip işlemlerinden elde edilen bilgiler emniyet risk yönetimi süreçlerine geri besleme yapmaktadır.						
3.1.8	Emniyet güvence, anlaşmalı kuruluşlar tarafından uygulananlar da dahil olmak üzere risk kontrollerinin etkinliğini takip edecektir.						

EN İYİ UYGULAMA GÖSTERGELERİ		P	S	O	E	Nasıl edinildi	Doğrulama
3.1.9	Kuruluş halihazırdaki, gelecekteki ve üçüncü taraf emniyet risklerini takip etmekte ve kabul edilemez emniyet risklerini ele almak üzere tedbir almaktadır.						
3.1.10	Hedefleri ve performans göstergelerini belirlerken ve gözden geçirirken, kuruluş, tehlikeleri ve riskleri, finansal, operasyonel ve ticari gereklilikleri, ilgili tarafların görüşünü göz önünde bulundurmaktadır.						
3.1.11	Emniyet hedefleri ve performans göstergeleri kuruluşun tüm alanlarını kapsamaktadır.						
3.1.12	Emniyet risk profilinde saptanan ciddi emniyet riskleri için performans ölçümleri tanımlanmıştır.						
3.1.13	Tüm seviyelerdeki personel kendi sorumluluk alanlarındaki emniyet performansı ölçümlerinden haberdardır ve performans ölçümlerinin sonuçları kendilerine iletilmektedir.						
3.1.14	Emniyet performans göstergeleri kuruluşun emniyet hedefleri ile bağlantılı olup, uygun olduğu hallerde Devlet Emniyet Performans Göstergeleri (SPI'ler) dikkate alınmaktadır.						
3.1.15	Kaynakların analizi ve tahsisatı performans ölçümünden kaynaklanan çıktılara dayalıdır.						
3.1. ÖZET AÇIKLAMALAR							

3.2. DEĞİŞİKLİĞİN YÖNETİMİ

Kuruluş, kuruluş ve operasyonu dahilinde gerçekleşen, tesis edilmiş süreçlere ve hizmetlere etki edebilecek değişikliklerin saptanmasına, değişikliklerin uygulanması öncesinde emniyet performansının sağlanmasına yönelik düzenlemelerin tanımlanmasına ve operasyon ortamındaki değişiklikler sebebiyle artık ihtiyaç duyulmayan emniyet riski kontrollerinin giderilmesine veya değiştirilmesine yönelik resmi bir süreç oluşturacak ve muhafaza edecektir.

ETKİNLİK, kuruluş tarafından söz konusu kuruluştaki ve operasyonlarındaki tüm büyük çaplı değişiklikleri proaktif bir şekilde değerlendirecek emniyet risk yönetim sistemi kullanıldığında edinilir.

UYUMLULUK + PERFORMANS GÖSTERGELERİ		P	S	O	E	Nasıl edinildi	Doğrulama
3.2.1	Kuruluş tarafından büyük çaplı operasyonel değişikliklere, büyük çaplı organizasyonel değişikliklere ve kilit personeldeki değişikliklere yönelik olarak bir süreç tesis edilmiş olup resmi tehlike analizleri ve risk değerlendirmeleri yapılmaktadır.						
3.2.2	Emniyet Olay/Risk değerlendirmeleri havacılık emniyetine odaklıdır.						
3.2.3	Değişim yönetim sürecine kilit paydaşlar da katılmaktadır.						
3.2.4	Değişim yönetim süreci sırasında olası etki bakımından önceki risk değerlendirmeleri ve mevcut tehlikeler gözden geçirilmektedir.						
EN İYİ UYGULAMA GÖSTERGELERİ		P	S	O	E	Nasıl edinildi	Doğrulama
3.2.5	Organizasyonel ve operasyonel değişikliklerin gerçekleşmesi sonrasında varsayımların geçerli olmaya devam ettiğini ve değişikliğin yürürlüğe girdiğini güvence altına almak üzere emniyet performansının onaylanması.						
3.2.6	Tüm organizasyonel ve operasyonel değişiklikler değişim yönetim sürecine tabidir.						
3.2.7	Emniyet mesuliyetleri, yetkileri ve sorumlulukları değişim kapsamında gözden geçirilir.						

3.2. ÖZET AÇIKLAMALAR

3.3. EMNİYET YÖNETİM SİSTEMİNİN (SMS) SÜREKLİ İYİLEŞTİRİLMESİ

Kuruluş, Emniyet Yönetim Sisteminin (SMS) standart altı performansının sebeplerinin saptanmasına, Emniyet Yönetim Sisteminin (SMS) standart altı performansının yansımalarının tespit edilmesine, operasyonlardaki standart altı performansın belirlenmesine ve bu sebeplerin giderilmesine veya hafifletilmesine yönelik resmi bir süreç oluşturacak ve bu süreci sürdürecektir.

ETKİNLİK, söz konusu kuruluş tarafından potansiyel iyileştirme alanlarını saptamak üzere Emniyet Yönetim Sistemi (SMS) performansı düzenli olarak takip edildiğinde ve bu sürecin sonucu emniyet yönetim sisteminde iyileştirmelere yol açtığıda edinilir.

UYUMULUK + PERFORMANS GÖSTERGELERİ		P	S	O	E	Nasıl edinildi	Doğrulama
3.3.1	Emniyet Kurulu, Emniyet Yönetim Sisteminin (SMS) iyileştirilmesine ve etkinliğine ilişkin kararların alınması hususunda gerekli yetkiye sahiptir.						
3.3.2	Emniyet Yönetim Sistemi (SMS), emniyet performansında yapılacak iyileştirmeler için periyodik olarak gözden geçirilir.						

EN İYİ UYGULAMA GÖSTERGELERİ		P	S	O	E	Nasıl edinildi	Doğrulama
3.3.3	Öğrenilen derslerin politikaya ve prosedürlere derç edildiğine dair kanıt mevcuttur.						
3.3.4	Kuruluş, kendi Emniyet Yönetim Sistemini diğer kuruluşlar karşısında karşılaştırarak değerlendirmekte ve havacılık sektörü dahilinde Emniyet Yönetim Sistemini faal bir şekilde teşvik etmektedir.						
3.3.5	En iyi uygulama aramakta ve benimsenmektedir.						
3.3.6	Organizasyonel kültüre yönelik etütler ve değerlendirmeler düzenli olarak yürütölmekte ve bunlara dayalı olarak hareket edilmektedir.						
3.3.7	Emniyet ile ilgili hizmetler için, kuruluş, mevzuat tarafından gerekli görölmeyen anlaşmalı kuruluşların Emniyet Yönetim Sistemine sahip olmasını öngörmektedir.						
3.3.8	Anlaşmalı kuruluşlar, Emniyet Yönetim Sistemine katılma ve bu sistemde bilgi paylaşma yeteneğine sahiptirler.						
3.3. ÖZET AÇIKLAMALAR							

4. EMNİYETİN TEŞVİK EDİLMESİ

4.1. EĞİTİM VE ÖĞRETİM

Kuruluş, personelin Emniyet Yönetim Sistemi görevlerini ifa etmek üzere eğitim görmesini ve yetkin olmasını sağlayan bir emniyet eğitimi programı geliştirecek ve sürdürecektir. Emniyet eğitiminin kapsamı bu eğitimin verileceği her bir kişinin Emniyet Yönetim Sistemine (SMS) katılım düzeyine uygun olacaktır.

ETKİNLİK, tüm personel Emniyet Yönetim Sistemi ile ilgili görevlerini ifa etmek üzere eğitim gördüğünde ve yetkin olduğunda ve söz konusu eğitim programı etkinliği bakımından takip edildiğinde ve güncellendiğinde edinilir.

UYUMLULUK + PERFORMANS GÖSTERGELERİ		P	S	O	E	Nasıl edinildi	Doğrulama
4.1.1	Personelin görevlerini ifa etmeye yetkin olmasını sağlayacak şekilde Emniyet Yönetimi eğitimi gerekliliklerinin saptanmasına yönelik belgelenmiş bir süreç mevcuttur.						
4.1.2	Eğitimin etkinliğinin ölçülmesine ve müteakip eğitimin iyileştirilmesi için uygun tedbirin alınmasına yönelik olarak uygulanan bir süreç mevcuttur.						
4.1.3	Bireyin yetkinliğini değerlendiren ve gerektiğinde uygun iyileştirici tedbir alan bir süreç mevcuttur.						
4.1.4	Eğitim, başlangıç ve yenileme eğitimini içermektedir.						
4.1.5	Eğitime tabi tutulan tüm personel için bir eğitim kaydı muhafaza edilir.						

EN İYİ UYGULAMA GÖSTERGELERİ		P	S	O	E	Nasıl edinildi	Doğrulama
4.1.6	Eğitim, insan hatasının azaltılması amacıyla teknik olmayan beceriler de dahil olmak üzere insan faktörleri ile organizasyonel faktörleri içermektedir.						
4.1.7	Eğitim gerekliliklerinin mevzuat kapsamında tanımlanmadığı alanlar da dahil olmak üzere, kuruluş bünyesindeki her bir faaliyet alanı için eğitim gereklilikleri dokümente edilmektedir.						
4.1.8	Tüm personel için bir eğitim ihtiyaçları analizi yürütülmekte ve düzenli olarak gözden geçirilmektedir.						
4.1.9	Operasyon ile ilgili anlaşmalı kuruluşlar için çalışan personele eğitim sağlanmaktadır.						

4.1.10	Personel, Emniyet Yönetim Sistemindeki (SMS) görevlerine ilişkin olarak ilave Emniyet Yönetim Sistemi (SMS) eğitimi talep etmek üzere bir mekanizmaya sahiptir.						
4.1.11	Yönetim, emniyet yönetimi konusunda tüm personele eğitim vermenin önemini bilmekte ve bu hususta resmi olmayan fırsatlardan yararlanmaktadır.						
4.1.12	Eğitim, sempozyumlara ve sektör konferanslarına katılımı kapsamaktadır.						
4.1.13	Tüm personele ilişkin eğitim egzersizleri ve yöntemleri yeni teknikleri, teknolojileri, soruşturma sonuçlarını, düzeltici faaliyetleri ve mevzuat değişikliklerini yansıtmak üzere güncel tutulmaktadır.						

4.2. EMNİYET İLETİŞİMİ

Kuruluş, emniyet iletişimine yönelik olarak, tüm personelin Emniyet Yönetim Sistemi (SMS) konusunda tamamen bilinçli olmasını, emniyet açısından kritik bilgilerin iletilmesini ve emniyete ilişkin belirli tedbirlerin alınmasının nedenlerini ve emniyet prosedürlerinin uygulamaya konulmasının ve bunlar üzerinde değişiklik yapılmasının nedenlerinin açıklanmasını sağlayacak resmi bir yöntem geliştirecek ve sürdürecektir.

ETKİNLİK, tüm personel, Emniyet Yönetim Sistemi (SMS), emniyet açısından kritik bilgiler ve havacılık emniyetindeki rolleri bakımından bilinçli olduğunda edinilir.

UYUMLULUK + PERFORMANS GÖSTERGELERİ		P	S	O	E	Nasıl edinildi	Doğrulama
4.2.1	Emniyet planları ve stratejileri kuruluş bünyesindeki tüm personele bildirilmektedir.						
4.2.2	Kuruluş ile ilgili önemli olaylar ve soruşturma sonuçları, uygun olduğunda anlaşmalı kuruluşlar da dahil olmak üzere, tüm personele bildirilmektedir.						

EN İYİ UYGULAMA GÖSTERGELERİ		P	S	O	E	Nasıl edinildi	Doğrulama
4.2.3	Elektronik haberleşmeyi, sıkça gerçekleştirilen toplantıları, Emniyet Yönetim Sistemi (SMS) ödül sistemlerini, çalışan tanıma sistemini, Emniyet Yönetim Sistemi (SMS) bültenlerini vb. içeren bir emniyet iletişim stratejisi mevcuttur.						

4.2.4	Harici kaynaklardan gelen önemli olaylar ve soruşturma sonuçları, uygun olduğunda anlaşmalı kuruluşlar da dahil olmak üzere, tüm personele bildirilmektedir.						
4.2.5	Emniyet iletişiminin etkinliği düzenli olarak değerlendirilmekte olup, strateji gerektiği şekilde revize edilmektedir.						
4.2.6	Emniyet ile ilgili bilgiler diğer taraflarla proaktif bir şekilde paylaşılır.						
4.2. ÖZET AÇIKLAMALAR							

Bu doküman, Emniyet Yönetimi Uluslararası İşbirliği Grubu (SM ICG) tarafından oluşturulmuştur. Emniyet Yönetimi Uluslararası İşbirliği Grubu'nun (SM ICG) amacı, Emniyet Yönetim Sistemi (SMS)/Devlet Emniyet Programı (SSP) esaslarının ve gerekliliklerinin uluslararası havacılık topluluğu genelinde uygulanmalarını kolaylaştırarak, söz konusu esaslara ve gerekliliklere yönelik ortak bir anlayışı teşvik etmektir.

Emniyet Yönetimi Uluslararası İşbirliği Grubu'nun (SM ICG) halihazırdaki esas üyeleri arasında, Brezilya Ulusal Sivil Havacılık Ajansı (ANAC), Hollanda Sivil Havacılık Otoritesi (CAA NL), Yeni Zelanda Sivil Havacılık Otoritesi, Avustralya Sivil Havacılık Emniyeti Otoritesi (CASA), Fransa Sicil Havacılık Genel Müdürlüğü (DGAC), Avrupa Havacılık Emniyeti Ajansı (EASA), İsviçre Federal Sivil Havacılık Dairesi (FOCA), Japonya Sicil Havacılık Bürosu (JCAB), Birleşik Devletler Federal Havacılık İdaresi (FAA) Havacılık Emniyeti Kuruluşu, Kanada Ulaştırma Bakanlığı Sivil Havacılık Otoritesi (TCCA) ve Birleşik Krallık Sivil Havacılık Otoritesi (UK CAA) yer almaktadır. Bunlara ek olarak; Uluslararası Sivil Havacılık Teşkilatı (ICAO), bu gruba yönelik gözlemci görevini üstlenmektedir.

Emniyet Yönetimi Uluslararası İşbirliği Grubu (SM ICG) üyeleri:

- Kendilerini ilgilendiren ortak Emniyet Yönetim Sistemi (SMS)/Devlet Emniyet Programı (SSP) ile ilgili konularda işbirliği yapmakta,
- Öğrenilen dersleri paylaşmakta,
- Uyumlu hale getirilmiş bir Emniyet Yönetim Sisteminin (SMS) gelişimini teşvik etmekte,
- Sonuçları/Ürünleri havacılık camiası ile paylaşmakta,
- Uluslararası Sivil Havacılık Teşkilatı (ICAO) ve Emniyet Yönetim Sistemini (SMS) ve Devlet Emniyet Programını (SSP) uygulamış veya uygulamakta olan sivil havacılık otoriteleri gibi uluslararası kuruluşlar ile işbirliği içerisinde oldukları.

SM ICG, değerlendirme aracına veya söz konusu aracın uygulanmasına ilişkin her nevi geri bildirimini memnuniyetle karşılamaktadır.

SM ICG hakkında daha fazla bilgi veya değerlendirme aracına ilişkin geri bildirim için lütfen aşağıdaki detaylar doğrultusunda temas kurunuz:

Regine Hamelijck, SM ICG Başkanı	Jacqueline Booth	Amer Younossi
Avrupa Havacılık Emniyeti Ajansı (EASA)	Kanada Ulaştırma Bakanlığı Sivil Havacılık Otoritesi (TCCA)	Birleşik Devletler Federal Havacılık İdaresi (FAA) Havacılık Emniyeti
+49 221 899 90 5064	(613) 952-7974	(202) 267-5164
regine.hamelijck@easa.europa.eu	jacqueline.booth@tc.gc.ca	amer.m.younossi@faa.gov
Carlos Eduardo Pellegrino	Wayne Jones	
Brezilya Ulusal Sivil Havacılık Ajansı (ANAC)	Avustralya Sivil Havacılık Emniyeti Otoritesi (CASA)	
+55 213 5015 444	+61 7 3144 7494	
sso@Anac.gov.br	jones@casa.gov.au	

BÖLÜM 2

Emniyet Performans Ölçümüne Ortak Yaklaşım

Bu doküman, Emniyet Yönetimi Uluslararası Grubunun (SM ICG) Ölçümler Çalışma Grubu tarafından hazırlanmıştır. Emniyet Yönetimi Uluslararası İşbirliği Grubu'nun (SM ICG) amacı, Emniyet Yönetim Sistemi (SMS)/Devlet Emniyet Programı (SSP) esaslarının ve gerekliliklerinin uluslararası havacılık topluluğu genelinde uygulanmalarını kolaylaştırarak, söz konusu esaslara ve gerekliliklere yönelik ortak bir anlayışı teşvik etmektir.

Emniyet Yönetimi Uluslararası İşbirliği Grubu'nun (SM ICG) hali hazırdaki esas üyeleri arasında, Brezilya Ulusal Sivil Havacılık Ajansı (ANAC), Avustralya Sivil Havacılık Emniyeti Otoritesi (CASA), Avrupa Havacılık Emniyeti Ajansı (EASA), İsviçre Federal Sivil Havacılık Dairesi (FOCA), Birleşik Devletler Federal Havacılık İdaresi (FAA) Havacılık Emniyeti Kuruluşu, Uluslararası Sivil Havacılık Organizasyonu (ICAO), Kanada Ulaştırma Bakanlığı Sivil Havacılık Otoritesi (TCCA) ve Birleşik Krallık Sivil Havacılık Otoritesi (UK CAA) yer almaktadır.

Emniyet Yönetimi Uluslararası İşbirliği Grubunun (SM ICG) üyeleri:

- İlgili duyulan ortak Emniyet Yönetim Sistemi (SMS)/Devlet Emniyet Programı (SSP) konularına yönelik işbirliği kurmaktadırlar.
- Alınan dersleri paylaşmaktadırlar.
- Uyumlu hale getirilmiş bir Emniyet Yönetim Sisteminin (SMS) gelişimini teşvik etmekte,
- Ürünleri, sivil havacılık topluluğu ile paylaşmaktadırlar.
- ICAO ve Emniyet Yönetim Sistemini (SMS) uygulamış bulunan veya uygulamakta olan sivil havacılık otoriteleri gibi uluslararası kuruluşlar ile işbirliği yapmaktadır.

Emniyet Yönetimi Uluslararası İşbirliği Grubu (SM ICG) ile ilgili ayrıntılı bilgi almak için, lütfen aşağıda belirtilen kişilerle iletişim kurun:

Amer M.Younossi, SM ICG Başkanı

Federal Havacılık İdaresi

Havacılık Emniyeti

(202) 267-5164

Amer.M.Younossi@faa.gov

Charles Huber, SM ICG Başkan Vekili

Federal Havacılık İdaresi

Havacılık Emniyeti

(425) 917-6732

Charles.Huber@faa.gov

Not: Bu belgenin içeriği, 2010 yılında Montreal, Kanada'da düzenlenen ICAO Yüksek Düzey Emniyet Konferansına bir çalışma belgesi olarak sunulmuştur.

ÖZET

Bu belgenin amacı, emniyet performans ölçümüne yönelik ortak bir yaklaşıma ilişkin tartışmaya katkı sağlamaktır. Devlet seviyesindeki ve her bir hizmet sağlayıcı seviyesindeki emniyet performansı ölçümleri etkin emniyet yönetimi için elzemdir. Bu sadece esaslı bir emniyet yönetimi uygulaması olmayıp, ICAO bünyesinde önerilen sürekli izleme yaklaşımını (CMA) desteklemek için emniyet performans tedbirlerinin ve emniyet performans göstergelerinin (SPI'ler) oluşturulmasına yönelik bir metodolojiye de ihtiyaç duyulacaktır. Bu belgede, sistem davranışının üç katmanlık dayanağına dayalı olan bir emniyet ölçüm matrisi önerilecektir.

1. GİRİŞ

Etkin emniyet yönetimi ve karar alma süreci için emniyet performansı tedbirleri gereklidir. Ölçüm stratejisi, tek bir "sihirli sayıdan" ziyade bir dizi tedbir sunmalıdır. Bu tedbirler aynı zamanda interaktif olmalı, işaret ettikleri sistemlerin tüm yönlerini kapsamalı ve kritik sistem bileşenlerinin uygun işlemlerine dair göstergeler ile sistem arızalarını (örneğin, kazalar, olaylar, mevzuat ihlalleri) yansıtmalıdır.

Bu tür tedbirlerin nasıl geliştirileceğine dair rehberlik oluşturmak amacıyla, Emniyet Yönetimi Uluslararası İşbirliği Grubu (SM ICG) bünyesinde bir alt grup oluşturulmuştur. Bu belge söz konusu SM ICG çalışma grubu tarafından işbirliği içerisinde oluşturulmuştur.

SM ICG'nin amacı, emniyet performansı ölçümü kavramını uyumlaştırılmış bir şekilde etraflıca tanımlamaktır.

2. SİSTEM DAVRANIŞI VE EMNİYET PERFORMANSI ÖLÇÜMÜ

"Emniyetin" sözlük anlamına baktığımızda karşımıza sadece potansiyel zararın olmaması çıkacaktır. Bu, açıkçası, ulaşılamayacak bir hedeftir. Bununla birlikte, etki (zarar ölçüsü) ve olasılık (zarar görme ihtimali) bakımından standart risk tanımı bize kaza oranları gibi sonuçlar arasındaki korelasyona ve daha somut olarak kontrolümüz altında olabilecek ölçülebilir şeylere yönelik daha pratik bir temel vermektedir.

ICAO Doc 9859, *Emniyet Yönetimi El Kitabı (SMM)* emniyetin faydalı bir operasyonel tanımını vermektedir (paragraf 2.2.4) "Kişilerde veya mallarda oluşacak zarar olasılığının, tehlike tanımı ve emniyet riski yönetimine ilişkin sürekli bir süreç vasıtasıyla kabul edilebilir bir seviyeye indirilmesi veya bu seviyede veya daha alt bir seviyede tutulması".

Bu tanımdan emniyet ve emniyet performansı tedbirlerinin havacılık sistemlerinin emniyet riskini kabul edilebilir seviyelerde yönetme becerisine odaklanması gerektiği sonucu çıkmaktadır. Herhangi bir kazanın olasılığını veya gerçekleşen kazalarda ortaya çıkan şiddeti azaltabilecek sistem davranışlarını vurgulamamız halinde, tedbirlere yönelik anlamlı hedefleri daha iyi tanımlayabiliriz.

Emniyet yönetimine ilişkin kuralcı düzenleme sınırlamaları uluslararası olarak artarak kabul edilmektedir.¹ Performansa dayalı düzenleme yüksek sonuçlu operasyonlarda emniyet yönetimine yönelik etkin bir araç olarak değerlendirilmektedir. Performansa dayalı düzenleme sistem emniyet performansını değerlendirmek için ölçülebilir sonuçlara yoğunlaşmaktadır.

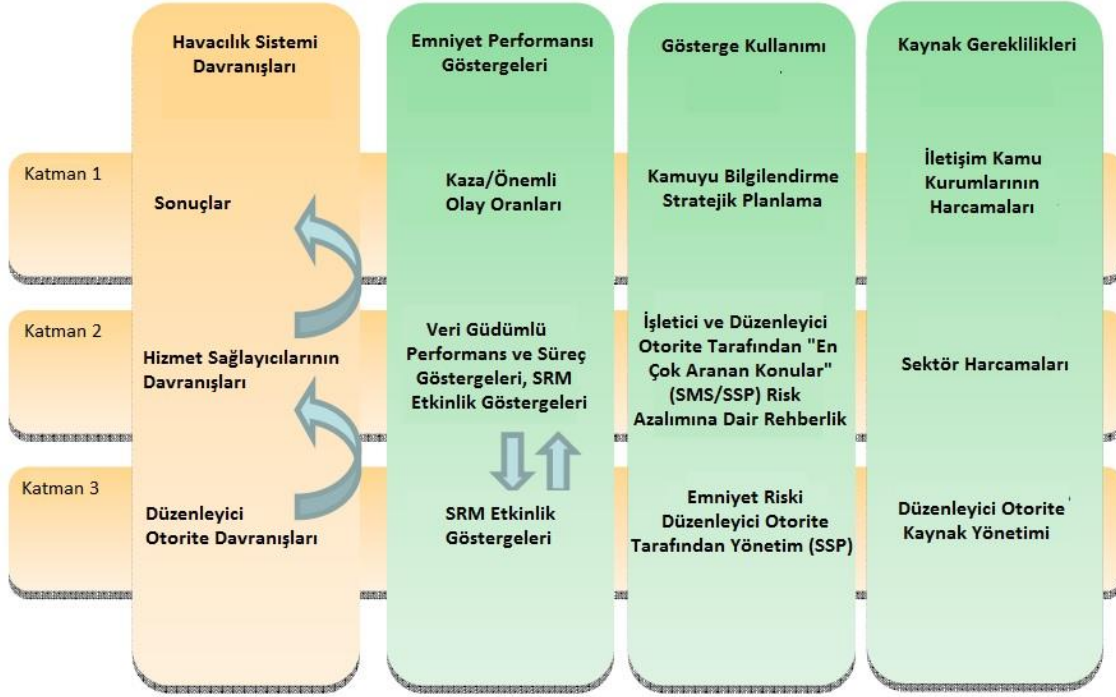
Performansa dayalı düzenleme uygulamak için emniyet performans göstergelerinin (SPI'ler) tanımlanması gerekmektedir. Böylelikle, uygun bir ölçülebilir Emniyet Performans Göstergesinin (SPI) tanımı düzenleyici otorite için önemli bir görev haline gelmektedir. Göstergenin kalitesi, uygulandığı konunun yanı sıra kullanımına bağlıdır.

¹ Kuralcı düzenlemeler, havacılık sistemindeki tehlikelere karşılık olarak kontrolleri gerekli görmektedir. Biri dizi esas tehlikeye işaret edilmesini sağlamaları sebebiyle önemli olmakla birlikte, havacılık sisteminde mevcut olabilecek tüm spesifik tehlikelere işaret edemezler.

3. EMNİYET ÖLÇÜM MATRİSİ - GENEL BAKIŞ

Matris, sistemin farklı seviyelerini tanımlayan üç katmandan ve emniyetin ölçülme ve yönetilme yolunu tanımlayan üç temel direkten oluşmaktadır.

Şekil 1: Emniyet ölçüm matrisi



Katmanlar havacılık sistemi davranışının farklı seviyelerini temsil etmektedir. 1. Katman, emniyet bakımından genel sistem davranışına, başka bir deyişle emniyet sonuçlarına bakmaktadır. 2. Katman, hizmet sağlayıcısının davranışlarına, 3. Katman ise düzenleyici otorite davranışına yoğunlaşmaktadır. Düzenleyici otoritenin davranışının, sırasıyla genel emniyet seviyesi üzerinde etkiye sahip olan hizmet sağlayıcısı davranışına etki etme amaçlı olması sebebiyle söz konusu üç katman birbirleriyle dikey olarak etkileşim halindedir.

Şekil 1'deki üç katman, her bir katmanda sistem davranışının nasıl ölçüldüğünün (emniyet performansı göstergeleri), göstergelerin nasıl kullanıldığının (gösterge kullanımı) ve diğer katmanların her birinde emniyetin ölçülmesi için hangi kaynak gerekliliklerinin yer aldığı tanımlanmasına yardımcı olur.

1. Katmandaki Emniyet Performansı Göstergeleri (SPI'ler) (sonuç göstergeleri) Devletler ve bölgeler genelinde büyük çaplı olarak uyumlaştırılabilir ve önsel tanımlanabilir. 2. ve 3. Katmandaki göstergeler bölgeye özgü olacak ve bölgesel veya ulusal duruma ve ilgili Devlet için geliştirilen SSP'ye bağlı olacaktır.

4. EMNİYET ÖLÇÜM MATRİSİ - EMNİYET PERFORMANSI GÖSTERGELERİ

Emniyet Performansı Göstergeleri (SPI'ler) basit, ölçülebilir ve güvenilir olmalıdır. Emniyet yönetimi için kullanılabilirliği için, sonuç göstergeleri (örneğin, kaza oranları) ile süreç göstergelerinin (örneğin, emniyet bakımından kritik süreçler, kayıt tutma ve personelin kalifikasyonu) bir karışımı mevcut olmalıdır. Emniyet ölçümünün bir şeyin yokluğunun ölçümü olmasına bağlı olarak süreç göstergeleri çok önemli bir unsurdur. Ortaya çıkan çıktının ölçülemediği bu gibi hallerde sektör standardı, bunun yerine dayanak süreçlerin onaylanması yönündedir.²

Kalitatif veriler karşısında kantitatif verilerin mevcut olması önemli bir kaygı teşkil etmektedir. Kantitatif veriler, ölçülmekte olan alanın daha açık bir resmini verirken, kantitatif verilerin edinilmesinin imkansız veya zor olduğu pek çok alan mevcuttur. Bu sebeple, bu yönler sadece ölçülebilir verilerin mevcut olmaması dolayısıyla hariç tutulmamalıdır. Çalışanların emniyet raporları ve kaza raporlarındaki derinlemesine etken analizleri gibi veri kaynakları genel olarak kalitatif olmakla birlikte tehlike tanımlaması için değerli olabilirler.

1. Katman Emniyet Performans Göstergeleri (SPI'ler), kaza verilerini (hasarlar, yaralanmalar, ölümcül olaylar) kapsamakta olup, bu veriler, yüksek düzeyde kamu yararını çeken gerçeklere dayalı verileri temsil etmektedir. Bununla birlikte, emniyet performansı ölçümü perspektifinden bir takım mülahazalar gözlemlenmelidir:

Ölümcül kaza oranları gibi 1. Katman göstergeleri uzun vadeli eğilim belirleme ve stratejik planlamaya uygulanan faktör analizi için çok uygundur. Bununla birlikte, bu olayların düşük sıklığına ve sonraki büyük değişimlere bağlı olarak münferit hizmet sağlayıcılarının performans ölçümü veya kısa vadeli eğilim belirleme için dikkatli bir şekilde kullanılmalıdırlar.

1. Katman göstergelerin bir diğer önemli potansiyel kaynağı da olay verileridir. Bununla birlikte, olay verilerinin kestirimci tedbirlerde kullanılmaları için ölümcül kazalara yol açan nedensel zincir ile ilişkilendirilmeleri gerekmektedir. Halihazırda pek çok türden tipik olarak düşük seviye olayın (örneğin, yerde oluşan hasar, uçuş sırasındaki türbülans yaralanmaları) ölümcül kaza oluşumunu yeterli bir şekilde tahmin edemeyebileceği geniş ölçüde kabul edilmektedir. Dayanak nedenler etraflıca analiz edilmediği sürece, küçük olaylara ilişkin kök nedenler daha ciddi olayların nedenleri ile yüksek ölçüde ilişkilendirilemez. Bu husus ayrıca, çalışan raporlaması ve uçuş veri analiz programları gibi kaynaklardan ilave olay verilerinin kullanılmasına yönelik ihtiyacı vurgulamaktadır.

² Örneğin. ISO 9001, 7.5.2 "Kuruluş, ortaya çıkan çıktının müteakip izleme ve ölçüm ile doğrulanamadığı hallerde üretime ve hizmet sunumuna ilişkin süreçleri onaylayacaktır."

2. Katman Emniyet Performans Göstergeleri (SPI'ler) havacılık hizmet sağlayıcılarına (örneğin, işleticiler, bakım kuruluşları, imalatçılar vb. dahil) işaret etmektedir. Bu seviye, aşağıdakiler gibi üç farklı Emniyet Performans Göstergesi (SPI) tipi arasında ayırt edilebilir:

Veri güdümlü performans ve süreç göstergeleri 1. Katman Emniyet Performans Göstergelerini (SPI) başlangıç noktası olarak alırlar, ancak nedensel zinciri ana sonuçlardan daha aşağı düzeyde geliştirmişlerdir. Bu yaklaşımda, risk yönetimine ilişkin hedeflerin saptanması için ana kaza senaryolarının ve ilgili emniyet hususlarının belirlenmesi amaçlanmaktadır.

Senaryo bazlı göstergeler, potansiyel kaza senaryolarından türeyen tehlikeleri saptar ve bunları herhangi bir kazanın veya büyük çaplı olayın daha önce hiç yaşanmadığı emniyet performans göstergelerinin gelişiminde tatbik ederler. 2. ve 3. Katmanı etkilerler.

Risk hafifletme etkinliğini ölçen göstergeler hizmet sağlayıcısı seviyesini ölçer ("emniyet yönetimi etkinliği"). Ticari Havacılık Emniyet Ekibinin, Havacılık Emniyet Bilgileri Analizi ve Paylaşımının ve Avrupa Stratejik Emniyet İnisiyatifi tavsiyelerinin uygulanması bu yaklaşıma ilişkin örneklerdir.

3. Katman göstergeler, düzenleyici otorite tarafından uygulamaya konulan hafifletme tedbirlerinin etkinliğine bakar. Düzenleyici otoritenin emniyet tedbirlerinin, faaliyetlerinin ve inisiyatiflerinin emniyet hedeflerine ne ölçüde ulaştığını ölçerler. Emniyet sonuçları ve hizmet sağlayıcılarının davranışı tümüyle düzenleyici otoriteye yansır ve zinciri yukarıya doğru hareket ettirerek etkin düzenleyici otorite faaliyetlerinin hizmet sağlayıcı davranışlarını toplamda sonuçlarda genel iyileştirmelere yol açacak şekilde harekete geçirmesi gerekmektedir.

5. EMNİYET ÖLÇÜM MATRİSİ - GÖSTERGE KULLANIMI

Bu temel direkt, üç katmadaki Emniyet Performans Göstergelerinin (SPI'ler) ne için kullanılacağını tanımlamaktadır. Fiili kullanım, göstergelerin ne şekilde formüle edilmesi gerektiğine dair bilgi verebilir ve bu husustaki tartışmayı yönlendirebilir.

1. Katmandaki Emniyet Performans Göstergeleri (SPI'ler) ağırlıklı olarak stratejik planlama ve kamunun bilgilendirilmesi içindir. Kamu nezdindeki ana endişeyi teşkil eden, sistemin genel sonucunu tanımlarlar.

2. Katmandaki Emniyet Performans Göstergeleri (SPI'ler), eylemlerinde (SMS/SSP) kapsamında emniyet risklerini hafifletmek üzere hizmet sağlayıcılarına ve düzenleyici otoritelere rehberlik için kullanılırlar. Bu sebeple kaynak tahsisatı üzerinde etkiye de sahiptirler.

3. Katmandaki Emniyet Performans Göstergeleri (SPI'ler), düzenleyici otoritelere sürekli ve geleceğe dönük karar verme sürecine ilişkin rehberlik olarak SSP'lerinin performansı hakkında geri bildirim sunarlar. Ayrıca, CMA altında SSP'nin performansının ölçümüne ve izlenmesine yönelik süreçleri desteklerler.

6. EMNİYET ÖLÇÜM MATRİSİ - KAYNAK GEREKLİLİKLERİ

Her bir seviyede, emniyeti yönetmek için düzenleyici otorite veya hizmet sağlayıcısı tarafından temin edilen kaynaklar hazır bulundurulmalıdır. Bu temel direk, her bir katmanda performans ve emniyet davranışı üzerindeki etkiye ilişkin olarak kaynak tahsisatını ve önceliklendirmesini ele alır.

7. GİDİLECEK YOL

SM ICG üyeleri, her bir kuruluşla ilgili olan hizmet sağlayıcısı Emniyet Yönetim Sistemi (SMS) ile SSP'leri için emniyet performans göstergelerinin her bir Devlet tarafından belirlenmesi ihtiyacını duymuşlardır. Bu tedbirler ve göstergeler yukarıda tanımlanan emniyet matrisine uygun olarak geliştirilmelidir.

BÖLÜM 3

Risk Bazlı Karar Alma İlkeleri

Bu doküman, Emniyet Yönetimi Uluslararası İşbirliği Grubu'nun (SM ICG) Standardizasyon Çalışma Grubu tarafından hazırlanmıştır. Emniyet Yönetimi Uluslararası İşbirliği Grubu (SM ICG)'nin amacı, Emniyet Yönetim Sisteminin (SMS)/Devlet Emniyet Programının (SSP) ilkelerine ve gerekliliklerine ilişkin ortak bir anlayış geliştirerek bunların uluslararası havacılık camiası genelinde uygulanmalarını kolaylaştırmaktır.

Emniyet Yönetimi Uluslararası İşbirliği Grubu (SM ICG)'nin hâlihazırdaki esas üyeleri arasında İspanya Havacılık ve Emniyet Ajansı (AESA), Brezilya Ulusal Sivil Havacılık Ajansı (ANAC), Hollanda Sivil Havacılık Otoritesi (CAA NL), Yeni Zelanda Sivil Havacılık Otoritesi, Avustralya Sivil Havacılık Emniyeti Otoritesi (CASA), Fransa Sicil Havacılık Genel Müdürlüğü (DGAC), Avrupa Havacılık Emniyeti Ajansı (EASA), İsviçre Federal Sivil Havacılık Dairesi (FOCA), Japonya Sicil Havacılık Bürosu (JCAB), Birleşik Devletler Federal Havacılık İdaresi (FAA) Havacılık Emniyeti Kuruluşu, Kanada Ulaştırma Bakanlığı Sivil Havacılık Otoritesi (TCCA) ve Birleşik Krallık Sivil Havacılık Otoritesi (UK CAA) yer almaktadır. Bunlara ek olarak; Uluslararası Sivil Havacılık Teşkilatı (ICAO), bu gruba yönelik gözlemci görevini üstlenmektedir.

Emniyet Yönetimi Uluslararası İşbirliği Grubu (SM ICG) üyeleri:

- Kendilerini ilgilendiren ortak Emniyet Yönetim Sistemi (SMS)/Devlet Emniyet Programı (SSP) ile ilgili konularda işbirliği yapmakta,
- Öğrenilen dersleri paylaşmakta,
- Uyumlu hale getirilmiş bir Emniyet Yönetim Sisteminin (SMS) gelişimini teşvik etmekte,
- Sonuçları/Ürünleri havacılık camiası ile paylaşmakta,
- ICAO ve Emniyet Yönetim Sistemini (SMS) uygulamış bulunan veya uygulamakta olan sivil havacılık otoriteleri gibi uluslararası kuruluşlar ile işbirliği yapmaktadır.

Emniyet Yönetimi Uluslararası İşbirliği Grubu (SM ICG) ile ilgili ayrıntılı bilgi almak için, lütfen aşağıda belirtilen kişilerle iletişim kurun:

Regine Hamelijnck
Avrupa Havacılık Emniyeti
Ajansı (EASA)

+49 221 8999 1000
regine.hamelijnck@easa.europa.eu

Carlos Eduardo
Pellegrino Brezilya
Ulusal Sivil Havacılık
Ajansı (ANAC)
+55 213 5015 147
carlos.pellegrino@anac.gov.br

Jacqueline Booth
Kanada Ulaştırma
Bakanlığı Sivil Havacılık
Otoritesi (TCCA)

(613) 952-7974
jacqueline.booth@tc.gc.ca

Peter
Boyd
Avustralya
Sivil
Havacılık
Emniyeti
Otoritesi
(CASA)
+61 2 6217 1534
peter.boyd@casa.gov.au

Amer M.Younossi
Birleşik Devletler
Federal Havacılık
İdaresi (FAA) Havacılık
Emniyeti
(202) 267-5164
Amer.M.Younossi@faa.gov

YÖNETİCİ ÖZETİ

Bu doküman, risk bazlı karar alma sürecinin etkili olması için gerekli olan ilkeleri ortaya koymaktadır. Ayrıca, risk bazlı kararların alınması amacıyla veri kullanımına imkân verilmesi için gerekli olan uygun veri özniteliklerini tanımlamakta ve veri yönetimine yönelik hususları ortaya koymaktadır.

Emniyet yönetimi, dünya havacılık emniyetine ilişkin standart haline gelmektedir. Risk yönetimi, emniyet yönetiminin ana bileşenlerinden biri olup, tehlikelerin belirlenmesi, bu tehlikelerin sonuçları ile ilintili risklerin değerlendirilmesi ve risklerin hafifletilmesi etkili bir risk yönetimi sürecine ilişkin temel etmenleri oluşturmaktadır. Havacılık risk yönetiminde hem hizmet sağlayıcıların hem de düzenleyici otoritelerin görevleri vardır. Tehlikelerin ve süreçlerin niteliği ve kapsamı farklı olabilmekle birlikte her ikisinin de riski yönetmesi gerekmektedir. Örneğin; bir hizmet sağlayıcı, tehlikeleri kendi kuruluşu özelinde tanımlayabilirken bir otorite, tehlikeleri çeşitli sektörden elde edilen toplam verilere dayalı olarak tüm havacılık sistemi dahilinde ortaya çıkan trendlerden tanımlayabilmektedir.

İster Emniyet Yönetim Sistemi (SMS) ister Devlet Emniyet Programı (SSP) kapsamında oluşturulmuş olsun, iyi işleyen emniyet yönetim süreçleri, analizleri ve değerlendirmeleri destekleyen verilerin yanı sıra söz konusu veri süreçlerinin veri geçerliliği, tamlığı, vakitliliği, mevcudiyeti ve doğruluğu gibi belirli öznitelikleri taşıdığı garanti eden stratejilere de gereksinim duymaktadır. Ayrıca; emniyet yönetimi veriye dayalı bir sistem olduğu için, etkili bir veri yönetim sürecine bağlıdır. Veri yönetimi; bir kuruluşun, ihtiyaç duyduğu verilere sahip olduğunu ve verilerin düzenli, güvenilir ve uygun olduğunu temin eden süreçlerin ve prosedürlerin sürekli olarak geliştirilmesi ve sürdürülmesidir. Veri öznitelik gerekliliklerinin ve bir veri yönetiminin oluşturulması, tehlike tespiti ve risk azaltımının etkili olmasını sağlayacaktır.

