



T.C. ULAŖTIRMA VE ALTYAPI BAKANLIĐI
SİVİL HAVACILIK GENEL MÜDÜRLÜĐÜ

HAVACILIK SEKTÖRÜ İÇ KONTROL METODOLOJİSİ

HAVACILIK GÜVENLİĐİ DAİRE BAŐKANLIĐI-SİBER GÜVENLİK KOORDİNATÖRLÜĐÜ



T.C. ULAřTIRMA VE ALTYAPI BAKANLIđI
SİVİL HAVACILIK GENEL MÜDÜRLÜđÜ

1. GRUP HAVACILIK
SEKTÖRÜ İřLETMELERİ

HAVACILIK GÜVENLİđİ DAİRE BAřKANLIđI-SİBER GÜVENLİK KOORDİNATÖRLÜđÜ



SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi (1. Grup Havacılık İşletmeleri)

Sıra	Kontrol Maddesi	Seviye 1	Seviye 2	Seviye 3	Seviye 4	Toplam
1	Erişim Yönetimi	5	7	5	4	21
2	Varlık Yönetimi	1	3	3	2	9
3	İz Kayıt	4	6	3	4	17
4	Farkındalık	3	5	3	2	13
5	Olay Yönetimi	2	3	1	2	8
6	Bakım	3	1	1	1	6
7	İnsan Kaynakları Güvenliği	3	2	1	0	6
8	Fiziksel Güvenlik	2	3	1	1	7
9	Yedekleme	2	1	1	2	6
10	Risk Yönetimi	3	3	3	3	12
11	Durumsal Farkındalık ve Sistem Test	3	4	3	4	14
12	Sistem ve Haberleşme Güvenliği	9	20	11	11	51
13	Siber Güvenlik Yapılanması	2	5	3	2	12
14	İş Sürekliliği	1	1	3	3	8
15	Tedarikçi Yönetimi	2	2	3	1	8
16	Yasal Uyum	1	1	1	1	4
17	İşletim Güvenliği	2	2	1	0	5
18	Sistem Temini, Geliştirme ve Bakım	2	3	1	1	7
19	Yerli Milli Ürün Kullanılması	1	1	1	1	4
20	İletişim	1	1	1	1	4
Seviye Toplam		52	74	50	46	222



SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi (1. Grup Havacılık İşletmeleri)

No	1. Erişim Yönetimi			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	Erişim Yönetimi Kontrol Prosedürünün Oluşturulması	Son kullanıcılara verilecek yetkilerin en az yetki prensibine göre verilmesi	Kritik varlıklara usb, harici harddisk vb. cihazlar ile erişimin kısıtlanması	Son kullanıcı hakları ve ayrıcalıklı erişim hakları sahiplerinin, sahip oldukları yetkileri kullanımını user behaviour inceleme teknikleri ile analiz et, yetkilerini kullanmıyorsa yetkiyi iptal et.
2	Ayrıcalıklı erişim hakkının belirlenmesi ve yönetilmesi	Çalışan grupları dışında kalan kritik varlıklara usb, harici harddisk vb. cihazlar ile erişimin yönetilmesi	Son kullanıcılara ait bt varlıklarına usb, harici harddisk vb. cihazlar ile erişimin kısıtlanması	Son kullanıcılara ait BT varlıklarına usb, harici harddisk vb. cihazlar ile erişimin engellenmesi
3	Son kullanıcı erişim hakları matrisinin oluşturulması	Ayrıcalıklı erişim hakkına sahip kullanıcılarda en az yetki prensibinin uygulanması	Erişim yetki tanımlaması yapan personel ve erişim yetki gözden geçirmesini yapan personelin farklı olması	Son kullanıcı hakları ve ayrıcalıklı erişim hakları sahiplerinin, sahip oldukları yetkileri kullanımını kullanıcı davranışları inceleme teknikleri ile analiz edilmesi, yetkilerin kullanılmaması durumunda yetkinin iptal edilmesi
4	Ayrıcalıklı erişim hakları matrisinin oluşturulması	Son kullanıcı erişim haklarının ilgili birim yöneticileri ile gözden gözden geçirilmesi	İşletme BT varlıklarına erişim sağlaması gereken tedarikçiler için erişim yöntemi ve kontrol mekanizmasının oluşturulması ve yürütülmesi	Tedarikçi firmalara verilen erişim yetkisinin ihtiyacın bitmesi sonucunda yetkinin ivedilikle sonlandırılması
5	Varlıkların kritiklik seviyesine uygun bir parola yönetim süreci tesis edilmesi, uygulanması ve denetlenmesi	Ayrıcalıklı kullanıcı erişim haklarının ilgili birim yöneticileri ile gözden geçirilmesi	Tedarikçi firmalar işletme BT varlıklarına erişim sağlaması sürecinde çok faktörlü doğrulama kullanılması	
6		Kayıtlı olmayan cihazların networke erişiminin kısıtlanması		
7		Tedarikçi firmalara verilen erişim haklarının ilgili süreç bazında ihtiyaç duyulan minimum süre ve minimum yetki bazında verilmesi		



SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi (1. Grup Havacılık İşletmeleri)

No	2. Varlık Yönetimi			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	Varlık yönetimi prosedürünün hazırlanması	İşletme BT varlıklarının ve varlık gruplarının gizlilik, bütünlük ve erişilebilirlik kapsamında değerlerinin alan uzmanları ile birlikte belirlenmesi	Varlık gruplarının puan ve etki analizinin ihtiyaçlar ve güncel siber tehditler kapsamında güncellenmesi	Havacılık kritik data ve sistemlerin imha süreçlerinin belirlenmesi
2		BT varlıklarının kabul edilebilir kullanımlarının belirlenmesi, dokümanite edilmesi ve ilgili paydaşların bilgisine sunulması	Kritik BT süreçlerine yönelik varlıkların imha süreçlerinin belirlenmesi	Havacılık kritik data ve sistemlerin imha süreçlerinin denetlenmesi
3		Varlık gruplarının puan ve etki analizinin periyodik olarak gözden geçirilmesi	Kritik BT süreçlerine yönelik varlıkların imha süreçlerinin denetlenmesi	



SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi (1. Grup Havacılık İşletmeleri)

No	3. İz Kayıt			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	İz kayıt alınması gereken varlıkların belirlenmesi ve söz konusu bu varlıklardan toplanacak iz kayıt niteliğinin tespit edilip dokümanite edilmesi	İz kayıt toplama sürecinin herhangi bir sebepten ötürü sektöre uğraması durumuna karşı bir alarm mekanizması oluşturulması	Toplanan iz kayıtlarının söz konusu uygulama veya sistemlerden farklı bir serverda tutulması	İz kaydı yönetim sürecinde görevlerin ayrılığı ilkesine uygun bir şekilde görevlendirme yapılması
2	Belirlenen varlıklardan ihtiyaç duyulan iz kayıtlarının alınması	Herhangi bir sebepten dolayı iz kayıt sağlayamayan sistemlerin tespit edilmesi için bir tespit mekanizmasının oluşturulması	İşletme veya sektör paydaşlarının karşılaştığı siber güvenlik olaylarına yönelik korelasyonların oluşturulması	Mevcut korelasyon setlerinin periyodik olarak gözden geçirilmesi ve iyileştirilmesi
3	NTP server kullanılması	İz kayıtlarına erişimin yönetilmesi ve kayıt altına alınması	İz kayıtları alarmlarına yönelik yapılan çalışmalar hakkında periyodik olarak analiz yapılması ve söz konusu bu analiz raporunun SGsYY'ye sunulması	Tehdit istihbarat verilerinden gelen bilgiler kapsamında iz kayıt korelasyon sürecinin geliştirilmesi
4	İşletme tarafından alınan iz kayıtları kapsamında toplanan kayıtların nitelik bakımından inkar edilemez olmasının sağlanması	Olası bir siber güvenlik olayına karşı iz kayıtlarının korale edilerek, istenmeyen durumların tespiti için bir süreç oluşturulması		Alarmların ve olayların incelenmesi sonucunda mevcut korelasyonların değerlendirilerek iyileştirilmesi
5		İz kayıtlarına yönelik periyodik analiz raporlarının oluşturulması ve gözden geçirilmesi		
6		Korelasyonlar sonucunda oluşan alarmların incelenerek ihtiyaç duyulması halinde diğer güvenlik süreçlerinin tetiklenmesi		



SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi (1. Grup Havacılık İşletmeleri)

No	4. Farkındalık			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	İşletme personellerine etkin bir siber güvenlik farkındalığı eğitiminin sağlanması	İşletme üst yönetimine özelleştirilmiş bir siber güvenlik farkındalık eğitiminin verilmesi	İşletme personeline en az senede bir siber güvenlik farkındalığı tazeleme eğitimi verilmesi	Verilen farkındalık eğitimleri sonrasında yapılan sınav sonuçlarının analiz edilmesi ve hedeflenen farkındalık artışını sağlamaması durumunda eğitim sürecinin(eğitim materyali, eğitmen, eğitim verilme şekli vb.) gözden geçirilerek iyileştirilmesi
2	İşletme tesislerinde görev alan tedarikçi personele için etkin bir siber güvenlik farkındalığı eğitiminin sağlanması	İşletme tarafından hazırlanan siber güvenlik eğitim materyallerinin periyodik olarak gözden geçirilmesi ve ihtiyaçlar ve güncel siber tehditler kapsamında güncellenmesi	İşletme çalışanlarının siber güvenlik farkındalığı seviyesinin ölçülmesi için işletme çalışanlarının tümünü kapsayacak şekilde en az 6 ayda bir sosyal mühendislik testlerinin yapılması	Yapılan farkındalık sınav ve testlerinde hedeflenen başarı oranının altında kalan personelin farkındalık seviyesini arttırmak amacıyla faaliyetlerde bulunulması
3	Son kullanıcıların siber olay yönetimindeki rollerinin açık bir şekilde dokümente edilmesi ve son kullanıcıların bu süreçteki rollerinin içselleştirilmesi	Siber güvenlik farkındalığı eğitiminin ve sıklığının eğitimi alan personelin icra ettiği görevin kritikliğine uygun olarak verilmesi	İşletme içi siber güvenlik kültürünün artırılması için bülten, poster vb. materyallerin hazırlanması	
4		İşletme personeline verilen siber güvenlik farkındalık eğitimlerinin sonrasında eğitimin yarattığı farkındalık seviyesinin ölçülmesi amacı ile sınavların yapılması		
5		İhtiyaç duyulması halinde işletme paydaşlarının söz konusu siber risk ve tehditler kapsamında bilgilendirilmesi		



SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi (1. Grup Havacılık İşletmeleri)

No	5. Olay Yönetimi			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	Siber güvenlik ihlal olay yönetim ve müdahale süreçlerini kapsayacak politika veya prosedürlerin oluşturulması	Son kullanıcılar ve ilgili paydaşların kullanımına sunulmuş bir siber olay raporlama mekanizmasının oluşturulması	Siber güvenlik ihlal olay yönetim süreçlerinde olay inceleme süreçlerinin etkin bir şekilde yürütülmesi	Siber güvenlik ihlal olay yönetim süreçlerinde tehdit istihbarat hizmetlerinin kullanılarak olası saldırgan gruplarının belirlenmesi, olağan saldırgan gruplarının davranış şekillerinin incelenerek olay yönetim sürecinin yürütülmesi
2	Dokümante edilmiş bir siber güvenlik ihlal olay müdahale sürecinin oluşturulması	İşletmenin yaşadığı siber güvenlik ihlal olaylarını analiz etmesi, kayıt altına alması ve bir daha benzer bir siber güvenlik ihlal olayının yaşanmaması için gerekli önlemleri alması		Haberli veya habersiz olmak üzere periyodik olarak işletmenin siber güvenlik ihlal olaylarına karşı yanıt verme yetkinliğini test edilmesi
3		İşletmenin yaşadığı siber güvenlik ihlal olaylarının nedenlerini alınan dersleri ve bir daha yaşanmaması için alınacak önlemleri kayıt altına alması ve ilgili otoriteler ile paylaşması		



SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi (1. Grup Havacılık İşletmeleri)

No	6. Bakım			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	Bakım amacıyla işletme dışına çıkarılacak sistemlerin içerisinde hiçbir data barındırmamasının sağlanması	BT süreçlerini etkileyecek varlıkların bakım sürelerinin dokümente edilmesi, izlenmesi ve bu sürelerle uygun olarak bakım çalışmalarının gerçekleştirilmesi	Bakım verilerin kayıt altında tutulması ve gizliliğinin sağlanması	Bakım sürecinde yer alan sistemlerin operasyonel süreçlere dahil edilmeden önce güvenlik testlerinin yapılarak söz konusu sistemlerin gizlilik, bütünlük ve erişilebilirlik unsurlarının etkilenmediğinden emin olunması
2	Bakım süreçlerinde görev alacak personelin izlenmesi			
3	BT ve OT süreçlerini etkileyecek varlıkların bakımlarının yetkili işletmeler tarafından görevlendirilen yetkili personel tarafından yapılması			



SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi (1. Grup Havacılık İşletmeleri)

No	7. İnsan Kaynakları Güvenliği			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	İşletme kritik BT varlıklarına erişim sağlayacak personelin işe alım sürecinden önce güvenlik soruşturmalarının yapılması	İş sonlandırma süreçlerinde ilgili personelin yetki ve hesap iptaline yönelik oluşturulan mekanizmanın uygulanmasının denetlenmesi	İşletme siber güvenlik politika ve prosedürleri ile belirlenmiş kural setlerine uyulmaması durumunda uygulanmak üzere bir disiplin sürecinin oluşturulması, dokümente edilmesi ve uygulanması	
2	İş sonlandırma süreçlerinde ilgili personelin yetki ve hesap iptaline yönelik mekanizmanın oluşturulması	Görev değişikliği süreçlerinde ilgili personelin eski görevine yönelik yetki ve hesap iptali mekanizmasının denetlenmesi		
3	Görev değişikliği süreçlerinde ilgili personelin eski görevine yönelik yetki ve hesap iptali mekanizmanın oluşturulması			



SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi (1. Grup Havacılık İşletmeleri)

No	8. Fiziksel Güvenlik			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	Fiziksel güvenlik prosedürünün oluşturulması, periyodik olarak gözden geçirilmesi ve ihtiyaç duyulması halinde güncellenmesi	Kritik BT varlıklarına fiziksel erişimin yetki kapsamında kısıtlanması	Kritik BT varlıklarının bulunduğu alanlara erişim yetkisine sahip olmayan iç ve dış kaynaklı çalışanlara ve ziyaretçilere söz konusu kritik bu alanlara erişimlerinde eşlik edilmesi, bu kişilerin aktivitelerinin izlenmesi	İşletmenin ISO 27001 Ek.A.11 kapsamında senede en az 2 kere denetim faaliyeti gerçekleştirmesi
2	Kritik BT varlıklarını etkileyen fiziksel ortam ve unsurların envanterinin oluşturulması	Kritik BT varlıklarına fiziksel erişimi izlenmesi ve yetkisiz erişimlerin tespit edilmesi		
3		Kritik BT varlıklarının bulunduğu alanlarda, yaka kartı takılmasının zorunlu olması ve kritik BT varlıklarına erişimde kişi yaka kartı eşleştirmesinin yapılması		



SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi (1. Grup Havacılık İşletmeleri)

No	9. Yedekleme			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	İşletmenin süreç kritikliğinde göz önüne alarak bir yedekleme politika veya prosedürü oluşturması	Periyodik olarak yedekten geri dönme test çalışmalarının gerçekleştirilmesi	Alınan yedeklerin farklı bir sunucuda yer alması	Farklı bir risk bölgesinde işletme kritik dataların hepsini içerecek bir FKM yapısının kurulması
2	İşletme yedekleme politika ve prosedürüne uygun şekilde düzenli olarak backup alınması.			Bilgi işleme olanaklarının, erişilebilirlik gereksinimlerini karşılamak için yeterli fazlalık ile gerçekleştirilmesi



SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi (1. Grup Havacılık İşletmeleri)

No	10. Risk Yönetimi			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	Siber Güvenlik Risk Değerlendirme Metodolojisinin belirlenmesi, dokümante edilmesi	Varlık envanteri kapsamında belirlenmiş varlıkları 27001 Ek.A maddeleri kapsamında her bir madde ayrı ayrı olacak şekilde değerlendirilmesi	Risk indirgeme çalışmalarının ilgili birimler ile koordine edilerek yürütülmesi, takip edilmesi ve dokümante edilmesi	Siber Güvenlik sigortası bulunması
2	Siber Güvenlik Etki Değerlendirme Metodolojisinin belirlenmesi, dokümante edilmesi	İşletmenin üretici veya tedarikçi bağımlılığı kapsamında siber güvenlik risklerinin belirlenmesi ve dokümante edilmesi	Risk kabulü ile ilgili sürecin aktif bir şekilde yürütülmesi ve dokümante edilmesi	Siber güvenlik risk değerlendirme çalışmasının tehdit istihbarat çalışmaları çıktıları sonucuna göre güncellenmesi ve iyileştirilmesi
3	Siber Güvenlik Risk Değerlendirme çalışmasının periyodik olarak gözden geçirilmesi ve güncellenmesi	Siber Güvenlik risk değerlendirme çalışmasının işletme iç ve dış kaynaklar tarafından yapılan sızma testi, zafiyet taraması, kırmızı takım vb. çalışmaların sonuçlarına göre güncellenmesi ve iyileştirilmesi	Siber Güvenlik risk değerlendirme çalışmasının işletme iç ve dış kaynaklar tarafından yapılan denetim faaliyetlerinin sonuçlarına göre güncellenmesi ve iyileştirilmesi	Siber Güvenlik Risk Değerlendirme faaliyetlerinin yeterliliğinin ölçülmesi ve iyileştirilmesi



SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi (1. Grup Havacılık İşletmeleri)

No	11. Durumsal Farkındalık ve Sistem Test			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	Mevcut güvenlik mimarisinin güncelliğinin ve işletme ihtiyaçlarını karşılayıp karşılamadığının değerlendirmesinin yapılması	Havacılık Sektörü İç Kontrol Metodolojisine uygun olarak en üst seviyeye erişmek için gerekli olan aksiyonların belirlenmesi	İşletmenin tabi olduğu yasal düzenlemelere uygun hale gelmek için gerekli aksiyonların belirlenmesi	7x24 prensibine göre siber tehdit veya siber güvenlik ihlal olayı müdahale görevini icra edecek bir mekanizmanın kurulması
2	Mesai saatleri içerisinde siber tehdit veya siber güvenlik ihlal olayı tespit görevini icra edecek bir mekanizmanın kurulması	7x24 prensibine göre siber tehdit veya siber güvenlik ihlal olayı tespit görevini icra edecek bir mekanizmanın kurulması	TSE akredite firmalar tarafından en az senede bir geniş kapsamlı sızma testi faaliyetinin gerçekleştirilmesi	Tehdit avcılığı mekanizmasının oluşturulması ve kullanılması
3	Mesai saatleri içerisinde siber olay müdahale görevini icra edecek bir mekanizma kurulması	Siber tehdit veya siber güvenlik ihlal olayı tespit yapılanmasının yeterliliğinin ölçülmesi ve iyileştirilmesi	Siber güvenlik alanında icra edilen iç ve dış kaynaklı test, denetim, zafiyet taraması vb. çalışmalar sonucu tespit edilen bulguların ve risklerin giderilmesi amacıyla bir bulgu yönetim sürecinin tesis edilmesi ve uygulanması	Kırmızı takım çalışmalarının yapılması
4		Siber olay müdahale yapılanmasının yeterliliğinin ölçülmesi ve iyileştirilmesi		Bug bounty çalışmalarının gerçekleştirilmesi
5		Periyodik zafiyet taraması yapılması		



SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi (1. Grup Havacılık İşletmeleri)

No	12. Sistem ve Haberleşme Güvenliği			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	Genel Müdürlük ve taşıra teşkilatı bazında ağ segmentasyonunun yapılması	Birim bazında ağ segmentasyonunun yapılması	Görev ve kritiklik bazında ağ segmentasyonunun yapılması	Risk teşkil eden BT varlıklarına yönelik disk şifreleme çözümlerinin kullanılması
2	İşletme iç ağında internete çıkış noktasına yerleştirilmiş bir güvenlik duvarı cihazının bulunması	Her bir ağ segmentasyonu için ayrı ayrı güvenlik duvarı yapılanmasının oluşturulması	Firewall trafiğinin izlenmesi, analiz edilmesi ve yapılan analiz sonucunda riskli görülen trafiğin engellenmesi	Mevcut DNS filtreleme çalışmalarının KamuDNS projesi ile entegrasyonunun sağlanması
3	Port, protokol ve servis kısıtlamasının minimum yetki prensibine uygun olarak uygulanması	Diştan içe veya içten içe iletilen medyanın taranması için sandbox uygulamalarının kullanılması	DMZ yapılanmasının oluşturulması ve efektif bir şekilde kullanımının sağlanması	İşletme mobil cihazlarının tek bir merkezden güvenlik operasyonlarının yürütülmesi amacıyla MDM kullanılması
4	Network cihazlarının fiziksel güvenliğinin sağlanarak yetkisiz erişiminin engellenmesi	Firewall kurallarının periyodik olarak gözden geçirilmesi ve iyileştirilmesi	Kritik bilgi akışının şifreli bir şekilde yapılması	Network ve sunucu mimarisinin görevler ayrılığı ilkesi gözetilerek değerlendirilmesi, dokümanite edilmesi ve iyileştirilmesi
5	Mac filtreleme metodu ile kayıtlı cihazların işletme iç ağına erişiminin engellenmesi	Ağ güvenlik cihazlarının ve sunucu güvenlik konfigürasyon setlerinin USOM,SHGM gibi üst kuruluşlardan gelen talimatlara göre sıklaştırması	Kritik operasyonlarda erişim yönetim süreçlerinde kullanılmak üzere kriptografik şifreler oluşturulması ve bu şifrelerin kullanımının yönetilmesi	Güvenlik sıkılaştırmalarının yeterliliğinin görevler ayrılığı ilkesi gözetilerek değerlendirilmesi, dokümanite edilmesi ve iyileştirilmesi
6	İnaktif oturumların belirli bir süre sonrasında otomatik kilitlenmesi	İşletme siber güvenlik kabiliyetinin artırılması amacı ile siber istihbarat hizmetlerinin kullanılması	VOİP teknolojileri kullanılıyorsa, söz konusu bu teknolojiye yönelik sıkılaştırmaların yapılması	Network güvenlik cihazlarının konumlandırılmasının ve konfigürasyonlarının görevler ayrılığı ilkesi gözetilerek değerlendirilmesi, dokümanite edilmesi ve iyileştirilmesi
7	İşletme BT sistemleri ile ilgili konfigürasyon envanterlerinin ve temel konfigürasyon setlerinin oluşturulması ve dokümanite edilmesi	Network cihazlarının yönetiminde şifrelenmiş oturumlar kullanılması	Ağ güvenlik cihazlarının ve sunucu güvenlik konfigürasyon setlerinin siber tehdit istihbarat hizmeti verilerine göre sıklaştırması	İşletme bilgi teknolojileri altyapısını korumak için honeypot çözümlerinin kullanılması
8	Mobil cihazlar, sunucular ve son kullanıcılara ait BT varlıklarında antivirüs yazılımı kullanılması	802.1x metodu ile kayıtlı cihazların veya kullanıcıların networke erişiminin engellenmesi	Tüm son kullanıcı gruplarının yüklemeye izni olan uygulamaların belirlenmesi amacıyla whitelist ve blacklist uygulanması ve söz konusu sistemin 7x24 izlenmesi	İşletme bünyesinde kullanılan EKS,SCADA ve IOT teknolojileri için özelleştirilmiş firewall çözümlerinin kullanılması
9	DDoS saldırılarına karşı önlem alınması ve alınan bu önlemlerin yeterliliğini periyodik olarak test edilmesi	DNS filtreleme çalışmasının gerçekleştirilmesi	Sanallaştırma sistemlerinde kullanılacak olan imajların sıkıştırılmasının yapılması ve sürecin denetlenmesi	Veri aktarımı için diyet ürünlerinin kullanılması
10		URL filtreleme çalışmasının gerçekleştirilmesi	İşletme bünyesinde DLP çözümlerinin kullanılması	İşletme bünyesinde kullanılan EKS,SCADA ve IOT teknolojileri için veri aktarımı şifreleme çözümlerinin kullanılması
11		Son kullanıcılar tarafından ziyaret edilen web sitelerinin zararlı bir bileşen(exploit kit vb.) içermediğinin doğrulanması	Son kullanıcılara yönelik cihazlarda EDR çözümlerinin kullanılması	İşletme bünyesinde bulunan sunucularda EDR çözümlerinin kullanılması
12		İhtiyaç duyulduğu kadar yetki prensibine bağlı kalarak güvenlik kontrollerinin uygulanması		
13		Eposta hizmetlerinin güvenliğini sağlamak üzere spam koruma ve email gateway kullanılması		
14		Network trafiğinde şüpheli hareket analizinin yapılması		
15		Kullanıcı bazında şüpheli hareket analizinin yapılması		
16		İşletme bünyesinde NAC çözümlerinin kullanılması		
17		İşletme bünyesinde load balancer çözümlerinin kullanılması		
18		İşletme bünyesinde WAF çözümlerinin kullanılması		
19		İşletme bünyesinde IDS ve IPS çözümlerinin kullanılması		
20		İşletme iç paydaşlarının kullanımına yönelik olan sistemlerin uzaktan erişiminin ipsec vpn üzerinden olması		



SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi (1. Grup Havacılık İşletmeleri)

No	13. Siber Güvenlik Yapılanması			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	SOME'nin kurulmuş olması	SOME'nin BT birim ve süreçlerinden görevlerin ayrılığı ilkesi kapsamında ayrılması	SGSYY'nin SHT-Siber EK-5'de yer alan sertifikalara sahip olması	Siber Güvenlik Stratejik Planı'nın oluşturulması, gözden geçirilmesi ve güncellenmesi
2	SOME birimi personelinin kapsam ve görev tanımlarının belirlenmiş ve dokümante edilmiş olması	SOME biriminin en az Genel Müdür Yrd. seviyesine bağlanması	İstihdam devam ederken rastgele güvenlik soruşturması araştırmalarının yapılması(adli sicil kaydı, şahıs güvenlik belgesi v.b.)	SOME personeli memnuniyetinin ölçülerek birim bazında personel değişiklik oranının düşürülmesi için faaliyetlerde bulunulması
3		SGSYY'nin en az lisans derecesine sahip olması ve siber güvenlik konusunda uzmanlaşmış olması	Görevlendirilecek personelin some kapsamındaki görev ve sorumluluklarını yerine getirebilmesi için sorumlu olduğu konuda uzman olması	
4		Some personeli işe alım sürecinden önce güvenlik soruşturmasının yapılması (adli sicil kaydı, şahıs güvenlik belgesi v.b.)		
5		Some'de görev alan personelin ön lisans veya lisans programlarından mezun olması ve en az iki yıl bilgi işlem tecrübesine sahip olması veya bilgi güvenliği/siber güvenlik konularında bilgi ve tecrübeye sahip olması		



SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi (1. Grup Havacılık İşletmeleri)