Tehlike tespiti, sistem tasarımı ve sistem değişim süreçleri boyunca kullanılmalı, tehlikeler ise, sistemin çalıştığı süre boyunca sürekli olarak izlenerek tespit edilmeye devam edilmelidir. Tehlike tespiti esnasında, tehlikelere ilişkin tüm olası kaynaklar göz önünde bulundurulmalıdır. Her bir belirli tehlikeye ilişkin olası sonuçlar ile ilintili risk değerlendirilmeli veya incelenmeli; bu süreçte, her bir risk önem derecesinin ve olasılığın ürünüdür. Bunun ardından, kuruluş tarafından kabul edilemez olarak değerlendirilen riskler azaltılmalıdır.

Bu doküman kapsamında; risk bazlı karar alma sürecine, veri özniteliklerine, veri yönetimine ve emniyet risk yönetiminin etmenlerine ilişkin genel bir bakış ortaya konmaktadır. Bu dokümanın son Bölümünde; Emniyet Yönetimi Uluslararası İşbirliği Grubu (SM ICG) üye otoritelerinden alınan mevcut veri toplama, tehlike tanımlama ve analiz süreçlerine ilişkin örnekler yer almaktadır.

1. AMAÇ

Bu dokümanın amacı, etkili bir risk bazlı karar alma süreci için gerekli olan ilkeleri ortaya koymaktır. Bu, risk bazlı kararların alınması amacıyla veri kullanımına imkân sağlanması için gerekli olan uygun veri özniteliklerini ve bu verilerin genel yönetimini içermektedir. Bu dokümanın, emniyet yönetimi geliştirme/uygulama süreçlerinin ilk aşamalarında olan otoriteler ve hizmet sağlayıcıları tarafından kullanılması amaçlanmaktadır. Bu doküman kapsamında yalnızca temel ilkeler ortaya konmakta olup, bu dokümanla birlikte ilave kaynakların kullanılması tavsiye edilmektedir.

2. GİRİŞ

Emniyet yönetimi, dünya havacılık emniyetine ilişkin standart haline gelmektedir. Bu, yöneticilerin kuruluşlarında veya çevrelerinde mevcut olan risklere dayalı olarak karar almalarına yardımcı olan bir araçtır. Risk yönetimi, kuruluşların maruz kaldığı emniyet risklerinin değerlendirilmesini ve hafifletilmesini de kapsadığı için emniyet yönetiminin ana bileşenlerinden biridir.

Havacılık risk yönetiminde hem hizmet sağlayıcılarının hem de otoritelerin üzerine görevler düşmektedir; tehlikelerin ve süreçlerin niteliği ve kapsamı farklı olabilmekte birlikte her ikisinin de riski yönetmesi gerekmektedir. Örneğin; bir hizmet sağlayıcı, tehlikeleri kendi kuruluşu özelinde tanımlayabilirken bir otorite, tehlikeleri çeşitli sektörden elde edilen toplam verilere dayalı olarak tüm havacılık sistemi dahilinde ortaya çıkan trendlerden tanımlayabilmektedir.

Tehlikelerin belirlenmesi, bu tehlikelerin sonuçları ile ilintili risklerin değerlendirilmesi ve risklerin hafifletilmesi risk yönetimi sürecine ilişkin temel etmenleri oluşturmaktadır. Bu faktörlerin tamamı, etkili risk yönetimini destekleyecek verilere gereksinim duymaktadır. Sonuç itibarıyla; risk yönetimi yaşam döngüsü boyunca verilerin uygun şekilde yönetilmesi, sağlam bir emniyet yönetim sürecinin desteklenmesi açısından elzemdir.

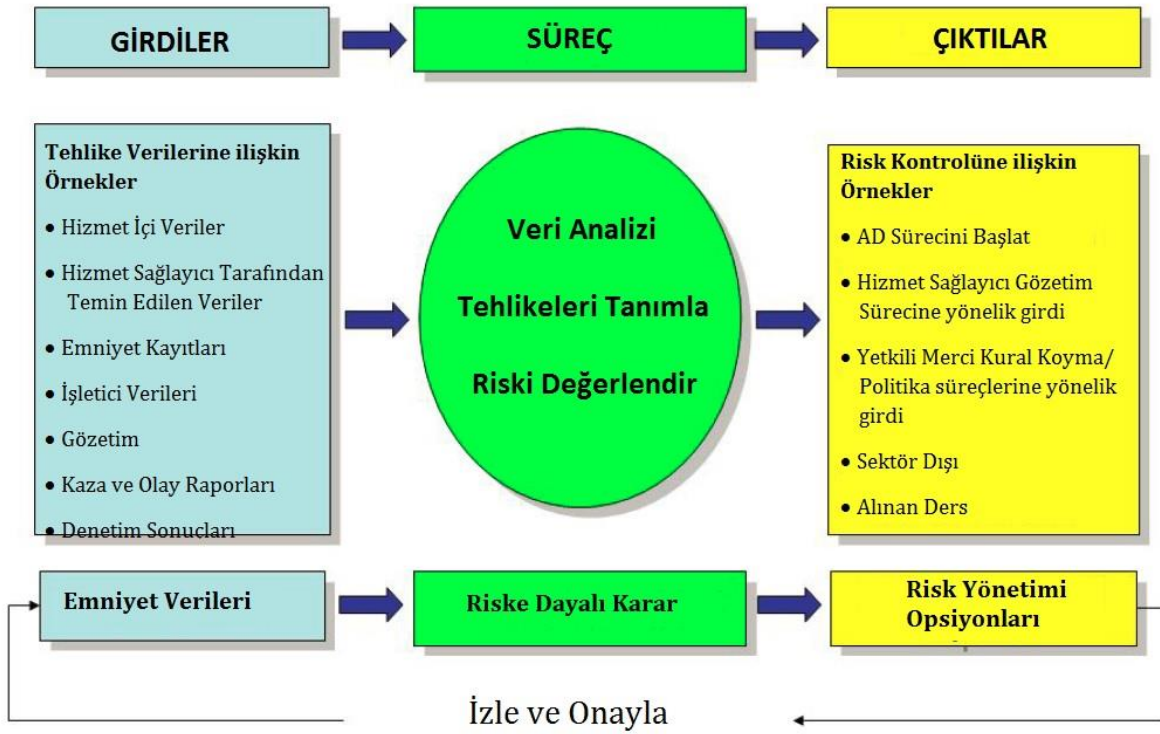
Bu dokümanın ilk kısmında, genel veri kullanım kavramları ele alınmaktadır. Ardından veri öznitelikleri, veri yönetimi, tehlike tanımlama, risk analizi ve risk azaltım süreçleri ile ilgili ayrıntılı bilgiler sunulmaktadır. Son olarak ise, mevcut otoritelerin veri toplama, tehlike tanımlama ve analiz yöntemlerine ilişkin örnekler verilmektedir.

Bir kuruluşun emniyet yönetim sürecinin ve/veya emniyet yönetim aracının karmaşıklık ve kapsamlılık seviyesi, belirli bir Devlet ya da endüstri kuruluşu dahilindeki belirli bir havacılık sektörünün büyüklüğüne, gelişmişliğine ve karmaşıklığına bağlıdır. Dolayısıyla; bu doküman dahilinde yer alan ilkelerin, belirli bir havacılık sektörünün ya da hizmet sağlayıcısının büyüklüğüne, gelişmişliğine ve karmaşıklığına göre ayarlanmış olan bir emniyet yönetim uygulaması ile başarılı bir şekilde uygulanacağı planlanmaktadır. Örneğin; görece küçük ve/veya basit havacılık sektörleri için, risk yönetiminin karmaşık Bilgi Teknolojisi (IT) araçlarından ziyade manuel veri toplama, analiz ve depolama kullanılarak gerçekleştirilmesi kabul edilebilirdir.

3. RİSK BAZLI KARAR ALMA SÜRECİNE GENEL BAKIŞ

Risk yönetiminin esas amacı, herhangi bir kaza ya da ciddi olay meydana gelmeden önce, havacılık sistemindeki tehlikelerin olası sonuçlarını tanımlayacak ve kontrol altına alacak emniyet ile ilgili verileri geliştirmektir. Emniyet verilerinin, tehlikelerin daha etkili şekilde tespit edilmesi için verilerin daha fazla açıdan incelenmesine imkân tanıyan genel taksonomiler kullanılarak sınıflandırılması ile risk yönetimi daha etkin bir hale gelmektedir.

Veri analizi, bir veya daha fazla havacılık sektöründen alınan havacılık emniyeti ile ilgili verilerden elde edilen girdileri içerebilmektedir; bu nedenle, genel taksonomilerin kullanılması önemlidir. Veri analiz sürecinin çıktıları ise risk yönetim opsiyonlarıdır. Şekil 1 kapsamında, çıktıların ve girdilerin türlerine ilişkin örnekler gösterilmektedir.



Şekil 1: Veri Analiz Sürecine yönelik Girdiler ve Çıktılar

Daha önce bahsedildiği üzere; girdiler, yeni süreçlerin veya ürünlerin tehlike analizi, mevcut havacılık sistemlerinin gözetimi, hizmet içi olaylar, kaza/olay soruşturmaları, gönüllü raporlama sistemleri vb. dahil olmak üzere havacılık sisteminin herhangi bir kısmından kaynaklanabilmektedir. Gerekli olduğunda, tehlikenin ortadan kaldırılması veya risk seviyesinin azaltılması için çıktılar veya risk kontrolleri uygulanmaktadır.

Etkili tehlike tanımlaması, verilerin mevcut olup olmamasına bağlıdır. Tehlike analizi, henüz uygulamaya konmamış olan yeni süreçler veya ürünler üzerinde gerçekleştirilse de, süreci veya ürünü açıklayan veriler gereklidir. Aynı zamanda, veriler yönetilmeli ve gerekli veri öznitelikleri ele alınmalıdır. Bunlara ilaveten; tanımlanan her bir tehlikenin kapsamlı bir şekilde anlaşıldığından emin olunması amacıyla, birden fazla havacılık sektöründen elde edilen verileri birleştirmek veya toplamak uygun olabilmektedir. Bu dokümanın 4 ve 5 sayılı bölümleri kapsamında, veri öznitelikleri ve veri yönetimi konusunda ilave bilgiler sunulmaktadır.

Ayrıca; tehlikelerin tanımlanması için, Şekil 1'de gösterilen süreç reaktif, proaktif ve prediktif metodolojilerden yararlanmalıdır. Olay veya kaza soruşturması sonucunda tanımlanan tehlikelerin analiz edilmesi, reaktif metodolojiye bir örnektir. Proaktif metodoloji denetimlerden, incelemelerden veya zorunlu raporlardan sonra risklerin değerlendirilmesini içerirken, prediktif metodoloji, sistemin sonuçları göz önünde bulundurularak, operasyonların günlük esasta hassasiyet analizini içerebilmektedir. Bu dokümanın 6, 7 ve 8 sayılı bölümleri kapsamında; tehlikelerin tanımlanmasına, risk analizine ve risk azaltımına dair ilave bilgiler yer almaktadır.

4. VERİ ÖZİNİTELİKLERİ

İster Emniyet Yönetim Sistemi (SMS) ister Devlet Emniyet Programı (SSP) kapsamında oluşturulmuş olsun, iyi işleyen emniyet yönetim süreçleri verilere gereksinim duymaktadır. Bu bölümde, sistem tasarımı, veri toplama, analiz ve dağıtım süreçleri esnasında göz önünde bulundurulması gereken veri öznitelikleri incelenmektedir.

Veri öznitelikleri ele alınmadan önce, emniyet verilerinin çok kapsamlı bir şekilde pek çok kategoriye ayrılabilirdiği düşünülmelidir: raporlanabilir olay verileri, gönüllü olay verileri, gözlem verileri ve gözetim verileri. Raporlanabilir verilerin, düzenlemeler kapsamında sunulması gerekmektedir. Kazaların ve ciddi olayların yanı sıra belirli teknik olayların soruşturulmasından elde edilen veriler buna dahildir. Düzenlemeler kapsamında gerekli olmamasına rağmen, gönüllü verileri, tehlikelerin tanımlanmasında yardımcı olmak amacıyla raporlanmakta, olaylara ve hatalara ilişkin raporlara içermektedir. Gözlem, tehlikelerin normal operasyonlarda uç değerler¹ gözlemlenerek tanımlanması için kullanılabilir. Uçuş Verileri İzleme ve Uçuş Operasyonel Kalite Güvence gibi programları içermektedir. Gözetim verileri ise; belirli gerekliliklere uyumu kontrol eden denetimlerden, anketlerden ve incelemelerden elde edilmektedir. Tüm veri kategorileri, iyi işleyen bir emniyet yönetim sürecinin önemli parçalarıdır.

¹ Uç değer, herhangi bir dağılımın genel yapısının dışına çıkan bir gözlemdir. Dikkat edilmesi gereken bir alanın ya da yapılan bir veri hatasının göstergesi olabilmekle birlikte, her halükarda, ayrıntılı bir incelemeye tabi tutulmalıdır.

Veri türüne bakılmaksızın; verilerin analiz amaçları doğrultusunda bir araya getirilerek uygun şekilde kullanılmasının sağlanması konusunda en önemli faktörlerden biri kalitedir. Veri kalite ilkelerinin ve uygulamalarının, veri yakalama sürecinden analize entegrasyonuna kadar süreçlerin tamamında uygulanması önemlidir. En önemli veri özneliklerinden bazıları şunlardır: geçerlilik, tamlık, vakitlilik, mevcudiyet ve doğruluk.

Veri Geçerliliği

Veri geçerliliği, yalnızca diğer veri öznelikleri kadar önemli olmakla kalmamakta olup çok daha önemli olabilmektedir. Belirli bir analizin sonuçları, yalnızca analizin yapıldığı veri girdilerinin geçerliliği kadar geçerlidir. Geçerli veriler olmaksızın gerçekleştirilen bütün analizlerin sonuçları, tanımlanan trendler ve neticeler yanlış olabilmekte ve yanıltıcı olma ihtimali taşımaktadır. Veri geçerliliği; verilerin doğruluğuna ve akla yatkınlığına işaret etmekle kalmayıp aynı zamanda toplanan verilerin istenen şeyleri ölçmesini sağlamaktadır. Bu da, verilerin tüm gerekli haneleri içerdiği ve doğru bir şekilde yazıldığı anlamına gelmektedir. Örneğin; tarihler geçerli bir gün, ay ve yıldan oluşmaktadır; bir ayda 32 gün ya da bir yılda 13 ay yoktur.

Veri geçerliliği hataları genellikle veri tabanına çok ciddi miktarda veri girişi yapıldığında veya farklı veri yapılarına sahip farklı veri tabanları birleştirildiğinde yapılan yanlış veri girişlerinden kaynaklanmaktadır. Veri geçerliliği hatalarını azaltmak amacıyla, basit alan doğrulama teknikleri benimsenebilir. Örneğin; bir veri tabanındaki tarih alanı AA/GG/YYYY formatını kullanıyorsa, aşağıdaki iki doğrulama kuralına sahip olan bir program kullanılabilir: "AA" alanı "12"yi, "GG" alanı ise "31"yi geçmemelidir. Bu yöntem genellikle veri uygunluk kontrolü olarak ifade edilmektedir.

Veri Tamlığı

Tamlık, belirli bir analiz için ne kadar verinin gerekli olduğuna kıyasla ne kadar verinin mevcut olduğunun ölçülmesidir. Risk odaklı karar almayı destekleyen yeni bir analiz sürecinin geliştirilmesi öncesinde, gerekli olan asgari veriler tanımlanmalıdır. İhtiyaç duyulan verinin hacmi ne kadar fazla olursa, söz konusu verileri elde etmek için gerekli olacak kaynakların (örneğin; zaman, iş gücü) da o kadar fazla olacağı kayda alınmalıdır. Bu, veri toplama sistemleri tasarlanırken ciddi bir şekilde göz önünde bulundurulması gereken bir şeydir. Tamlığa ilişkin gereklilikler aynı zamanda mevcut olan bilgilerle orantılı olmalıdır. Örneğin; büyük ihtimalle, herhangi bir kazaya ilişkin bilgilerin miktarı, küçük bir olaya ilişkin bilgilerin miktarından daha fazla olacaktır.

Veri Vakitliliği

Vakitlilik kullanıcı beklentileri kapsamında belirtilmesine rağmen, genellikle en iyi veri, en güncel veridir. Tarihte, teknoloji ve süreç sınırlamaları, gerçek zamanlı verilerin sunulması ihtimalinin ortadan kaldırılmasına yol açmıştır. Ancak; bilgisayarların ve ağ teknolojisinin gelişmesi ile birlikte, verilerin gerçek zamanlı mevcudiyeti önündeki engeller kalkmaya başlamıştır. Sonuç olarak; bir kuruluş, kendi emniyet yönetim süreçlerinde, havacılık emniyet verilerine mümkün olduğu ölçüde gerçek zamanlı erişim elde etmeye çalışmalıdır. Örneğin; uçuş verileri izleme (FDM) verilerinin kablosuz olarak indirilmesine ilişkin mevcut sistemler, operatörlerin verilere neredeyse gerçek zamanlı erişim sağlamalarına imkân sağlamaktadır.

Veri Mevcudiyeti

Veriler, aynı zamanda, ihtiyaç duyuldukları anlarda da mevcut olmaya devam etmelidir. Genel itibariyle; veri mevcudiyeti, verilerin nerede saklandığının ve verilere nasıl erişilebileceğinin dahil olduğu bir çok kapsamlı süreç ile elde edilmektedir. Veri mevcudiyeti, verilerin ne sıklıkla mevcut olduğu (örneğin; %99.9 oranında mevcudiyet) ve bir seferde ne kadar veri akışının sağlandığı yönlerinden ölçülebilmektedir.

Veri Doğruluğu

Veri doğruluğu, verilerin ne ölçüde gerçek dünyaya ait bir nesneyi veya tanımlanan herhangi bir olayı yansıttığını ifade etmektedir. Veri yanlışlığının pek çok kaynağı ve nedeni vardır. Bunlardan en yaygını ilk veri girişidir; yani, ya kullanıcı yanlış değer girmiştir ya da matbaa hataları yapılmıştır. Bu durum, veri girişlerini yapan kişilerin gerekli becerilere sahip olmasının ve yeterli ölçüde eğitim almasının sağlanması yoluyla ortadan kaldırılabilir. Veri girişi kaynaklı veri yanlışlığı, uygulamalarda baskı hatalarını (örneğin; yazım yanlışları) tespit edecek program bileşenleri veya muhtemel değerlere ilişkin listelerin önerilmesi dahil olmak üzere veri doğruluğunu sağlayacak diğer yöntemler ile de ortadan kaldırılabilir.

Özetle; her veri özneliği ele alınmalıdır. Bazı durumlarda, her hususun ele alınması ciddi bir gayret gerektirebilmektedir. Bir kuruluşun veri güvenilirliği, tek bir öznelik kullanılarak elde edilen bir şey değildir. Aksine, veri güvenilirliği katmanlı bir kavram olup bir seferde tek bir katman tamamlanmaktadır. Yeni bir katmanın eklendiği her zaman, veri güvenilirliği faktörü artmaktadır. Ek olarak; tüm bu öznelikler, bir sürecin veya sistemin tasarlanma aşamasının başlangıcında göz önünde bulundurulmalıdır; çünkü, süreç veya sistem oluşturulduktan sonra, yönetimin verilere dayalı karar almasına imkân sağlamak amacıyla ihtiyaç duyulan verileri elde etmek için çok geç olabilmektedir.

5. VERİ YÖNETİMİ

Emniyet yönetimi veriye dayalı bir sistem olduğu için, etkili bir veri yönetim sürecine bağlıdır. Veri Yönetimi; bir kuruluşun, ihtiyaç duyduğu verilere sahip olduğunu ve verilerin düzenli, güvenilir ve uygun olduğunu temin eden süreçlerin ve prosedürlerin sürekli olarak geliştirilmesi ve sürdürülmesidir. Bir kuruluş verileri yönetirken, hangi bilgilerin gerekli olduğunu tanımlamalı ve söz konusu bilgilerin kendi süreçleri içerisinde nasıl kullanılacağını planlamalıdır.

Etkili emniyet veri yönetimi için, bir kuruluş:

- İstenen hedeflere ulaşmak için gerekli olan verileri tanımlamalıdır;
- Verilerin kullanım amacına dayalı olarak, veri mimarilerini ve veri tabanı yapılarını tasarlamalıdır;
- Gerekli veri toplama sıklığı dahil olmak üzere, verilere ilişkin standartları ve formatları tanımlamalıdır;

- Toplanan verilerin tanımlı standartlara ve formatlara uygun olduğunu temin edecek bir süreç geliştirmelidir;
- Toplanan verinin gerekliliğini ve söz konusu verinin kullanımını göz önünde bulundurmak suretiyle veri toplama araçları geliştirmelidir;
- Pek çok kaynaktan toplanacak verileri tanımlamalıdır;
- Emniyet verilerini, ilgili olabilecek diğer ilintili verilere entegre etmelidir;
- Kullanıcılar için yeterli veri erişimi sağlamalıdır;
- Veri koruma hususlarını göz önünde bulundurmalıdır;
- Kuruluş dahilinde ve kuruluş dışında, verilerin kurumlarla paylaşılması hususunu göz önünde bulundurmalıdır;
- Konfigürasyon kontrolü de dahil olmak üzere, bütün yaşam döngüsü boyunca verileri yönetmelidir.

Bu bölümde, emniyet yönetimine ilişkin verileri etkin bir şekilde kullanmak için göz önünde bulundurulması gereken veri yönetiminin bazı temel noktalarına yer verilmektedir.

Veri Toplama Planlaması

Bir kuruluş (otorite veya hizmet sağlayıcı), verileri toplamadan önce, hangi bilgilerin gerekli olduğunu belirlemelidir. Örneğin; otoriteler ve hizmet sağlayıcılar, genellikle, kazalara ve ciddi olaylara ilişkin detaylı verilere sahiptir. Ancak; tüm emniyet olaylarına ilişkin veriler sistemlerinde mevcut olmayabilir. Sonuç itibarıyla; kuruluş bu bilgileri elde etmek amacıyla, söz konusu verileri toplamak için bir plan geliştirmelidir.

Toplanacak verilerin belirlenmesinin ardından, kuruluş bilginin kaynağının yanı sıra toplama ve depolama süreçlerini de belirlemelidir. Örneğin; sistem halka, ekip üyelerine, hizmet sağlayıcılara, vb. açık olacak mı? Bu soruyu yanıtlamak için, 4 sayılı Bölümde ele alınan veri özniteliklerini göz önünde bulundurarak kaynağın, ilgili bilgi seviyesini temin edip edemeyeceğinin tespit edilmesi gerekmektedir.

Veri Standardizasyonu

İçeriğin standardizasyonu, verilerin kullanımı doğrudan etkilemektedir. Bu nedenle; farklı kaynaklardan elde edilen verileri karşılaştırmak, bir araya toplamak ve birleştirmek için verileri standardize etmek gerekmektedir. Farklı kaynaklardan elde edilen verileri bir araya getirebilmek için, genel taksonomilere ilişkin standartları geliştirmek ve sürdürmek ya da farklı taksonomiler arasında dönüştürme veya çevirme yapabiliyor olmak gerekmektedir. Taksonomiler, verilerin aynı nomenklatür kullanılarak tanımlanmasına ve depolanmasına imkân sağlamaktadır. Örneğin; bir uçak tipi "737-200" veya Boeing 737-200" veya "732" olarak kaydedilebilmektedir. Standartlara ilişkin bazı örnekler aşağıda açıklanmaktadır:

- Uçak modeli: Kuruluş, uçuş operasyonu gerçekleştirmek üzere onaylanan tüm modellerin olduğu bir veri tabanı oluşturabilmektedir.
- Havaalanı: Kuruluş, havaalanlarını tanımlamak amacıyla Uluslararası Sivil Havacılık Teşkilatı (ICAO) veya Uluslararası Hava Taşımacılığı Birliği (IATA) kodlarını kullanabilmektedir.

- Olay tipi: Kaza soruşturma kuruluşu, olayları sınıflandırmak amacıyla ICAO veya diğer uluslararası kuruluşlar tarafından geliştirilen taksonomileri kullanabilmektedir.

Mevcut sorunlar ve diğer faktörler nedeniyle, genel taksonomiler farklı veri tabanları arasında zaman zaman mevcut olmayabilmektedir. Böyle bir durumda, verilerin eşdeğerliğe dayalı olarak standardizasyonuna imkân sağlamak amacıyla veri haritalama oluşturulmalıdır. Yukarıda yer alan uçak tipi örneğinden yola çıkılırsa, verilerin haritalaması, bir veri tabanında "737-200" olan değer bir başka veri tabanında "732" olan değere eşdeğer olduğunu gösterebilmektedir. Bazı durumlarda, veri yakalama esnasındaki bilgi seviyesinin farklı olması nedeniyle bu, doğru bir yöntem olmayabilmektedir. Genel taksonominin yüksek veri çoktüreliği nedeniyle kullanışlı olmadığı zamanlarda, diğer veri entegrasyon şekilleri göz önünde bulundurulmalıdır.

Yeni bir standardın oluşturulması halinde, kuruluşun, gerekli standartların geliştirilmesi için hem iç hem de dış kaynakları hesaba katması gerekebilmektedir.

Veri Yapısı ve Formatı

Verilerin toplanması için yararlanılacak süreçlerin kuruluş tarafından belirlenmesinin ardından gelen aşama toplanacak verilerin yapısının tanımlanmasıdır. Aynı zamanda verilerin nerede tutulacağına da düşünülmesi gerekecektir. Verilerin mevcut veri tabanlarıyla birleştirilmesi durumunda, hâlihazırda toplanmış olan verilerin aynı yapısının kullanılması gerekecektir. Örneğin; herhangi bir mevcut veri tabanının uçuş saatleri, ekip üyeleri, hava araçları, havaalanları ve diğer detaylı bilgileri içermesi durumunda, bu veri tabanını yeni bir veri tabanıyla birleştirmek için, bu bilgilerin etkin bir şekilde entegre edilmesi amacıyla mevcut veri tabanı ile aynı formatlara sahip olan veri alanları gerekli olacaktır.

Sistemler arasındaki her ortak alanın formatı aynı olmalıdır. Örneğin; bir "tarih" alanı her sistemde aynı olmalıdır (örneğin; "AA/GG/YYYY"). Verilerin farklı yapılar ve formatlarla birleştirilmesine imkân tanıyan başka bir olası strateji de veri dönüştürmenin kullanılmasıdır. Bu strateji, farklı kaynaklardan elde edilen verilerin eşit olması durumunda uygulanabilmektedir. Veriler dönüştürüldükten sonra, birbirinin yerine kullanılabilir hale gelmekte ve farklı veri tabanlarını kapsayan analizler mümkün hale gelmektedir.

Veri Toplama Araçları

Kaynaklar, içerik, formatlar ve standartlar tanımlandıktan sonra, verilerin toplanması için uygun araçların tesis edilmesi gerekmektedir. Bu noktada, aşağıdaki öznitelikleri öz önünde bulundurmak çok önemlidir:

Erişim kolaylığı: Raporlama sistemi, bulunması ve erişimi kolay bir yerde olmalıdır (örneğin; kuruluşun internet sayfasındaki anasayfanın üzerinde büyük bir link şeklinde). Erişim, yetkisiz kişileri engellemeli, ancak hedeflenen kullanıcılar tarafından

kolayca ulařılabilmelidir. Örneđin; bir ekip üyesi (hedeflenen kullanıcı), kendi pilot lisansı numarası ve diđer kuruluş sistemlerine erişim için kullanılanla aynı olan bir şifre ile erişim sağlamalıdır.

Raporlama kolaylığı: Raporu doldururken, kullanıcı bilgi giriři yapmak için mümkün olduđunca az çaba harcamalıdır. Örneđin; tarih ve saat alanları, bir takvim üzerinde seçenekleri tıklayarak kendi kendine doldurulan alanlar olmalıdır.

Gereksiz bilgilerin mevcut olmaması: Kuruluş nezdinde hâlihazırda mevcut olan bilgilerin yeniden toplanmaması sağlanmalıdır. Örneđin; kuruluşun ekip üyelerine ilişkin bilgileri içeren bir veri tabanının hâlihazırda mevcut olması halinde, yalnızca pilot lisansı numaraları ile sorgu yapmak yeterli olmalıdır.

Girdilerin kontrolü: bilgilerin istenen formatta elde edilebilmesi için format kısıtlamaları tasarlanabilmektedir. Örneđin; zamanın "0954" olarak girilmesi halinde, sistem bunu "09.54" formatı ile aynı olan tanımlanmış yapıya uygun olarak formatlandırmalıdır.

Bunlar, veri toplama araçlarının tasarlanması esnasında göz önünde bulundurulması gereken noktalardan yalnızca birkaç tanesidir. Ayrıca; toplanan verinin türüne ve miktarına bađlı olarak, veri toplama araçlarının kâğıt veya bilgisayar tabanlı olabileceđi kayda alınmalıdır.

Veri Depolama ve Veri Tabanı Bakımı

Veriler toplandıktan sonra, zaman zaman yaygın bir şekilde "güvenlik kitaplığı" olarak ifade edilen yerde depolanmalıdır. Veri depolama konusuna ilişkin göz önünde bulundurulacak noktalardan bazıları, toplanan veriler için yeterli depolama kapasitesinin olduđundan emin olmak içindir. Belirli bir sürenin ardından bazı verilerin güncellenmesi veya elden çıkarılması da gerekebilmektedir. Ayrıca; bu verileri içeren veri tabanı da ihtiyaç duyulduđunda geçerli ve güvenilir verilerin mevcut olmasının sağlanması amacıyla bakıma tabi tutulmalıdır. Depolama planı kapsamında, veri mevcudiyetinin sağlanması amacıyla fazladan depolama alanlarına ilişkin ihtiyaç da ele alınmalıdır.

Veri Eriřimi ve Mevcudiyeti

Veri tabanı kullanıcılarının veri ihtiyaçlarının yanı sıra verilere erişim sağlamak için gerekli olan araçlar da tanımlanmalıdır. Ayrıca; erişimin kısıtlanması ihtiyacı değerlendirilerek periyodik olarak gözden geçirilmelidir. Veri yönetim planı aynı zamanda kuruluş bünyesinde, depolanan verilere erişim kontrolü, hedeflenen kullanıcıların sayısını destekleyen yeterli bant genişliğinin belirlenmesi ve yeterli fazlalığın tespit edilmesi gibi veri yönetim sorumluluklarını da hesaba katmalıdır.

Verilerin Korunmasına İlişkin Kılavuz

Veri koruma ilkeleri tüm emniyet veri türleri için geçerlidir. Halka açık olan kaza raporu verileri bile, ekip üyelerinin isimleri veya bu kişileri doğrudan tanımlayan diğer bilgiler gibi bir takım korumalı veriler içermektedir. Gönüllü veriler söz konusu olduğunda ise, yalnızca raporlama yapan bireylerin doğrudan tanımlanmasının korunması değil aynı zamanda raporlamanın teşvik edilmesi amaçlandığından koruma daha üst düzeyde bile olabilmektedir. Ancak; verilerin ve bunun beraberinde gelen emniyet faydalarının korunması, raporlamayı teşvik eden veya engelleyen yerel/ulusal kanunlar ve Devlet/hizmet sağlayıcı emniyet kültürü ile yakından ilgilidir.

Emniyet yönetiminin temel taşlarından biri, düzenleyici bir makama sunulan pek çok gönüllü verinin gizli tutulması gerektiğinin ve raporlama yapan bireylerin kimliğinin kanun kapsamında izin verildiği ölçüde gizli kalacağına anlaşılmasıdır. Cezalandırmaya dayanmayan gönüllü veri raporlama anlaşmalarına kanun kapsamında izin verilmemesi ve sertifikasyon/yetkilendirme sürecinin bir parçası olarak düzenlemeye tabi tutulmaması durumunda, Devletler, bu kanıtlanmış veri paylaşımı kavramına izin verilmesi için kanunlarda veya düzenlemelerde değişik yapmasını önermeyi düşünmelidir.

Ele alınması gereken diğer bir önemli konu, emniyet bilgilerinin kullanılmasına ilişkin otorite/hizmet sağlayıcı politikasıdır. Emniyet verilerinin aşırı derecede veya orantısız ölçüde korunması, emniyet yönetiminin gerçekleştirilmesi için gerekli olan verilerin elverişliliğini olumsuz etkileyebilmekte ve otoritenin/hizmet sağlayıcısının söz konusu verileri etkin bir şekilde kullanma kabiliyetini sınırlandırabilmektedir. Bu nedenle; emniyet verilerinin korunmasının sağlanmasına yönelik gayretler, emniyet verilerinin korunması ihtiyacı ve adaletin uygulanması sorumluluğu arasındaki menfaatlere ilişkin çok hassas bir denge kurmalıdır. Politika kapsamında, emniyet verilerinin koruyucusunun sorumluluğuna ve bilgilerin ifşasına yönelik kurallara ilişkin kılavuz yer almalıdır. Havacılık dışı kurumlar tarafından bilgilere erişim ile ilgili mevzuat, hangi verilerin toplanacağı ve verilerin hangi prosedürlere ve şartlara uygun olarak dağıtılacağına tespit edilmesi esnasında daima göz önünde bulundurulmalıdır.

Verilerin korunması ve söz konusu korumanın etkin olduğuna dair güven duyulması çeşitli yöntemlerle sağlanabilmektedir. Olası yöntemlerden biri, verilerin üçüncü bir tarafça toplanmasıdır. Bu, kuruluşun bağımsız bir bölümü olabilir. Başarılı bir şekilde yararlanılan diğer bir yöntem ise, hizmet sağlayıcı verilerinin sektörel gruba veya düzenleyici otoriteye sunulması öncesinde söz konusu verilerin toplanması, kimliksizleştirilmesi, bir araya getirilmesi ve işlenmesi için tarafsız bir üçüncü tarafın tesis edilmesidir. Böylece tarafsız üçüncü taraf, koruyucu bir bariyer teşkil ederek veri gizliliğini sağlamaktadır. Bazı durumlarda; üçüncü tarafın verileri havacılık emniyeti amaçları doğrultusunda doğrulama ve analiz etme konularında yeterli uzmanlığa sahip olmaması nedeniyle bu yöntem dezavantajlar içerebilmektedir.

Özetle; herhangi bir veri koruma süreci, asgari olarak aşağıdaki hususları ele alan müzakere edilmiş resmi anlaşmalara dayalı olmalıdır:

Anonimlik: Analiz süreci esnasında gerekli olan tanımlanabilir herhangi bir verinin, ilgili veri koruma anlaşmasına uygun olarak mümkün olan en kısa süre içerisinde tamamen ortadan kaldırılmasını sağlamaktadır.

Veri erişimi ve kontrolü: Koruma gerektiren verileri tanımlayarak veri korumasına yönelik sorumluluğun tamamını belirlemektedir. Ayrıca; veri erişimi ve kontrolü, verilerin korunmasına yönelik kılavuz ilkeleri ve prosedürleri, verilere, veri işleme ve depolama lokasyonlarına yetkili erişimi, raporlara ve diğer veri çıktılarına yetkili erişimi temin etmekte ve saklama süresi sona erdikten sonra verilerin imhasını gerektirmektedir.

Veri analiz olanakları: Tüm sistemlere, ofislere, ekipmanlara, çalışma yerlerine, bilgisayarlara ve veri analizi programı ile ilgili tüm çevreye ilişkin emniyetli ve kontrollü erişim olanakları temin etmektedir. Emniyetli sistemlerin aynı zamanda kâğıt, medya ve yedekleme cihazları dahil olmak üzere tüm veri analizi ile ilgili materyallerin depolanmasını da sağlaması gerekmektedir.

Emniyet Verilerinin Paylaşımı

Havacılık sisteminin birbiriyle etkileşim içinde olan ve tüm havacılık ürünü yaşam döngüsünü etkileyen pek çok paydaştan oluşması nedeniyle emniyet veri analizi bütünlük bir şekilde gerçekleştirilmelidir. Emniyet yönetimine ilişkin en iyi uygulamalar, hizmet sağlayıcıları kimliksizleştirilerek bir araya getirilmiş bilgileri otorite ile paylaşmaları konusunda teşvik etmektedir; böylece, düzenleyici otoriteler, en yüksek riskli alanların üzerine eğilmek için havacılık sistemindeki trendleri (sektör bazında veya bütün olarak) takip edebilmekte ve kaynaklarını hedefleyebilmektedir.

Hangi verilerin paylaşılması gerektiğinin ve ilgili güvenlik sorunlarının belirlenmesi öncesinde, genel taksonomilerin ele alınması önemlidir. Veri paylaşımı; tüm bilgi kaynaklarının aynı alanlara sahip verileri sağlamasını veya bu özelliğe yönelik olarak dönüştürülmesini gerektirmektedir. Bu konu, bu bölümün yukarıda yer alan *Veri Standardizasyonu* kısmında ele alınmıştır.

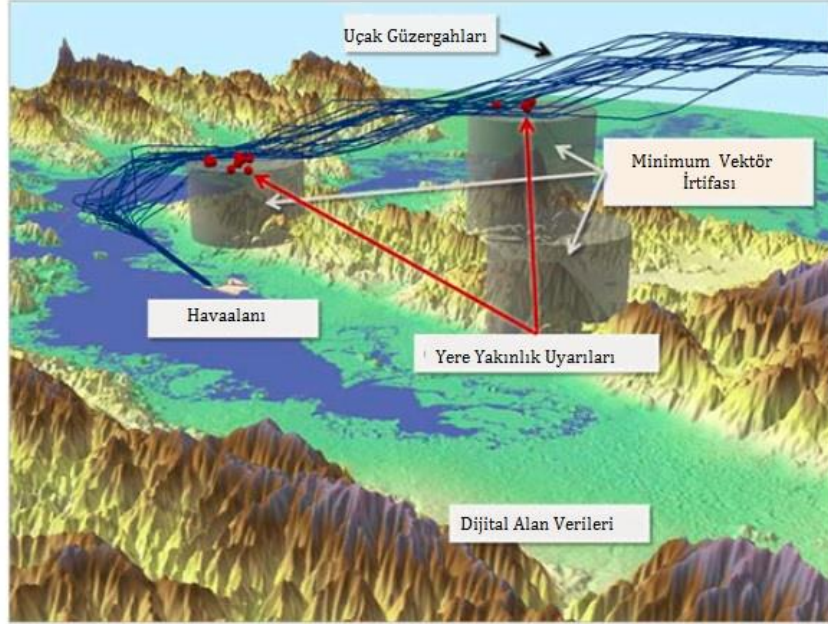
Veri Entegrasyonu/Birleşimi

Günümüz araçları, mevcut veri tabanlarının bir araya getirilmesi ile elde edilen zengin veriler ile verilerin entegrasyonuna ve yeni veri tabanlarının sentezine imkân sağlamaktadır. Teknoloji sayesinde, veri tabanlarının, korumalı bilgiler (örneğin; sefer sayıları, havayolları ve pilot kimlikleri) ifşa edilmeden havacılık veri tabanları arasında bağlantı kurulmasına izin veren sistemler ile entegrasyonu (örneğin; havaalanı hava bilgileri, kimliksizleştirilerek birleştirilen sefer bilgileri) önündeki engeller kalkmıştır.

Ek olarak; düzenleyici otoriteler, verileri bir araya getirip entegre ederek veri paylaşımını herhangi bir tek havacılık sektörünün kapasite sınırından daha ileriye taşımaktadır. Tipik olmayan olaylar, anormallikler ve aşmalar, veri entegrasyonu yoluyla oluşturulan bilgisayar grafiklerinde bariz hale gelebilmektedir. Örneğin; uçak verilerinden veya radar takip verilerinden sapan uçuş güzergâhları, bir analistin hangi

uçuşların diğerlerinden ciddi oranda farklı olduğunu tespit etmesine imkân verebilmektedir. Ardından, konunun uzmanları farklılıkları araştırmalı ve olayın nedenini daha iyi anlamalıdır.

Şekil 2'de veri entegrasyonunun konseptine yer verilmektedir. Bu örnekte; havaalanları etrafındaki uçuş emniyeti farklı kaynaklardan elde edilen verilerin birleştirilmesi veya entegrasyonu yoluyla incelenebilmektedir. Bu resim, bir havaalanının etrafındaki dijital alan verileri ile havaalanına yaklaşan ve havaalanından ayrılan uçakların uçuş güzergâhlarının (mavi çizgi) entegrasyonudur.



Şekil 2: Veri Entegrasyon Örneği

Veriler ile İlgili Diğer Hususlar

İyi işleyen bir risk yönetim süreci oluştururken göz önünde bulundurulması gereken emniyet verilerine ilişkin ilave hususlar şunlardır: veri güvenliği, veri bütünlüğü ve veri bozunumu. Veri güvenliği, verilerin güvenli olmasının ve herhangi bir kayıptan korunmasının sağlanması anlamına gelmektedir. Bu, önemli bir konu olmasına rağmen bu dokümanın kapsamını aşmaktadır.

Emniyet verilerinin havacılık sistemi içerisinde nasıl ele alındığı, işlendiği ve iletiildiğine dikkat edilmeli ve veri bütünlüğünü koruyan araçlar kapsama dahil edilmelidir. İnsan hatası, donanım arızası ve yazılım işleme hatalarından kaynaklanan veri bozulması,

veri bütünlüğünü tehlikeye atabilmekte ve geçersiz veri ve analiz sonuçlarına yol açabilmektedir. Verileri ele alınması/işlenme süreçleri boyunca meydana gelebilecek veri bozulmalarını tespit etmek amacıyla, dönüşel artıklık kontrolü (CRC) veya diğer eşdeğer güvence teknikleri gibi uçtan uca bütünlük kontrollerinden yararlanılmalıdır.

Tüm bunların yanı sıra, veri bozunumu hatalı verilere neden olabilmektedir. Doğru olan pek çok veri değeri, zamanla hatalı hale gelebilmektedir (başka bir deyişle; veri bozulması). Örneğin; uçak tescil ve uçak tip sertifikası hamili bilgileri ve herhangi bir taşıyıcı tarafından işletilen uçakların sayısı zamanda değişebilmektedir. Güncellenmemesi halinde, veriler hatalı verilere dönüşmektedir. Sonuç olarak da, bazı durumlarda, bir gerekliliğin tam anlamıyla yerine getirilmesi diğerini ciddi oranda tehlikeye atabilmektedir. Örneğin; veri koruma, veri güvenilirliğini azaltmakta olup durum aşırı boyutlara vardığında, veri kalite kontrollerinin gerçekleştirilmesini imkânsız hale getirebilmektedir.

Özetle; bu dokümanın 4 ve 5 sayılı Bölümleri kapsamında veri özneliklerinin ve veri yönetiminin önemi ele alınmaktadır. Bir sonraki bölüm, bu verilerin tehlikelerin tanımlanmasında ve risk yönetim sürecinde kullanılmasını açıklayacaktır.

6. TEHLİKE TANIMLAMA

Emniyet Yönetimi Uluslararası İşbirliği Grubu (SM ICG), tehlikeyi *bir uçak olayına veya kazasına sebep olabilecek veya yol açabilecek herhangi bir durum* olarak tanımlamaktadır. Tehlike tanımlama aşamasında, otoritenin veya hizmet sağlayıcısının emniyet analisti, olası tehlikelerin yanı sıra bu tehlikelerin etkilerini veya neticelerini belirlemek ve dokümante etmek için verileri analiz etmektedir.² Tehlike tanımlama sürecinde gerekli olan bilgilerin seviyesi, üzerinde düşünülen havacılık sürecinin karmaşıklığına bağlıdır.

² Bu doküman bağlamında; emniyet analisti, özellikle veri analizi alanında bir uzmanı kast etmemektedir. Analist, belirli bir havacılık sektöründen ya da bir grup emniyet analisti ve uzmanından oluşan bir emniyet heyetinden bir uzman olabilir. Tek nokta emniyet kritik karar alma süreçlerinin, teknik açıdan farklılıklar barındıran bir grup tarafından yapılan kapsamlı inceleme ile asgariye indirilmesi genellikle iyi bir uygulamadır.

Tehlike Tanımlamasına İlişkin Göz Önünde Bulundurulması Gereken Hususlar

Etkin tehlike tanımlamasının sağlanması için pek çok faktörün göz önünde bulundurulması gerekmektedir. İlk olarak; sistemdeki tehlikeleri tanımlayacak sistematik bir süreç geliştirilmelidir. Kullanılacak çok çeşitli yöntem olmakla birlikte hepsi aşağıdaki üç faktörü içermektedir:

- a) Emniyet analistleri, teknik uzmanlığa ve/veya yönetim uzmanlığına sahip olmalıdır.
- b) Emniyet analistleri, çeşitli tehlike analizi teknikleri konusunda eğitilmiş veya tecrübeli olmalıdır.
- c) Tanımlı bir tehlike analizi aracı/araçları mevcut olmalı veya geliştirilmelidir.

İkinci olarak; emniyet analisti, tehlikeleri tanımlamak için gerekli olan veri kaynaklarını tespit etmelidir. Son olarak; emniyet analisti, mevcut veri ve değerlendirilmekte olan havacılık sistemi türüne en uygun olan tekniği veya aracı seçmelidir.

Olası Tehlike Kaynakları

Tehlike tespiti esnasında, tehlikelere ilişkin tüm olası kaynaklar göz önünde bulundurulmalıdır. Bunlar, incelenen sistemin mahiyetine ve büyüklüğüne bağlı olarak aşağıdakileri içerebilmektedir:

- a) Uçakla taşınan teçhizat veya yer ekipmanı (donanım ve yazılım);
- b) İşletme çevresi (çevre koşulları, havaalanı altyapı eksiklikleri, hava sahası, havaalanı tasarımı ve uçuş güzergâhı tasarımı dahil olmak üzere);
- c) İnsan performansı;
- d) İnsan-makine arayüzü;
- e) İşletme usulleri;
- f) Bakım prosedürleri;
- g) Harici arayüzler (örneğin; dış kaynak yoluyla temin edilen hizmetler);
- h) Kuruluşa ait prosedürler ve
- i) Kuruluşa ait değişiklik.

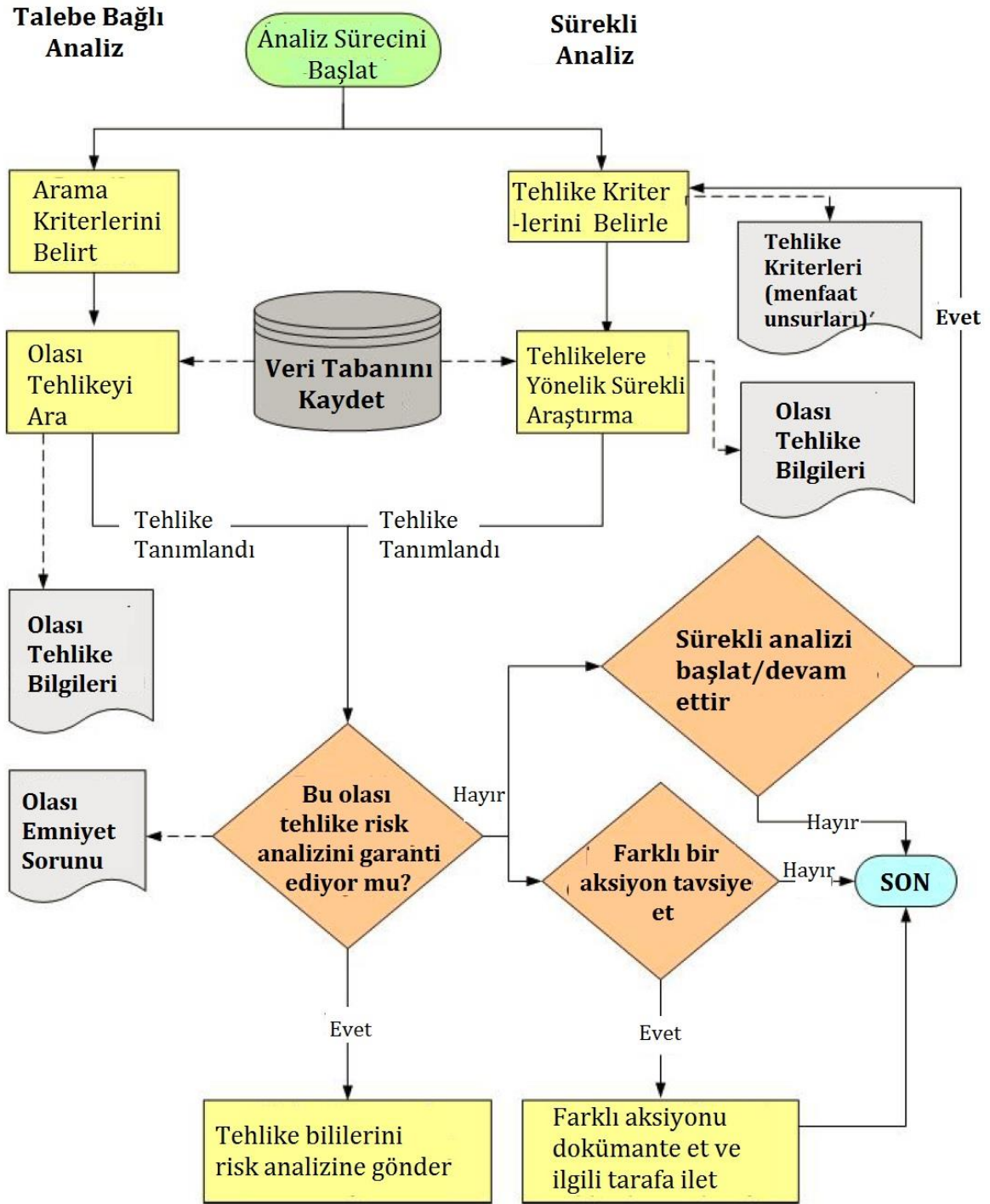
Tehlike Tanımlamasının Nedenleri

Tehlike tanımlama sürecinin kullanılması için farklı durumlar vardır. En önemlilerinden bazıları şunlardır:

- **Sistem Tasarımı:** Tehlike tanımlama, operasyonların başlangıcı öncesinde, belirli havacılık sisteminin ve çevresinin detaylı bir şekilde tanımlanmasıyla başlamaktadır. Ardından, sistem ile ilişkili çeşitli olası tehlikeler ve bunların diğer arayüz sistemlerine etkileri emniyet analisti tarafından belirlenmektedir.
- **Sistem Değişikliği:** Tehlike tanımlama, sistemde herhangi bir (operasyonel veya organizasyonel) değişiklik yapılmadan önce başlamakta olup, havacılık sistemindeki belirli değişikliğin detaylı bir şekilde tanımlanmasını içermektedir.

Ardından, önerilen deęişiklik ile ilişkili çeşitli olası tehlikeler ve bunların dięer arayüz sistemlerine etkileri emniyet analisti tarafından belirlenmektedir.

Talebe Bağlı ve Sürekli İzleme: Tehlike tanımlama, işler durumda olan mevcut sistemler için geçerlidir. Şekil 3, hem talebe bağlı analizi hem de sürekli izlemeyi içeren bir sürecin örneğini göstermektedir. Veri izlemenin aynı zamanda beklenenden daha sık veya daha ciddi tehlikelerin ve beklenenden daha az etkili olan hafifletme stratejilerinin tespit edilmesine yardımcı olduğu da kayda alınmalıdır. Ayrıca; sürekli analiz, birtakım kritik menfaat unsurlarına bağlı bildirim eşikleri ile tesis edilebilmektedir.



Şekil 3: Talebe Bağlı ve Sürekli Analizde Tehlike Tanımlama

Tehlike Tanımlama Yöntemleri ve Araçları

Tehlike tanımlamaya yönelik pek çok yöntem ve araç vardır. Üç örnek aşağıda yer almaktadır.³

Beyin Fırtınası

Beyin fırtınası, bir grup uzman arasında ucu bucağı olmayan fakat yönlendirilen bir tartışmadır. Yönlendiren kişi, grup oturumu öncesinde bilgi istemlerini veya sorunları hazırlar ve ardından grup üyeleri arasında yaratıcı düşünceyi teşvik ederek oturumlar esnasında tartışmaların olmasını sağlar. Yönlendiren kişi tartışmanın fitilini ateşler ve bir sonraki tartışmada neyin kapsama dahil olup olmadığına dair herhangi bir kural yoktur. Tüm katkılar kabul edilerek kaydedilir ve hiçbir görüş sorgulanmaz ya da eleştirilmez. Bu, uzmanların etraflıca düşünmeleri konusunda kendilerini rahat hissetmelerini sağlayacak bir ortam temin eder.

Avantajlar:

- Yeni veya karmaşık olmayan sistemlerdeki yeni tehlikelerin tanımlanması açısından iyidir.
- Tüm kilit paydaşları içerir.
- Denenmesi daha hızlı ve kolaydır.
- Çok çeşitli sistem türleri için uygulanabilir.

Dezavantajları:

- Görece yapılandırılmamıştır; bu nedenle çok kapsamlı değildir.
- Uzmanlığa ve katılımcıların profiline bağlıdır.
- Grup dinamiklerinin ve üst yönetim amaçlarının etkisi karşısında dirençli olmayabilir.
- Başarıya ulaşmak büyük oranda yönlendiren kişinin yeteneklerine dayalıdır.

Tehlike ve İşletilebilirlik (HAZOP) Çalışması

Tehlike ve İşletilebilirlik (HAZOP) Çalışması, parametre ve sapma rehber sözcüklerini kullanan sistematik ve yapılandırılmış bir yaklaşımdır. Bu teknik, çalışmaya elverişli çok detaylı bir sistem tanımına dayalı olup, genellikle sistemin iyi tanımlanmış alt sistemlere ve alt sistemler arasındaki fonksiyonel akışlara veya süreç akışlarına bölünmesini içerir. Ardından, sistemin her bir unsuru rehber sözcüklerin ve sapmaların çeşitli kombinasyonlarına karşı çokdisiplinli bir uzmanlar grubu içerisinde tartışılmaya başlanır. Grup tartışması, bir başkan tarafından yönlendirilir ve belirli bir rehber sözcük ve sapma kombinasyonu tartışılırken tanımlanan tehlikeler dahil olmak üzere tartışmanın sonuçları bir sekreter tarafından kayıt altına alınır.

³ Avrupa Ticari Havacılık Emniyet Ekibi (ECAST) Emniyet Yönetim Sistemi ve Emniyet Kültürü Çalışma Grubu'nun Tehlike Tanımlama Kılavuzu

Belirli bir rehber sözcük ve sapma kombinasyonunun herhangi bir tehlike oluşturmaması veya güvenilir olmadığı düşünülmesi durumunda, bu da tamlığın kanıtlanması için kaydedilmelidir. Rehber sözcükler ve sapmalar Tehlike ve İşletilebilirlik (HAZOP) başkanı tarafından önceden hazırlanmalıdır; ancak, bunların sisteme veya incelemeye tabi tutulan operasyona göre özelleştirilmesi gerekebilmektedir.

Havacılık bağlamında, tipik rehber sözcükler aşağıdakileri içerebilmektedir:

- Tespit
- Koordinasyon
- Bildirim
- Aktarım
- Klerans
- İzin/Yetkilendirme
- Seçim
- Kopya Çıkarma (Transkripsiyon)
- Dönüş
- Tırmanma
- Alçalma
- Hız
- Talimat tekrarı (read-back)
- İzleme
- Yön işaretleri
- El değiştirme
- Gözetim

Tipik sapmalar aşağıdakiler içerebilmektedir:

- Çok yakın / erken
- Çok geç
- Çok fazla
- Çok az
- Çok yüksek
- Çok alçak
- Kayıp/Eksik
- İki defa / mükerrer
- Sıra dışı
- Muğlak
- Ters / alt üst

Tehlike ve İşletilebilirlik (HAZOP) Yaklaşımının Avantajları:

- Sistematik ve kesin.
- Çokdisiplinli uzmanların görüşlerinin etkileşimini içerir.
- Çok çeşitli sistem türleri için uygulanabilir.
- Tehlike tanımlama sürecine ilişkin detaylı ve denetlenebilir bir kayıt oluşturur.

Tehlike ve İşletilebilirlik (HAZOP) Yaklaşımının Dezavantajları:

- Ciddi bir hazırlık gerektirir.
- Karmaşık olmayan bir sistemde kullanılması zordur.
- Büyük oranda Tehlike ve İşletilebilirlik (HAZOP) başkanının yeteneklerine dayalıdır.
- Zaman alıcı ve bu nedenle pahalı olabilir.
- Yaratıcı düşüncüyü ve dolayısıyla bazı tehlike türlerini engelleyebilir.

Kontrol Listesi

Kontrol listeleri, geçmiş deneyimlerden ortaya çıkan bilinen tehlikelerin veya tehlike nedenlerinin listeleridir. Geçmiş deneyim, benzer sistemlerin veya operasyonların geçmiş risk değerlendirmeleri olabileceği gibi geçmişte meydana gelen fiili olaylardan da kaynaklanabilmektedir. Bu teknik, uygun kontrol listesinin sistematik bir şekilde kullanılmasını ve kontrol listesinde yer alan her bir ögenin belirli bir sistem bakımından olası uygulanabilirliğinin değerlendirilmesini içermektedir. Kontrol listeleri kullanılmadan önce daima uygulanabilirlik açısından doğrulanmalıdır.

Avantajlar:

- Sistem dışı uzmanlar tarafından kullanılabilirler.
- Çok çeşitli geçmiş bilgileri ve deneyimi yakalarlar.
- Ortak ve daha belirgin sorunların gözden kaçmamasını sağlarlar.

Dezavantajları:

- Yeni sistemler veya karmaşık olmayan sistemlere uygulandıklarında sınırlı bir kullanım alanına sahiptirler.
- Tehlike tanımla sürecinde hayal gücünü engelleyebilirler.
- Daha önce görünmeyen tehlikeleri gözden kaçırabilirler.

7. RİSK ANALİZİ

Emniyet yönetim sürecinde bir sonraki adım, her bir riskin ciddiyetin ve olasılığın ürünü olduğu her bir belirli tehlikeye yönelik olası sonuçlarla ilişkili riskin değerlendirilmesi veya analiz edilmesidir. Bu nedenle, ciddiyet ve olasılık tanımlanan tehlikelerin olası neticelerine bağlı olarak ölçülebilir şekilde ifade edilmelidir; böylece, tehlikeler tesis edilen risk kılavuzlarına göre derecelendirilebilmekte ve kıyaslanabilmektedir, bu da risk azaltımının uygun kapsamının ve zamanlamasının belirlenmesinde yardımcı olmaktadır.

Riskin değerlendirilmesinde hem kantitatif hem kalitatif yöntemler kullanılabilir. Kantitatif veriler daha objektif olma eğilimli olduğu için bu verilerin kullanılması tercih edilmektedir. Ancak; kantitatif verilerden bazılarının mevcut olmaması durumunda, kalitatif verilere ve uzman yargılarına güvenmek kabul edilebilir. Kalitatif yargı kişiden kişiye değişiklik göstermektedir; bu nedenle, analizin yalnızca bir kişi tarafından yapılması durumunda, sonucun bir görüş olduğu düşünülmelidir. Uzmanlardan oluşan bir ekibin analize müdahil olması durumunda, sonucun kalitatif veri ve uzman yargısı

olduđu düşünülebilir. Bu nedenle; analizin kalitesi, seçilen ekipteki uzmanların geçmişine dayanmaktadır.

Kantitatif verilerin avantajları:

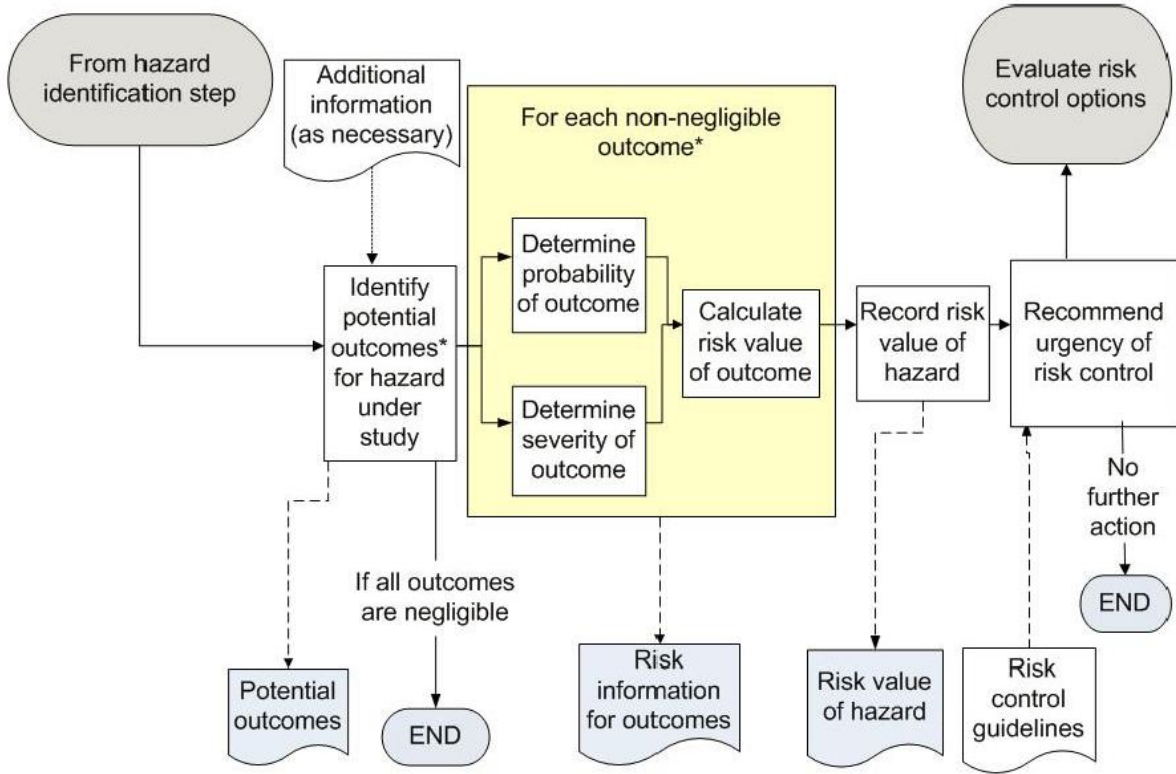
- a) Veriler nicelik, sayı veya miktar cinsinden ifade edilir.
- b) Veriler daha objektif olma eğilimindedir.
- c) Veriler, bulguların daha mantıklı analizine ve kanıtlanmasına imkân sağlar.
- d) Veriler, modelleme için kullanılabilir.

Kalitatif verilerin avantajları:

- a) Veriler, kalite ölçüsü cinsinden ifade edilir.
- b) Veriler sübjektiftir.
- c) Veriler, genelde sayılarla değil uzman yargıları ile ifade edilen konuların incelenmesine imkân sağlar.

Modellemenin gerekli ve verilerin mevcut olması durumunda, risk değerlendirmesinin istatistikî veya gözlemsel verilere (örneğin; radar izlemeleri, donanım arıza oranları) bağlı olması gerektiği kayda alınmalıdır. Riskin bütünüyle istatistiksel değerlendirmelerinin yapılmasını sağlayacak verilerin yetersiz olması durumunda, yargısal girdiler kullanılabilir ancak kantitatif olarak ifade edilmelidir. Örneğin; belirli bir operasyon türünün gerçek oranı bilinmeyebilir; ancak, yargısal girdi kullanılarak tahmin edilebilir. Her halükarda; kantitatif tedbirler, tarihi verilerin geleceğe yönelik işletim çevrelerini temsil etmeyebileceğini veya geleceğe yönelik işletim çevrelerinin yanlış bir konfigürasyonuna neden olabileceğini hesaba katmalıdır. Bu tür durumlarda, girdi verilerinde birtakım düzenlemeler yapılması gerekli olabilir.

Şekil 4, düzeltici risk kontrollerinin türünü ve önceliğini belirlemek amacıyla kullanılan risk analiz sürecinin bir örneğini göstermektedir.



Şekil 4: Örnek Risk Analizi Süreci

Riskin tek bir uçuş, uçak filosu, endüstri segmenti veya segmentleri bazında incelenebildiği çeşitli risk profillerine karşı risklerin incelenerek kontrol edilebildiği kayda alınmalıdır. Risk profili, belirli bir havacılık sektörünün (otorite veya hizmet sağlayıcı) genel emniyet amaçlarına bağlıdır.

Ayrıca; herhangi bir risk analizinin temel noktası, belirli bir risk sınıflandırmasına yol açan çeşitli varsayımların dokümantasyonudur. Bunlar, özellikle işletme ortamının değişmesi durumunda gerekli olması halinde ileride yeniden incelenerek güncellenebilmektedir.

8. RİSK AZALTIM STRATEJİLERİ

Risk azaltımının amacı, kabul edilebilir emniyet seviyesine ulaşana kadar, tanımlanan tehlikelerin her bir sonucu ile ilgili riski azaltmaya yönelik uygun planları uygulamaktır. Uygun risk azaltım veya risk kontrol stratejileri emniyet analisti tarafından geliştirilmekte, dokümanite edilmekte ve tavsiye edilmektedir. Risk kontrolü, herhangi bir tehlikenin etkilerini/neticelerini azaltan herhangi bir şeydir. Bir risk kontrol stratejisi, riski azaltan veya tehlikeyi ortadan kaldıran seçenekleri ve alternatifleri içermektedir. Örneğin; ilave politikaların veya prosedürlerin uygulanması, yedek sistemlerin ve/veya bileşenlerin geliştirilmesi, eğitim spesifikasyonunun ve sonuçlarının gözden geçirilmesi ve alternatif üretim kaynaklarının kullanılması.

Risk seviyesinin kabul edilemez olduğunun tespiti halinde, kuruluşa ait (otorite veya hizmet sağlayıcı) politikalarda ifade edildiği üzere, riski kuruluş yönetimi nezdinde kabul edilebilir bir seviyeye indirecek olası risk azaltım stratejileri analist tarafından belirlenerek değerlendirilmektedir. Ardından, önerilen olası azaltım stratejilerinin genel riski nasıl etkileyeceği analist tarafından değerlendirilmektedir. Gerekli olması halinde, strateji kombinasyonları riski kuruluş yönetimi nezdinde kabul edilebilir bir seviyeye indirene kadar, süreç analist tarafından tekrar edilmektedir. Risk değerlendirmesinin sonucunda riskin kabul edilemeyecek seviyede olduğunun ortaya çıkması halinde, birtakım azaltım aksiyonları riskin kabul edilebilir seviyeye indirilmesini sağlayana kadar, operasyonlar veya süreçler derhal durdurulmalıdır.

Bir sonraki adımda, önerilen her bir risk kontrolün değerlendirmesi yapılmalıdır. İdeal risk kontrol alternatifleri ucuz olup kolayca gerçekleştirilir, hızlıca uygulanır, tamamen etkilidir ve yeni bir risk (istenmeyen neticeler riski) ortaya çıkarmaz. Pek çok durum bu idealleri karşılamadığı için alternatif risk kontroller; etkililik, maliyet, uygulama dakikliği ve karmaşıklık öznitelikleri arasında kurulacak dengeye bağlı olarak değerlendirilmeli ve seçilmelidir. Risk kontrolleri seçilip uygulandıktan sonra, hedeflenen amaçların elde edildiğinden emin olmak için bu kontroller izlenmeli ve doğrulanmalıdır.

Seçilen risk azaltım yaklaşımı aşağıdaki bir ya da birkaç kategori kapsamına girebilir:

- **Risk Önleme Stratejisi:** Risk önleme stratejisi, farklı bir yaklaşım seçerek veya operasyona, prosedüre ya da sistem (donanım ve yazılım) geliştirmeye katılım göstermeyerek meydana gelme ve/veya sonuç olasılığını önler. Bu teknik, birden fazla alternatif veya seçenek mevcut olduğunda uygulanmalıdır. Risk önleme stratejisi daha ziyade bir operasyonun veya programın başlangıcında "devam etme" veya "devam etmeme" kararına ilişkin bir dayanak noktası olarak kullanılır.
- **Risk Azaltım Stratejisi:** Risk azaltım stratejisi, kabul edilen risklerin sonuçlarının ciddiyetini azaltmak için operasyonun veya faaliyetin sıklığının azaltılması veya belirli aksiyonların benimsenmesi anlamına gelir. Bu strateji, riski azaltacak belirli aksiyonların başka bir tarafça kontrol edilmesi durumunda risk devir aksiyonuna neden olabilir.
- **Risk Devir Stratejisi:** Risk devir stratejisi, riske ilişkin sorumluluğu başka bir tarafa yükler. Kuruluşlar riske ilişkin sorumluluğu genellikle söz konusu riski en iyi yönetebilecek kuruluşa veya operasyona devreder. Alıcı taraf söz konusu riski kabul ederek belgelendirmelidir (örneğin; Mutabakat Mektubu, Mutabakat Beyanı, Mutabakat Muhtırası). Herhangi bir havacılık sisteminin satın alan kuruluştan bakım hizmeti veren bir kuruluşa devri, risk devrine ilişkin bir örnektir.
- **Risk Maruziyetinin Ayrılması Stratejisi:** Bu strateji kapsamında, risklere karşı koruma sağlamak amacıyla risklerin veya oluşmuş fazlalıkların etkilerini izole etmek için önlem alınmaktadır. Etrafı karmaşık coğrafyayla sarılan bir hava meydanına yapılan bir operasyonun özel seyrüsefer yeteneklerine sahip olan bir uçak ile sınırlandırılması, maruziyetin ayrılmasına ilişkin bir örnektir.

- **Risk Varsayım Stratejisi:** Basit şekilde söylemek gerekirse; risk varsayım stratejisi, bir riskin meydana gelmesi ile ilişkili sonuçların ihtimalini veya olasılığını ve ciddiyetini kabul etmektir. Herhangi bir tehlikeyle ilişkili yüksek risklerin ele alınması için varsayım stratejisinin kullanılması genellikle kabul edilebilir değildir. Emniyet riski, kabul edilmeden önce daha düşük seviyelere indirilmesi için yine azaltılmalıdır. Bu yaklaşımı seçerken, varsayılan risklere ilişkin mevcut karşı önlemler önceden hazırlanmalıdır.

Özetle; 6,7 ve 8 sayılı Bölümler kapsamında açıklanan rehberlik, tehlikelerin tanımlanması, tehlikelerin sonuçları ile ilişkili risklerin değerlendirilmesi ve riskin kabul edilebilir seviyelere indirilmesi amacıyla kullanılabilecek genel yöntemleri ortaya koymaktadır. Bir sonraki bölümde, bazı otoritelerce yararlanılan tehlike tanımlama ve analiz yöntemlerine ilişkin örnekler yer almaktadır.

9. MEVCUT OTORİTELERİN RİSK YÖNETİMİ YÖNTEMLERİNE İLİŞKİN ÖRNEKLER

Emniyet Yönetimi Uluslararası İşbirliği Grubu (SM ICG), mevcut uygulamaların dayanak noktasını tespit etmek üzere katılımcı otoritelerin hâlihazırda mevcut olan veri toplama, tehlike tanımlama ve analiz süreçlerine ilişkin bir anket gerçekleştirmiştir. Dayanak noktasının tespit edilmesinin altında yatan amaç, kendi emniyet yönetim süreçlerini geliştiren Devletlere, ilave bilgiye yönelik referans URL'ler ile birlikte mevcut yöntemlerin ve araçların örneklerini sunmaktır. Otoriteler hem uzunca bir süredir uygulanan hem de yakın zaman içerisinde uygulamaya konacak süreçleri belirtmiştir. Anketin birkaç sonucu aşağıdaki tabloda yer almaktadır. Tablonun ardından, tablodaki ilk örnek olan *Decolagem Certa* (DCERTA) Sistemi, mevcut bir risk yönetim sürecine ilişkin bir vaka çalışması olarak daha etraflıca ele alınmaktadır.

Tablo 1: Otoritelerin Risk Yönetimi Yöntemlerine İlişkin Örnekler

Düzenleyici Otorite	Süreç/ Sistem	Sürecin/Sistemin Açıklaması ve Amacı	İlave Bilgiye Yönelik Referanslar
Brezilya Ulusal Sivil Havacılık Ajansı (ANAC)	<i>Decolagem Certa</i> (DCERTA) Sistemi	Brezilya; teknik ekip (lisans, yetki ve sağlık raporu), uçak, sefer düzenlenen hava meydanları ile ilgili olarak genel havacılık uçuşlarının düzenlemelere uyumunu, havaalanları AIS'te pilotlar tarafından sunulan Uçuş Planlarında yer alan bilgilere dayanarak doğrulayan otomatik bir sistem olan <i>Decolagem Certa</i> (DCERTA) Sistemi'ni geliştirmiştir. Bu sistem, emniyet analizlerine ilişkin veri sağlamakta olup, karşılığında, söz konusu analizler, riske dayalı bir	http://www2.anac.gov.br/d ecolagemcerta/

		denetim programının tesis edilmesine imkân veren trend göstergelerini oluşturmak amacıyla kullanılmıştır.	
Avrupa Havacılık Emniyeti Ajansı (EASA)	Kaza ve Olay Raporlama Sistemlerine yönelik Avrupa Koordinasyon Merkezi (ECCAIRS)	Kaza ve Olay Raporlama Sistemlerine yönelik Avrupa Koordinasyon Merkezi (ECCAIRS)'nin misyonu; toplu taşıma emniyetinin geliştirilmesi amacıyla kendi emniyet bilgilerinin toplanması, paylaşılması ve analiz edilmesi hususlarında Ulusal ve Avrupa taşımacılık otoritelerine ve kaza soruşturma organlarına yardımcı olmaktır.	http://eccairsportall.jrc.ec.europa.eu/index.php?id=1
İsviçre Federal Sivil Havacılık Dairesi (FOCA)	SRM (Emniyet Risk Yönetimi)	İsviçre Federal Sivil Havacılık Dairesi (FOCA) tarafından, ICAO çerçevesi (Doc. 9859) ile uyumlu bir kurum içi Emniyet Yönetim Sistemi (SMS) uygulanmıştır. Tehlike tanımlama ise, olay raporlarından, gözetim bulgularından, Hava Kazaları Araştırma Dairesi (AAIB) soruşturmalarından ve diğer kaynaklardan elde edilen veriye dayalı tetikleyicilere dayalı olarak gerçekleştirilmektedir. Analiz genellikle kalitatif (tehlike tanımlama çalışmaları (HAZID), HAZOP). Daha sonraki risk analizi ya kalitatif ya kantitatif, ya da hem kalitatif hem kantitatif. Sonuçlar, bir tehlike kataloğu/risk portföyü içerisinde alınmaktadır. Herhangi bir paydaşın Emniyet Yönetim Sistemi (SMS)'nden gelen girdiler de entegre edilmektedir.	http://www.bazl.admin.ch/

<p>Birleşik Devletler Federal Havacılık İdaresi (FAA)/ Uçak Sertifikasyon Hizmeti (AIR)</p>	<p>Emniyet İzleme/ Veri Analizi (MSAD)</p>	<p>Emniyet İzleme/ Veri Analizi (MSAD); kullanımda olan uçak ürünleri tehlikelerini tespit eden, değerlendiren, azaltan ve havacılık emniyet verileri içerisindeki olası tehlikeleri ortaya çıkarmak için ürün tanımlı tehlike kriterlerini kullanan veriye dayalı bir metodolojidir. Emniyet İzleme/ Veri Analizi (MSAD), ortaya çıkan emniyet trendlerinin bağımlı değişken analizi ile hızlı bir şekilde tespit edilmesini kolaylaştırmak için sürekli operasyonel emniyet (COS) verilerinin organize edilmesine yönelik standart bir taksonomiden yararlanmaktadır. Emniyet sorunları, düzeltici önlemin kapsamını ve zamanlamasını tespit etmek üzere kullanılan riskin belirlenmesi amacıyla analiz edilmektedir. Emniyet İzleme/ Veri Analizi (MSAD) kapsamında etken analizi yaklaşımı kullanılmaktadır. Bu yaklaşım, daha sonradan ilgili Havacılık Emniyeti Kuruluşu (AVS) gözetim iş süreci sahibine iletilen süreç aksaklıkları gibi altta yatan faktörleri tespit edebilmektedir.</p>	<p>http://www.faa.gov/regulations_policies/orders_notices /index.cfm/go/document.information/documentID/215154</p>
<p>Kanada Ulaştırma Bakanlığı Sivil Havacılık Otoritesi (TCCA)</p>	<p>TP 13905 "Risk Yönetimi, Tip 2A (Kısa Süreç)"</p>	<p>TP 13905 "Risk Yönetimi, Tip 2A (Kısa Süreç)" dokümanı, izlenecek süreci ayrıntılı bir şekilde tanımlamaktadır. 107-001 "Emniyet Yönetim Sistemi (SMS) Geliştirilmesine İlişkin Kılavuz" adlı Tavsiye Niteliğindeki Genelge (AC) kapsamında da risk yönetimine ilişkin detaylar yer almaktadır.</p>	<p>http://www.tc.gc.ca/eng/civilaviation/publications/tp13905-menu-1906.htm</p>

Yeni Zelanda Sivil Havacılık Otoritesi	Risk Profili Dereceleri	<p>İşleticiler, her bir değerlendirme alanında, 1 (örnek alınması gereken derece) ile 5 arasındaki skalada derecelendirilecektir. Bu, kalitatif bir derecelendirme olup yalnızca, Sivil Havacılık Otoritesi çalışanının o an müşteri ile etkileşimi veya Sivil Havacılık Otoritesinin veri tabanında kaydedilen organizasyondaki değişiklikler ile ilgilidir.</p> <p>2 ile 5 arasındaki derecelendirmeler, daha yüksek risk seviyelerini kayıt altına almak amacıyla kullanılacaktır. Risk unsurları, bir işleticinin genel riski üzerindeki olası etkilerine ilişkin Sivil Havacılık Otoritesi tarafından yapılan değerlendirmeye dayalı olarak ölçülmektedir.</p> <p>Değerlendirme alanlarının her birindeki dereceler birleştirildiğinde, karşılaştırmalı bir risk profili oluşturulabilecek olup; burada, münferit bir işleticinin risk profili derecesi (olasılık yüzdesi olarak ifade edilir), diğer tüm işleticilerin dereceleri ile karşılaştırmalı olarak aynı dokümanda grafik şeklinde gösterilebilmektedir. Dereceler, her bir işletici ve Sivil Havacılık Otoritesi arasında gizlidir.</p>	http://www.caa.govt.nz/Surveillance_System/The_Risk_Profile_Ratings.htm
Japonya Sicil Havacılık Bürosu (JCAB)	Havacılık Emniyet Bilgileri Yönetimi ve Paylaşımı Sistemi (ASIMS)	<p>İşleticilerin kazaları, olayları ve emniyetli operasyonu etkileyebilecek vakaları ASIMS sistemine raporlamaları gerekmektedir. Japonya Sicil Havacılık Bürosu (JCAB), raporlanan bu olayların sebeplerini analiz ederek emniyet risklerini değerlendirmektedir. Sonuçlar, etkili gözetim yapılması ve gerekli emniyet önlemlerinin alınması için kullanılmaktadır.</p>	

Sivil Havacılık Otoritesi Veri Kullanımına Yönelik Örnek

Vaka İncelemesi: ANAC - Brezilya Ulusal Sivil Havacılık Ajansı - *Decolagem Certa* (DCERTA) Sistemi.

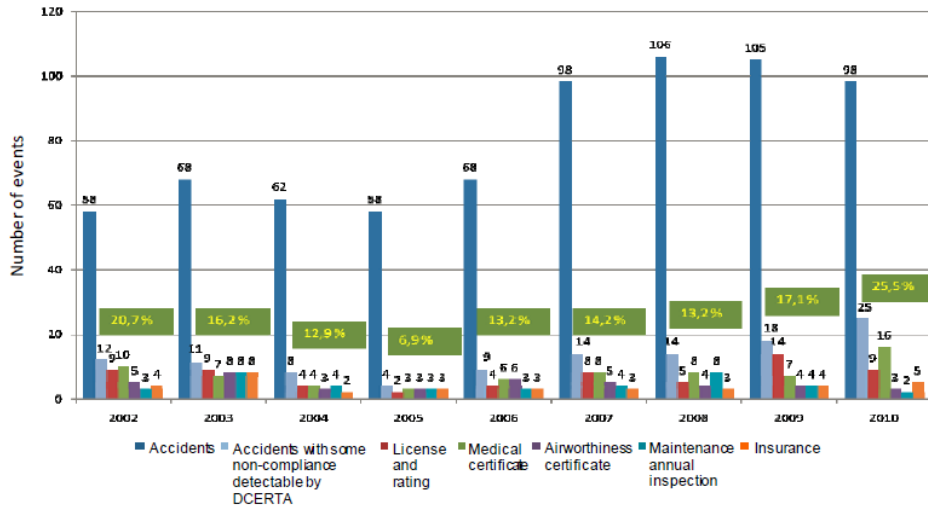
Brezilya Ulusal Sivil Havacılık Ajansı (ANAC), Genel Havacılık sektöründeki kaza ve olay verilerini analiz ederek, kazayla sonuçlanan operasyonların büyük bir kısmının regülasyonlara bir şekilde uyumsuzluk gösterdiğini gözlemlemiştir. Genel Havacılık sektöründeki işleticilerin sayıca çok fazla oluşu ve ANAC'ın hem finans hem de insan kaynakları konusundaki sınırlamaları nedeniyle, bu durumların denetim faaliyetleriyle kontrol edilmesi zor olmuştur. ANAC, bu sorunu çözmek amacıyla, veriye dayalı bir yöntem ile risk odaklarını tespit etmek ve denetimleri optimize etmek için sistematik bir yaklaşım oluşturma kararını vermiştir.

ANAC, "Emniyetli Kalkış Sistemi" olarak çevrilen *Sistema Decolagem Certa* (DCERTA) aslı sistemi geliştirmiştir. Bu sistem; yapıldıkları anda uçuş planlarını toplar ve Ajans'ın veritabanına erişerek her bir uçuş için pilot lisansları, yetkileri, sağlık raporu, uçak sertifikası ve operasyonel prosedürlerle ilgili uygunsuzlukları araştırır. DCERTA sistemi ile toplanan bu veriler, temelde regülasyon uyum verileri olup, toplum için emniyet havacılık hizmetlerinin güvence altına alınması amacıyla regülasyonlar yürürlüğe konduğunda aynı zamanda emniyetle ilgili veriler halini de almaktadır.

Veriler; en sık karşılaşılan uyumsuzlukları, her bir uyumsuzluğun daha sık ortaya çıktığı bölgeleri ve hatta uyumsuzluk oranı daha yüksek olan hizmet sağlayıcılarını tespit etmek amacıyla kullanılmaktadır. Hafifletici önlemler alınırken iki farklı yaklaşım sergilenmektedir:

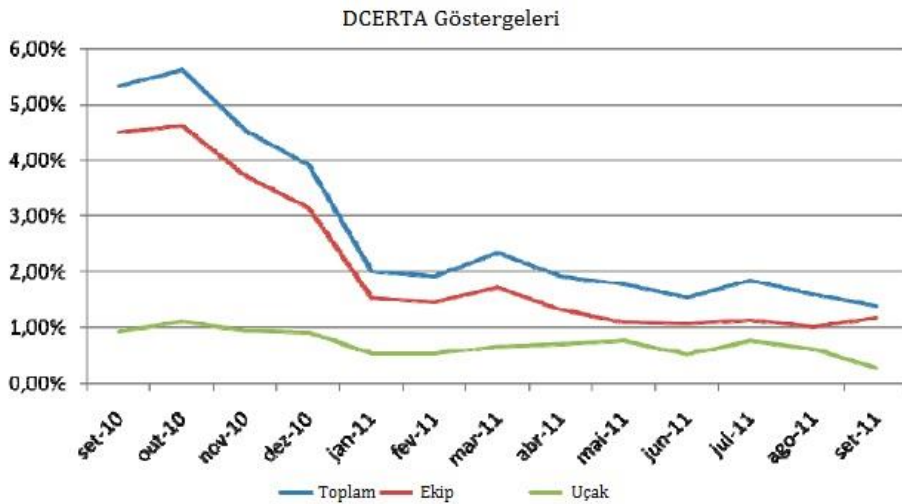
1. Öncelikle; ihlal olduğu teyit edildikten sonra uyumsuzluk, düzenlemelere uygun olarak ele alınmalıdır. Bu yaklaşım *reaktif risk yönetimi* olup, hizmet sağlayıcının kanunlara aykırı ve dolayısıyla emniyetsiz operasyonlarını sürdürmesini önlemek amacıyla ihlalleri cezalandırmaktadır.
2. İkinci yaklaşım ise, *proaktif risk yönetimidir*. Verilerin istatistiki olarak analiz edilmesi ile, en "uyumsuz" işleticilerin ve söz konusu işleticilere hangi sektörde daha çok dikkat edilmesi gerektiğini (örneğin; personel lisanslarının kontrolünü olması gereken seviyenin altında gerçekleştiren bir işletici) tespit etmek mümkündür. Bu, ANAC'ın daha yüksek riske sahip olduğu tespit edilen işleticilere ilişkin düzenli denetimler planlayarak daha büyük bir olay meydana gelmeden önce söz konusu işleticilerin operasyonlarını düzeltmesine imkân vermektedir.

Proaktif risk yönetimi yaklaşımında, uçak işleticilerini uzaktan denetlemek ve hem göstergeleri hem de ileride elde edilecek hedefleri tanımlamak mümkündür. Örneğin; ANAC, pek çok havacılık sektörünü (ticari havacılık, talimat, genel havacılık vb.) uç ana gösterge ile denetlemektedir: biri uyumsuzlukların tamamına yönelik, biri personel ile ilgili uyumsuzluklar, diğeri ise uçak ile ilgili uyumsuzluklar. Uyumsuzluklar ve emniyetsiz operasyonlar arasındaki ilişkin 4 ve 5 sayılı Şekillerde görülebilmektedir.



Şekil 5: Uyumsuzluklar ve İlişkili Olaylar

Şekil 5'teki mavi çubuklar, Brezilya Sivil Havacılığındaki (genel havacılık dahil) kazaların miktarını temsil ederken, diğer çubuklar DCERTA Sisteminin tespit ettiği farklı bir uyumsuzluğu temsil etmektedir.



Şekil 6: DCERTA Göstergeleri

Şekil 6'daki mavi çizgi, DCERTA Sisteminde birtakım uyumsuzlukları temsil eden uçuşların yüzdesini göstermektedir. Kırmızı çizgi, ekip durumu ile ilgili uyumsuzlukları

gösterirken yeşil çizgi, uçak durumlarını göstermektedir. Grafikten görüldüğü üzere, 2011 Eylül döneminde ortaya çıkan birtakım uyumsuzlukları temsil eden uçuşların sayısı, toplam uçuş sayısının %1.5'inden az bir yüzdeye tekabül etmektedir. Diğer yandan; Şekil 5'te, kazayla sonuçlanan operasyonlar arasında birtakım uyumsuzluklar gösteren uçuşların sayısı, 2010 yılındaki toplam uçuşların %25.5'ini temsil etmektedir.

Uyumsuzluk ile operasyon dahilindeki risk seviyesi arasındaki ilişkiyi çok net bir şekilde gösteren analiz, DCERTA'nın Brezilya Sivil Havacılık Ajansı'nın emniyet riski yönetimi için çok yararlı bir araç olduğunu ortaya koymaktadır.

BÖLÜM 4

Hizmet Sağlayıcılara Yönelik Olarak Emniyet Performansının Ölçülmesine İlişkin Kılavuz İlkeler

Yönetici Özeti

Bu dokümanın amacı, emniyet yönetim sisteminizin kapsamında yer alan bir dizi emniyet performans göstergesinin tanımlanmasına ve uygulanmasına ilişkin kılavuz ilkeler sağlamaktır.

Bu doküman kapsamında, şirketinizin sistemik ve operasyonel sorunları göz önünde bulunduran etkin emniyet yönetimi potansiyelini arttırmayı amaçlayan bir emniyet performans ölçümü yaklaşımı önerilmektedir. Etkili emniyet performans ölçümü, emniyet yönetim sisteminizi mükemmele doğru yönlendirmede belirleyici olacaktır.

Bu dokümanın genelinde:

- 'Hizmet sağlayıcı' terimine yapılan herhangi bir atıf, havacılık ürünlerinin ve hizmetlerinin sağlayıcılarını kapsamaktadır;
- 'Operasyonlar' terimine yapılan herhangi bir atıf, havacılık emniyeti yönetmelikleri ile düzenlenen temel faaliyetleriniz anlamına gelmektedir ve
- 'Düzenleyici' terimine yapılan herhangi bir atıf, geniş anlamda, havacılık emniyetinin yönetilmesi ile ilgili tüm Devlet görev ve sorumluluklarını kapsamak üzere kullanılmaktadır.

Bu dokümanın genelinde kullanılan terimler ve tanımlar ile ilgili olarak, Uluslararası Sivil Havacılık Örgütü (ICAO) Annex 19 Baskı 1 ve Emniyet Yönetimi Uluslararası İşbirliği Grubu (SM ICG) Emniyet Yönetimi Terminoloji dokümanında yer alan tanımlar göz önünde bulundurulmaktadır.

1. Kavram

1.1. Emniyet performansı nedir?

ICAO Annex 19 kapsamında, **emniyet** terimi, 'uçak operasyonu ile ilgili olan veya uçak operasyonunu doğrudan destekleyen havacılık faaliyetleri ile ilgili risklerin, kabul edilebilir bir seviyeye düşürülerek kontrol edilmesi durumu' olarak tanımlanırken, **emniyet performansı** terimi, 'hizmet sağlayıcının, emniyet performansı hedefleri ve emniyet performansı göstergeleri doğrultusunda tanımlanan emniyet başarısı' olarak tanımlanmaktadır. Bu tanımlar, emniyet performansının ölçülmesi ilgili karmaşıklığın iyi bir göstergesidir. Birçok alanda, emniyet metrikleri, ölçümü kolay olduğu ve genellikle daha fazla dikkat çektiği için, ciddi olaylara ve kazalara odaklanmaya eğilimlidir. Emniyet yönetimi açısından, bu gibi olumsuz olaylara odaklanması hususuna, dikkat edilmelidir; çünkü:

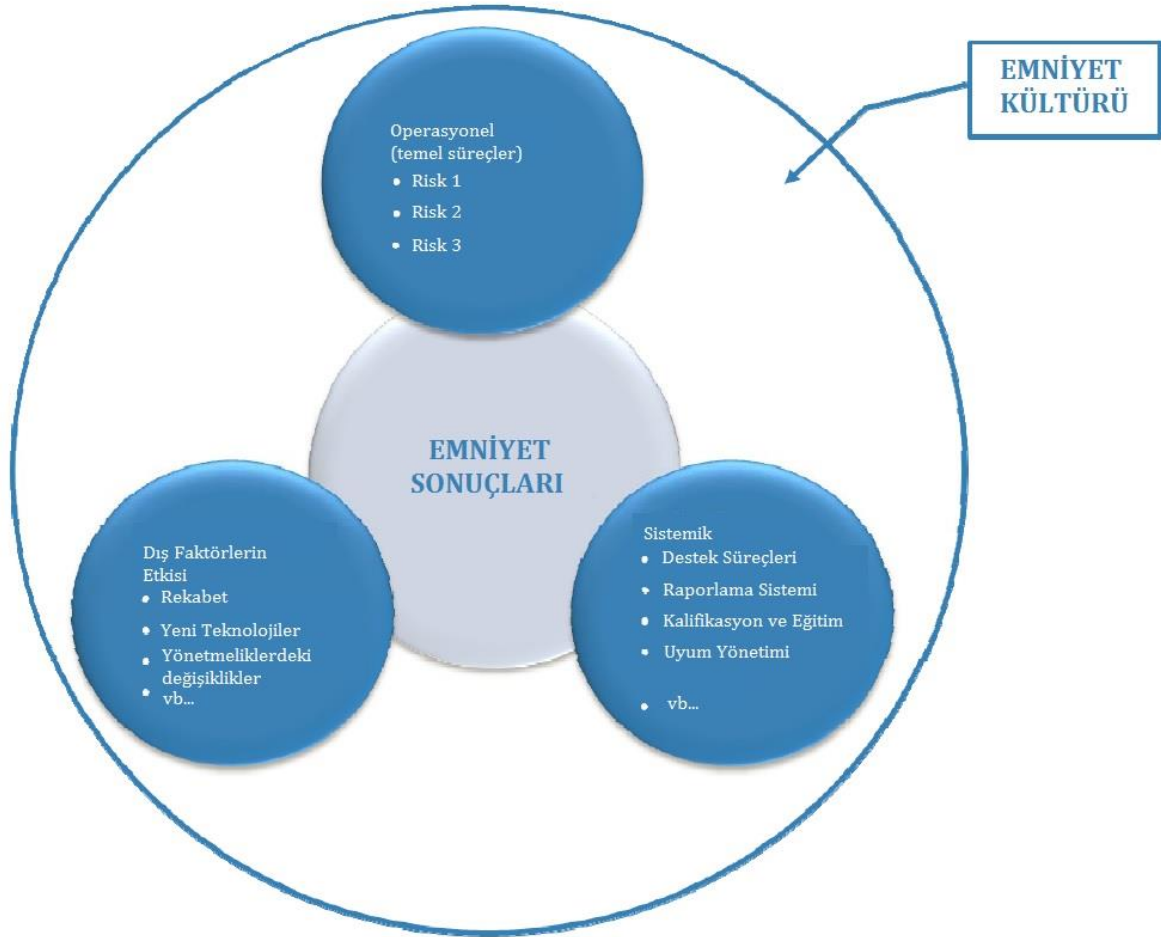
- oldukça olumsuz sonuçların düşük sayıda gerçekleştiği havacılık gibi sistemlerde, bu tür sonuçların düşük sıklıkta gerçekleşmesi, sisteminizin emniyetli olduğuna dair yanlış izlenim verebilir;
- (edinilecek bilgiler doğrultusunda) hareket etmek üzere gerekli olan bilgiler çok geç elde edilebilir;
- nihai sonuçların sayımı, aynı koşullar altında, oldukça olumsuz sonuçlara sebep olması muhtemel olan sistemik faktörlerin, tehlikelerin veya gizli koşulların herhangi birini açığa çıkarmayacaktır ve
- herhangi bir sistemin esnekliğinin azalmış olduğu durumlarda, bu tür sonuçların tesadüfen oluşma olasılığı daha yüksektir; bu nedenle, bu sonuçlar, sonraki olayları öngörememeleri halinde, yersiz bir dikkat çekebilir ve yetersiz kaynaklar kullanabilir.

Havacılık sistemi nihai emniyet sonuçlarını etkileyebilecek çok sayıda farklı oyuncu, etkileşim, bağımlılık ve parametreye sahip olan oldukça dinamik ve karmaşık bir sistem olduğundan dolayı, sorun daha da karmaşıktır. Bu nedenle, çoğu durumda, spesifik parametreler veya emniyet aksiyonları ile nihai toplam emniyet sonucu arasında doğrusal bir ilişki kurulması mümkün değildir. Dolayısıyla, mutlak emniyet ölçümü kendi başına başarısızdır. Emniyet seviyesini tamamlayan birçok model (ve buna karşın riske maruz kalma seviyesi) olmasına rağmen, göstergeler, daima, bu seviyelerin hatalı belirleyicilerini teşkil edecektir.

Emniyet, riskin söz konusu olmaması durumunun ötesinde bir husus olup, bilinen riskler ile başa çıkmak, henüz bilinmeyen bu riskler ile başa çıkmak için hazırlıklı olmak ve zaman içerisinde risk kontrollerinin doğal "erozyonunu" ele almak üzere, belirli sistemik emniyet sağlayıcılarının daima sağlanmasını gerektirmektedir. Dolayısıyla, şirketinizin bakış açısı doğrultusunda, doğrudan emniyet ölçümleri olamaz.

Ölçümler, özellikle, emniyetli sonuçlara yönelik organizasyonel sağlayıcıları, tanımlanan risklere yönelik belirli emniyet kontrollerini ve bariyerlerini teşkil edecek unsurlar olarak, sisteminizin emniyetli sonuçların sağlanmasına yönelik olarak tasarlanan özelliklerine odaklanmalıdır. Ayrıca, ölçümlerin, dış faktörlerin söz konusu kolaylaştırıcı unsurları, risk kontrollerini ve bariyerlerini nasıl etkilediğini veya bu kontrollerin ve bariyerlerin birbirlerini nasıl etkilediğini de ele alması gerekmektedir. Bu yaklaşım, örneğin, Uluslararası Standartlar Örgütü (ISO) 9000 serisi standartları ile desteklenen kalite yönetimi alanındaki mevcut sanayi uygulamaları ile uyumlu olup, ortaya çıkan sonucun doğrudan ölçülememesi halinde, bunun yerine, alt sistemlerin ve süreçlerin valide edilmesi gerekmektedir.

Yukarıda belirtilen esaslar, gerek herhangi bir düzenleyici otoritenin bakış açısından gerek her bir hizmet sağlayıcının bakış açısından geçerli olup, her durumda, emniyet performansının sistemik, operasyonel ve harici bileşenlerinin dinamik yapısı göz önünde bulundurulmalıdır.



Şekil 1: Emniyet performansı bileşenleri

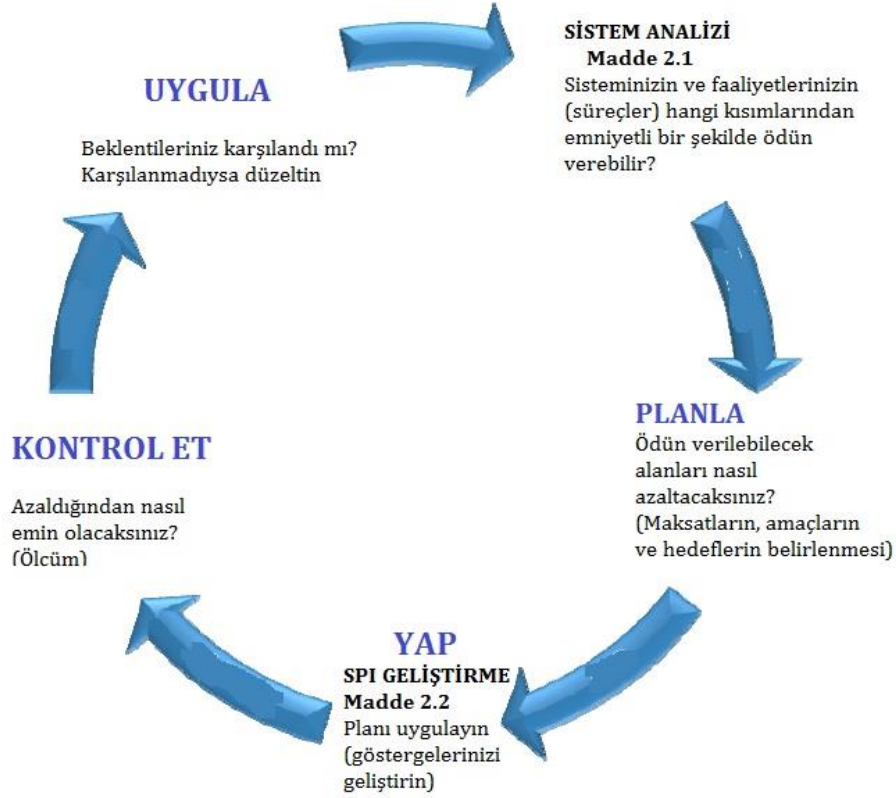
1.2. Emniyet performansı neden ölçülür?

ICAO Emniyet Yönetim Sistemi (SMS) standartları ve önerilen uygulamalar, kuruluşunuzun emniyet performansını doğrulayacak ve emniyet risk kontrollerinin etkinliğini valide edecek yöntemlerin geliştirilmesini ve muhafaza edilmesini sağlamaktadır.

Şirketinizin 'fonksiyonlarının', faaliyetlerini nasıl sunacağına ilişkin analiz ve değerlendirme, emniyet politikanızın, ilgili emniyet hedeflerinizin ve bunlara uygun emniyet performans göstergelerinin ve hedeflerinin tanımlanmasına yönelik zemin oluşturmaktadır.

SMS, işletme yönetiminin diğer unsurlarıyla (örneğin; kalite, finans) olduğu gibi sistematik bir yaklaşım gerektirmekte olup, bu bağlamda, emniyet performans ölçümü, yönetim ve etkili kontrol için gerekli olan bir unsur sağlamaktadır: "geri bildirim".

- Geri bildirim, yönetimin, kuruluşunuzun emniyet açısından ne kadar iyi çalıştığına ilişkin analizi ve değerlendirmeyi valide etmesine ve gerekli düzenlemeleri gerçekleştirmesine olanak tanıyacaktır (Planla-Yap-Kontrol Et-Uygula).
- Yönetiminize sağlanan geri bildirim, karar verme ve kaynak tahsisinde rehberlik sağlayacaktır.
- Tüm personele sağlanan geri bildirim, herkesin, şirketinizin emniyet başarıları hakkında bilgi sahibi olmasını sağlayacaktır. Bu husus, bağlılığın oluşturulmasını sağlayacak ve şirketinizin emniyet kültürünün geliştirilmesine katkıda bulunacaktır.



Şekil 2: Ölçüm döngüsü

Etkili bir emniyet performansı ölçümü, yalnızca emniyet ile ilgili değil, aynı zamanda, etkinlik ve kapasite ile ilgili iyileştirme olanaklarının belirlenmesini destekleyecektir.

Emniyet yönetimi, faaliyetlerinize yönelik emniyetli sonuçlar elde edilmesini sağlamak üzere, kuruluşunuzun, organizasyonel performansınızı sistematik bir şekilde tahmin etme, izleme ve daha da geliştirme yeteneklerine dayanmaktadır. Etkili bir emniyet yönetimi, sisteminizin ve süreçlerinizin kapsamlı bir şekilde anlaşılmasını ve sağlıklı bir şekilde yönetilmesini gerektirmektedir. Bu husus, herhangi bir ölçüm yapılmadan sağlanamaz. Ölçümü kolay olan sonuçları rastgele seçmek yerine, şirketinizin, emniyet yönetimi kabiliyetlerinin doğru bir şekilde değerlendirip geliştirilebilmesini sağlamak için gerekli olan geri bildirim türünü göz önünde bulunduran emniyet performans göstergelerini seçmelisiniz. Bu husus, sisteminizin temel özelliklerini ve operasyonları içeren ve bu temel özelliklerin farklı yollarla ölçülmesini sağlayan geniş bir göstergeler grubu kullanarak, kuruluşunuzun tüm seviyelerindeki performansı ölçmeniz gerekeceği anlamına gelmektedir.

1.3. 1.3 Nasıl Ölçülür: emniyet performansı göstergelerinin türleri

ICAO kapsamında, **emniyet performans göstergesi** terimi, 'performansın izlenmesinde ve değerlendirilmesinde kullanılan veri tabanlı bir emniyet parametresi olarak tanımlanırken, **emniyet performans hedefi** terimi, 'belirli bir süre boyunca emniyet performansı göstergesine/göstergelerine ilişkin olarak planlanan ve amaçlanan hedef.' olarak tanımlanmaktadır.

Emniyet performans göstergeleri (SPI), spesifik özellikler doğrultusunda sınıflandırılabilir; farklı alanlarda genellikle farklı sınıflandırmalar kullanılmaktadır. Bu dokümanda tanımlanan gösterge türleri, ortak noktaları belirlemek için yaygın olarak kullanılan sınıflandırmaların ve tanımların incelenmesinden sonra tanımlanmıştır. Her birinin kullanımıyla ilgili bir açıklama yapılmıştır. Spesifik emniyet performans göstergeleriniz için uygun gördüğünüz terimleri kabul edebilirsiniz; aşağıdaki bilgiler, etkili bir emniyet performansı ölçümü için gerekli olan kavramsal bilgileri desteklemek üzere sağlanmaktadır.

- **Gecikmeli göstergeler**

'Önemeye çalıştığınız istenmeyen emniyet olayları da dahil olmak üzere daha önce meydana gelen emniyet olaylarını ölçmek üzere kullanılan metrikler' (SM ICG).

Gecikmeli göstergeler, özellikle, kuruluşun önlemeyi amaçladığı olumsuz sonuçlar olmak üzere, emniyet olaylarına yönelik ölçümlerdir. Gecikmeli göstergeler, ağırlıklı olarak, yüksek düzeyde ya da belirli olay türlerine veya konularına ilişkin toplam, uzun vadeli eğilim için kullanılmaktadır. Emniyet sonuçlarını ölçtüklerinden dolayı, emniyet ölçümlerinin, aksiyonlarının veya girişimlerinin etkinliğini değerlendirmek için kullanılabilirler; bunlar, sistemin emniyet performansını valide etmek üzere kullanılan bir yöntemdir. Ayrıca, bu göstergelerdeki eğilimler, ele alınması gereken mevcut sistemlerde gizli koşulların mevcut olup olmadığını belirlemek üzere analiz edilebilir.

Genel olarak, iki tür gecikmeli gösterge tanımlanmaktadır:

1. Kazalar veya ciddi olaylar gibi oldukça şiddetli seviyedeki olumsuz sonuçlara ilişkin göstergeler.

Oldukça şiddetli seviyedeki olumsuz sonuçların meydana gelme sıklığının düşük olması, toplamın (örneğin; sektör segmenti düzeyinde veya bölgesel düzeyde), daha anlamlı analizler üretebileceği anlamına gelmektedir.

Örnek: her 1000 inişte meydana gelen pistten çıkmaların sayısı.

2. Kendilerini ciddi olaylarda veya kazalarda (sistem hataları ve prosedürel

sapmalar da dahil olmak üzere) göstermeyen alt düzey sistem hatalarına ve emniyet olaylarına ilişkin göstergeler; ancak, emniyet analizi, diğer emniyet olayları veya koşullar ile birlikte ele alındığında, ciddi bir olaya veya kazaya neden olma potansiyelinin bulunduğunu göstermektedir. Bu tür göstergeler, bazen 'öncü olay' göstergeleri olarak adlandırılmaktadır¹.

Daha düşük düzeydeki sistem arızalarına ve emniyet olaylarına ilişkin göstergeler, öncelikli olarak spesifik emniyet sorunlarını izlemek ve söz konusu tehlikeler ile bağlantılı riskleri azaltmak üzere uygulanan emniyet kontrollerinin veya bariyerlerinin etkinliğini ölçmek için kullanılır.

Örnek: her 1000 inişte meydana gelen istikrarsız yaklaşımların sayısı

- **Öncü göstergeler**

'Geleceğe yönelik performansı etkileyebilecek olan mevcut durum hakkında bilgi sağlayan metrikler' (SM ICG).

Öncü göstergeler, gerek geleceğe yönelik olumsuz bir sonuca haline gelme veya katkıda bulunma potansiyeline sahip hususları ('olumsuz' göstergeler) gerek emniyete katkıda bulunan hususları ('olumlu' göstergeler) ölçmelidir. Herhangi bir emniyet yönetimi perspektifinden bakıldığında, şirketinizin emniyet yönetimi kabiliyetini oluşturan olumlu faktörlerin artırılmasını sağlamak üzere olumlu göstergelerin izlenmesine yeterli bir şekilde odaklanılması önem arz etmektedir.

Özellikle herhangi bir yönetim açısında ilgili olan öncü göstergeler, emniyet yönetimi önceliklerinin etkili olmasını sağlamak ve emniyet iyileştirme aksiyonlarını belirlemek için kullanılabilir. Bu tür bir göstergeyi, özellikle Emniyet Yönetim Sisteminin (SMS) ilk olarak uygulanması sırasında, şirketinizin emniyet yönetimi kabiliyetlerini proaktif bir şekilde geliştirmek için bu gösterge türünü ('tahrik') kullanabilirsiniz. Bu husus, performans hedeflerinin belirlenmesini gerektirebilir.

¹ Bu terim kullanılırken dikkate edilmelidir: Bir olay veya durum, daha ciddi bir olayın veya durumun öncüsü olarak tanımlanmadan önce (örneğin, kazaların öncüsü olarak meydana gelen olaylar), ikisi arasında açık bir korelasyon bulunması sağlanmalıdır. Bu korelasyon, ölçüm geçerliliği kavramının temelini oluşturmaktadır. "Öncü" olarak tanımlanan olaylara neden olan faktörler, söz konusu olaylar ile öngördüğü varsayılan olayların meydana gelme olasılığı arasında ortak olmalıdır.

Örneğin: Tehlike tanımlama ve emniyet risk yönetimine tabi olan Standart İşletim Prosedürlerine ilişkin olarak gerçekleştirilen değişiklik yüzdesi

Öncü göstergeler, yönetiminize, sisteminizin dinamikleri ve işletim ortamındaki değişiklikler de dahil olmak üzere, herhangi bir değişiklikte nasıl baş çıkıldığı konusunda bilgi sağlamak üzere kullanılabilir. Odak noktası; aksiyon ihtiyacını belirlemek üzere ortaya çıkan zayıf noktaların ve zaafaların tahmin edilmesine veya emniyet için gerekli olan belirli faaliyetlerin gerçekleştirildiği kapsamın takip edilmesine odaklanacaktır. Söz konusu 'izleme' göstergelerine ilişkin olarak uyarı seviyeleri tanımlanabilir.

Örneğin: İşin, Standart İşletim Prosedürlerine uygun olarak gerçekleştirildiği kapsam

Öncü ve gecikmeli göstergeler kavramı, havacılık dışındaki alanlarda uzun yıllar var olmuştur. Özellikle, ekonomistler, bu kavramları, ekonominin sağlığını ölçmek üzere bir araç olarak kullanmaktadır.

Emniyet performans ölçümünde, ideal olarak, öncü ve gecikmeli göstergeler kombinasyonunu göz önünde bulundurulmalıdır. Temel odak noktası, şirketinizin bünyesinde etkili bir emniyet yönetiminin gerçekleştirilmesini sağlayan sistemik ve operasyonel özelliklerin varlığının ölçülerek bu doğrultuda hareket edilmesi olmalıdır ve söz konusu emniyet yönetiminin etkili olmasını sağlamak için gecikmeli göstergeler kullanılmalıdır. Spesifik emniyet aksiyonlarının ve risk bariyerlerinin etkinliğini valide etmek veya öncü göstergelerinizden elde edilen bilgilerin analizini desteklemek için, bilhassa alt düzey sistem hatalarına ilişkin göstergeler olmak üzere, gecikmeli göstergeler kullanışlıdır.

2. Emniyet performansı ölçüm süreci

2.1. Etkili bir emniyet performansı ölçümüne ilişkin ön koşullar

Esas itibarıyla, emniyet performansınız, emniyetli sonuçlar elde etmek için gerekli olan organizasyonel unsurları uygulama ve muhafaza etme kabiliyetiniz doğrultusunda belirlenmektedir. Emniyet Yönetim Sisteminizin (SMS) amacı, bu kabiliyeti oluşturmak, muhafaza etmek ve sürekli geliştirmektir. Etkili bir emniyet sistemine ilişkin bir ön şart olarak, kuruluşunuzun, organizasyon yapılarınız, politikalarınız, prosedürleriniz, süreçleriniz, personeliniz, ekipmanınız ve tesisleriniz hakkında doğru ve güvenilir bir tanımlama yapacak bir sistem analizi gerçekleştirilmesi gerekmektedir. Bu analiz kapsamında, bilhassa, sistem bileşenleri ve dış faktörler arasındaki etkileşimlere odaklanılmalıdır. Bu, sistem unsurlarınızın ve faaliyetlerinizin, beklenen emniyet sonuçlarını üretmek için nasıl etkileşime girdiğine ilişkin bir model sunacak ve

sisteminizin güçlü ve zayıf noktalarını tespit etmenizi sağlayacaktır. Faaliyetlerinizin nasıl beklenen sonuçları verdiği ile ilgili sistem açıklaması ve ilgili model, emniyet performansını artırmak için ölçülmesi gereken husus ve kuruluşunuzun emniyet performansını etkileyebilecek olan unsurların tamamını gözlemlemek için izlenecek olan husus hakkında sizi bilgilendirecektir².

Tasarım ve üretim kuruluşlarına ilişkin sistem açıklaması ve tehlike tanımlama kılavuzu, örneğin, Federal Havacılık İdaresi (FAA) Uçak Sertifikasyon Hizmeti (AIR) SMS Pilot Proje Kılavuzu kapsamında bulunabilir. Bu rehber dokümanda geliştirilen unsurların çoğu, diğer sektörler için uyarlanabilir³. Düzenleyici otoritelere yönelik olarak tasarlanmasına rağmen, SM ICG SMS Değerlendirme Aracı⁴, Emniyet Yönetim Sisteminizin (SMS) tamlığını ve yeterliliğini değerlendirmede yararlı olabilir. Kurum içi denetim sisteminiz ve düzenleyici otorite denetimleri ve incelemeleri, ilgili alanları veya kritik emniyet görevlerini de belirleyebilir.

Kuruluşunuzun, ISO 9001 / AS9100 veya muadili standartlar kapsamında tanımlananlar gibi bir kalite yönetim sistemine sahip olması halinde, mevcut sistem ve süreç tanımı, sistem analiziniz için bir başlangıç noktası olmakla birlikte, sistem ve süreç tanımınızın havacılık emniyetinin yanı sıra iş risklerini uygun bir şekilde ele almasını sağlamalısınız.

Analiz ve değerlendirme de dahil olmak üzere sistem tanımlamasının tamamlanmasının ardından, şirketiniz emniyet ile ilgili olarak bulunduğu konumu anlamış veya teyit etmiş olmalıdır. Bu egzersiz sayesinde aşağıdaki hususları tespit etmiş olmalısınız:

Sistemik düzeyde:

- etkili bir emniyet yönetiminin sağlayıcılarını oluşturan unsurların mevcut, uygun ve etkili olup olmadığı;
- etkili bir emniyet yönetimi için eksik olan unsurlar;
- unsurların birbirleriyle ve kuruluşunuzun temel yönetimi ve operasyonel süreçleri ile yeterince entegre olup olmadığı ve
- kuruluşunuzdaki zayıf noktalar ve zaafklar.

Operasyonel düzeyde:

- ele alınması gereken operasyonlara ilişkin temel riskler ('bir sonraki kazaya' neden olabilecek hususlar).

Bu, emniyet politikanızın yeterliliğini incelemek, emniyet hedeflerinizi tanımlamak veya uyarlamak ve emniyet performans göstergelerinizi türetmek üzere esas oluşturacaktır.

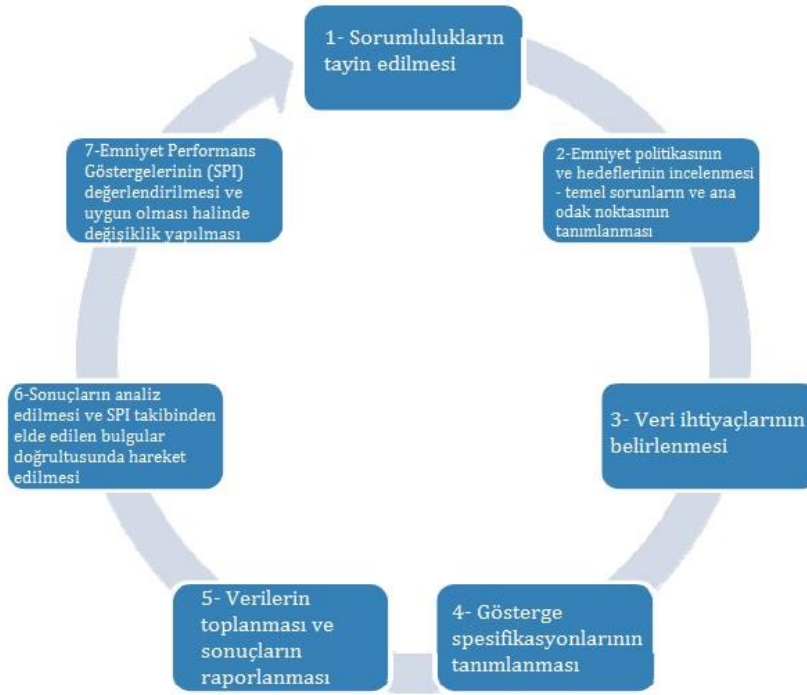
² Ayrıca, bkz. ICAO Doc 9859 3. Basım "7.4 SİSTEM TANIMI"

³http://www.faa.gov/about/initiatives/sms/pilot_projects/guidance/media/DM_SMS_PilotProjectGuide.pdf

⁴ http://www.skybrary.aero/index.php/SM_ICG_SMS_Evaluation_Tool

2.2. Emniyet performansı göstergelerinin tanımlanma ve incelenme süreci

Etkili bir emniyet yönetimi ile ilgili herhangi bir konuda olduğu gibi, emniyet performans göstergelerinin tanımlanması ve kullanılması dinamik bir süreç olmalıdır. Kendi emniyet performans göstergelerinizin geliştirilmesi ile ilgili olarak, sürekli gelişmeye yönelik 'Planla-Uygula-Kontrol Et-Önlem Al' mantığına uygun olan adım adım bir süreç önerilmektedir. Bu, ilgili tüm personelin dahil olmasını ve katkıda bulunmasını sağlamanıza yardımcı olmalıdır.



Şekil 3: Süreç adımları

1. Adım: Sorumlulukların tayin edilmesi

Genel anlamda SMS süreci açısından, yönetiminizin, Emniyet Performans Göstergelerini (SPI), şirketinizin emniyet yönetimi yaklaşımının temel bir parçası olarak tam anlamıyla uygulaması SPI projesinin başarılı olması için önem arz etmektedir. Yönetim, yalnızca herhangi bir SPI sistemini desteklemek yerine, kuruluşunuzun, ölçüm ve yönetim gerektiren yönlerini tanımlamalı ve sonrasında, emniyet politikası ve tanımlanan emniyet hedefleriniz gereğince bu unsurların yönetilmesine ilişkin sistematik bir yaklaşım uygulamalıdır.

Emniyet Performans Göstergelerinin (SPI) oluşturulması için ilk adım, yönetimin, Emniyet Performans Göstergelerinin (SPI) tanıtımının etkili bir şekilde sağlanmasına ve koordine edilmesine ilişkin sorumlulukları yerine getirecek bir personel tayin etmesi

olacaktır. Bu, emniyet yönetimi ile ilgili mevcut organizasyonel planınızı göz önünde bulundurarak, etkili bir iletişimin sağlanması ve genel olarak uygulamanın denetlenmesi sorumluluğunu gerektirecektir. Söz konusu personel (bundan böyle 'SPI ekibi' olarak anılacaktır), ideal olarak, emniyet ve/veya kalite yönetimi esaslarına ve veri analizine ilişkin olarak uygun tecrübeye ve bilgiye sahip personelden oluşmalı ve bu personelin söz konusu bilgilere erişim hakkı olmalıdır.

Ayrıca, söz konusu personelin, bu bilgileri ve bu becerileri politikalarınız, programlarınız, operasyonel prosedürler ve uygulamalarınız bağlamında uygulama deneyimi olmalıdır. 'Uzmanlar', ölçüm uzmanlığı sağlamak ya da SPI geliştirme sürecini desteklemek/kolaylaştırmak üzere kullanılsalar dahi, süreç sahipleri doğrudan müdahil olmalıdırlar. Ayrıca, süreç sahiplerinin, süreçlerine ilişkin emniyet performansı ölçümünün mülkiyetini almaları gerekmektedir. SPI ekibinin (ya da kuruluşunuzun büyüklüğüne ve karmaşıklığına bağlı olarak tayin edilmiş sorumluluklara sahip olan şahısların), yönetim ve süreç sahiplerine destek ya da danışmanlık sağlayıcı bir role sahip oldukları açıkça gösterilmelidir.

Yönetim, ilerleyiş ile ilgili olarak düzenli bir şekilde bilgilendirilmeli ve Emniyet Performans Göstergelerinin (SPI) uygulanması sürecinin yönlendirilmesinde etkin bir rol almalıdır. Daha büyük kuruluşlar ile ilgili olarak, bilhassa, şirketinizin, gelişmiş bir kaynak tahsisi sağlayacak olan "yönetim bilgi sistemi" üzerindeki olumlu etkilerine odaklanılarak, SPI geliştirme projesine ilişkin bir maliyet ve fayda analizi geliştirilmesi yararlı olabilir.

Son olarak, SPI ekibi, Emniyet Performans Göstergelerinin (SPI) geliştirilmesi ile ilgili olarak yeterli seviyede bir ilerleme sağlamak amacıyla, önemli hususlar da dahil olmak üzere, makul bir zaman çizelgesi oluşturmalıdır.

2. Adım: Emniyet politikasının ve hedeflerinin incelenmesi - temel sorunların ve ana odak notasının tanımlanması

Bu adımda, SPI ekibi, Emniyet Yönetim Sisteminizin (SMS) tamlığına ve yeterliliğine özellikle dikkat ederek ve sistem analizinin sonuçlarını göz önünde bulundurarak, ölçümün kapsamını ve odak noktasını belirlemelidir (Madde 2.1).

Spesifik operasyonel emniyet sorunlarına ilişkin göstergeleri tanımlamak üzere, operasyonel Emniyet Performans Göstergelerinin (SPI) tanımlanması için en uygun olan emniyet aksiyonlarını ve risk bariyerlerini belirlemede kullanılabilir olan bow-tie metodolojisi⁵ veya benzeri araçlar kullanılabilir. Operasyonlarınıza yönelik emniyet tehditlerini iyi anlamanızı sağlamak için, sistem analizinizin bir parçası olarak kapsamlı bir tehlike tanımlaması gerekecektir.

⁵ http://www.skybrary.aero/index.php/Bow_Tie_Risk_Management_Methodology

SPI ekibi, ayrıca, sektör segmentiniz içerisinde kullanılan tipik göstergeleri inceleyerek, bu göstergelerin kuruluşunuz ile ilgili olup olmadıklarını belirlemek için değerlendirebilir. Örneğin, sistem analiziniz, raporlama yapmak için kolaylıkla erişilebilen bir araç olmadığını veya gizlilik ile ilgili kaygılar bulunduğunu tespit etmesi halinde, kurum içi rapor sayısının ölçülmesi anlamlı olmayabilir.

3. Adım: Veri ihtiyaçlarının belirlenmesi

Anlamlı olmak amacıyla, performans ölçümleri, gerek nitelik gerek nicelik açısından güvenilir ve geçerli verilere dayandırılmalıdır. Bu nedenle, SPI ekibi, şirketinizde mevcut olan tüm ilgili verileri ve bilgileri tanımlamalı ve ihtiyaç duyulan ilave bilgileri belirlemelidir. Ayrıca, kurum içi denetim/uygunluk izleme sistemi aracılığıyla elde edilen bilgileri de göz önünde bulundurmalıdır.

Veri türüne bakılmaksızın; verilerin analiz amaçları doğrultusunda bir araya getirilerek uygun şekilde kullanılmasının sağlanması konusunda en önemli faktörlerden biri kalitedir. Veri kalite esasları ve uygulamaları, veri yakalama ve entegrasyonu sürecinden analize kadar süreçlerin tamamında uygulanmalıdır. Gerekli veri özellikleri ve veri yönetimi ile ilgili kılavuz bilgiler, SM ICG "Risk Bazlı Karar Alma Esasları" dokümanında bulunmaktadır⁶.

Ölçmeniz gereken hususları tanımlamak yerine, kendilerini ölçülmek üzere sunan hususları tanımlamak cazip gelebilir. Bu, muhtemelen, etkili bir güvenlik yönetimi için en değerli olan Emniyet Performans Göstergelerinden (SPI) ziyade en açık ve kolay ölçülebilen Emniyet Performans Göstergelerinin (SPI) tanımlanmasına neden olur. Bu nedenle, sürecin bu adımında, kuruluşunuzun hangi değişiklikleri "uygulamak" istediğine ve hangi hususları "izleme" ihtiyacı duyduğuna odaklanmak önemlidir. Ayrıca, sistem emniyetini değerlendirmede etkili olabilmesi için, sisteminizin ve operasyonların temel yönlerini içeren geniş bir göstergeler dizisinin geliştirilmesi gerektiğini de göz önünde bulundurmalısınız; bu, dar ve dolayısıyla şirketinizin emniyet performansı hakkında potansiyel olarak kusurlu bir görünüme sahip olma olasılığını azaltacaktır.

Aynı zamanda, emniyet performansının gerçek seviyesi hakkında daha kesin bir fikir edinmek için aynı sistemin çeşitli şekillerde ölçülmesi gerekebilecektir. Örneğin; operasyonel parametreleri ölçmeden, yalnızca şirketinizin emniyet kültürünü değerlendirmek, emniyet performansının oldukça kısmi bir göstergesini sağlayacaktır.

Operasyonlarda tehlike tanımı ve risk yönetimi (temel süreçler) alanında, veri kullanılabilirliği, kısmen, kurum içi emniyet raporlama planlarının olgunluğuna bağlı olacaktır. Özellikle, Emniyet Yönetim Sisteminizin (SMS) henüz yeterli veri üretmediği durumlarda, sektör segmentiniz için toplam veriler de göz önünde bulundurabilecektir. Uçuş sayısı, filo büyüklüğü ve finansal ciro gibi diğer bilgiler, operasyonların bağlamının daha iyi anlaşılmasına katkıda bulunabilecektir. İlgili ve zamanında göstergeler üretmek için verilerin sürekli olarak kullanılabilirliği sağlanmalıdır. Göstergelerin üretimi için verilerin derlenmesindeki gecikmelerin, gerekli olabilecek her türlü emniyet aksiyonunu geciktirmesi muhtemeldir.

⁶ http://www.skybrary.aero/index.php/Risk_Based_Decision_Making_Principles

4. Adım: Gösterge spesifikasyonlarının tanımlanması

Emniyet Performans Göstergelerinizin (SPI) kapsamı ve odağı belirlenip, mevcut veriler/bilgiler incelendikten sonra, özelliklerin tanımlanması gerekmektedir. Her bir Emniyet Performans Göstergesi (SPI), herhangi bir kullanıcının, gerek bilgilerin kaynağını ve kalitesini belirlemesini gerek bu göstergenin etkili bir şekilde yorumlanması ve yönetilmesi için gerekli olan bağlamda yer almasını sağlayan yeterli bilgi (veya meta veriler) ile birlikte sağlanmalıdır.⁷

Mümkün olması halinde, karşılaştırma ve tespit etme eğilimlerini kolaylaştırdığından dolayı, göstergeler, kantitatif olmalıdır. Kantitatif metrikler, zaman içerisindeki emniyet performansındaki eğilimlerin veya beklenen emniyet sonuçlarından veya hedeflerinden sapmaların vurgulanmasını sağlayacak kadar kesin ve doğru olmalıdır.

Kalitatif Emniyet Performans Göstergeleri (SPI) ile ilgili olarak, sübjektifliğin en aza indirgenmesi önemlidir. Bu, Emniyet Performans Göstergelerinin (SPI) tanımlanması sürecinde doğrudan yer almayan personelin değerlendirilmesi yoluyla gerçekleştirilebilir.

Şirketinizin büyüklüğüne ve faaliyetlerinizin karmaşıklığına bağlı olarak, organizasyon yapınızdaki farklı süreçleri ve alt sistemleri yansıtmak üzere, Emniyet Performans Göstergelerinize (SPI) ilişkin hiyerarşik bir çerçeve tanımlanabilir. Sistemik sorunları değerlendirmeye yönelik birtakım göstergeler farklı süreçler ve alt sistemler için ortak olabilecek olmasına rağmen, operasyonel sorunları değerlendirmeye yönelik göstergelerin spesifik olması gerekecektir. Bu, Emniyet Yönetim Sisteminin (SMS) uygulanması için bir ön şart olarak tüm sistem bileşenlerini ve alt sistemleri tanımlayan doğru bir sistem analizi gerçekleştirmiş olmanın önemini vurgulamaktadır (Madde 2.1).

İyi bir Emniyet Performans Göstergesine (SPI) ilişkin hususlar aşağıdakileri içermektedir:

- Gösterge:
 - geçerli ve güvenilirdir;
 - ölçtüğü değişikliklere duyarlıdır ve
 - hesaplamada veya yorumlamada önyargılara karşı duyarlı değildir.
- Verilerin yakalanması maliyet etkindir.
- Gösterge:
 - genel olarak şirket operasyonlarında geçerli olup, ideal olarak daha büyük havacılık sektöründe geçerlidir ve
 - kolaylıkla ve doğru bir şekilde iletilmektedir.⁸

⁷ Aşağıdaki adreste söz konusu ilişkin bir örnek yer almaktadır:

http://aviationsafetywiki.org/index.php/Reporting_metadata_specification. Meta veriler; veri kaynakları, güncellik ve doğruluk ile ilgili bilgilerin yanı sıra diğer her türlü ilgili bilgileri içermelidir.

⁸ Emniyet kültürü göstergeleri - öncü emniyet performans göstergelerinin seçimi ve kullanımı, Reiman ve Pietikainen. Finlandiya VTT Teknik Araştırma Merkezi 2010:07

5. Adım: Verilerin toplanması ve sonuçların raporlanması

Emniyet Performans Göstergelerinizi (SPI) tanımladıktan sonra, verileri nasıl toplayacağınıza ve sonuçları nasıl raporlayacağınıza karar vermelisiniz. Veri toplama yaklaşımlarının (örneğin; veri kaynakları, verilerin nasıl derleneceği ve raporların nasıl görüneceği) yanı sıra toplama ve raporlama görevleri ve sorumlulukları da belirtilmeli ve dokümanite edilmelidir. Ayrıca, veri toplama prosedürleri kapsamında, verilerin toplanması gereken sıklık ve her SPI için raporlanan sonuçlar da göz önünde bulunmalıdır. Bu sorunlardan bazıları, 3. ve 4. adımlardaki Emniyet Performans Göstergelerine (SPI) karar verirken ele alınmış olacaktır.

Gösterge sonuçlarının sunum biçimi, hedef kitleyi göz önünde bulunduracak şekilde olmalıdır. Örneğin; aynı temel sorunu ele alan birkaç göstergelyi takip etmeniz halinde, üst yönetime raporlamaya yönelik olarak vurgulanacak olan en kritik göstergelerin bir alt grubunun tanımlanması yararlı olabilir. Gösterge sonuçlarının sunumu, herhangi bir sapmanın anlaşılmasını ve önemli eğilimlerin (örneğin, trafik ışıkları bulunan skorboardlar, histogramlar, doğrusal grafikler) tanımlanmasını kolaylaştırmalıdır.

6. Adım: Sonuçların analiz edilmesi ve SPI takibinden elde edilen bulgular doğrultusunda hareket edilmesi

Emniyet Performans Göstergelerinin (SPI) uygulanmasının nihai amacı şirketinizin emniyet performansını zaman içerisinde korumak ve geliştirmek olduğundan dolayı, bu, emniyet yönetimi açısından en ilgili adımdır. Sonuçlar kullanılmazsa, bilgi toplamanın hiçbir anlamı olmaz. Emniyet Performans Göstergelerinin (SPI), emniyet performansının göstergeleri olduğu, doğrudan emniyet ölçümleri olmadığı unutulmamalıdır. Farklı Emniyet Performans Göstergeleri (SPI) yoluyla toplanan bilgilerin, dikkatli bir şekilde analiz edilmesi gerekmekte olup, kuruluşun emniyet performansının genel bir resmini elde etmek için farklı sorunlara ilişkin olarak toplanan Emniyet Performans Göstergelerinin (SPI) perspektife yerleştirilmesi ve sonuçların yorumlanması gerekmektedir. Tek bir gösterge aracılığıyla elde edilen sonuçlar, ayrı olarak ele alındığında önemsiz olabilir, ancak, diğer göstergeler ile birlikte göz önünde bulundurulduğunda önemli olabilir.

Emniyet Performans Göstergeleri (SPI) arasındaki tutarsızlıklar, yanlış bir sistem açıklaması veya Emniyet Performans Göstergelerinin (SPI) kendileri ile ilgili sorunların bir göstergesi olabilir. Örneğin; aynı emniyet sorunu ile ilgili öncü ve gecikmeli göstergelerin, çelişkili sonuçlar vermesi veya sistemik göstergelerdeki olumlu bir eğiliminin, operasyonel göstergelerde olumsuz bir eğilime ile sonuçlandığı durumlar ile karşılaşabilirsiniz.

Metriklerin, emniyet açısından kritik olan bilgileri yakalayacak kadar iyi tanımlanmadığını tespit etmeniz halinde, Emniyet Performans Göstergeleri (SPI) incelenmelidir. Genel resimdeki herhangi bir tutarsızlık, yalnızca Emniyet Performans Göstergelerinin değil (bkz. 7. Adım), aynı zamanda, Emniyet Yönetim Sisteminizin (SMS) kendisinin öğrenilmesi ve ayarlanması için potansiyel bir fırsatı temsil eder.

Göstergeler, emniyet performansını iyileştirmekten ziyade, iyi bir skor elde etmek için alınan önlemler ile birlikte, sadece bir metrik olarak görülmemelidir. Emniyet Performans Göstergelerinin (SPI) toplanması, analizi ve yorumlanması yoluyla elde edilen sonuçların, karar ve aksiyon için yönetiminize iletilmesi önemlidir. İdeal olarak, bu sonuçların, eksikliklerin giderilmesi için veya sistemin daha da geliştirilmesi için hangi aksiyonların alınması gerektiğini belirlemek için düzenli toplantılarda (örneğin; yönetim incelemeleri, emniyet inceleme kurulu toplantıları) sunulmalıdır. Bu tür aksiyonların belirli göstergelere ayrı ayrı odaklanması değil, kuruluşunuzun genel emniyet performansını optimize etmeye odaklanması önemlidir.

Emniyet iletişiminizin ve teşvikinizin kapsamında, tüm personel, Emniyet Performans Göstergelerinin (SPI) toplanması, analizi ve yorumlanması yoluyla elde edilen sonuçlar hakkında bilgilendirilmelidir.

7. Adım: Emniyet Performans Göstergelerinin (SPI) değerlendirilmesi ve uygun olması halinde değişiklik yapılması

Metrikler ve tanımlanmış hedefler de dahil olmak üzere Emniyet Performans Göstergeleri (SPI) ve spesifikasyonları ile birlikte, kuruluşunuzun sistem analizi, periyodik olarak incelenmeli ve aşağıdaki hususlar göz önünde bulundurularak değerlendirilmelidir:

- edinilen tecrübenin değeri;
- tanımlanan yeni emniyet sorunları;
- riskin mahiyetinde değişiklikler;
- emniyet politikasında ve hedeflerinde değişiklikler ve tanımlanan öncelikler;
- geçerli yönetmeliklerde değişiklikler ve
- organizasyonel değişiklikler, vb.

İnceleme döngüsünün sıklığı tanımlanmalıdır. Periyodik incelemeler, göstergelerin iyi tanımlanmasını ve emniyet performansını artırmak ve izlemek için gerekli bilgilerin temin edilmesini sağlamaya yardımcı olacaktır. Periyodik incelemeler, ayrıca, spesifik 'artış' göstergelerine ihtiyaç duyulmadığı durumlarda (örneğin; amaçlanan pozitif değişiklikler elde edildiğinde) tespit edilmesine yardımcı olacak ve Emniyet Performans Göstergelerinin (SPI), emniyet açısından daima en önemli sorunlara odaklanacak şekilde ayarlanmalarını sağlayacaktır. Ancak, stabil bir sistem kurmalarına izin vermeyebileceğinden, incelemeler, çok sık aralıklarla gerçekleştirilmemelidir.

İlk iki ila üç döngüden sonra, yeterli verileri toplamış ve "temel" Emniyet Performans Göstergelerinizi (SPI) belirleyebilmeniz için yeterli tecrübeyi edinmiş olmalısınız; bu göstergeler, emniyet performansını artırmak ve izlemek için en değerli ve en etkili göstergelerdir. Bu aşamada, önceki döngüler sırasında toplanan verileri tahmin ederek söz konusu temel Emniyet Performans Göstergeleri (SPI) için hedefler türetebilirsiniz. Söz konusu herhangi bir tahmin yapılırken, kuruluşunuzun 'dinamiklerinin' göz önünde bulundurulması gerekmektedir. Emniyet Performans Göstergelerinizi (SPI), sektör segmentinizdeki diğer kuruluşlar tarafından uygulanan göstergeler ile

karşılaştırabilirsiniz; ancak, kuruluşunuz için anlamlı olup olmadıklarını kontrol etmeden, başka bir kuruluşun Emniyet Performans Göstergelerini (SPI) kopyalamamalısınız.

3. SPI örnekleri

Aşağıda, 2.2 sayılı Maddede açıklanan sürece uygun olarak, kuruluşunuza, kendi emniyet performans göstergelerinizin belirlenmesi konusunda yardımcı olmaya yönelik göstergelere ilişkin örnekleri içeren kapsamlı olmayan bir liste yer almaktadır. Bunlardan herhangi birini kendi Emniyet Performans Göstergeleriniz (SPI) olarak kabul etmeden önce, Emniyet Yönetim Sisteminizin (SMS) olgunluğunu ve iyileştirmek istediğiniz veya dikkat edilmesi gereken spesifik özellikleri göz önünde bulundurarak, spesifik göstergelerin, sizin spesifik kuruluşunuza ile ilgili olup olmadığını belirlemelisiniz.

3.1. Sistemik sorunlara ilişkin göstergeler

Alan	Ölçümün odak noktası	Metrikler
Uygunluk	- kurum içi denetimler/uygunluk takibi: tüm uygunsuzluklar	- her denetim planlaması döngüsü/eğilimi için toplam sayı - emniyet önem derecelerine ilişkin olarak analiz edilen bulguların yüzdesi (%),
	- kurum içi denetimler/uygunluk takibi: önemli uygunsuzluklar	- toplam bulgu sayısına karşı önemli bulguların sayısı - denetim planlaması döngüsü içerisindeki tekrar eden bulguların sayısı
	- kurum içi denetimler/uygunluk takibi: düzeltici faaliyet taleplerine cevap verilebilirlik	- her gözetim planlaması döngüsü - eğilimi için düzeltici faaliyetlerin tamamlanmasına ilişkin ortalama süre
	- dış denetimler/uygunluk takibi: tüm uygunsuzluklar	- her gözetim planlaması döngüsü/eğilimi için toplam sayı - emniyet önem derecelerine ilişkin olarak analiz edilen bulguların yüzdesi (%),
	- dış denetimler: önemli uygunsuzluklar	- toplam bulgu sayısına karşı önemli bulguların sayısı
	- dış denetimler: düzeltici faaliyet taleplerine cevap verilebilirlik	- her gözetim planlaması döngüsü - eğilimi için düzeltici faaliyetlerin tamamlanmasına ilişkin ortalama süre
	- dış ve iç denetimler/uygunluk takibi arasındaki sonuçların tutarlılığı	- yalnızca dış denetimler yoluyla açığa çıkan önemli bulguların sayısı

SMS etkinliđi	- stratejik yönetim	- kuruluşun resmi planlarında ve strateji dokümanlarında göz önünde bulundurulan emniyet derecesi - kuruluşun resmi planlarında ve strateji dokümanlarında emniyet açısından gerçekleştirilen incelemelerin sıklığı
	- yönetim taahhüdü	- aylık/üç aylık/yıllık olarak emniyete özgü dolaşılarak gerçekleştirilen yönetim kontrollerinin sayısı - aylık/üç aylık/yıllık emniyete özgü yönetim toplantılarının sayısı
	- kilit emniyet personelinin ciro oranı	- süre - kilit personelinin ayrılış nedenlerinin analiz edilmiş olduğu durumlar

Alan	Ölçümün odak noktası	Metrikler
	- gözetim	- gözetmenlerin, personelinizin emniyet bilinci davranışı ile ilgili olarak aylık/üç aylık/yıllık olarak olumlu geri bildirim vermiş olduğu durumların sayısı
	- raporlama	- aylık/üç aylık/yıllık olarak alınan raporların sayısı ve eğilim - 10 iş günü içerisinde rapor eden kişiye geribildirim sağlandığı raporların yüzdesi (%) - herhangi bir bağımsız emniyet incelemesinin ardından raporların yüzdesi (%)
	- tehlike tanımı	- Emniyet Risk Yönetimini (SRM) desteklemek üzere aylık/üç aylık/yıllık olarak analiz edilen kaza/ciddi olay senaryolarının sayısı - kurum içi raporlama sistemi aracılığıyla aylık/üç aylık/yıllık olarak gerçekleştirilen yeni tehlike tanımlarının sayısı ve eğilim

	<ul style="list-style-type: none"> - personel/yönetim tarafından daha önceden algılanmış olan tehlikeler ile ilgili dış denetimlerden elde edilen bulgular - aylık/üç aylık/yıllık olarak personelden alınan emniyet raporlarının sayısı ve eğilim
- risk kontrolleri	<ul style="list-style-type: none"> - aylık/üç aylık/yıllık olarak valide edilen yeni risk kontrollerinin sayısı - yeni risk kontrollerine tahsis edilen genel bütçenin yüzdesi (%)
- İK yönetimi ve yetkinlik gelişimi	<ul style="list-style-type: none"> - herhangi bir yetkinlik profilinin tesis edilmiş olduğu personelin yüzdesi (%) - emniyet yönetimi eğitimi almış olan personelin yüzdesi (%) - yetkinlik profillerinin incelenme sıklığı - eğitim programlarının kapsamının, içeriğinin ve kalitesinin incelenme sıklığı - aylık/üç aylık/yıllık olarak personelden alınan geribildirim doğrultusunda eğitim programlarında gerçekleştirilen değişikliklerin sayısı - aylık/üç aylık/yıllık olarak dahili emniyet raporlarının analizinin ardından eğitim programlarında gerçekleştirilen değişikliklerin sayısı
- değişim yönetimi	<ul style="list-style-type: none"> - aylık/üç aylık/yıllık olarak herhangi bir resmi emniyet risk değerlendirmesinin gerçekleştirilmiş olduğu organizasyonel değişikliklerin sayısı ve eğilim - aylık/üç aylık/yıllık olarak herhangi bir resmi emniyet risk değerlendirmesinin gerçekleştirilmiş olduğu Standart İşletim Prosedürlerine (SOP) ilişkin değişikliklerin sayısı ve eğilim

Alan	Ölçümün odak noktası	Metrikler
		<ul style="list-style-type: none"> - aylık/üç aylık/yıllık olarak herhangi bir resmi emniyet risk değerlendirmesinin gerçekleştirilmiş olduğu teknik değişikliklerin (örneğin; yeni ekipman, yeni kolaylıklar, yeni donanım) sayısı ve eğilim - aylık/üç aylık/yıllık olarak değişikliklere ilişkin olarak uygulanan risk kontrollerinin sayısı ve eğilim - risk değerlendirmesine tabi tutulan değişikliklerin (organizasyonel/SOP/teknik, vb.) yüzdesi (%)
	- yüklenicilerin yönetimi	<ul style="list-style-type: none"> - emniyet performansının değerlendirilmiş olduğu yüklenicilerin yüzdesi (%) - yüklenicilerin emniyet performanslarını değerlendirme sıklığı - şirketinizin emniyet raporlama planı ile entegre olan yüklenicilerin yüzdesi (%) - emniyet eğitiminin verilmiş olduğu yüklenicilerin yüzdesi (%) - eğitim kontrolü prosedürlerini uygulamış olan yüklenicilerin yüzdesi (%) - müşterileri ile mevcut emniyet sorunlarına ilişkin geribildirim almış olan yüklenicilerin yüzdesi (%) - aylık/üç aylık/yıllık olarak yüklenicilerden alınan emniyet raporlarının sayısı ve eğilim - emniyet performansının değerlendirilmesinin ardından başlatılan emniyet aksiyonlarının ve aylık/üç aylık/yıllık olarak alınan emniyet raporlarının sayısı ve eğilim

	<ul style="list-style-type: none"> - acil durum eylem planı (ERP) 	<ul style="list-style-type: none"> - yıllık acil durum tatbikatlarının sayısı - acil durum müdahale planlamasının (ERP) incelenme sıklığı - aylık/üç aylık/yıllık olarak gerçekleştirilen ERP eğitimlerinin sayısı - üç ay/bir yıl içerisinde acil durum müdahale planlamasına (ERP) ilişkin olarak eğitilen personelin sayısı - aylık/üç aylık/yıllık olarak acil durum müdahale planlamasını (ERP) koordine etmek üzere ana ortaklar ve yükleniciler ile gerçekleştirilen toplantıların sayısı
	<ul style="list-style-type: none"> - emniyet teşviki 	<ul style="list-style-type: none"> - yayınlanan emniyet haberleşmelerinin sayısı - gerçekleştirilen eğitimlerin sayısı - gerçekleştirilen emniyet brifinglerinin sayısı - (aylık/üç aylık/yıllık)

Alan	Ölçümün odak noktası	Metrikler
	<ul style="list-style-type: none"> - emniyet kültürü 	<ul style="list-style-type: none"> - personelin, emniyeti, günlük işlerini yönlendiren bir değer (örneğin; 1 (düşük) ila 5 (yüksek) ölçeğinde) olarak değerlendirme derecesi - personelin, emniyetin, kendi yönetimleri tarafından yüksek olarak değerlendirilme derecesi - beşeri performans esaslarının uygulanma derecesi - personelin, organizasyonel uygulamaların veya yönetime raporlanan sorunların

		iyileştirilmesinde inisiyatif alma derecesi - emniyet bilinci davranışının desteklenme derecesi - personelin ve yönetimin kendilerine ve diğer kişilere yönelik olarak belirtilen risk operasyonlarınızın farkında olma derecesi
--	--	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

3.2. Operasyonel sorunlara ilişkin göstergeler

Alan	Önlenecek olan oldukça şiddetli sonuç	Metrikler
Havayolu İşleticileri:	- Traffic Collision	- her 1000 uçuş saati (FH) için TCAS RA sayısı
Ayrıca bkz.	- pistten çıkma	- her 1000 inişte meydana gelen unstabilized approach sayısı
Hava Trafik Yönetimi/Hava Seyrüsefer Hizmetleri	- yerde meydana gelen çarpışmalar.	- her 1000 kalkışta meydana gelen pistten çıkmaların sayısı
	- controlled flight into terrain	- her 100 kalkış için Yere Yakınlık İkaz Sistemi (GPWS) ve Geliştirilmiş Yere Yakınlık İkaz Sistemi (EGPWS) uyarılarının sayısı
ilave göstergeler için	- yetersiz uçuş hazırlığı ile ilgili kazalar/olaylar	- uçuş operasyonunun, normal olarak tahsis edilen süreden kısa bir süre içerisinde gerçekleştirilmiş olduğu durumların sayısı - her 100 uçuştaki yetersiz yakıt olaylarının sayısı - her 100 uçuştaki yakıt hesaplama hatalarının sayısı
	- yorgunluk ile ilgili kazalar/olaylar	- aylık/üç aylık/yıllık olarak uçuş sürelerinin uzatılma sayısı ve eğilimler

	<ul style="list-style-type: none"> - yer hizmetleri ile ilgili kazalar/olaylar 	<ul style="list-style-type: none"> - aylık/üç aylık/yıllık olarak yer hizmetleri sağlayıcıları ile ilgili olayların sayısı ve eğilimler - aylık/üç aylık/yıllık olarak her yer hizmetleri sağlayıcısı için ağırlık ve denge hatalarının sayısı ve eğilimler - aylık/üç aylık/yıllık olarak yer hizmetleri sağlayıcıları ile ilgili fonksiyon bozukluklarının sayısı ve eğilimler
	<ul style="list-style-type: none"> - bakım ile ilgili kazalar/olaylar 	<ul style="list-style-type: none"> - her 100 kalkış için Pilot Raporları (PIREPS) - her ay ve her uçak başına ertelenmiş kalemler - her 1000 uçuş saati (FH) için Uçuş Sırasında Motor Durması (IFSD) - her 100 kalkışta In Flight Turn Backs (IFTB) ve sapmalar - Sivil Havacılık Otoritesinde dosyalanan hizmet zorluğu raporlarının sayısı - dispeç güvenilirliği: - her 100 kalkış için teknik sorunlardan kaynaklanan ve 15 dakikadan fazla süren tehirlerin sayısı - her 100 tarifeli uçuş için teknik sorunlardan kaynaklanan iptallerin sayısı - her 100 kalkış için teknik sorunlardan kaynaklanan, reddedilen kalkışlar
Bakım kuruluşları	<ul style="list-style-type: none"> - bakım planlaması/görevlendirmesi ile ilgili kazalar/olaylar 	<ul style="list-style-type: none"> - ayrıntılı bir planlamanın gerçekleştirilmiş olduğu iş emirlerinin yüzdesi (%)
Alan	Önlenecek olan oldukça şiddetli sonuç	Metrikler
	<ul style="list-style-type: none"> - bakım planlaması/görevlendirmesi ile ilgili kazalar/olaylar 	<p>bakım mühendisinin yorgun olması/bakım hatası:</p> <ul style="list-style-type: none"> - öngörülen hazırlık süresi ile fiili işleme süresi arasında >%10'luk bir fark olan iş emirlerinin yüzdesi (%) - tahmin edilen iş gücü ile fiili ihtiyaçlar arasında >%10'luk bir

Hava Trafik Yönetimi/Hava Seyrüsefer Hizmetleri		fark olan iş emirlerinin yüzdesi (%)
	- bakım ile ilgili kazalar/olaylar	bakım hatası: - yeniden çalışma gerektiren iş emirlerinin yüzdesi (%) - herhangi bir bakım hatası veren çift denetimlerin sayısı
	- bakım verileri ile ilgili kazalar/olaylar	- belirsiz bakım verileri ile ilgili emniyet raporlarının sayısı
	- bakım ile ilgili kazalar/olaylar	- komponentlerin, öngörülen yaşam ömrüne ulaşmadan çok önce hizmetten alınmasının ardından gerçekleştirilen araştırmaların sayısı
	- traffic collision	- seviye sapması sayısı/maruziyet - aksiyon gerektiren (RA) TCAS (ayırma kaybı olsun ya da olmasın) sayısı/maruziyet - asgari ayırma ihlali sayısı/maruziyet - uygun olmayan ayırma sayısı (asgari ayırmanın uygulanmadığı hava sahası)/maruziyet - hava trafik kontrol (ATC) izninden sapan uçak sayısı/maruziyet - hava sahası ihlalleri sayısı/maruziyet
	- traffic collision / controlled flight into terrain	- hava trafik yönetimi (ATM) prosedürlerinden sapan uçak sayısı/maruziyet - sıkıntı halindeki uçağa yönelik uygun veya mevcut olmayan ATC desteği sayısı
	- controlled flight into terrain	- near controlled flight into terrain (CFIT) IFSD sayısı/maruziyet
	- pistten çıkma	- uygun olmayan ATC talimatı sayısı (herhangi bir talimatın mevcut olmaması, yanlış talimat, çok geç iletilen aksiyon, vb.)

	- pist ihlalleri	- herhangi bir önleyici faaliyetin gerekli olmadığı pist ihlallerinin yüzdesi (%) - önleyici faaliyetin gerekli olduğu pist ihlallerinin yüzdesi (%)
--	------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------

Alan	Önlenecek olan oldukça şiddetli sonuç	Metrikler
Havaalanları	- kaza/olay sonrası yangın	- Yangın Söndürme Hizmetleri (ICAO Havaalanı Yangınla Mücadele Kategorileri) değerinde azalma (# azalımı - saat/ # havaalanı yıllık işletim saati sayısı) - her 100 operasyonda meydana gelen telsiz/telefon arızası sayısı her 100 operasyonda meydana gelen yangından kurtarma aracı arızası sayısı
	- pist ihlalleri	- her 100 operasyonda meydana gelen pist ihlalleri yön işaretleri: - rutin denetim sırasında tespit edilen arıza veya kusur sayısı - raporlanan kusur sayısı - onarım/ikame için gerekli olan ortalama hazırlık süresi - (aylık/üç aylık/yıllık ve eğilimler)
	- yer aracı/yer ekipmanı ile meydana gelen kazalar	- her 1000 operasyonda bildirilen platform emniyet kuralları ihlalleri
	- yerde yabancı hayvanlar ile meydana gelen kazalar	- yerde yabancı hayvanlar ile meydana gelen kazaların sayısı - aylık/üç aylık/yıllık olarak çitlerin/diğer koruyucu ekipmanın incelenme sayısı
	- FOD (Yabancı Madde Hasarı)	- rutin denetimler sırasında tespit edilen Yabancı Madde Hasarının (FOD) sayısı - denetimsiz ve raporlamanın ardından tespit edilen Yabancı Madde Hasarının (FOD) sayısı

	<ul style="list-style-type: none"> - pist ihlalleri 	<p>pist ışıkları</p> <ul style="list-style-type: none"> - rutin denetim sırasında tespit edilen arıza veya kusur sayısı - raporlanan kusur sayısı - onarım/ikame için gerekli olan ortalama hazırlık süresi (aylık/üç aylık/yıllık ve eğilimler)
	<ul style="list-style-type: none"> - kuş çarpması sonucu Uçuş Sırasında Motor Durması (IFSD) 	<p>kuş çarpması sonucu her 1000 uçuş saatinde (FH) meydana gelen IFSD sayısı</p>
Uçuş eğitimi kuruluşları	<ul style="list-style-type: none"> - yetersiz uçuş eğitimi ile ilgili kazalar/olaylar 	<ul style="list-style-type: none"> - eğitmen başına kursiyer sayısı - eğitim başına eğitmen değişikliği sayısı - eğitim programında gerçekleştirilen önemli değişikliklerin sayısı (aylık/üç aylık/yıllık ve eğilimler)
	<ul style="list-style-type: none"> - sınavlar sırasında eğitim/rehavet ile ilgili kazalar/olaylar 	<ul style="list-style-type: none"> - ortalama geçiş oranlarında meydana gelen önemli sapmaların sayısı
Tasarım kuruluşları	<ul style="list-style-type: none"> - tasarım ile ilgili kazalar/olaylar 	<p>Tasarım aşaması sırasında:</p> <ul style="list-style-type: none"> - program başına ve dönem başına meydana gelen tasarım hatalarından dolayı talep edilen tasarım değişikliği sayısı - program başına ve dönem başına reddedilen uygunluk kanıtı sayısı
	<ul style="list-style-type: none"> - tasarım planlaması ile ilgili kazalar/olaylar 	<ul style="list-style-type: none"> - öngörülen hazırlık süresi ile fiili işleme süresi arasında >%10'luk bir fark olan teknik raporların yüzdesi (%)

Alan	Önlenecek olan oldukça şiddetli sonuç	Metrikler
Üretim kuruluşları		<ul style="list-style-type: none"> - tahmin edilen iş gücü ile fiili ihtiyaçlar arasında >%10'luk bir fark olan teknik raporların yüzdesi (%)
	<ul style="list-style-type: none"> - tasarım ile ilgili kazalar/olaylar 	Sertifikasyon sonrası: <ul style="list-style-type: none"> - program başına ve dönem başına meydana gelen tasarım hatalarından kaynaklanan hizmet zorluğu/emniyet raporları sayısı - belirsiz tasarım verileri ile ilgili emniyet raporlarının sayısı - dönem başına yanlış olarak sınıflandırılan (önemli/önemsiz) tasarım değişikliği sayısı
	<ul style="list-style-type: none"> - üretim ile ilgili kazalar/olaylar 	<ul style="list-style-type: none"> - program başına ve dönem başına meydana gelen üretim hatalarından kaynaklanan hizmet zorluğu/emniyet raporları sayısı
	<ul style="list-style-type: none"> - üretim süreci ile ilgili kazalar/olaylar 	<ul style="list-style-type: none"> - yeniden çalışma gerektiren iş emirlerinin yüzdesi (%) - yeniden çalışma gerektiren iş emirlerinin ardından gerçekleştirilen araştırmaların sayısı
	<ul style="list-style-type: none"> - üretim süreci ile ilgili kazalar/olaylar 	<ul style="list-style-type: none"> - herhangi bir üretim hatasının tespit edildiği çift denetimlerin sayısı
	<ul style="list-style-type: none"> - üretim süreci ile ilgili kazalar/olaylar 	<ul style="list-style-type: none"> - nihai teslimatın önemli uygunsuzluklardan dolayı tehir edildiği durumların sayısı - tehirlenmiş teslimatın ardından gerçekleştirilen araştırmaların sayısı
	<ul style="list-style-type: none"> - üretim verileri ile ilgili kazalar/olaylar 	<ul style="list-style-type: none"> - belirsiz üretim verileri ile ilgili emniyet raporlarının sayısı
	<ul style="list-style-type: none"> - üretim planlaması ile ilgili kazalar/olaylar 	Üretim personelinin yorgun olması/üretim hatası: <ul style="list-style-type: none"> - tahmin edilen iş gücü ile fiili ihtiyaçlar arasında >%10'luk bir fark olan iş emirlerinin yüzdesi (%) - öngörülen hazırlık süresi ile fiili işleme süresi arasında >%10'luk bir fark olan iş emirlerinin yüzdesi (%)

3.3. Dış faktörlerin takibine ilişkin göstergeler

Alan	Takip odak noktası	Metrikler
Yönetmelikler	- yeni yönetmelikler	- bir sonraki 12 ay içerisinde kuruluşunuzu etkileyecek olan yeni düzenleyici gerekliliklerin sayısı
	- yönetmeliklere yönelik olarak gerçekleştirilen tadiller	- bir sonraki 6 ay içerisinde kuruluşunuzu etkileyecek olan, tadil edilen düzenleyici gerekliliklerin sayısı
	- performansa dayalı yönetmeliklere yönelik değişiklik	- kendi uygunluk yöntemlerinizi tanımlamış olduğunuz hedefe dayalı kuralların sayısı
Teknoloji	- temel faaliyetleriniz – donanım ile ilgili yeni teknolojiler	- yeni teknolojiler için harcanan yatırımın yüzdesi (%)
	- temel faaliyetleriniz – yazılım ile ilgili yeni teknolojiler	- yeni teknolojiler için harcanan yatırımın yüzdesi (%)
	- temel faaliyetleriniz ile ilgili yeni teknolojiler	- mevcut kalifikasyonların tükenme (eskime) oranı
	- uçağa tesis edilen yeni teknolojiler	- şirketinizin derecelendirmesine yönelik olarak değişiklik gerektiren uçak modifikasyonlarının/İlave Tip Sertifikalarının (STC) sayısı
	- uçağa tesis edilen yeni teknolojiler	- yeni kalifikasyonlar gerektiren yeni modifikasyonların/İlave Tip Sertifikalarının (STC) sayısı
Rekabet	- finansal ciro	- cironuzda artış
	- personel cirosu	- boş yerin ortalama doldurulma süresi - rakip şirket için işten ayrılan personel sayısı
	- pazar fırsatları	- yeni müşterilerden gelen fiyat tekliflerinin değerlendirilmesine ilişkin taleplerin sayısında artış - kesin siparişin ardından yeni müşterilerden gelen fiyat teklifi taleplerinin oranı
	- rakip şirketler	- doğrudan rakiplerinizin sayısında artış

Referans Dokümanlar

1. Sistem emniyetinin öncü göstergeleri – organizasyonel emniyet potansiyelinin izlenmesi ve teşvik edilmesi, Teemu Reiman, Elina Pietikäinen, Emniyet Bilimi Dergisi 50 (2012)
2. Öncü Performans Göstergeleri – 'Emniyet ile ilgili Adım Değişikliğinin' etkili kullanımı Kılavuzu
<http://www.stepchangeinsafety.net/knowledgecentre/publications/publication.cfm/publicationid/26>
3. ICAO Dokümanı 9859 'Emniyet Yönetimi El Kitabı', Üçüncü basım - düzeltilmemiş ileri versiyon
http://www2.icao.int/en/ism/Guidance%20Materials/SMM_3rd_Ed_Advance_R4_19Oct12_clean.pdf
4. Emniyet Performans Göstergelerine ilişkin Ekonomik İşbirliği ve Kalkınma Teşkilatı (OECD) Kılavuzu – 18 sayılı kimyasal kazalara serileri, İkinci basım 2008 <http://www.oecd.org/chemicalsafety/risk-management/41269639.pdf>
5. Öncülerin Tanımlanması ve Kullanılması Kapıdan kapıya emniyet yönetimine geçiş
<http://www.skybrary.aero/bookshelf/books/1442.pdf>
<http://www.skybrary.aero/bookshelf/books/1443.pdf>

Bu doküman, Emniyet Yönetimi Uluslararası İşbirliği Grubu (SM ICG) tarafından hazırlanmıştır. Emniyet Yönetimi Uluslararası İşbirliği Grubu'nun (SM ICG) amacı, Emniyet Yönetim Sistemi (SMS)/Devlet Emniyet Programı (SSP) esaslarının ve gerekliliklerinin uluslararası havacılık topluluğu genelinde uygulanmalarını kolaylaştırarak, söz konusu esaslara ve gerekliliklere yönelik ortak bir anlayışı teşvik etmektir.

Emniyet Yönetimi Uluslararası İşbirliği Grubunun (SM ICG) halihazırdaki esas üyeleri arasında İspanya Havacılık ve Emniyet Ajansı (AESA), Brezilya Ulusal Sivil Havacılık Ajansı (ANAC), Hollanda Sivil Havacılık Otoritesi (CAA NL), Yeni Zelanda Sivil Havacılık Otoritesi, Avustralya Sivil Havacılık Emniyeti Otoritesi (CASA), Fransa Sicil Havacılık Genel Müdürlüğü (DGAC), Avrupa Havacılık Emniyeti Ajansı (EASA), İsviçre Federal Sivil Havacılık Dairesi (FOCA), Japonya Sicil Havacılık Bürosu (JCAB), Birleşik Devletler Federal Havacılık İdaresi (FAA) Havacılık Emniyeti Kuruluşu, Kanada Ulaştırma Bakanlığı Sivil Havacılık Otoritesi (TCCA) ve Birleşik Krallık Sivil Havacılık Otoritesi (UK CAA) yer almaktadır. Bunlara ek olarak; Uluslararası Sivil Havacılık Teşkilatı (ICAO), bu gruba yönelik gözlemci görevini üstlenmektedir.

Emniyet Yönetimi Uluslararası İşbirliği Grubunun (SM ICG) üyeleri:

- İlgili duyulan ortak Emniyet Yönetim Sistemi (SMS)/Devlet Emniyet Programı (SSP) konularına yönelik işbirliği kurmaktadırlar.

- Alınan dersleri paylaşmaktadırlar.
- Uyumlu hale getirilmiş bir Emniyet Yönetim Sisteminin (SMS) gelişimini teşvik etmekte,
- Ürünleri, sivil havacılık topluluğu ile paylaşmaktadırlar.
- ICAO ve Emniyet Yönetim Sistemini (SMS) uygulamış bulunan veya uygulamakta olan sivil havacılık otoriteleri gibi uluslararası kuruluşlar ile işbirliği yapmaktadır.

Emniyet Yönetimi Uluslararası İşbirliği Grubu (SM ICG) ile ilgili ayrıntılı bilgi almak için, lütfen aşağıda belirtilen kişilerle iletişim kurun:

Regine Hamelijck Avrupa Havacılık Emniyeti Ajansı (EASA)	Jacqueline Booth Kanada Ulaştırma Bakanlığı Sivil Havacılık Otoritesi (TCCA)	Amer M. Younossi Birleşik Devletler Federal Havacılık İdaresi (FAA) Havacılık Emniyeti
+49 221 8999 1000	(613) 952–7974	(202) 267–5164
regine.hamelijck@easa.europa.eu	jacqueline.booth@tc.gc.ca	Amer.M.Younossi@faa.gov
Carlos Eduardo Pellegrino ANAC	Ian Banks Avustralya Sivil Havacılık Emniyeti Otoritesi (CASA)	
+55 213 5015 147	+61 2 6217 1513	
carlos.pellegrino@anac.gov.br	ian.banks@casa.gov.au	

Emniyet Yönetimi Uluslararası İşbirliği Grubu (SM ICG) ürünlerini, aşağıdaki adreste üzerinden SKYbrary'de bulabilirsiniz:

[http://www.skybrary.aero/index.php/Safety_Management_International_Collaboration_Group\(SM_ICG\)](http://www.skybrary.aero/index.php/Safety_Management_International_Collaboration_Group(SM_ICG))

BÖLÜM 5

Emniyet Yönetimi

Sistemi (SMS) Entegrasyonu

1. Amaç

Bu dokümanın amacı, okuyucuya, birden fazla yönetim sisteminin kuruluşlar bünyesinde entegrasyonu ile ilgili en iyi uygulamaları sağlamaktır. Belge kapsamında, işletim sistemlerinin entegrasyonu ile ilgili birden fazla senaryo göz önünde bulundurulmakta olup, yalnızca, emniyet yönetim sistemleri (SMS) ele alınmamaktadır. Bununla birlikte, bu doküman, dikkat ve gözden geçirme gerektirebilecek olan pek çok önemli alan kapsamakta olup, okuyucuya, başarılı sistemler entegrasyonu ile ilgili olarak tavsiyede bulunmaktadır.

İlaveten, bu doküman kapsamında, diğer yasallaştırılmış ve yasallaştırılmamış sistemlerin (örneğin; iş sağlığı ve güvenliği, çevre) emniyet yönetimi ortamına entegrasyonu ile ilgili olarak diğer düzenleyici otoritelere rehberlik sağlamaktadır. Buna ek olarak, çeşitli entegrasyon senaryolarını kapsamakta ve bu durumlarla nasıl başa çıkılacağına ilişkin yararlı ipuçları sunmaktadır.

Doküman, Emniyet Yönetimi Uluslararası İşbirliği Grubu (SM ICG) üyelerinin deneyimlerine dayanmakta olup, mümkün olması halinde, okuyucuya, konuyla ilgili bilgilerini geliştirmeleri için ilave okuma imkanı sağlamaktadır.

2. Hedef

Bu dokümanın hedefi, entegre sistemlerin uygulanmasına ve gözetimine uyumlu bir yaklaşım geliştirmek ve yönetim sisteminin etkinliğini değerlendirmek üzere, performansa dayalı bir yaklaşımı teşvik etmektir.

Sistemlerin etkin entegrasyonunun, emniyet risk yönetiminin etkinliğini ve etkililiğini artırması beklenmektedir. Emniyet Yönetim Sistemini (SMS) diğer yönetim sistemleri türleriyle entegre etmek üzere çeşitli yöntemlerin geliştirilmesi, daha fazla SMS desteği sağlayacaktır.

Bu kılavuz doküman kapsamında, aşağıdaki hususlar özetlenmektedir:

- a) Uygulamada entegrasyonun anlamı (örneğin, mesuliyetler, politika ve hedefler, kaynaklar, süreçler ve araçlar);
- b) Etkili Emniyet Risk Yönetimi (SRM) açısından organizasyonel kabiliyet sağlamak üzere, entegrasyon sırasında bilhassa dikkat edilmesi gereken alanlar;
- c) Hizmet sağlayıcının (SP), düzenleyici otoriteye, tam entegre bir SMS sunacak olan ve böylece, otoritenin gözetim yükümlülüklerini uygun bir şekilde yerine getirmesi sağlayan bir mekanizma ve
- d) Spesifik senaryolar ve tanımlanmış konular ile ilgili oldukları üzere en iyi uygulamalar, uyarılar ve muhtemel çözümler.

3. Sistem Entegrasyonu ile İlgili Sorunlar

Aşağıda, entegrasyon ile ilgili olarak yaygın bir şekilde mevcut olan sorunlardan bazıları tanımlanmaktadır.

A. Entegre Yönetim Sistemleri

Sorunun Açıklanması: Bu madde kapsamında, çeşitli yönetim sistemlerinin tek bir SP bünyesinde entegrasyonu ile ilgili sorunlar ele alınmaktadır.

Yönetim sistemlerinin, iş sağlığı ve güvenliği, güvenlik, çevre ve kalite yönetim sistemleri (QMS) gibi diğer yasal veya düzenleyici gereklilikler doğrultusunda gerekli olan sistemler ile entegrasyonu da dahil olmak üzere, göz önünde bulundurulacak olan çeşitli hususlar bulunmaktadır. Ayrıca, finans ve insan kaynakları gibi düzenlenmeye tabi olmayan sistemlerin entegrasyonunu da içerebilecektir.

Kılavuz Bilgiler

Düzenleyici otorite, birden fazla yönetim sisteminin hizmet sağlayıcının (SP) Emniyet Yönetim Sistemine (SMS) entegrasyonunu değerlendirirken aşağıdaki hususları göz önünde bulundurmalıdır:

1. Etkili entegrasyon aşağıdaki durumlarda mümkündür:

- a. Otoritenin, otorite gözetiminin kapsamını tanımlayan politikalara/mevzuata sahip olması; Bazı durumlarda, sivil havacılık otoritesinin, tüm alt yönetim sistemlerinin gözetiminden sorumlu olmayabileceği belirtilmelidir. Bu durumda, her sistemin gerekliliklerini karşılamak üzere belgelerin köprülenmesi gerekebilecektir.
- b. Hizmet sağlayıcının (SP), entegre edilen yönetim sistemlerinin yanı sıra her bir gerekliliğin nasıl karşılandığını, yönetildiğini ve idame edildiğini açık bir şekilde belgelemiş olması;
- c. Hizmet Sağlayıcının (SP), ISO Yüksek Seviyeli Yapılar (HLS) standardı, Uluslararası Hava Taşımacılığı Birliği (IATA) Entegre Havayolu Yönetim Sistemi (IAMS) veya benzeri standartları içeren yönetim sistemlerinin entegrasyonu ile ilgili sektör standartlarını kullandığına dair kanıtlar bulunması;
- d. Otorite bünyesinde gözetim görevlerini yerine getiren personelin uzmanlığa sahip olması ve entegre bir yönetim sistemi aracılığıyla herhangi bir Hizmet Sağlayıcıyı (SP) denetlemek için gerekli eğitimi almış olması;
- e. Otoritenin, entegre bir yönetim sistemi aracılığıyla herhangi bir Hizmet Sağlayıcıyı (SP) denetlemek için gerekli olan süreçlere, prosedürlere ve araçlara sahip olması;
- f. Otoritenin, entegre yönetim sistemleri aracılığıyla hizmet sağlayıcılarını denetlemek için gerekli olan kaynaklara sahip olması.

2. Aşağıdaki hususlar göz önünde bulundurulduğunda, SMS de dahil olmak üzere, entegre yönetim sistemi uygun ve yeterli midir?

- a. Entegre yönetim sistemi, mesuliyetleri ve sorumlulukları açık bir şekilde tanımlamaktadır.
- b. Hizmet Sağlayıcı (SP), yönetim sistemlerinin işlevsel olarak nasıl bağlantılı olduğunu belgelemiş olup, sistemlerin birbirleriyle ve entegre yönetim sistemi ile nasıl arayüz oluşturduğunu tanımlamıştır.
- c. Hizmet Sağlayıcının (SP), entegre yönetim sistemi ve etkileşimli yönetim sistemlerinin her biri için gerekli öncelikleri ve kaynakları tahsis ettiğine dair kanıtlar bulunmaktadır.
- d. Hizmet Sağlayıcı (SP), etkileşimli yönetim sistemlerinden gelen ve bu sisteme gönderilen birden fazla girdinin nasıl ele alınacağını açıkça tanımlamakta ve belgelemektedir.
- e. Hizmet Sağlayıcı (SP), entegre yönetim sistemlerinin etkinliğini değerlendirerek, sistemi, uygun görüldüğü üzere, gerçekleştirilen değişiklikler ve alınan dersler sonucunda modifiye etmektedir.
- f. Hizmet Sağlayıcı (SP), her otoritenin, kendi sorumluluk alanındaki yönetim sistemini denetlemesini sağlayacak süreçlere/araçlara sahiptir.

Daha fazla okumak ister misiniz?

- **Agência Nacional de Comunicações (ANAC) Brezilya:** ABNT NBR 16189 sayılı Standart - *Entegre Yönetim Sistemleri*. Daha fazla bilgili için, roberto.santos@abnt.org.br adresi üzerinden iletişime geçebilirsiniz.
- Avrupa: <http://www.thecqi.org/Community/Special-Interest-Groups-SIGs/Integrated-Management-Group/Research-and-reports/>

B. Birden Fazla Sertifika

Sorunun Açıklanması: Bu madde kapsamında, birden fazla sertifikanın, her bir kuruluş tarafından sahip olunan SMS gereklilikleri ile entegrasyonu ile ilgili hususlar ele alınmaktadır.

Kılavuz Bilgiler

Düzenleyici otorite, aşağıdaki hususları göz önünde bulundurmalıdır:

1. SMS gözetim politikalarının ve süreçlerinin, Ülke genelinde tutarlı bir şekilde uygulanması sağlanmalıdır.
 - a. Gözetimin tutarlı bir şekilde uygulanmasına ilişkin yönetim taahhüdü kanıtlanmalıdır.
 - b. Tüm gözetim personeline standartlaştırılmış bir eğitim sağlanmalıdır.
 - c. Tüm gözetim kuruluşları, standartlaştırılmış politikalar, prosedürler ve denetim araçları kullanılmalıdır.
 - d. Sorumlu birimler arasında tutarlı ve devamlı bir iletişim olmalıdır.
 - e. Gözetim faaliyetinin standardizasyon derecesini izlemek üzere mekanizmalar bulunmalı ve sistemin sürekli geliştirildiği kanıtlanmalıdır.
2. Birden fazla sertifikaya sahip olan kuruluşların tek bir SMS uygulamayı seçebileceği bilinmelidir.
 - a. Emniyet Yönetim Sisteminin (SMS), uygun görüldüğü üzere, her bir Hizmet Sağlayıcıya (SP) uyarlanılabileceği bilinmelidir. Hizmet Sağlayıcı (SP), bu

sistemlerin, ana kuruluşun Emniyet Yönetim Sistemi (SMS) ile nasıl uyumlu olduğunu göstermelidir.

- b. Her bir Hizmet Sağlayıcıda (SP) bulunan Emniyet Yönetim Sisteminin (SMS), üst düzeydeki yüksek seviyeli bir sisteme entegre edilebileceği bilinmelidir.
- c. Ana kuruluşun, gerek ulusal gerek uluslararası sertifikaları idare etmesi halinde, bu senaryonun, farklı otoriteler arasındaki karşılıklılık gibi ilave zorluklara sebep olabileceği bilinmelidir.
- d. Hizmet Sağlayıcının (SP), verilerin nasıl paylaşıldığı, iletişimlerin nasıl iletiildiği, kararların nasıl alındığı ve kaynakların nasıl tahsis edildiği ile ilgili politikalarını ve prosedürlerini belgelemiş olması sağlanmalıdır.
- e. Her Hizmet Sağlayıcı (SP), kendi Emniyet Yönetim Sistemleri (SMS) ile ilişkili görevlerin ve sorumlulukların yanı sıra Emniyet Yönetimi Sistemine (SMS) ilişkin hiyerarşik çerçeveyi veya mesuliyet çerçevesini açık bir şekilde belgelemelidir.
- f. Hizmet Sağlayıcı (SP), SMS ile ilgili gönüllü anlaşmalarının, ana kuruluşu ile kardeş kuruluşları arasında uygun bir şekilde nasıl çalıştığını ya da çalışmadığını göstermelidir.
 - Bu ilişkileri tanımlayan bir politika veya diğer türde dokümanlar mevcut olmalıdır.
 - Gönüllü anlaşmaların, etkilenen kuruluşlar bünyesinde yeterli bir şekilde iletiildiğine dair kanıtlar bulunmaktadır.
 - Bu tür bilgilerin örgütler arasında nasıl paylaşıldığına dair kanıtlar da bulunmaktadır.

Daha fazla okumak ister misiniz?

Avrupa Havacılık Emniyeti Ajansı (EASA):

[http://easa.europa.eu/ws_prod/r/doc/NPA/final%20A-NPA%2015-2006%20COra%20\(26.09.06\).pdf](http://easa.europa.eu/ws_prod/r/doc/NPA/final%20A-NPA%2015-2006%20COra%20(26.09.06).pdf)

C. Birden Fazla Kuruluş (Havacılık Topluluğu)

Sorunun Açıklanması: Bu madde kapsamında, birden fazla kuruluşun özel bir çalışma ortamında etkileşim içerisinde olduğu durumlarda, her bir Emniyet Yönetim sisteminin birlikte çalışabilirliği ile ilgili sorunlar ele alınmaktadır. Bu husus aşağıdaki içerebilecektir:

1. Havaalanı, havayolları, hava trafik yönetimi (ATM) ve üçüncü taraflar arasındaki bağlantı;
2. Ortak uçuş ve/veya müttefik hava yolları arasındaki ilişki;
3. Havayolları veya onaylanmamış üçüncü taraflar arasındaki bağlantı ve
4. Havayolları ve imalatçılar.

Kılavuz Bilgiler

Düzenleyici otorite, aşağıdaki hususları göz önünde bulundurmalıdır:

1. Her Hizmet Sağlayıcı (SP), görevlerini, sorumluluklarını ve ilgili pek çok paydaş ile ilişkisini tanımlamaktadır. Hizmet Sağlayıcı (SP), aynı zamanda, SMS faaliyetlerinin kolaylaştırılmasında liderlik görevini üstlenecek olan şahısları tanımlamakta olup, bilginin paylaşılması için düzenlemelere tabi bir zorunluluk bulunmayabileceğinin bilincindedir.
2. Hizmet Sağlayıcı (SP), kendi kuruluşu ve diğer ilgili paydaşlarının bünyesindeki değişim yönetimi ile nasıl ilgileneceğini ele alan dokümente edilmiş politikalara ve süreçlere sahiptir.
 - a. Hizmet Sağlayıcı (SP) politikaları ve süreçleri, açık bir şekilde dokümente edilerek iletilmektedir.
3. Her hizmet sağlayıcının Emniyet Yönetimi Sisteminin (SMS), tüm paydaşlar tarafından tam olarak idrak edildiğine ve paydaşlar arasındaki farklılıkların, tehlikeler, riskler, olaylar vb. ile ilgili olarak ortak bir anlayış geliştirmek üzere karşılaştırıldığına dair kanıtlar bulunmaktadır.
 - a. Örneğin; bir havaalanı emniyet komitesi, birden çok kuruluşu etkileyebilecek tehlikelerin belirlenmesine yardımcı olmak için, ayrı ayrı işletilen Emniyet Yönetim Sistemleri (SMS) aracılığıyla toplanan bilgilerin değişimini kolaylaştırmaktadır.
4. Paydaşlar arasında SMS ile ilgili gönüllü anlaşmalar bulunmalıdır.
 - a. Bu sistemlerden elde edilen bilgilerin çeşitli paydaşlar ile paylaşılmasını sağlayan süreçler mevcuttur.
 - b. Paydaşların, kendi aralarında, emniyet ilgili bilgileri paylaştıklarına dair kanıtlar bulunmaktadır.

D. SMS Unsurları ile ilgili Dış Kaynak Kullanımı

Sorunun Açıklanması: Bu madde kapsamında, Emniyet Yönetim Sisteminin (SMS) unsurlarının onaylı olabilecek ya da olmayabilecek olan başka bir işletmeye dış kaynak kullanımı yoluyla temin edilmesi ile ilgili sorunlar ele alınmaktadır.

Kılavuz Bilgiler

Düzenleyici otorite, aşağıdaki hususları göz önünde bulundurmalıdır:

1. Hizmet Sağlayıcı (SP), SMS bileşenlerinin kendi adına yönetilmesinden sorunlu olan tüm kuruluşları tanımlamaktadır.
 - a. Hizmet Sağlayıcı (SP) ile dış kaynak kullanımı yoluyla temin edilen hizmetleri sağlayan kuruluş arasında resmi bir anlaşma bulunmaktadır.
 - b. Dış kaynak kullanımı yoluyla temin edilen kuruluşun, dış kaynak kullanımı yoluyla temin edilen hizmetleri üstlenmek üzere uygun niteliklere sahip olduğuna dair kanıtlar bulunmaktadır.
 - c. Hizmet sağlayıcının Emniyet Yönetimi Sisteminde (SMS), Emniyet Yönetimi Sisteminden (SMS) daima Hizmet Sağlayıcının (SP) sorumlu olduğu açık bir şekilde belirtmelidir.
 - d. Dış kaynak kullanımı yoluyla temin edilen SMS bileşenlerinin uygunluğunu gösteren kanıtlar bulunmaktadır.

- e. Emniyet Yönetim Sisteminin (SMS) politikalar, yönetim hesap mesuliyeti ve yönetim faaliyetleri gibi belirli unsurlarının, dış kaynak kullanımı yoluyla temin edilmemesi gerektiği belirtilmelidir.

2. Hizmet Sağlayıcı (SP), kendisi ile dış kaynaklı hizmetleri sağlayan kuruluşlar arasındaki görevleri ve sorumlulukları açık bir şekilde dokümante etmiştir.

- a. Hizmet Sağlayıcı (SP) ve dış kaynak kullanımı yoluyla temin edilen hizmetler sağlayan kuruluş, uygun verileri/bilgileri paylaşmakta olup, bu verilerin/bilgilerin paylaşılmasını sağlamak üzere dokümante edilmiş süreçlere sahiptir.
- b. Hizmet Sağlayıcının (SP), dış kaynak kullanımı yoluyla temin edilen unsurların SMS dahilindeki zayıf bağlantılar olmamasının sağlanması hususu da dahil olmak üzere, genel Emniyet Yönetim Sisteminin (SMS) etkinliğini değerlendirdiğine dair kanıtlar bulunmaktadır.

E. Dış Kaynak Kullanımı Faaliyetleri – Onaylı Kuruluşlar

Sorunun Açıklanması: Bu madde kapsamında, bakım, tasarım, imalat ve eğitim gibi onaylanmış işlevlerin diğer Hizmet Sağlayıcılara (SP) ve harici kuruluşlara dış kaynak kullanımı yoluyla temin edilmesi ile ilgili sorunlar ele alınmaktadır.

Kılavuz Bilgiler

Düzenleyici otorite, aşağıdaki hususları göz önünde bulundurmalıdır:

1. Hizmet Sağlayıcı (SP) ile dış kaynak kullanımı yoluyla temin edilen işlevleri sağlayan kuruluş arasında resmi bir anlaşma bulunmaktadır. Bu anlaşma, örneğin, dış kaynak kullanımının kapsamının değişmesi veya her iki işletmenin organizasyonunun değişmesi halinde, uygun bir şekilde ve zamanında revize edilmelidir.
2. Hizmet Sağlayıcı (SP), dış kullanımı yoluyla gerçekleştirilen faaliyetlere ilişkin SMS ile ilgili mesuliyeti muhafaza etmekte olup, bu husus, hizmet sağlayıcı Emniyet Yönetimi Sisteminde (SMS) veya diğer uygun dokümanlarda açıklanmaktadır.
3. Hizmet sağlayıcı Emniyet Yönetim Sistemi (SMS), önemli ölçüde farklı olma ihtimaline rağmen, dış kaynak kullanımını sağlayan kuruluşların emniyet yönetim sistemleri ile etkili bir şekilde bağlantılıdır.
4. Hizmet Sağlayıcı (SP), tehlikelere, risk analizine ve risk yönetimine ilişkin bilgileri, dış kaynak kullanımı yoluyla gerçekleştirilen işlevler sağlayan kuruluşlar ile nasıl paylaştığını dokümante etmiştir. Bu husus ile ilgili olarak mutabakata varılmış ve söz konusu husus paydaşlar arasında paylaşılmıştır.
5. Hizmet Sağlayıcının (SP), dış kaynak kullanımı yoluyla gerçekleştirilen işlevler sağlayan tüm kuruluşlardan elde edilen birden fazla girdiyi ve çıktıyı yönettiğine dair kanıtlar bulunmaktadır.
6. Hizmet Sağlayıcı (SP), çeşitli paydaşlar arasındaki birden fazla arayüzü ve iletişimi etkili bir şekilde yönetmektedir.
7. Herhangi bir görevin, onaylanmamış bir işletmeye dış kaynak kullanımı yoluyla sağlanması halinde, tehlikeler, risk analizi ve risk yönetimi hakkında bilgi paylaşımını sağlamak üzere, Hizmet Sağlayıcı (SP) ile onaylanmamış bir işletme arasında uygun anlaşmalar bulunmaktadır.

F. Dış Kaynak Kullanımı Faaliyetleri – Onaylanmamış Kuruluşlar

Sorunun Açıklanması: Bu madde kapsamında, ikram, yakıt ikmali, bagaj taşıma ve diğer apron hizmetleri gibi herhangi bir SMS gerektirmeyen onaylanmamış faaliyetlerin, üçüncü taraf işletmelere tayin edilmesi ile ilgili sorunlar ele alınmaktadır.

Kılavuz Bilgiler

Düzenleyici otorite, aşağıdaki hususları göz önünde bulundurmalıdır:

1. Hizmet Sağlayıcı (SP), tehlike, risk analizi ve risk yönetimi hakkında bilgi paylaşımı ile ilgili olarak hizmet sağlayan onaylanmamış işletmeler ile uygun anlaşmalara akdetmelidir.
2. Düzenleyici otorite, Uluslararası Hava Taşımacılığı Birliğinin (IATA) Yer İşletme Emniyet Denetimi (ISAGO), Uluslararası Hava Taşımacılığı Birliğinin (IATA) Havaalanı Yer Hizmetleri El Kitabı ve Avrupa Ticari Havacılık Emniyet Ekibi (ECAST) Apron Kaynak Yönetimi dokümanı da dahil olmak üzere, bu konuyla ilgili olarak yeni geliştirilen sektör kılavuz materyallerini kullanmak üzere sektörü teşvik etmelidir.
3. Emniyet için faydalı olabileceğinden dolayı, bilginin gönüllü olarak paylaşımı teşvik edilmelidir (emniyet teşviki).

G. Devlet Emniyet Programı (SSP) veya Devlet Emniyet Yönetimi Sistemi (SSMS) Entegrasyonu

Sorunun Açıklanması: Bu madde kapsamında, Devlet Güvenlik Programı (SSP) ile ilgili SMS entegrasyonu ele alınmaktadır. Dikkat edilmesi gereken çok sayıda arayüz bulunmaktadır. Bunlar; emniyet veri toplama, değerlendirme ve paylaşma arayüzünü, emniyet gözetimini (uyumluluğa, riske ve performansa dayalı), emniyet kültürü gelişimini ve son olarak, Devletin genel emniyet hedefleri ile paydaşın fiili emniyet performansı arasındaki arayüzü içermektedir. Paydaşların emniyet performansı, Devlet için makbul seviyede bir emniyet performansı (ALoSP) beklentileri ile uyumlu ve tutarlı olmalıdır.

Kılavuz Bilgiler

Düzenleyici otorite, aşağıdaki hususları göz önünde bulundurmalıdır:

1. Devlet ve paydaş seviyesinde açık ve etkili bir raporlama kültürünün geliştirilmesi gerekmektedir.
2. Etkili bir SMS uygulaması ve entegrasyonu için "adil kültür" yaklaşımına ilişkin yasal hükümler gerekmektedir.
3. Sektörün ve Devletin emniyet performansı arasında bağlantıların olduğu bilinmelidir.
4. Devletin, paydaş emniyet performansı ile ilgili beklentilerini açık bir şekilde belirtmesi gerekmektedir.
5. Her bir Hizmet Sağlayıcı (SP), emniyet ölçümlerinin uygunluğunu değerlendirmekte olup, Devletin makbul seviyede bir emniyet performansı (ALoSP) kapsamında

tanımlanan Devlet emniyet performans göstergelerine nasıl bağlanabileceğini bilmektedir.

6. Gözetim personeline, Devlet ile Hizmet Sağlayıcıların (SP), emniyet performans göstergelerini (SPI) nasıl tanımlandığını anlamaları ve idrak etmeleri amacıyla eğitim sağlanmaktadır.

7. Devlet, Emniyet Yönetimi Uluslararası İşbirliği Grubu (SM ICG) dokümanı, *Emniyet Performansının Ölçülmesine İlişkin Sistem Yaklaşımı – Düzenleyici Otorite Perspektifi* kapsamında açıklandığı üzere, "3. Sırada" (SM ICG SPMA) yer alan emniyet performans göstergelerini tespit edebilmeli ve değerlendirebilmelidir.

8. Devlet kültür gelişimi ve emniyet teşviki faaliyetleri, devlet ile paydaşlar arasında koordinasyon sağlanması yoluyla geliştirilebilir.

4. Tüm İşletmeler için Geçerli Olan Sorunlar

Sorunun Açıklanması: Bu madde kapsamında, yukarıdaki 3.A ila 3.G Maddelerinde tanımlanan tüm SMS entegrasyon sorunları için geçerli olabilecek sorunlar ele alınmaktadır.

Kılavuz Bilgiler

Düzenleyici otorite ve hizmet sağlayıcı, aşağıdaki hususları göz önünde bulundurmalıdır:

1. Gerek düzenleyici otorite personeline gerek onaylanmış hizmet sağlayıcılara, entegrasyona ilişkin uygun eğitim sağlanmalıdır.

2. Emniyet Yönetim Sisteminin (SMS) sektör genelinde teşvik edilmesi, Devlet gözetiminin, uyumluluğa dayalı bir sistemden performansa dayalı bir sistem geliştireceği anlamına gelmektedir. Bu, "anahtar teslim" bir süreç değildir ve zaman içerisinde olgunlaşması gerekmektedir. Ödenekler bu doğrultuda oluşturulmalıdır.

3. Dil, normlar ve davranışlar gibi hususlar da dahil olmak üzere, kültürün ve insan faktörlerinin etkisine gereken önem verilmelidir.

4. Özel bilgilerin paylaşımı ve verilerin korunması ile ilgili sorunlar da dahil olmak üzere, herhangi bir raporlama kültürünün önemi (veri/emniyet bilgisi paylaşımı) vurgulanmalıdır.

5. Etkili bir iletişim geliştirmek için, tüm paydaşlar arasında yeterli arayüzler bulunmalıdır ve bu arayüzler mümkün olduğunca basit bir şekilde muhafaza edilmelidir.

6. Hizmet Sağlayıcı (SP), SMS faaliyetlerinin dış kaynak kullanımı yoluyla ya da sair düzenleyici gereklilikler doğrultusunda gerçekleştirildiğine bakılmaksızın daima kendi Emniyet Yönetim Sisteminden (SMS) sorumludur.

7. Emniyet Yönetim Sisteminin (SMS) ölçeklenebilirliği, gerek büyük gerek küçük kuruluşlara yönelik olarak ve uygun olması halinde, diğer Emniyet Yönetim Sistemleri (SMS) ile nasıl etkileşim kurabileceğine yönelik olarak daima göz önünde bulundurulmalıdır.

8. Sertifikaların yurtiçinde ya da uluslararası olarak düzenlendiğine bakılmaksızın, bu dokümanda sağlanan tüm kılavuz ilkeler göz önünde bulundurulmalıdır.

9. Düzenleyici otorite ve sektör, yabancı Hizmet Sağlayıcıların (SP), SMS, veri koruma ve veri paylaşımı hususunda farklı politikalara/yönetmeliklere tabi olabileceğini belirtmelidir. Bu koşullar altında, ikili anlaşmalar kapsamında öngörülen hükümler ve bu tür anlaşmaların şartları ve koşulları geçerli olacaktır. Bu nedenle, düzenleyici otorite, ikili anlaşmalar geliştirirken bu konuları göz önünde bulundurmalıdır.

Bu doküman, Emniyet Yönetimi Uluslararası İşbirliği Grubu (SM ICG) tarafından hazırlanmıştır. Emniyet Yönetimi Uluslararası İşbirliği Grubu'nun (SM ICG) amacı, Emniyet Yönetim Sistemi (SMS)/Devlet Emniyet Programı (SSP) esaslarının ve gerekliliklerinin uluslararası havacılık topluluğu genelinde uygulanmalarını kolaylaştırarak, söz konusu esaslara ve gerekliliklere yönelik ortak bir anlayışı teşvik etmektir.

Emniyet Yönetimi Uluslararası İşbirliği Grubunun (SM ICG) halihazırdaki esas üyeleri arasında İspanya Havacılık ve Emniyet Ajansı (AESA), Brezilya Ulusal Sivil Havacılık Ajansı (ANAC), Hollanda Sivil Havacılık Otoritesi (CAA NL), Yeni Zelanda Sivil Havacılık Otoritesi (CAANZ), Avustralya Sivil Havacılık Emniyeti Otoritesi (CASA), Fransa Sicil Havacılık Genel Müdürlüğü (DGAC), Avrupa Havacılık Emniyeti Ajansı (EASA), İsviçre Federal Sivil Havacılık Dairesi (FOCA), Finlandiya Ulaşım Emniyeti Ajansı (Trafi), Japonya Sicil Havacılık Bürosu (JCAB), Birleşik Devletler Federal Havacılık İdaresi (FAA) Havacılık Emniyeti Kuruluşu, Kanada Ulaştırma Bakanlığı Sivil Havacılık Otoritesi (TCCA) ve Birleşik Krallık Sivil Havacılık Otoritesi (UK CAA) yer almaktadır. Bunlara ek olarak, Hong Kong Sivil Havacılık Teşkilatı (CAD HK), Uluslararası Sivil Havacılık Teşkilatı (ICAO) ve Birleşik Arap Emirlikleri Genel Sivil Havacılık Otoritesi (BAE GCAA) bu gruba yönelik gözlemci görevini üstlenmektedir.

Emniyet Yönetimi Uluslararası İşbirliği Grubunun (SM ICG) üyeleri:

- İlgili duyulan ortak Emniyet Yönetim Sistemi (SMS)/Devlet Emniyet Programı (SSP) konularına yönelik işbirliği kurmaktadır.
- Alınan dersleri paylaşmaktadırlar.
- Uyumlaştırılmış bir Emniyet Yönetim Sisteminin (SMS)/Devlet Emniyet Programının (SSP) gelişimini desteklemektedirler.
- Ürünleri, sivil havacılık topluluğu ile paylaşmaktadırlar.
- Uluslararası Sivil Havacılık Teşkilatı (ICAO) ve Emniyet Yönetim Sistemini (SMS) ve Devlet Emniyet Programını (SSP) uygulamış veya uygulamakta olan sivil havacılık otoriteleri gibi uluslararası kuruluşlar ile işbirliği içerisinde oldukları.

Emniyet Yönetimi Uluslararası İşbirliği Grubu (SM ICG) ile ilgili ayrıntılı bilgi almak için, lütfen aşağıda belirtilen kişilerle iletişim kurun:

Regine Hamelijck Avrupa Havacılık Emniyeti Ajansı (EASA)	Jacqueline Booth Kanada Ulaştırma Bakanlığı Sivil Havacılık Otoritesi (TCCA)	Amer M. Younossi Birleşik Devletler Federal Havacılık İdaresi (FAA) Havacılık Emniyeti
+49 221 8999 1000	(613) 952-7974	(202) 267-5164
regine.hamelijck@easa.europa.eu	jacqueline.booth@tc.gc.ca	Amer.M.Younossi@faa.gov
Igor enna ANAC	Stephen Duffield CASA	
+55 213 5015 268	+61 7 3144 7362	
igor.penna@anac.gov.br	stephen.duffield@casa.gov.au	

Emniyet Yönetimi Uluslararası İşbirliği Grubu (SM ICG) ilave ürünlerini, aşağıdaki adreste üzerinden SKYbrary'de bulabilirsiniz:
[http://www.skybrary.aero/index.php/Safety_Management_International_Collaboration_Group\(SM_ICG\)](http://www.skybrary.aero/index.php/Safety_Management_International_Collaboration_Group(SM_ICG))

BÖLÜM 6

Emniyet Yönetim Sistemi (SMS) Değerinin Tespit Edilmesi

Bu doküman, Emniyet Yönetimi Uluslararası İşbirliği Grubu (SM ICG) tarafından hazırlanmıştır. Bu dokümanda, "kuruluş" terimi, herhangi bir ürün veya hizmet sağlayıcı, işletmeci, işletme ve şirketin yanı sıra havacılık sektörü kuruluşları anlamına gelmekte olup, "otorite" terimi ise, düzenleyici otorite, otorite, Sivil Havacılık Otoritesi (CAA), Ulusal Havacılık Otoritesi (NAA) ve gözetim sorumluluğu bulunan diğer ilgili devlet dairesi veya kurumu anlamına gelmektedir.

Emniyet Yönetimi Uluslararası İşbirliği Grubu'nun (SM ICG) amacı, Emniyet Yönetim Sistemi (SMS)/Devlet Emniyet Programı (SSP) esaslarının ve gerekliliklerinin uluslararası havacılık topluluğu genelinde uygulanmalarını kolaylaştırarak, söz konusu esaslara ve gerekliliklere yönelik ortak bir anlayışı teşvik etmektir.

Emniyet Yönetimi Uluslararası İşbirliği Grubu (SM ICG)'nun halihazırdaki esas üyeleri arasında İspanya Havacılık ve Emniyet Ajansı (AESA), Brezilya Ulusal Sivil Havacılık Ajansı (ANAC), Hollanda Sivil Havacılık Otoritesi (CAA NL), Yeni Zelanda Sivil Havacılık Otoritesi, Singapur Sivil Havacılık Otoritesi (CAAS), Avustralya Sivil Havacılık Emniyeti Otoritesi (CASA), Fransa Sicil Havacılık Genel Müdürlüğü (DGAC), Avrupa Havacılık Emniyeti Ajansı (EASA), İsviçre Federal Sivil Havacılık Dairesi (FOCA), Finlandiya Ulaşım Emniyeti Ajansı (Trafi), İrlanda Havacılık Otoritesi (IAA), Japonya Sicil Havacılık Bürosu (JCAB), Birleşik Devletler Federal Havacılık İdaresi (FAA) Havacılık Emniyeti Kuruluşu, Kanada Ulaştırma Bakanlığı Sivil Havacılık Otoritesi (TCCA) ve Birleşik Krallık Sivil Havacılık Otoritesi (UK CAA) yer almaktadır. Bunlara ek olarak, Hong Kong Sivil Havacılık Teşkilatı (CAD HK), Uluslararası Sivil Havacılık Teşkilatı (ICAO) ve Birleşik Arap Emirlikleri Genel Sivil Havacılık Otoritesi (BAE GCAA) bu gruba yönelik gözlemci görevini üstlenmektedir.

Emniyet Yönetimi Uluslararası İşbirliği Grubunun (SM ICG) üyeleri:

- İlgili duyulan ortak Emniyet Yönetim Sistemi (SMS)/Devlet Emniyet Programı (SSP) konularına yönelik işbirliği kurmaktadırlar.
- Alınan dersleri paylaşmaktadırlar.
- Uyumlaştırılmış bir Emniyet Yönetim Sisteminin (SMS)/Devlet Emniyet Programının (SSP) gelişimini desteklemektedirler.
- Ürünleri, sivil havacılık topluluğu ile paylaşmaktadırlar.
- Uluslararası Sivil Havacılık Teşkilatı (ICAO) ve Emniyet Yönetim Sistemini (SMS) ve Devlet Emniyet Programını (SSP) uygulamış veya uygulamakta olan sivil havacılık otoriteleri gibi uluslararası kuruluşlar ile işbirliği içerisinde oldukları.

Emniyet Yönetimi Uluslararası İşbirliği Grubu (SM ICG) ile ilgili ayrıntılı bilgi almak için, lütfen aşağıda belirtilen kişilerle iletişim kurun:

Regine Hamelijnck
Avrupa Havacılık Emniyeti
Ajansı (EASA)

+49 221 8999 000

regine.hamelijnck@easa.europa.eu

Igor Penna

Brezilya Ulusal Sivil Havacılık
Ajansı (ANAC)

+55 613 3144 826

igor.penna@anac.gov.br

Jacqueline Booth
Kanada Ulaştırma
Bakanlığı Sivil Havacılık
Otoritesi (TCCA)

(613) 952-7974

jacqueline.booth@tc.gc.ca

Mike Hutchinson

Avustralya Sivil
Havacılık Emniyeti
Otoritesi (CASA)

+03 9518 2774

Mike.Hutchinson@casa.gov.au

Amer M. Younossi
Birleşik Devletler
Federal Havacılık
İdaresi (FAA) Havacılık
Emniyeti

(202) 267-5164

amer.m.younossi@faa.gov

Emniyet Yönetimi Uluslararası İşbirliği Grubu (SM ICG) ürünlerini, aşağıdaki adreste üzerinden SKYbrary'de bulabilirsiniz:
[http://www.skybrary.aero/index.php/Safety_Management_International_Collaboration_Group\(SM_ICG\)](http://www.skybrary.aero/index.php/Safety_Management_International_Collaboration_Group(SM_ICG))

Önsöz

Bu doküman, emniyetli faaliyetler sağlamak için emniyet müdahalelerine ve Emniyet Yönetim Programlarına yatırım yapılması gerektiğini anlayan emniyet uzmanlarına yönelik olarak hazırlanmıştır. Emniyet uzmanları ve ekonomik ortakları, ciddi bir olay veya kaza durumunda söz konusu olan beşeri ve finansal etkinin farkındadırlar. Böyle bir zararı önlemek, emniyet yatırımının getirisidir. Ancak, yatırımın geri dönüşü, programlara riayet, memnun müşteriler, daha sağlıklı iş yerleri ve çalışanlar, daha az mühendislik yeniden işleme süreci ve yetkili makamlar ile artan işbirliği gibi operasyonel tasarruflardan etkilenmektedir. Bu dokümanda, emniyet uzmanının, yatırımın geri dönüşünü hesaplaması için gerekli aşamalar açıklanmaktadır. Matematiksel olarak basit olmakla birlikte, karmaşıklığın sebebi, masraflarınızı, gerçekleşmeyen olayların değeri (emniyetli faaliyetlerin maddi olmayan yüksek değeri) ile dengelemektir. Bu doküman, tüm tarafların, emniyet maliyetini ve değerini değerlendirmelerini ve hesaplamalarını sağlamaya yöneliktir.

“Yatırımın Geri Dönüşü” (ROI) veya Maliyet-Fayda Analizi teriminin, emniyet uzmanları toplantısından ziyade herhangi bir ekonomistin elektronik çizelge programında kullanılması daha muhtemeldir. Günümüz havacılık işletme kuruluşlarının, finansmanı emniyetten ayırma seçeneği bulunmamaktadır. Ekonomi/kazanç ve emniyet, karşılıklı olarak birbirini kapsamaktadır; biri olmadan diğere sahip olamazsınız.

William B. Johnson – Federal Havacılık İdaresi (FAA)

FAA Bakım Alanında İnsan Faktörleri Baş Uzmanı

1. Giriş

Karlılık, herhangi bir ticari kuruluşun amaçları arasında yer almaktadır; dolayısıyla, kuruluşlar, Emniyet Yönetim Sistemlerinin (SMS) ve ilgili emniyet aksiyonlarının finansal yönlerini, işle ilgili herhangi bir diğer karar verme süreci gibi ele almalıdır.

Emniyet Yönetim Sisteminin (SMS) uygulanması ile ilişkili maliyetlerin ve faydaların kapsamlı bir şekilde anlaşılması, uygun kaynak tahsisini ve aksiyonların önceliklendirilmesini sağlayacak olup, Emniyet Yönetim Sisteminin (SMS) devamlı olarak geliştirilmesi için sağlam bir temel oluşturacaktır.

Zorluklar:

Geleneksel maliyet-fayda analizinde, genel olarak, sistem bileşenlerinin ve maaşların maliyetleri gibi genellikle maddi duran varlıklara yönelik olarak, uygulama ile ilişkili maliyetlerin belirlemesine ve finansal açıdan ilgili yatırım geri dönüşünün (ROI) tahmin edilmesine odaklanılmaktadır. Bununla birlikte, Emniyet Yönetim Sisteminin (SMS) maliyet-fayda analizi, emniyetin mahiyeti gereği daha zorlayıcıdır. Geliştirilmiş emniyet kültürü, etkin düzenleyici uygunluk, emniyete yönelik yönetim taahhüdü, hissedar değeri ve kamu güveni gibi maddi olmayan faydaların belirlenmesi zordur. Ayrıca, etkili bir SMS, ilgili kuruluşun mevcut sistemi dahilinde ideal bir şekilde yer alan birçok farklı organizasyon unsurunun, eyleminin ve sürecinin etkileşiminden meydana gelmektedir. Dolayısıyla, SMS çerçevesinin ayrı unsurlarının etkilerini, maliyet fayda analizinin amaçları doğrultusunda ayırmak her zaman kolay değildir. Özellikle, etkin SMS uygulamasının kuruluşun emniyet kültürü üzerindeki genel etkisinin, gelişmiş bir maliyet fayda analizinden anlamlı seviyede daha fazla olabileceği öngörülebilir.

Gerçekte SMS, acil ve doğrudan masraflara sebep olurken, faydaları çoğunlukla maddi olmayacak ve gerçekleşmesi muhtemelen zaman alacaktır. Etkili bir SMS, zaman içerisinde, yalnızca önemli olayların meydana gelme riskini ele almamakta, aynı zamanda, üretim verimsizliklerini belirlemekte, iletişimi geliştirmekte ve bunlarla mücadele etmekte, iletişimi iyileştirmekte, daha iyi bir organizasyon kültürünü teşvik etmekte ve yüklenicileri ve tedarikçileri daha etkili bir şekilde kontrol etmektedir. İlâveten, otorite ile olan ilişkilerin geliştirilmesi yoluyla, SMS uygulaması, gözetim yükümlülüğünün azalması ile sonuçlanabilir. Geleneksel olarak, havacılık emniyet yönetmelikleri, temel olarak maliyet-fayda hususlarından meydana gelmemesine karşın, SMS, emniyet ekonomisine karşı daha fazla yetki hassasiyeti sağlamalıdır.

Bu nedenle, Emniyet Yönetim Sisteminin (SMS), sadece olayları ve kazaları önlemek için değil, aynı zamanda herhangi bir kuruluşun faaliyetine ilişkin birçok unsurun mümkün olduğunca başarılı olmasını sağlamak için uygulanan bir uygulama olarak görülmesi, herhangi bir emniyet yatırımının, verimlilik ve organizasyon başarısı yatırımı olarak görülmesini sağlayacaktır.

2. Maliyet ile ilgili Hususlar

SMS ile ilişkili maliyetleri (veya yatırımları) yeterli bir şekilde göz önünde bulundurmada önce, Emniyet Yönetim Sisteminin (SMS) uygulayacağı sistem sınırlarını belirlemelisiniz. Sistem sınırları belirlendikten sonra, sektör standartları, çalışan raporlama sistemleri ve uygunluk izleme fonksiyonları doğrultusunda, SMS unsurlarının bir kısmının amacını karşılayan, Kalite Yönetim Sistemleri (QMS) gibi mevcut sistemleri ve süreçleri tanımlamak daha kolay olacaktır. Kuruluşlar, uygulama maliyetlerini azaltmak için mevcut sistemleri ve süreçleri maksimum düzeyde kullanmalıdır.¹

İlaveten, Emniyet Yönetim Sisteminin (SMS) uygulanmasını ve devam etmekte olan bakımını destekleyecek pozisyonları belirlerken, kuruluşunuzun mevcut iç bilgilerini göz önünde bulundurmalısınız. Kuruluşunuz bünyesinde gerekli uzmanlığa sahip olmanız durumunda, söz konusu hususu sağlamak için herhangi bir kişiyi istihdam etmenize gerek yoktur; böylece, maliyetleri düşük seviyede tutmuş olursunuz. Kuruluşunuzun dışarıdan destek alması durumunda, Emniyet Yönetim Sisteminin (SMS) kuruluşa uygun olacak ve rafta bekletilmeyecek şekilde yönetildiğinden emin olunmalıdır. Yardım sağlamak üzere çok sayıda danışmanlık şirketi ve SMS programı bulunmaktadır ve kuruluşunuz için hangisinin en iyi çalışacağını tavsiye edememekle birlikte, personelin SMS ile ilgili olarak eğitilmiş veya bilgi sahibi olmaması durumunda, maliyetlerin daha yüksek olacağı konusunda uyarabiliriz. Kuruluşunuzun danışmanlardan faydalanması halinde, kuruluşunuz, Emniyet Yönetim Programını (SMS) tamamen danışmanlara devretmemeli, bunun yerine, sistemin desteklenmesini sağlamak üzere kendi hizmetlerini kullanmalıdır. SMS, genellikle, kısayolların etkisiz olmadığı ve beklenenden daha fazla masraf yapmanızı sona erdirecek olan bir durumdur.

Tek başına ele alındığında SMS ile ilişkili başlangıç maliyetlerinin yüksek görünebilecek olmasına karşın, Emniyet Yönetim Sisteminin (SMS) sağlayabileceği faydaların ve Yatırım Geri Dönüşünün (ROI) incelenmesi önemlidir. Daha güçlü bir risk yönetimi süreci ile kaçınılması muhtemel olaylar düşünülmeli ve gelecekteki maliyet veya verimlilik kazanımları için daha iyi faaliyetler, daha hızlı ürün-piyasa süreleri veya daha kaliteli ürünler sunabilecek olaylar göz önünde bulundurulmalıdır.

İlaveten, SMS ile ilişkili olarak meydana gelen doğrudan ve dolaylı masraflar, genel olarak, kuruluş giderlerine dahil edilecektir; kuruluşun Emniyet Yönetim Sistemine (SMS) yapılacak olan genel yatırımını belirlerken her ikisi de dikkate alınmalıdır. Büyük olasılıkla, bilgi teknolojisi (BT) sistemleri geliştirme, BT bakım, eğitim ve insan kaynaklarının, SMS ile birlikte başlıca doğrudan maliyet etmenleriniz olduğunu tespit fark edeceksiniz. Dolaylı maliyetleri miktarını belirlemek oldukça zor olmakla birlikte, mümkün olduğunca çok yansıtmaya çalışarak, genel yatırım anlayışını belirlemenin önemli bir yoludur. Aşağıda yer almakta olan Tablo 1 ile Tablo 4, bu alanlarda göz önünde bulundurulacak olan maliyetlere ilişkin rehberlik sağlamaktadır.

¹ Kuruluşlar bünyesindeki birden fazla yönetim sisteminin entegrasyonuna ilişkin daha fazla bilgiye buradan ulaşılabilir:

http://www.skybrary.aero/index.php/SMS_Integration_%E2%80%93_93_Points_to_Consider

3. Fayda ile ilgili Hususlar

Genellikle, emniyet ve üretim arasında, üretim giderlerinde yüksek emniyet seviyesi ya da emniyet giderlerinde yüksek verimlilik ile sonuçlanan bir denge olduğu düşünülmektedir. Bu husus, aşırıya kaçıldı bu doğru olabilir; ancak, genel olarak bakıldığında, emniyet ve üretim birbirinin karşıtı değildir. Aslında, emniyet yönetimi faaliyetlerine yapılan yatırımlar, genellikle, herhangi bir kuruluşun verimliliğine gerek doğrudan gerekse dolaylı olarak fayda sağlamaktadır. Güvenliğe yapılan yatırım, kazaların ve ciddi olayların olmaması durumunda dahi iyi bir iş anlayışı oluşturmaktadır.

Herhangi bir Kalite Yönetim Sistemi (QMS) göz önünde bulundurulduğunda, maliyet ve faydaları belirlemek nispeten kolaydır; örneğin, herhangi bir bileşenin reddedilme oranının düşük olması, doğrudan, karlılığın artmasına neden olur. Benzer şekilde, doğrudan finansal faydalar, Emniyet Yönetim sisteminin (SMS) etkili bir şekilde uygulanmasına atfedilebilir. Sadece herhangi bir kaza veya olay ile değil, aynı zamanda, finansal etkileri bulunan operasyonel yetersizlikler (örneğin; iptal edilen uçuşlar, yüksek oranlardaki bileşen reddi, yeniden işleme gerektiren durumlar) ile sonuçlanabilecek olan bir tehlike ile ilişkili riskin kontrol edilmesi veya ortadan kaldırılması gibi emniyet aksiyonlarının, karlılık üzerinde olumlu bir etkisi olacaktır. Bu faydalar ölçülebilir olduğu ve işin üretim tarafına (karlılığı) ilave edilebileceği için emniyet ile verimlilik arasındaki bağlantı gösterilebilir.

Hasarlara karşı koruma göz önünde bulundurulduğunda, potansiyel faydalar muhtemelen daha etkileyicidir. Emniyet, bazen risklerin kabul edilebilir bir seviyede tutulduğu ya da kötü bir durumun meydana gelmediği bir koşul olarak tanımlanmaktadır. Herhangi bir kaza veya ciddi bir olay meydana geldiğinde, faaliyetin karlılığını doğrudan etkileyen teminat maliyetleri söz konusu olacaktır. Maliyetlerin, olaydan önce emniyet ile ilgili hafifletici hususlara yatırım yapılmasının fayda sağladığına dair kanıt sunulmasının ardından hesaplanması kolaydır. Herhangi bir kuruluşa ilişkin olarak göz önünde bulundurulması gereken önemli hususlardan biri, söz konusu kuruluşun, kaçınılması gereken maliyetlerin değerini belirleyebilmesidir. Bu, zaman kaybı ve yeniden işleme gibi daha düşük düzeyli hususları içermelidir. Gerek emniyet risk yönetimi (SRM) gerek finansal ROI yönetimi, "...olursa ne olur" senaryolarına ve potansiyel kaybın miktarını belirleme becerisine yönelik proaktif bir değerlendirmeyi gerektirmektedir.

SMS uygulanırken göz önünde bulundurulması gereken ilave dolaylı faydaların yanı sıra bazen parasal olmayan faydalar da bulunmaktadır. Bu faydalar, kuruluşun riskleri yönetme ve olanakları mümkün olan en yüksek seviyeye çıkarma becerisini geliştirme çalışmalarından doğrudan faydalanacak olan, güvenlik, sağlık veya çevresel koruma gibi emniyet dışındaki alanlarda gerçekleşebilir.

Emniyet Yönetim Sisteminin (SMS) mevcut yönetim sistemlerine entegrasyonu, emniyete yönelik bağımsız bir yaklaşımdan daha verimli olacaktır. Kurum içi olarak, bu, mevcut uzmanlığın optimize bir şekilde kullanılmasını sağlayacak olup, çalışanların memnuniyetinin artırılmasına katkı sağlayacaktır. Kurum dışı olarak, entegre SMS,

kuruluşun riskleri yönetme kabiliyetine ilişkin olarak kamu (ve hissedar) güvenini artırarak olmanın yanı sıra rekabet avantajına da katkıda bulunacaktır. Emniyet Yönetim Sisteminin (SMS) tüm unsurları uygulandığında ve etkili bir şekilde çalıştığında, emniyet yönetimi kabiliyetlerinize ilişkin olarak otoritenin güveninin kazanılması nedeniyle gözetim yükünün de azalması beklenebilir.

Özet olarak, etkin SMS uygulamasının doğrudan ve dolaylı faydaları aşağıdaki hususlar yoluyla gerçekleşecektir:

- Daha iyi bir yönetim;
- Kuruluşun daha bütünsel bir bakış açısına sahip olması;
- Daha iyi bir değişim yönetimi;
- Organize sistemler;
- Kalite sistemleri ile sinerji sağlanması;
- Bulguların olasılığının ve öneminin azalması;
- Doğru ve uygun sürecin kanıtlanabilmesi;
- Çalışan memnuniyeti, değişikliklerin daha iyi bir şekilde kabul edilmesi ve personel cirosu oranlarının düşük olması;
- Hissedar güveni;
- İşletme giderlerinin azalması ve
- Otorite tarafından güvenin artırılması, düzenleyici ilişkilerde azalma ve doğrudan ve dolaylı gözetim maliyetlerindeki ilgili azalma.

4. Emniyet Yönetim Sistemi (SMS) Maliyet-Fayda Analizi

Emniyet yönetimi faaliyetleri ile birlikte yürütülen iyi bir maliyet-fayda analizi, karar verme sürecinizi destekleyecek olup, riskleri kabul edilebilir bir düzeye indirmek üzere, kaynakların emniyet programına/programlarına tahsis edilmesine yardımcı olacaktır.

Bu maddede, Uluslararası Sivil Havacılık Örgütü (ICAO) SMS çerçeve bileşenleri ve unsurları etrafında yapılandırılan maliyet-fayda analizinde göz önünde bulundurulacak olan unsurlara yönelik genel bir bakış sunulmaktadır.

Bu genel bakış açısı ve aşağıdaki tablolar, Emniyet Yönetim Sisteminin (SMS) maliyetlerinin ve faydalarının yanı sıra yatırımın etkinliğini tahmin etmek üzere metrik fikirlerin belirlenmesini de sağlamaktadır. Tabloda yer alan kalemler temsili olmasına karşın, her hususun dahil edildiği anlamına gelmemektedir. Kalem listeleri genişletilebilir; bu listeler, yalnızca, Yatırım Geri Dönüşünü (ROI) ölçmek üzere kullanılacak olan metriklerle ilişkin maliyetlere, faydalara ve fikirlere yönelik değildir.

Tablolarda doğrudan ve dolaylı maliyetler ve faydalar yer almaktadır. Kuruluşun yapısına, SMS uygulamasının aşamasına ve emniyet aksiyonunun mahiyetine bağlı olarak, maliyetlerin ve faydaların doğrudan veya dolaylı olarak kategorize edilmesi değişebilir (örneğin; personel eğitimi, geçici bir eğitim kursu olması halinde doğrudan maliyet olarak düşünülebilirken, söz konusu eğitimin, kuruluşun düzenli eğitim faaliyetleri kapsamında yer alması halinde, dolaylı maliyet olarak düşünülebilir).

Dengeli bir bakış açısından bakıldığında, miktarının belirlenmesi zor olmasına karşın, maliyet-fayda analizi göz önünde bulundurulurken dolaylı faydalar da dahil edilmelidir.

"Potansiyel Metrikler" sütunlarında, SMS uygulamasının etkililiğinin belirlenmesini sağlamak üzere kullanılabilir olan performans ölçümlerine yönelik bazı öneriler yer almaktadır. Emniyet Yönetim Sistemi Yatırım Geri Dönüşünün (SMS ROI) gerçekçi bir şekilde belirlenmesini sağlamak amacıyla, herhangi bir Emniyet Yönetim Sisteminin (SMS) etkinlik katsayısının kullanılması önerilmektedir (bkz. Ek 1 *Emniyet Yönetimi Sisteminin (SMS) Bir Bütün Olarak Uygulanmasına İlişkin Olarak Yatırımın Geri Dönüşü (ROI) – Elektronik Çizelge Şeklinde Hesaplayıcı*).

a. Genel Maliyetler ve Faydalar (Tüm Emniyet Yönetim Sistemine (SMS)/Kuruluşa yönelik olarak)

Yönetim sisteminin herhangi bir unsurunda olduğu gibi, kuruluşun geneline atfedilebilecek olan maliyetler ve faydalar bulunmaktadır. Bu nedenle, her bir kuruluşta halihazırda mevcut olanın üzerine ekleme yaparak geliştirmek mantıklıdır. Bu, maliyet etkin nitelikte olacaktır ve daha az zaman almalıdır. Emniyet Yönetim Sisteminin (SMS) avantajlarını en üst düzeye çıkarmak için, uygulanmakta ve etkili tüm SMS bileşenlerine sahip olmalısınız. Benzer şekilde, SMS kuruluş genelinde uygulanmalı ve tüm havacılık hizmetlerinize yönelik olmalıdır.

İlk uygulamanın ardından, sisteminize ve süreçlerinize yönelik bir tanım mevcut olmalıdır. Mevcut işletim el kitaplarınızın veya Kalite Yönetim Sisteminizin (KYS) kapsamında bir sistem tanımına sahip olmanız muhtemeldir. Bu durumda, mevcut sistem tanımının üzerine emniyet riski ve emniyet güvencesi odağını ilave ederek geliştirebilirsiniz. Benzer şekilde, kuruluşunuzun düzenli yönetim incelemeleri, iç denetim, işlemlerin takibi, performans ölçümü ve tedarikçilerin kontrolü için tipik QMS süreçlerini uygulamış olması halinde, Emniyet Risk Yönetimini (SRM) uygulamak için, söz konusu sistemi, aynı süreçler ve araçlar üzerine kurulabilirsiniz; bu da Emniyet Yönetim Sisteminizin (SMS) genel idaresine ilişkin maliyetlerin en aza indirgenmesini sağlayacaktır. Örneğin:

- Düzeltici faaliyetleri takip etmeye yönelik standart ofis yazılımı, ayrıca, risk hafifletme faaliyetlerini izlemek üzere kolaylıkla uyarlanabilir ve
- Süreç yetersizliklerini raporlamak veya iyileştirmeler önermeye yönelik standart araçlar, kurum içi emniyet raporlamasına yönelik olarak uyarlanabilir.

Ayrıca, ilk SMS uygulaması ile ilgili olarak, kuruluşunuzun sınırlarını ve gerek kuruluşunuz bünyesindeki gerek ortak kuruluşlar, yükleniciler veya tedarikçiler gibi üçüncü taraflar ile olan uygunluğu ve emniyet tehlikesi taşıyan arayüzleri açık bir şekilde tanımlamanız gerekmektedir. Genel sistemin ve yönetim, faaliyet ve destek süreçleriniz arasındaki etkileşimler ne kadar iyi anlaşılırsa, iyileştirme olanaklarının proaktif olarak tanımlanmasının yanı sıra faaliyetleriniz ile ilgili uygunsuzlukların ve risklerin tanımlanması ve yönetilmesi de o kadar iyi olur.

İlk uygulamanın ardından, sistem tanımı, organizasyonel veya operasyonel değişiklikler ile ilgili risklerin yönetilmesini sağlayacaktır; ayrıca, söz konusu sistem tanımı, SRM süreçlerinizin operasyonel süreçlerinize doğru şekilde yerleştirilmesini sağlamalıdır. Bu nedenle, sisteminizin ve süreçlerinizin kapsamlı bir şekilde analiz edilmesi de dahil olmak üzere, Emniyet Yönetim Sisteminin (SMS) uygulanmasına yönelik ilk çalışmalar ile ilişkili maliyetler, artan operasyonel etkinlik, emniyet performansı ve düzenleyici gerekliliklere uygunluk ile sigorta primleri ve işçi tazminat primlerinde bir düşüş yoluyla ödenebilir.

b. Emniyet Politikası ve Hedefleri

ICAO SMS Çerçeve bileşeni 1, Emniyet Politikası ve Hedefleri, "PLANLA-YAP-KONTROL ET-UYGULA" döngüsünün "PLAN" bileşenini içermektedir.

Bu, beş farklı unsuru kapsamaktadır:

- Aşağıdaki hususları yerine getirme yükümlülüğü de dahil olmak üzere, yönetim taahhüdü ve sorumluluğu:
 - Performans ölçümüne esas teşkil etmek üzere bir emniyet politikasının ve emniyet hedeflerinin tanımlanması ve
 - Yalnızca kültür ilkelerini uygulayarak, emniyet raporlama prosedürlerinin uygulanması.
- Emniyet sorumluluklarını, mesuliyetlerini ve yetkilerini dokümante etme ve iletme yükümlülüğü de dahil olmak üzere emniyet sorumlulukları;
- Emniyet yöneticisinin atanması da dahil olmak üzere temel emniyet personelinin atanması;
- Acil durum müdahale planlamasının koordinasyonu ve
- SMS el kitabının ve süreçlerinin geliştirilmesi de dahil olmak üzere SMS dokümantasyonu.

Genellikle, SMS uygulaması ile doğrudan ilişkili olan unsurlar; (1) emniyet yöneticisinin atanması, (2) SMS ile ilişkili dokümantasyonun oluşturulması ve muhafaza edilmesi, (3) kurum içi emniyet raporlama şemalarının uygulanması ve (4) önceden mevcut olmayabilecek olan ilave emniyet toplantılarının gerçekleştirilmesidir. İlgili maliyetler, mevcut sistemlere ve süreçlere entegrasyon seviyesine bağlı olacaktır. Kısmen veya tamamen SMS ile ilgili görevlere özgü bir emniyet yöneticisinin atanmasına veya işe alınmasına yönelik maliyetler, ilk SMS uygulamasının ardından önemli bir yatırım olabilir. Mevcut kaynaklara ve havacılık ürünlerinin veya hizmetlerin karmaşıklığına bağlı olarak, kuruluş, ilgili atamalar herhangi bir menfaat çatışması ile sonuçlanmadığı sürece, Emniyet Yönetim Sisteminin (SMS) uygulanması ve muhafaza edilmesi sorumluluklarını, tek başına veya diğer görevlerle birlikte, bir veya daha fazla kişiye atamayı tercih edebilir.

Emniyet performansının izlenmesi ve ölçümüne (bkz. Madde 4d, *Emniyet Güvencesi*) esas teşkil eden emniyet politikasına ve hedeflerine açıklık getirilmesi daha verimli bir uygulama sağlayacaktır. Genel yönlendirme sağlayan bir husus olduğundan dolayı, bu alandaki belirsizlikler, maliyetli olmaya eğilimlidir.

Emniyet politikasının iletilmesi, emniyet taahhüdünün yönetilmesi ve açık raporlamanın teşvik edilmesi ile ilgili olarak harcanan kaynaklar, Emniyet Yönetim Sisteminin (SMS) başarısı için büyük önem arz etmektedir. Olumlu bir emniyet kültürünün oluşturulması, finansal olarak ölçülebilir olmamasına karşın, genel sistemin başarısına katkıda bulunacaktır.

Tablo 1: Bir SMS Bileşeni Olan "Emniyet Politikası ve Hedefleri" ile ilgili Maliyetler ve Faydalar

	Doğrudan Maliyetler	Dolaylı Maliyetler	Faydalar
<i>İlk Uygulama</i>	<ul style="list-style-type: none"> - Danışmanlık - İlave kaynaklar veya mevcut kaynakların tekrar tahsis edilmesi - El kitaplarının ve prosedürlerin geliştirilmesi 	<ul style="list-style-type: none"> - Politikanın iletilmesi - Hedeflerin yayılması ve mevcut dokümanların gözden geçirilmesi - Toplantılarda harcanan zaman - yöneticilerin/personelin katılımı 	<ul style="list-style-type: none"> - Emniyet performansı ölçümüne yönelik olarak açık ve net bir yönlendirmenin ve çerçevenin sağlanması - Üst yönetim taahhüdü - Gelişmiş organizasyonel (emniyet) kültürü - Emniyet ve işletme risklerinin daha iyi bir şekilde kontrol edilmesi
<i>SMS Faaliyeti</i>	<ul style="list-style-type: none"> — El kitaplarının ve prosedürlerin muhafaza edilmesi 	<ul style="list-style-type: none"> - Politikanın sağlanması ve hedeflerin gözden geçirilmesi (yönetim incelemeleri) - Taahhüdün kanıtlanması - Toplantılarda harcanan zaman - yöneticilerin/personelin katılımı 	<ul style="list-style-type: none"> - Emniyet yöneticisinin işinin kolaylaştırılması - Daha proaktif davranış (emniyet kültürü)
SMS Etkinlik Katsayısının Belirlenmesinde Kullanılan Potansiyel Metrikler			
<ul style="list-style-type: none"> - Tüm seviyelerdeki emniyet politikasının farkında olunması - Üst yönetim taahhüdünün kanıtlanması:² <ul style="list-style-type: none"> o Aylık/Üç aylık/yıllık emniyete/Emniyet Yönetim Sistemine (SMS) özgü yönetim gezintilerinin/ziyaretlerinin sayısı o Aylık/Üç aylık/yıllık emniyete özgü yönetim toplantılarının sayısı o Temel yöneticilerin emniyet toplantılarına katılımı - Emniyet raporları 			

² Aşağıdaki adreste bulunan "Üst Yöneticinin Emniyet Yönetim Sistemindeki (SMS) Rolü" başlıklı SM ICG dokümanı üzerinden daha fazla bilgiye ulaşabilirsiniz: <http://www.skybrary.aero/bookshelf/books/1781.pdf>

	Doğrudan Maliyetler	Dolaylı Maliyetler	Faydalar
	<ul style="list-style-type: none"> ○ <i>Aylık/Üç aylık/Yıllık olarak alınan raporların sayısı ve eğilim (trend)</i> ○ <i>10 iş günü içerisinde rapor eden kişiye geribildirim sağlandığı raporların yüzdesi</i> ○ <i>Herhangi bir soruşturmanın ardından sunulan raporların yüzdesi</i> 		

c. Emniyet Risk Yönetimi

Emniyet Risk Yönetimi aşağıdaki unsurları kapsamaktadır:

- Reaktif ve proaktif yöntemler yoluyla tehlike tanımlama ve
- Tanımlanmış tehlikeler ve bu tehlikelerin hafifletilmesi ile ilişkili emniyet risklerinin analizi, değerlendirilmesi ve kontrolü.

Emniyet risklerinin yönetilmesi, Emniyet Yönetim Sisteminizin (SMS) temelini teşkil etmektedir. Bu, kötü hususların meydana gelmesinin önlenmeye çalışılması ya da herhangi bir hususun yolunda gitmemesi veya gözden kaçması halinde, olayın sonuçlarının en aza indirgenmeye çalışılması anlamına gelmektedir. Emniyet risklerinizi yönetebilmek için, kuruluşunuz etkili ve etkin tehlike tanımlama süreçlerine ve sağlam bir emniyet kültürüne sahip olmalıdır. Emniyet risklerini, yalnızca, kuruluşunuzun faaliyetlerine bağlı potansiyel tehlikelerin farkında olursanız yönetebilirsiniz.

Tehlikelerin farkında olabilmek, kuruluşunuzun SRM sürecinin temelini teşkil etmektedir. Ayrıca, tehlike tanımlamaya ve risk değerlendirmesine yönelik varsayımların geçerli olmaya devam etmesini sağlamak için risklerinizin yaşam döngüsünün yönetilmesi de önemlidir.

Yaygın SMS uygulamasıyla gerçekleşecek olan açık ve net bir fayda olarak, sektördeki ortak risk azalımındaki artıştır. Örneğin, bir operatör olmanız ve gerek operatörlerin gerek tasarım onay sahiplerinin Emniyet Yönetim Sistemini (SMS) uygulaması halinde, sistemlerinin birlikte nasıl çalıştığını görmek çok daha kolaydır. Bu, bilgi paylaşımını, faaliyet ile tasarım arasındaki bağlantıyı ve daha iyi bir risk yönetiminin gerçekleştirilmesini kolaylaştırmaktadır.

Spesifik operasyonel riskler ile ilişkili maliyetlerin ve faydaların değerlendirilmesi, daha az somut olan SMS unsurlarının değerlendirilmesi ile karşılaştırıldığında da açık ve anlaşılır niteliktedir. Ek 2, *Spesifik Emniyet Aksiyonlarına İlişkin Yatırımın Geri Dönüşü (ROI) Örnekleri* kapsamında, spesifik operasyonel risklere ilişkin birtakım emniyet aksiyonları yer almaktadır. Bu örnekler, SRM sürecinin işletme bakış açısından nasıl görülebileceğinin belirlenmesini sağlamak üzere temel ROI hesaplamalarını içermektedir.

Tablo 2: Bir SMS Bileşeni Olan "Emniyet Riski ve Yönetimi" ile ilgili Maliyetler ve Faydalar

	Doğrudan Maliyetler	Dolaylı Maliyetler	Faydalar
<i>İlk Uygulama</i>	<ul style="list-style-type: none"> • Veri toplama ve analiz sistemi • Aksiyon izleme sistemi (bu ikisi, genel SMS yazılımı paketi kapsamında yer alabilir) • Eğitim giderleri (gelişim ve sunma) • Analist (istihdam/eğitim) • Sistemlere veya donanımlar ilişkin değişiklikleri 	<ul style="list-style-type: none"> • Analist (personelin tekrar tahsis edilmesi – tekrar eğitilmesi) • Uygulama süresi (çalışmama süresi – personelin tekrar eğitilmesi) 	<ul style="list-style-type: none"> • Olayların önlenmesi (şiddetin/olasılığın azaltılması) • İyileşmeye yönelik potansiyel emniyet unsurları ve olanakları farkındalığının artırılması • Gerekli özenin gösterilmesi • Bilgili bir şekilde karar alınması • Risklerin hedeflenen şekilde yönetilmesi • Düzenleyici gerekliliklere uygunluk • Verimin artması • Müşteriler ve ortak kuruluşlar tarafından tanınma
<i>SMS Faaliyeti</i>	<ul style="list-style-type: none"> • Toplama ve analiz sisteminin yanı sıra izleme sistemi bakımı • Yenileme eğitimi giderleri (analist, vb.) 	<ul style="list-style-type: none"> • Operasyonel dokümantasyondaki ve prosedürlerdeki (örneği; eğitim müfredatı, çalışma kartları, kontrol listeleri ve standart işletim prosedürleri) değişiklikler • Emniyet analizi/soruşturmalar sırasında çalışmama süresi 	<ul style="list-style-type: none"> • Pazar erişimi • Rekabetin artması
SMS Etkinlik Katsayısının Belirlenmesinde Kullanılan Potansiyel Metrikler			
	Doğrudan Maliyetler	Dolaylı Maliyetler	Faydalar
	<ul style="list-style-type: none"> • Her faaliyet için genel risk puanı • Kuruluşa yönelik genel risk puanı • Şiddetli risk olaylarının sayısı • Raporlama kültürü (emniyet raporları): <ul style="list-style-type: none"> ○ Proaktif raporların reaktif raporlara oranı ○ Gönüllü raporların zorunlu raporlara oranı • Emniyet komitesi raporlarının sayısı (planlanan raporlara karşı fiili raporlar) • Olayların tekrar meydana gelme sayısı • Yeni risk kontrollerine tahsis edilen ilave fonlar (ilk bütçede yer almayan) 		

d. Emniyet Güvencesi

Kuruluşunuz bünyesindeki etkin emniyet güvencesi, havacılık otoriteniz tarafından doğrudan görülebilir nitelikte olacaktır.

Emniyet güvencesi üç unsur içermektedir:

- Emniyet hedeflerine karşı emniyet performansının izlenmesi ve ölçülmesi;
- Tesis edilen emniyet riski yönetimi sürecinden faydalanılarak gerçekleştirilen değişim yönetimi ve
- Emniyet Yönetim Sisteminin (SMS) sürekli iyileştirilmesi.

İlk unsur, emniyet güvencesi kapsamında sıklıkla daha zorlayıcı olarak görülmektedir. Emniyet hedeflerinizi (bkz. Madde 4b, *Emniyet Politikası ve Hedefleri*) tanımladıktan sonra, emniyet hedeflerinize ve faaliyetinize yönelik risklere bağlı emniyet performans göstergelerini (SPI) tanımlamanız gerekecektir. Genel göstergeler, emniyet hedeflerine yönelik olarak tanımlanmalı ve operasyonel göstergeler ise spesifik risk azaltımı aksiyonlarına yönelik olarak tanımlanmalıdır. Ayrıca, Emniyet Performans Göstergelerini (SPI), risk yönetimi süreçlerinizin ne kadar iyi çalıştığını ölçmek için de kullanabilirsiniz; dolayısıyla, faaliyetlerinizdeki riskleri yansıtan göstergeleri seçmeniz önemlidir. Bir dizi Emniyet Performans Göstergelerine (SPI) yapılan yatırımları en üst düzeye çıkarmak için, Emniyet Performans Göstergelerinin (SPI) toplanması, analizi ve yorumlanması yoluyla elde edilen sonuçlar, karar ve aksiyon almak üzere kuruluşunuzun yönetimine iletilmelidir.

İkinci unsur olan etkin değişim yönetimi, herhangi bir kuruluşun sürdürülebilirliğinin sağlanmasında önemli bir rol oynamaktadır. Değişim yönetimi, herhangi bir değişikliğin neden olduğu riskleri tanımlamanın ve azaltmanın yanı sıra olanakları tanımlamak ve en üst düzeye çıkarmak için planlı ve sistemli bir süreç gerektirmektedir. Değişikliklerin yönetilmesi, mevcut sistem tanımlamalarına dayandırılabilir; söz konusu değişim yönetimi, tesis edilen SRM süreçlerinden ve araçlarından faydalanacaktır. Ancak, değişiklik yönetimi sürecinin başlatılması ve emniyet durumu şablonu gibi destekleyici dokümantasyonun oluşturulması doğrudan maliyetlere neden olacaktır. Değişikliğin etkili bir şekilde yönetilmesi, çoğunlukla, operasyonel verimlilik için bir ön koşul olarak kabul edilmekte olup, finansal sonuçlar, bu durumu, kaynakların daha iyi bir şekilde tahsis edilmesi ve üretimde ve faaliyetlerde sonraki yeniden işleme veya düzeltmelerin azaltılması ya da ortadan kaldırılması yoluyla yansıtabilir.

Emniyet güvencesinin üçüncü unsuru Emniyet Yönetim Sisteminin (SMS) sürekli iyileştirilmesidir. SMS, çevre, havacılık teknolojisi ve yönetmelikler de dahil olmak üzere, daima değişikliklerin gerçekleştiği kuruluşlarda işe yaramaktadır. SMS, bu değişiklikleri yansıtabilecek şekilde kontrol edilmeli ve güncellenmelidir; kuruluş, faaliyetini iyileştirmek ve Emniyet Yönetim Sistemini (SMS), tüm kullanıcılar yararına, yaşayan bir sistem olarak devam ettirmek için gayret göstermelidir.

Herhangi bir Kalite Yönetim Sistemi (QMS) veya uygunluk izleme fonksiyonu uygulamış olmanız durumunda, söz konusu sistemi veya fonksiyonu, Emniyet Yönetim Sisteminizin (SMS) iyileştirme ihtiyacını belirlemek için kullanabilirsiniz. QMS, uyumluluk izleme ve SMS; raporlama, denetim ve inceleme gibi bazı ortak süreçlere sahiptir; ancak işlemin tamamlandığı perspektif farklıdır. Emniyet Yönetim Sistemini (SMS) oluştururken ya da iyileştirirken iki seçeneğiniz bulunmaktadır: (1) Emniyet Yönetim Sisteminin (SMS), genel yönetim sistemine entegre edilmesi için, Kalite Yönetim Sisteminiz (QMS) veya uygunluk izleme fonksiyonu ile birleştirilmesi veya (2) sistemlerin ayrı ayrı muhafaza edilmesi. Ancak, sistemlerin bir dizi ortak hedef ile tek bir sistemde birleştirilmesi tasarruf sağlayabilir.

Tablo 3: Bir SMS Bileşeni Olan "Emniyet Güvencesi" ile ilgili Maliyetler ve Faydalar

	Doğrudan Maliyetler	Dolaylı Maliyetler	Faydalar
<i>İlk Uygulama</i>	<ul style="list-style-type: none">• <i>SPI geliştirme: uzman gerekmektedir</i>• <i>Veri toplama ve SPI izleme sistemi (genel SMS yazılım paketi kapsamında olabilir)</i>	<ul style="list-style-type: none">• <i>Kaynakların tekrar tahsis edilmesi</i>	<ul style="list-style-type: none">• <i>Otorite güveni</i>• <i>Hissedar güveni</i>• <i>Risk yönetimi taahhüdünün kanıtlanması</i>
<i>SMS Faaliyeti</i>	<ul style="list-style-type: none">• <i>SPI takibi ve SPI dizisinin revizyonu</i>• <i>Kurum içi denetimler/kurum içi değerlendirmeler</i>• <i>Emniyet durumları (değişim yönetimi)</i>• <i>Verilerin performans raporlarında derlenmesi</i>	<ul style="list-style-type: none">• <i>Veri toplama sistemlerinin bakımı</i>	<ul style="list-style-type: none">• <i>Hedeflenen risk kontrolleri güvencesi</i>• <i>Sistem performansının validasyonu</i>• <i>Daha iyi bir sistem tahsisi</i>• <i>Değişikliklerin emniyetli ve etkin bir şekilde uygulanması</i>
SMS Etkinlik Katsayısının Belirlenmesinde Kullanılan Potansiyel Metrikler			
<ul style="list-style-type: none">• <i>Operasyonel emniyet hedeflerinin gerçekleştirilmesi</i>• <i>Kurum içi/kurum dışı denetimler sonucunda elde edilen bulguların sayısında azalma</i>• <i>Bulguların yeniden meydana gelmesinde azalma</i>• <i>Kabul edilen değişiklik sonrası emniyet güvencesi planı kapsamında gerçekleştirilen takip denetimlerinin oranı (%)</i>• <i>Herhangi bir resmi emniyet risk değerlendirmesinin gerçekleştirilmiş olduğu standart işletim prosedürlerine (SOP) yönelik değişikliklerin oranı (%)</i>• <i>Yıllık emniyet etütlerinde/anketlerinde artış</i>• <i>Gerçekleştirilen emniyet denetimlerinin sayısı</i>			

e. Emniyet Eğitimi ve Teşviki

Bu, birbiriyle ilişkili olan iki unsuru kapsamaktadır:

- Emniyet eğitim ve öğretimi ve
- Emniyet iletişimi.

Emniyet Yönetim Sistemini (SMS) uygulanmasında ve çalıştırılmasında emniyet eğitimi gereklidir. SMS eğitimini vermek için en iyi kimin olduğunu ve eğitimin kurum içi eğitimler tarafından mı yoksa kurum dışı eğitimler tarafından mı gerçekleştirildiğini göz önünde bulundurmalısınız. Etkili eğitim, gelişmek için zaman alır ve emniyet yöneticilerinin, bunu sağlamak için her zaman zamanları olmayabilir ya da söz konusu yöneticiler, eğitim becerilerine sahip olmayabilirler. SMS eğitimi, ilave faydalar sağlayabilecek olan, tehlike bilgilerinin toplanması için kullanılabilir.

Sorumlu yönetici, kuruluşunuz bünyesinde emniyet kültürünü teşvik ederken önemli bir rol oynamaktadır. Sorumlu yöneticinin, günlük görüşmelerde ve tazeleme seminerlerinde personel ile konuşurken sergilediği tavır, emniyet teşvikinin önemli yönlerinin dahil edilmesini sağlayabilir. Kuruluşun emniyet politikası, genellikle sorumlu yönetici tarafından hazırlanmaktadır; bu nedenle, sorumlu yönetici, politikanın içeriğini personel ile paylaşacak en iyi kişidir. Bu tür teşviklerin tek maliyeti, sorumlu yöneticinin ve personelin görev süresidir.

Tüm kilit personel, ideal olarak diğer eğitim kurslarına entegre edilmiş olan ve sorumluluk alanları ile doğrudan ilgili olan bazı özel emniyet yönetimi eğitimine sahip olmalıdır. Sorumlu yöneticinizin ve emniyet yöneticinizin, üst yönetim taahhüdünü kanıtlamanın bir yolu olarak harici eğitim kurslarına katılması makul olabilir. Sonrasında, emniyet yöneticisinin, önemli bilgileri ve yeni kavramları kuruluşun geri kalanına iletmesi sağlanarak, bu yatırımdan daha fazla yararlanılabilir.

Ayrıca, Emniyet Yönetim Sisteminin (SMS) uygulanmasına ve SMS faaliyetlerine ilişkin en iyi uygulamaların paylaşıldığı ulusal otoritelerin SMS seminerlerine ve sektör toplantılarına katılabilirsiniz.

SMS eğitimi ve teşviki günlük işiniz ile bütünleştirilmelidir; böylece, emniyet hususu, tüm havacılık faaliyetlerinizde yer alabilir. Günlük işler yaparken emniyet konularının tartışılması; bilginin yayılması ve olumlu bir emniyet kültürü oluşturulması için etkili bir yol olabilir.

Tablo 4: Bir SMS Bileşeni Olan "SMS Eğitimi ve Teşviki" ile ilgili Maliyetler ve Faydalar

	Doğrudan Maliyetler	Dolaylı Maliyetler	Faydalar
Başlangıç	<ul style="list-style-type: none"> Eğitim ihtiyaçları analizi Eğitim materyali geliştirme Potansiyel danışmanlık Eğitimin verilmesi Teşvikin sağlanması 	<ul style="list-style-type: none"> Üretim sırasında çalışmama süresi 	<ul style="list-style-type: none"> Özel eğitim Yeteneğin geliştirilmesi Olumlu emniyet kültürü - daha fazla SMS satın alınması Kurumsal karar verme sürecinin takviye edilmesi
Takip	<ul style="list-style-type: none"> Eğitimin etkinliğinin izlenmesi Yenileme eğitimi SRM sonuçları da göz önünde bulundurularak teşvikin sağlanması 	<ul style="list-style-type: none"> Üretim sırasında çalışmama süresi 	<ul style="list-style-type: none"> Doğru ve uygun sürecin kanıtlanması Emniyet Risk Yönetiminin (SRM) etkinliğinin ve etkinliğinin artması Aktif risk azaltımı Yatay iletişim ve işbirliğinin geliştirilmesi Ortak kuruluşlar, sektör birlikleri veya federasyonlar ile işbirliğinin geliştirilmesi

SMS Etkinlik Katsayısının Belirlenmesinde Kullanılan Potansiyel Metrikler

- Raporlama oranlarında artış
 - Tüm raporlar
 - Herhangi bir ilişkili emniyet olayı olmaksızın süreç iyileştirmelerinin önerildiği raporlar
- Diğer eğitim ile karşılaştırıldığında, HF eğitimi de dahil olmak üzere, SMS eğitimine harcanan zamanın ve paranın oranı (%)
- Emniyet iletişimi hususunda personel farkındalığı
- Toplantıların ve bilgilendirme seanslarının sayısı
- SMS teşvik eğitimi yeni çalışanların oranı (%)
- Gerekli eğitimi tamamlayan personelin oranı (%)
- SMS eğitim sınavlarının ortalama puanı
- Geliştirme amaçlı incelenen SMS kurslarının sayısı
- Eğitim programı ile ilgili olarak elde edilen denetim bulgularının sayısı

5. İlave Rehberlik

Etkili bir Emniyet Yönetim Sisteminin (SMS) nasıl uygulanacağına ilişkin rehberlik sağlanması ile ilgili olabilecek diğer SM ICG dokümanları aşağıda belirtilmektedir:

- SMS Değerlendirme Aracı;
- Üst Yöneticinin Emniyet Yönetim Sistemindeki (SMS) Rolü;
- Ön Hat Yöneticisinin Emniyet Yönetim Sistemindeki (SMS) Rolü;
- Hizmet Sağlayıcılara Yönelik Olarak Emniyet Performansının Ölçülmesine İlişkin Kılavuz İlkeler ve
- SMS Entegrasyonu – Göz Önünde Bulundurulacak Hususlar.

6. Ekler

Bu doküman üç ek içermektedir.

Ek 1, *Emniyet Yönetimi Sisteminin (SMS) Bir Bütün Olarak Uygulanmasına İlişkin Olarak Yatırımın Geri Dönüşü (ROI) – Elektronik Çizelge Şeklinde Hesaplayıcı* kapsamında, 5 yıldan uzun bir süre boyunca uygulanan Emniyet Yönetim Sisteminin (SMS) maliyetlerini ve faydalarını belirlemek üzere, basit bir elektronik çizelge şeklinde bir SMS hesaplayıcısı yer almaktadır. Bu çizelgede, genel maliyetler ve faydalar, spesifik operasyonel emniyet aksiyonlarına ilişkin maliyetler ve faydalar ile birleştirilmektedir.

Ek 2, *Spesifik Emniyet Aksiyonlarına İlişkin Yatırımın Geri Dönüşü (ROI) Örnekleri* kapsamında, spesifik operasyonel risklere ilişkin bir Yatırım Geri Dönüşününün (ROI) oluşturulmasında yararlı olabilecek ROI hesaplamalarına ilişkin örnekler yer almaktadır.

A.2.1 Üretim Kuruluşu

Örnek 1 - Başka bir Ülkede/Eyalette yeni bir üretim tesisinin açılması

A2.2 Hava Meydanı İşleticisi

Örnek 1 - Uçak yer hasarı olayları

Örnek 2 - Uçağın, yer araçlarının ve personelin zarar görmesi ile sonuçlanan apron kazaları

A2.3 Bakım Kuruluşu

Örnek 1 - Yer araçlarına erişimi kontrol etmek üzere yeni bir sistemin tanıtılması

A2.4 Pilot Eğitim Kuruluşu

Örnek 1 - İrtifa kaybı iyileştirme tekniklerinin güncellenmesi

Örnek 2 - Uygun ve açık/sade bir İngilizcenin kullanılmasını sağlamak amacıyla, tüm el kitaplarının, sınav sorularının, kontrol listelerinin, vb.'nin gözden geçirilmesi

A2.5 Hava Operasyonları

Örnek 1 - Üretici tarafından tavsiye edilen zamandan önce, problemlerin ve sensorların değiştirilmesi

Örnek 2 - Hat operasyonel emniyet denetimi müdahalesi

Örnek 3 - Uçuş Yönetimi Sistemi kontrol paneli üzerindeki herhangi bir anahtarın sürekli bozulmasının düzeltilmesi

Örnek 4 - Uçuş Verilerini İzleme Programı

Ek 3, *Referans Dokümanlar* kapsamında, referans dokümanlar listesi yer almaktadır.

Ek 1: Emniyet Yönetimi Sisteminin (SMS) Bir Bütün Olarak Uygulanmasına İlişkin Olarak Yatırımın Geri Dönüşü (ROI) – Elektronik Çizelge Şeklinde Hesaplayıcı

SMS Hesaplayıcı

Yatırım Geri Dönüşünün (ROI) ve SMS ekonomisinin hesaplanması

Pembe ile belirtilen kalemler, genel maliyetler ve faydaları belirtmekte olup, açık mavi ile belirtilen kalemler, temel faaliyetler ile bağlantılı spesifik emniyet müdahalelerini belirtmektedir.

Emniyet Yönetim Sisteminin (SMS) Uygulanması ve Bakımı Maliyeti

	1. Yıl	2. Yıl	3. Yıl	4. Yıl	5. Yıl
Emniyet Yönetim Sisteminin (SMS) genel yönetimi	\$	\$	\$	\$	\$
İletişim	\$	\$	\$	\$	\$
SMS uygulamasından kaynaklanan çalışmama süresi (örneğin; eğitim verilmesinden dolayı)	\$	\$	\$	\$	\$
Kurum içi denetimler ve değerlendirmeler	\$	\$	\$	\$	\$
Danışmanlık	\$	\$	\$	\$	\$
İlave kaynaklar veya mevcut kaynakların tekrar tahsis edilmesi	\$	\$	\$	\$	\$
Veri toplama ve analiz sistemi	\$	\$	\$	\$	\$
Aksiyon izleme sistemi	\$	\$	\$	\$	\$
Eğitim giderleri (eğitim malzemesinin geliştirilmesi ve/veya sözleşme yoluyla yükleniciye verilmesi)	\$	\$	\$	\$	\$
Toplantılar ve raporlama (örneğin; üst yönetim toplantıları, Emniyet Gözden Geçirme Kurulu (SRB) toplantıları)	\$	\$	\$	\$	\$
Emniyet Aksiyonu 1 - SA 1	\$	\$	\$	\$	\$
Emniyet Aksiyonu 2 - SA 2	\$	\$	\$	\$	\$
Emniyet Aksiyonu 3 - SA 3	\$	\$	\$	\$	\$
Toplam Uygulama Maliyeti	\$	\$	\$	\$	\$

Söz Konusu Hususların Gerçekleştirilmesinin Parasal Faydaları ve Olasılığı (SMS Etkinliği)

	1. Yıl	2. Yıl	3. Yıl	4. Yıl	5. Yıl
Çalışan memnuniyeti - ciro oranında ve istihdam maliyetlerinde azalma	\$	\$	\$	\$	\$
Düzenleyici gerekliliklere uygunluk - düzenleyici gözetim maliyetlerinde azalma	\$	\$	\$	\$	\$
Sigorta primlerinde ve/veya işçi tazminatı primlerinde azalma	\$	\$	\$	\$	\$
Diğer (örneğin; işletim maliyetlerinin azalması, verimin artması)	\$	\$	\$	\$	\$
Emniyet Aksiyonu 1 - SA 1	\$	\$	\$	\$	\$
Emniyet Aksiyonu 2 - SA 2	\$	\$	\$	\$	\$
Emniyet Aksiyonu 3 - SA 3	\$	\$	\$	\$	\$
Toplam tasarruflar	\$	\$	\$	\$	\$
SMS Etkinliği (%)					

SA 1–3 için geçerli değildir

SMS Hesaplayıcı

Yatırım Geri Dönüşünün (ROI) ve SMS ekonomisinin hesaplanması

Sonuçlar

	1. Yıl	2. Yıl	3. Yıl	4. Yıl	5. Yıl	Toplam
Söz Konusu Yıla Ait Yatırım	\$	\$	\$	\$	\$	\$
Söz Konusu Yıla Ait Faydalar	\$	\$	\$	\$	\$	\$
Olası ROI	\$	\$	\$	\$	\$	\$
Öngörülen Olası Tasarruflar	\$	\$	\$	\$	\$	\$
	#DEĞER	#DEĞER	#DEĞER	#DEĞER	#DEĞER	#DEĞER

Düzenlenebilir bir Microsoft Excel kopyası için, smicg.share@gmail.com adresini ziyaret ediniz.

SMS hesaplayıcı rehberi:

Maliyetler, aşağıdaki satırlara tahsis edilebilir:

1. *Emniyet Yönetim Sisteminin (SMS) genel yönetimi*
2. *İletişim*
3. *SMS uygulamasından kaynaklanan çalışmama süresi (örneğin; eğitim verilmesinden dolayı)*
4. *Kurum içi denetimler ve değerlendirmeler*
5. *Danışmanlık*
6. *İlave kaynaklar veya mevcut kaynakların tekrar tahsis edilmesi*
7. *Veri toplama ve analiz sistemi*
8. *Aksiyon izleme sistemi*
9. *Eğitim giderleri (eğitim malzemesinin geliştirilmesi ve/veya sözleşme yoluyla yükleniciye verilmesi)*
10. *Toplantılar ve raporlama (örneğin; üst yönetim toplantıları, SRB toplantıları)*

İlk kalem, 2 ile 10. kalemler ile ilgili olmayabilecek olan herhangi bir sabit ve tekrar eden idari maliyetlere yöneliktir. Söz konusu ayrıntılı kalemlerin her birine yönelik SMS uygulama maliyetlerini girmek istememeniz halinde, genel maliyetleri belirleyerek, bunları 1 ile 10 arasındaki MALİYET satırlarından herhangi birine girebilirsiniz.

Faydalar (tasarruflar) aşağıdaki satırlara tahsis edilebilir:

1. *Çalışan memnuniyeti - ciro oranında ve istihdam maliyetlerinde azalma*
2. *Düzenleyici gerekliliklere uygunluk - düzenleyici gözetim maliyetlerinde azalma (denetimlerde ve incelemelerde harcanan otorite ücretleri ve zaman)*
3. *Sigorta primlerinde ve/veya işçi tazminatı primlerinde azalma*
4. *Diğer (örneğin; işletim maliyetlerinin azalması, verimin artması)*

Söz konusu ayrıntılı fayda kalemlerinin her birine yönelik olarak girdi oluşturmak istememeniz halinde, genel faydaları belirleyerek, bunları 1 ile 4 arasındaki FAYDALAR satırlarından herhangi birine girebilirsiniz.

Bu SMS hesaplayıcısı, geleneksel ROI formülüne dayanmaktadır:

$$\text{ROI} = \frac{\text{Geri ödeme} - \text{Yatırım}}{\text{Yatırım}}$$

Hesaplayıcı, 1 ile 4 arasındaki "fayda" kalemlerine otomatik olarak uygulanan bir **SMS etkinlik katsayısının** kullanılmasını önermektedir. Bu, emniyet yönetimi süreçlerinizin tahmini etkinliği veya olgunluğuna uygun olarak, uygulama süresince Yatırım Geri Dönüşünün (ROI) modüle edilmesini sağlamaktadır.

İlk SMS uygulamasına yönelik olarak, söz konusu katsayıya ilişkin girdilerin örnekleri:

	1. Yıl	2. Yıl	3. Yıl	4. Yıl	5. Yıl
Emniyet Etkinliği %	%25	%40	%60	%75	%85

Yatırım Geri Dönüşünü (ROI), bu katsayıya göre ayarlamak istememeniz halinde, beş hücrenin tümüne "100" girmeniz gerekecektir. SA1 ile SA3 arasındaki spesifik emniyet aksiyonlarına yönelik maliyetlerin ve faydaların özel bir ROI hesaplaması yoluyla belirlenmesi gerektiğinden dolayı, bu "etkinlik katsayısı"nın, söz konusu emniyet aksiyonları için geçerli olmadığı belirtilmelidir. Söz konusu özel ROI hesaplamalarına ilişkin örnekler, Ek 2, Spesifik Emniyet Aksiyonlarına İlişkin Yatırımın Geri Dönüşü (ROI) Örnekleri kapsamında yer almaktadır.

Emniyet aksiyonları satırları: Spesifik operasyonel emniyet iyileştirmeleri için en fazla üç "emniyet aksiyonu" kalemi girebilirsiniz. İlave emniyet aksiyonlarına ilişkin maliyetleri ve faydaları eklemek istememeniz halinde, ilgili tutarları üç emniyet aksiyonu satırının herhangi birine ilave etmeniz gerekecektir. Excel tablosuna ilave satırlar eklenmesi, gömülü formülleri etkileyecektir; bu durumda, ROI hesaplaması çalışmayacaktır.

Ek 2: Spesifik Emniyet Aksiyonlarına İlişkin Yatırımın Geri Dönüşü (ROI) Örnekleri

A2.1 Üretim Kuruluşu – Değişiklik Yönetimi

Emniyet Yatırımı	<p>Pervaneler ve pervane düzenleyicileri üretin bir üretim kuruluşu, başka bir Ülkede/Eyalette yeni bir üretim tesisi açma sürecindedir. Hissedarlar söz konusu yatırımı onaylamışlardır. Kiralama sözleşmeleri, personel istihdamı ve ilave ekipman alımı devam etmektedir.</p> <p>Üretim kuruluşu, tesis edilen SMS kapsamında, bu projeye yönelik resmi bir değişim yönetimi süreci uygulamaktadır.</p>
Göz önünde bulundurulacak hususlar	<p>Uygun bir değişim yönetiminin bulunmaması.</p> <p>Projenin uygun olmayan bir şekilde hazırlanması.</p>
Muhtemel sonuçlar	<ul style="list-style-type: none">• <i>Yeni tesiste üretim sırasındaki tehlikeli durumlar</i>• <i>Eski tesiste değişimden kaynaklanan aksamalar ve üretim yetersizlikleri</i>• <i>İlave tesisin açılmasında önemli bir gecikme</i>• <i>Yetkili otoriteden izin alınmasında önemli bir gecikme</i>
Faydalar	<p>Etkili bir değişim yönetiminin uygulanması yoluyla iyi bir hazırlık sonucunda:</p> <ul style="list-style-type: none">• <i>Yeni tesisteki üretim, ilk olarak hedeflenen tarihten 6 ay önce başlatılabilecektir.</i>• <i>Otorite onayı, kuruluş el kitaplarına yönelik ilave denetimlere veya değişikliklere gerek olmaksızın, ilk olarak planlanan süre içerisinde verilmiştir.</i>
ROI	<p>Değişim yönetimi sürecinin MALİYETİ</p> <p>Değişiklik yönetimi kapsamında, her biri tehlike tanımı, risk değerlendirmesi, aksiyon takibi, raporlama, vb. ile ilgili olarak 1 tam gün (haftada 8 saat) çalışan 3 kişiden oluşan bir ekip</p> <p>Süre: 5 ay / 21 hafta Saat başına ücret: 60 USD <u>Toplam maliyet: 21 hafta x 3 kişi x 8 saat x 60 USD</u> Toplam maliyet = 30.240 USD</p> <p>FAYDA</p> <p>Yeni tesiste üretimin erken başlamasına ilişkin ilave net fayda: 8.000 USD aylık x 6 ay = 72.000 USD</p> <p>Yeni tesis için otorite onayının "sorunsuz" alınması sebebiyle maliyet tasarrufları (denetim tekrarı olmamıştır): Gözetim ücretleri: 1.400 USD x 3 günlük denetim = 4.200 USD Yerinde denetim sebebiyle "Çalışmama" = 3.000 USD <u>Yeniden yazım açıklaması</u> = 800 USD Toplam fayda: = 80.000 USD</p> <p>ROI = (80.000 USD – 30.240 USD) ÷ 30.240 USD ROI = %164</p>

A2.2 Hava Meydanı İşleticisi

Hava Meydanı İşleticisi - Örnek 1

Arka Plan	Herhangi bir havaalanı, son 12 ayda her ay ortalama 0,5 uçak yer hasarı olayı meydana gelmektedir. Olay başına ortalama maliyet 200.000 USD (onarımlar, yeniden planlama, vb.) veya yıllık olarak 1.200.000 USD	
Emniyet Aksiyonu	Yıllık olarak altı olay; iki tanesi havaalanı işleticisinin kontrolü dışında olduğundan dolayı, dört olarak ele almak makul olacaktır. Dolayısıyla, müdahaleler, 800.000 USD meblağında potansiyel kayıplara işaret etmektedir. GÖZ ÖNÜNDE BULUNDURULAN EMNİYET KONULARI: <ul style="list-style-type: none">• Açık bölgelerde yetersiz apron işaretlemeleri• Yetersiz yer ekipmanı bakımı• Prosedürlere yeterli bir şekilde riayet edilmemesi• Yeterli bir şekilde eğitilmiş personelin bulunmaması	
Maliyetler		
	Apronlardaki emniyet bölgelerinin yeniden boyanması	50.000 USD
	Seçilen yer ekipmanının yenilenmesi	200.000 USD
	İyileştirilmiş prosedürler ve personel eğitimi	30.000 USD
	Yer hasarını azaltmaya yönelik teşvik programı	100.000 USD
	Havaalanı toplam yatırımı	380.000 USD
Faydalar	Kaçınılan maliyetler: Müdahaleler olmaksızın yıllık KAYIP 4 Olay x 200.000 USD = 800.000 USD	
ROI	ROI = $(800.000 \text{ USD} - 380.000 \text{ USD}) \div 380.000 \text{ USD}$ ROI = %110	

Hava Meydanı İşleticisi - Örnek 2

Arka Plan	Herhangi bir uluslararası havaalanı, uçağın, yer hizmeti araçlarının ve personelin zarar görmesi ile sonuçlanan apron kazalarından dolayı, yıllık olarak, yaklaşık 2.000.000 USD meblağında bir masrafın altına girmektedir. Masraflar; uçak onarımları, yer ekipmanı onarımları, uçuşların gecikmesi ve yeniden planlanması ile ilgili giderler, yaralanma ile ilgili tıbbi masraflar, vb. masraflardan oluşmaktadır. Masrafların çoğu, sigorta şirketleri tarafından teminat kapsamında dahil edilmektedir. Uygulanmış olan etkili hafifletici aksiyonlardan biri, yıllık emniyet farkındalığının/tazeleme forumunun oluşturulmasıdır.
Emniyet Aksiyonu	Apron emniyeti ile ilgili hususlara ilişkin yüksek bir farkındalık seviyesi sağlamak üzere, havaalanı personeli için özel bir Emniyet ile ilgili "Walk-in-days" (Hızlandırılmış Eğitim Günleri) (yılıda 4–5 gün) sağlanması.
Göz önünde bulundurulacak tehlike	Yerdeki ayırımın yetersiz olması
Muhtemel sonuçlar	Bir veya daha fazla uçağın ciddi seviyede zarar gördüğü ve ciddi yaralanmalar ile sonuçlanan apron kazaları

Maliyetler	<i>"Walk-in-day" organize edilmesi ve gerçekleştirilmesi (Yıllık olarak tekrar eden maliyet)</i>	30.000 USD
	<i>Hafifletmenin etkinliğinden dolayı, giderler, havaalanı sigorta şirketi tarafından yerine getirilmiştir.</i>	—30.000 USD
	Havaalanı toplam maliyeti	0 USD

Faydalar (geleceğe yönelik olarak kaçınılacak olan giderler)	<i>Havaalanının SMS verileri doğrultusunda, "Walk-in-day" kampanyasının başlatılması, apron kazalarında %5 oranında bir azalma ile sonuçlanmıştır</i> <i>Yıllık 2.000.000 USD meblağındaki kaybın %5'i (tahmin edilen değil, kanıtlanan)</i>	100.000 USD
	Öngörülen toplam faydalar	100.000 USD
ROI	ROI = (100.000 USD – 30.000 USD) ÷ 30.000 USD ROI = %233	

A2.3 Bakım Kuruluşu

Emniyet Aksiyonu	<i>Çeşitli havayollarına hizmet veren büyük bir bakım, onarım ve revizyon (MRO) kuruluşu, hat bakımında ve üs bakımında kullanılanlar da dahil olmak üzere tüm yer araçlarına erişimi kontrol etmek üzere yeni bir sistem tesis etmiştir. Her personelin, motoru çalıştırmadan önce, kimlik kartlarını, araçta bulunan akıllı kart okuyucuya okutmaları gerekmektedir. Personelin, kullanmaya yetkin veya yetkili olmadığı bir aracı kullanmaya çalışması halinde, söz konusu personel motoru çalıştıramaz. İlave olarak, araçların hızı ve konumu, gerçek zamanlı olarak izlenmekte olup, aşırı hızlar, otomatik olarak kaydedilerek raporlanacaktır.</i>
Göz önünde bulundurulacak tehlike	<i>Yer aracının yetkisiz kullanımı Yer araçlarının yetkili personel tarafından uygun olmayan bir şekilde kullanılması</i>
Muhtemel sonuçlar (doğrudan)	<i>Yer aracı trafik kazaları Üs veya hat bakımında uçağın zarar görmesi</i>
En kötü durum sonucu	<i>Bir veya daha fazla uçağın ciddi seviyede zarar gördüğü ve bakım personelinin ciddi seviyede yaralandığı kazalar</i>

Maliyetler		
	<i>Akıllı kart okuyucularını uygulama maliyeti</i>	30.000 USD
	<i>Bireysel akıllı kartların personele tahsis edilmesi maliyeti (çalışmama süresi dahil)</i>	10.000 USD
	<i>Hız ve konum izleme yazılımı ile ilgili maliyet</i>	4.000 USD
	Yeni sistemin tüm yer araçlarına uygulanmasına ilişkin olarak altına girilen toplam maliyet	44.000 USD
	<i>Sistemin bakımı ve izleme verilerinin analizi ile ilgili yıllık maliyetler</i>	5.000 USD
Faydalar (geleceğe yönelik olarak kaçınılacak olan giderler)	<i>Son beş yıldır, MRO, yer aracı kazasından kaynaklanan yıllık ortalama 1,5 önemli olay ile karşılaşmıştır. Olay başına ortalama maliyet 22.000 USD meblağındadır (uçacağın zarar görmesi ve/veya yer aracının zarar görmesi)</i>	33.000 USD
	3 yıldan fazla bir süre boyunca kaçınılan tahmini maliyetler	99.000 USD
	5 yıldan fazla bir süre boyunca kaçınılan tahmini maliyetler	165.000 USD
3 yıldan fazla ROI	Kaçınılan maliyetler: 99.000 USD Sistemin uygulanması maliyeti + yıllık bakım maliyetleri: 44.000 USD + 15.000 USD 59.000 USD ROI = (99.000 USD – 59.000 USD) ÷ 59.000 USD ROI = %67	
5 yıldan fazla ROI	Kaçınılan maliyetler: 165.000 USD Sistemin uygulanması maliyeti + yıllık bakım maliyetleri: 44.000 USD + 25.000 USD 69.000 USD ROI = (165.000 USD – 69.000 USD) ÷ 69.000 USD ROI = %139	

A2.4 Pilot Eğitim Kuruluşu

Pilot Eğitim Kuruluşu - Örnek 1

Emniyet Aksiyonu	<i>Otorite tarafından yayınlanan en güncel iyileştirme tekniklerine uygun olarak hareket amacıyla, Pilot Eğitimi El Kitabı kapsamında özetlenen irtifa kaybı iyileştirme tekniklerinin güncellenmesi</i>
Göz önünde bulundurulacak tehlike	<i>Pilot Eğitim Kuruluşunun yetersiz eğitime sahip öğrencileri hizmete vermesi</i>
Muhtemel sonuçlar (doğrudan)	<i>Pilot Eğitim Kuruluşunun itibarının ve düzenleyici ilişkilerde güvenin etkilenmesi sonucu öğrencilerin sayısında muhtemel azalma</i>
En kötü durum sonucu	<i>Tespit edilmemesi halinde (uçuşu gerçekleştiren havayolu): havayolu operasyonunda kaza - kontrol kaybı</i>

Maliyetler	En güncel irtifa kaybı iyileştirme tekniklerini içeren ilave bir uçuş eğitimi ihtiyacı	
	<ul style="list-style-type: none"> Eğitmenlerin yeniden eğitilmesi (çalışmama süresi dahil) Pilot eğitimi el kitaplarının güncellenmesi (otorite onayı dahil) <p>Yeniden eğitim için kullanılan uçağın elverişsizliğinden kaynaklanan havayoluna ilişkin maliyetler göz önünde bulundurulmamaktadır</p>	<p>40.000 USD</p> <p>12.000 USD</p>
	Pilot Eğitim Kuruluşuna yönelik toplam maliyet	52.000 USD
Faydalar (geleceğe yönelik olarak kaçınılacak olan giderler)	Emniyetli ve doğru bir eğitim ile geleceğe yönelik yeniden eğitim ihtiyaçlarının önlenmesi	70.000 USD
	<ul style="list-style-type: none"> Örneğin: Her öğrenci için 1 saatlik uçuş (FH) x 7.000 USD/FH 50 öğrenci eğitimi geçmiş olacaktır (bu kuruluşa yönelik mevcut öğrenci sayısı doğrultusunda) İhtiyatlı tahmin, havayolu tarafından nihai olarak "tespit edilmiş" olanların %20'sidir (= 10 öğrenci) 	
	Pilot Eğitimi Kuruluşunun, önümüzdeki 24 ay boyunca öğrencilerin sayısında azalmaya yol açan itibar kaybından kaynaklanan maliyetlerin önlenmesi.	150.000 USD
	Genel fayda	220.000 USD
2 yıldan fazla ROI	ROI = (220.000 USD – 52.000 USD) ÷ 52.000 USD ROI = %323	

Pilot Eğitim Kuruluşu - Örnek 2

Emniyet Aksiyonu	Kurum içi emniyet raporlama şemasının sunulmasının ardından, Pilot Eğitim Kuruluşu, dil zorlukları ile ilgili bir sorun olduğunu farkına varmıştır. Sorunun büyüklüğünün analiz edilmesinin ardından, kuruluş, tüm el kitaplarını, sınav sorularını, kontrol listelerini incelemeye ve uygun ve sade bir İngilizce kullanılmasını sağlayacak şekilde ders vermeye karar vermiştir.
Göz önünde bulundurulacak tehlike	Dil zorlukları sebebiyle olumsuz eğitim meydana gelebilir. Havacılık dili İngilizce olmasına rağmen, ana dili İngilizce olmayanlar, dilin sadece çalışma dili hakkında bilgiye sahip olabilir ve az kullanılan veya karmaşık sözcükleri veya ifadeleri anlayamayabilirler

	İlaveten, kültürel özellikler, kişilerin, anlamada güçlük çektiklerini kabul etmelerini engelleyebilir.
Muhtemel sonuçlar (doğrudan)	Eğitim süresinin uzaması, öğrenci sayısının azalması, itibar kaybı
En kötü durum sonucu	Olumsuz eğitimden kaynaklanan uçak kazası veya olayı.

Maliyetler	Tüm dokümanların incelenmesine yönelik maliyetler: <ul style="list-style-type: none"> • El kitapları • Sınav soruları • Kontrol listeleri • Teknik materyal Belirsizlikleri raporlamak üzere öğrencilere yönelik bir geribildirim mekanizmasının uygulanmasına yönelik maliyetler	10.000 USD 12.000 USD 16.000 USD 22.000 USD 4.000 USD
	Pilot Eğitim Kuruluşlarına yönelik toplam maliyet	64.000 USD
	Geribildirim mekanizmasının sağlanmasına, geribildirimlerin analiz edilmesine ve gerekli görülmesi halinde değişiklik gerçekleştirilmesine ilişkin yıllık maliyetler	5.000 USD
Faydalar (geleceğe yönelik olarak kaçınılacak olan giderler)	Eğitim süresinin uzama olasılığının önlenmesi <ul style="list-style-type: none"> • Örneğin: <ul style="list-style-type: none"> ○ Eğitim süresinde %3 oranında artış/uzama ○ Yıllık 200 öğrenci x ortalama gelir doğrultusunda, öğrenci başına 15.000 USD Ortalama eğitim süresinin dil sorunlarından dolayı %3 oranında uzaması, Pilot Eğitim Kuruluşunun, altı öğrenciye eğitim veremeyeceği anlamına gelecek olup, bu da 6 x 15.000 USD/yıl meblağında bir potansiyel gelir kaybı anlamına gelecektir.	90.000 USD
	Pilot Eğitimi Kuruluşunun, önümüzdeki 12 ay boyunca öğrencilerin sayısında azalmaya yol açan itibar kaybından kaynaklanan maliyetlerin önlenmesi. <ul style="list-style-type: none"> • Örneğin: <ul style="list-style-type: none"> ○ Ortalama öğrenci sayısında %2 oranında azalma ○ Yıllık 200 öğrenci x ortalama gelir doğrultusunda, öğrenci başına 15.000 USD Ortalama öğrenci sayısında %3 oranında azalma, Pilot Eğitim Kuruluşunun, dört öğrenciye eğitim veremeyeceği anlamına gelecek olup, bu da 4 x 15.000 USD/yıl meblağında bir potansiyel gelir kaybı anlamına gelecektir.	60.000 USD
	Genel fayda	150.000 USD
1 yıldan fazla ROI	Kaçınılan maliyetler: Sistemin uygulanması maliyeti + yıllık bakım maliyetleri: 64.000 USD + 5.000 USD ROI = (150.000 USD – 69.000 USD) ÷ 69.000 USD ROI = %117	150.000 USD 69.000 USD
2 yıldan fazla ROI	Kaçınılan maliyetler: Sistemin uygulanması maliyeti + yıllık bakım maliyetleri: 64.000 USD + 10.000 USD ROI = (300.000 USD – 74.000 USD) ÷ 74.000 USD ROI = %305	300.000 USD 74.000 USD

A2.5 Hava Operasyonları

Hava Operasyonları - Örnek 1

Emniyet Aksiyonu	B737 filosu: Pilot arıza raporu veya yanlış alarmlar yoluyla tehlike tanımının ardından, üretici tarafından tavsiye edilen tarihten önce problemlerin veya sensorların değiştirilmesi
Göz önünde bulundurulacak tehlike	Hatalı uçuş parametrelerinin gösterilmesine sebep olan sensor arızası
Muhtemel sonuçlar (doğrudan)	Uçak gönderilemeyebilir
En kötü durum sonucu	Uçuş sırasında kontrol kaybı (LOC-I)
ROI	Uçak başına modifikasyon MALİYETİ: 1.200 USD Toplam maliyet: 1.200 USD x 8 = 9.600 USD Sonraki 3 yıl boyunca uçak başına FAYDA ("çalışmama süresi" önlenmiştir) 3.400 USD Toplam fayda: 3.400 USD x 8 = 27.200 USD ROI = (27.000 USD – 9.600 USD) ÷ 9.600 USD ROI = %183

Hava Operasyonları - Örnek 2

Emniyet Aksiyonu	Uçuş alanlarında, malzemelerde, gönderimde, bakımda, hava trafikte ve apron operasyonlarında Hat Operasyonel Emniyet Denetimi (LOSA) Müdahalesi	
Maliyetler	LOSA gözlemlerine ilişkin tipik giderler, personel giderlerini, veri analiz giderlerini ve müdahale giderlerini (eğitim değerlendirmesi, eğitim öncesi değerlendirme ve eğitim sonrası değerlendirme) içermektedir.	
	Sefer	15.000 USD
	Malzemeler	12.500 USD
	Gönderim	15.000 USD
	Bakım	15.000 USD
	Hava Trafik	4.000 USD
	Apron Operasyonları	15.000 USD
	TOPLAM	76.500 USD
Faydalar	Operasyonel Emniyet Denetiminden (LOSA) elde edilen faydalar, düzenleyici gereklilik ihlallerinde azalmayı, standart işletim prosedürlerine uygunlukta artışı, yakıt giderlerinde azalmayı, kaybedilen zaman yaralanmalarında azalmayı, ekipmanın zarar görmesinde azalmayı ve sistemik tehlikelerin/arızaların proaktif bir şekilde tanımlanmasını içermektedir.	
	Sefer	70.000 USD
	Malzemeler	10.000 USD
	Gönderim	90.000 USD
	Bakım	75.000 USD
	Hava Trafik	50.000 USD
	Apron Operasyonları	50.000 USD
	TOPLAM	345.000 USD
ROI	ROI = (345.000 USD – 76.500 USD) ÷ 76.500 USD ROI = %351	

Hava Operasyonları - Örnek 3

Emniyet Aksiyonu	<i>İki uçağa ilişkin olarak (sekiz uçaktan oluşan filo) Uçuş Yönetimi Sistemi (FMS) kontrol paneli üzerindeki herhangi bir anahtarın sürekli bozulmasının düzeltilmesi</i>	
Göz önünde bulundurulacak tehlike	<i>Anahtarın, uçuş ekibi kokpiti girdiğinde ve merkezi alet pedastalının üzerinden geçtiğinde, ayakları ile anahtarı tekmeleyebilecekleri ve anahtarı kırabilecekleri bir pozisyonda konumlandırılması</i>	
Muhtemel sonuçlar (doğrudan)	<i>FMS hizmet dışı bırakılabilir</i>	
En kötü durum sonucu	<i>Anahtar kırılması sonucunda, uçak, gönderilemeyecektir.</i>	
Maliyetler		
	<i>Anahtarı sökme ve değiştirme maliyeti (parçalar ve işçilik)</i>	1.775 USD
	<i>Programda gecikme cezaları maliyeti ve alternatif kaldırma sağlanmasına ilişkin maliyet (başka bir uçak kiralarak)</i>	18.000 USD
	Kuruluşa yönelik olarak iki olay için altına girilen toplam maliyet	19.775 USD
	<i>Onarım maliyeti</i>	1.200 USD
	<i>İki uçağa ilişkin olarak, küçük şalterin, düğmeli şalter ile değiştirilmesi (onay, parçalar ve işçilik de dahil olmak üzere modifikasyon)</i>	4.600 USD
	Tehlikenin giderilmesine ilişkin toplam maliyet	5.800 USD
ROI 1	Tehlikenin giderilmesi halinde, uygun ROI aşağıdaki şekilde olacaktır: ROI = (19.775 USD – 5.800 USD) ÷ 5.800 USD ROI = %241	
Faydalar (geleceğe yönelik olarak kaçınılacak olan giderler)	<i>Filo içerisinde geriye kalan altı uçağa ilişkin sorunun onarım maliyeti (uçak başına 4.600 USD)</i>	27.600 USD
	<i>Geriye kalan altı uçakta meydana gelen ilave olay ve tekrar eden olaylar da dahil olmak üzere, önlenebilir tahmini maliyetler (uçak başına 18.000 USD)</i>	108.000 USD
ROI 2	ROI = (108.000 USD – 27.600 USD) ÷ 27.600 USD ROI = %291	
<i>Bu örnek aşağıdaki kaynaktan elde edilmiştir: Havacılık Emniyet Yönetimi Sistemleri, Yatırım Geri Dönüşü Araştırması, Havacılık Emniyeti Araştırma Merkezi – St Louis Üniversitesi – Şubat 2011</i>		

Hava Operasyonları - Örnek 4

Uçuş Verilerini İzleme (FDM)					
<p>Muhtemelen, Uçuş Verilerini İzleme (FDM) Programının amacı, farklı uçuş aşamalarında meydana gelen olumsuz trendlerin ve davranışların düzeltilmesi yoluyla emniyeti iyileştirmektir. Pek çok Ülke, bunu zorunlu kılmamakla birlikte, Emniyet Yönetim Sistemi (SMS) aracılığıyla, Uçuş Verilerini İzleme (FDM) Programının uygulanması, genellikle olumlu sonuçlanan açık ve anlaşılır bir emniyet analizi programıdır.</p> <p>Uçuş Verilerini İzleme (FDM) Programına ilişkin ayrıntılı bir maliyet-fayda araştırması, kısmen sınırlandırılmakla birlikte, <i>Uçuş Verilerini İzleme (FDM) Programlarının Havayollarına Potansiyel Faydalarının Analizi</i>³ başlıklı ilginç bir tez araştırması, "...emniyet faydalarının yanı sıra FDM programına sahip bir havayolunun yararlanabileceği diğer faydalar da bulunmaktadır. Bunların bazıları, havayolu tarafından altına girilen maliyetleri azaltacak olup, bu maliyet tasarruflarının, FDM programını çalıştırılmasına ilişkin maliyetleri kapsayacak kadar yeterli olan miktardan fazla olması muhtemeldir" sonucuna varılmıştır.</p>					
Emniyet Faydaları			Maliyet Faydaları		
<p>Raporda, emniyet faydalarının aşağıdaki hususlarda tespit edildiği sonucuna varılmıştır:</p> <ol style="list-style-type: none"> 1. İyileştirilmiş pilot eğitimi programları; 2. Daha iyi işletim prosedürleri; 3. İyileştirilmiş uçuş operasyonları emniyeti ve 4. Daha kapsamlı emniyet raporu araştırmaları. 			<p>Raporda, ayrıca, aşağıdaki maliyet faydaları tespit edilmiştir:</p> <ol style="list-style-type: none"> 1. Bakım ve garanti taleplerinin azalması; 2. Uçağın uçuşa elverişlilik durumunun artması; 3. En yüksek seviyede yakıt tüketimi; 4. Sigorta giderlerinin azalması ve 5. Gürültü ihlallerine yönelik para cezalarını azalması 		
<p>Rakamlar</p> <p>Tez araştırmasından alınan aşağıdaki tablolarda, maliyetler ve tasarruflar özetlenmektedir (bu hesaplamaların, 1997 ile 2002 yılları arasında gerçekleştirildiği belirtilmelidir):</p> <p style="text-align: center;">Tablo 1: F5 Yıl Boyunca FDM Programından Elde Edilen Tahmini Toplam Yıllık Tasarruflar.⁴</p>					
<p>³ R. Vaz Fernandes, I. Stockman An Analysis of the Potential Benefits to Airlines of Flight Data Monitoring Programmes (Uçuş Verileri İzleme Programlarının Havayollarına Potansiyel Faydalarına İlişkin Analiz) Cranfield Üniversitesi, Eylül, 2002</p> <p>⁴ Cobert, Harlan ve Harris, Regina. UTRS. (2000). Justifying a Flight Operations Quality Assurance (FOQA) Program (Uçuş Operasyonları Kalite Güvence (FOQA) Programının Doğrulanması). FOQA 2000 Sempozyumu, 29 Mart 2000.</p>					
KALEM	1. YIL	2. YIL	3. YIL	4. YIL	5. YIL
Motor Sökülmelerinde Azalma	\$ 125.000,00	\$ 500.000,00	\$ 500.000,00	\$ 500.000,00	\$ 500.000,00
Kanat Uzatmalarındaki Motor	\$ 412.500,00	\$ 1.650.000,00	\$ 1.650.000,00	\$ 1.650.000,00	\$ 1.650.000,00
Düzensiz koşulların tespit edilmesi	\$ 3.141,00	\$ 12.563,00	\$ 12.563,00	\$ 12.563,00	\$ 12.563,00
Yakıt Tasarrufları	\$ 14.692,00	\$ 58.769,00	\$ 58.769,00	\$ 58.769,00	\$ 58.769,00
Kırılma ve Aşınmada Azalma	\$ 6.000,00	\$ 24.000,00	\$ 24.000,00	\$ 24.000,00	\$ 24.000,00
Sigorta İndirimi	\$ -	\$ 1.269,00	\$ 1.269,00	\$ 5.000,00	\$ 5.000,00
Gelişmiş Kalifikasyon Programı (AQP) Tek Ziyaret Eğitimi (SVT) Tasarrufları	\$ -	\$ 162.667,00	\$ 162.667,00	\$ 162.667,00	\$ 162.667,00
TOPLAM FAYDA	\$ 561.333,00	\$ 2.409.268,00	\$ 2.409.268,00	\$ 2.412.999,00	\$ 2.412.999,00

Tablo 2 Tahmini Başlangıç Maliyeti	
UÇUŞ VERİLERİ MUHAFAZA EKİPMANI (başka bir ifadeyle; Hızlı Erişim Kayıt Cihazları (QAR))	\$ 303.500,00
UÇUŞ VERİLERİNİN İNDİRİLMESİNE İLİŞKİN İŞ GÜCÜ	\$ 343.500,00
DANIŞMANLIK, YAZILIM VE DİĞER DONANIM	\$ 180.500,00
ANALİST MAAŞI	\$ 75.000,00
TOPLAM BAŞLANGIÇ MALİYETLERİ	\$ 902.500,00
FİLO BÜYÜKLÜĞÜNE GÖRE TAHMİNİ MALİYETLER VE FAYDALAR	
1997 yılında, Federal Havacılık İdaresi (FAA), uçuş verilerinin izlenmesine ilişkin olarak filo büyüklüğüne göre hesaplanan maliyetleri tahmin etmiştir. Bu veriler, aşağıdaki tablolarda yer almaktadır:	

Tablo 3: Filo Büyüklüğüne Göre Tahmini Maliyetler Ve Faydalar

FİLO BÜYÜKLÜĞÜ	15	50	100
EKİPMAN MALİYETLERİ	\$ 98.500,00	\$ 259.000,00	\$ 492.000,00
PERSONEL MALİYETLERİ	\$ 385.000,00	\$ 500.000,00	\$ 775.000,00
YAKIT TASARRUFLARI	—145.800,00	—48.500,00	—972.000,00
MOTOR TASARRUFLARI	—300.000,00	—1.000.000,00	—2.000.000,00
EMNİYET TASARRUFLARI	—49.500,00	—165.000,00	—330.000,00
TOPLAM YILLIK TASARRUFLAR HARIÇ TOPLAM YILLIK MALİYETLER	—11.800,00	—454.500,00	—2.035.000,00
	<i>NET TASARRUFLAR</i>	<i>NET TASARRUFLAR</i>	<i>NET TASARRUFLAR</i>
SONUÇLAR			
Emniyet yönetim sisteminizde bir emniyet analizi yöntemi olarak Uçuş Verilerini İzleme (FDM) Programının kullanılması, başlangıçta biraz yoğun maliyetli olsa dahi, orta ve büyük ölçekli işleticiler için büyük miktarda tasarruf sağlayabilir. Bu tür örnekler, emniyet ve analiz ile ilgili ek maliyetleri göstermekte olup, Emniyet Yönetim Sistemlerinizi (SMS) daha da geliştirmek için kullanılabilir.			

EK 3: REFERANS DOKÜMANLAR

EMNİYET MÜDAHALELERİNİN DEĞERLENDİRİLMESİNE İLİŞKİN YATIRIM GERİ DÖNÜŞÜ ARACI

William B. Johnson, Ph.D. / Katrina Avers, Ph.D. – FAA
https://www.faa.gov/about/initiatives/maintenance_hf/fatigue/publications/media/2012-10_return_on_investment_examples.pdf

HAVACILIK EMNİYET YÖNETİMİ SİSTEMLERİ, YATIRIM GERİ DÖNÜŞÜ ARAŞTIRMASI

*Havacılık Emniyeti Araştırma Merkezi – St Louis Üniversitesi –
Şubat 2011* <http://parks.slu.edu/research/centers-labs-facilities/CASR/research-papers/aviation-safety-management-systems-roi-study>

KISIM 21/SMS HAVACILIK KURAL KOYMA KOMİTESİ (ARC) – MALİYET-FAYDA ANALİZİ NİHAİ RAPORU

Maliyet Fayda Analizi Çalışma Grubu – Haziran 2014

Aşağıdaki adres üzerinde bir kopyasını talep edebilirsiniz
smicq.share@gmail.com

UÇUŞ VERİLERİ İZLEME PROGRAMLARININ HAVAYOLLARINA POTANSİYEL FAYDALARINA İLİŞKİN ANALİZ

R VAZ FERNANDES © Cranfield Üniversitesi 2002
<http://webcache.googleusercontent.com/search?q=cache:mdABu00P30MJ:www.aviassist.org/imageslog/o/Cranfield%20M.sc%20Thesis%20on%20Flight%20Data%20Monitoring.pdf%20>