No	14. İş Sürekliliği			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	BT varlıklarının iş sürekliliğine yönelik bir politika veya prosedürün oluşturulması	BT varlıklarına yönelik iş sürekliliği etki analizinin yapılması	İş sürekliliği risk ve etki analizinin periyodik olarak gözden geçirilmesi ve ihtiyaç duyulması halinde güncellenmesi	BT süreçlerini etkileyen tüm varlıklara yönelik iş sürekliliği yedekliliğinin sağlanması
2			İş sürekliliği planlarının oluşturulması, gözden geçirilmesi ve güncel tutulması	İş sürekliliği planlarına yönelik tüm hususların tatbikatının senede en az bir kere yapılması
3			İş sürekliliği çalışmalarının, görevler ayrılığı ilkesinde gözetilerek, objektif bir şekilde değerlendirilmesi	İş sürekliliği planı iyileştirme çalışmalarının gerçekleştirilmesi



SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi (1. Grup Havacılık İşletmeleri)

No	15. Tedarikçi Yönetimi			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	Tedarikçi yönetimi politikası veya prosedürünün oluşturulması	Tedarik ihtiyacı olan süreçle ilgili tedarikçi bilgi güvenliği gereksinim seviyelerinin belirlenmesi	Tedarikçi yönetim sürecinin değerlendirilmesi ve iyileştirilmesi	Kritik tedarikçilerin bilgi güvenliği kapsamında denetlenmesi
2	Dış kaynaklı olarak alınan hizmet ve ürünlerin işletmeye olan etkisine göre kritik tedarikçilerinin belirlenmesi	Tedarikçi çıkış stratejilerinin oluşturulması	Kritik tedarikçilerin sözleşmelerinde bilgi güvenliği unsurlarının yer alması	
3			Kritik tedarikçilerin denetim sonuçlarına göre ihtiyaç duyulması halinde çıkış stratejilerinin uygulanması	



SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi (1. Grup Havacılık İşletmeleri)

No	16. Yasal Uyum			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	İşletmenin ISO 27001 Sertifika belgesine sahip olması	ISO 27001 Ek.A.18.2.1 kapsamında yasal uyum süreci envanterinin oluşturulması	İşletmenin yasal sorumluluğunun olduğu alanlarda yeni çıkan regülasyonlar ile ilgili takip mekanizması oluşturması	Yasal uyum süreci ile alakalı boşluk analizinin yapılması



SİVİL HAVACILIK
GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(1. Grup Havacılık İşletmeleri)

No	17. İşletim Güvenliği			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	Yama yönetiminin uygulanması	Değişiklik yönetiminin uygulanması	Kullanıcının yükleme izni olan uygulamalar için whitelist ve blacklist uygulanması ve sürecin izlenmesi	
2	Lisanssız yazılımların kullanılmaması	Kapasite yönetiminin uygulanması		



SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi (1. Grup Havacılık İşletmeleri)

No	18. Sistem Temini, Geliştirme ve Bakım			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	Sistem temini geliştirme ve bakımı süreçlerini ele alan bir politika veya prosedürün oluşturulması	Geliştirilecek veya temin edilecek sistemin güvenliğini sağlamak amacıyla siber güvenlik test süreçlerinin gerçekleştirilmesi	Test verisinin kişisel veri veya operasyonel kritik veri içermemesi	Temin edilecek, geliştirilecek veya güncellenecek sistemlerin güvenliğini sağlamak amacıyla SHT-Siber Ek-10'da yer alan Havacılık Sektörü Güvenli Yazılım Yazılım Geliştirme Rehberi içerisinde bulunan kontrol listesinin kullanılması ve bu sürecin SOME tarafından denetlenmesi
2	Geliştirilecek veya temin edilecek sistemin güvenliğini sağlamak amacıyla analizin yapılması ve siber güvenlik gereksinimlerinin belirlenmesi	İç veya dış kaynaklı sistem temini, geliştirme veya güncelleme süreçlerinde değişiklik yönetimi süreçlerinin etkin bir şekilde yürütülmesi		
3		Test ve geliştirme ortamlarının ayrıştırılması		



SİVİL HAVACILIK
GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(1. Grup Havacılık İşletmeleri)

No	19. Yerli Milli Ürün Kullanılması			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	Yerli ve milli ürünlerin işletme BT ürün envanterindeki oranının %5'den az olması	Yerli ve milli ürünlerin işletme BT ürün envanterindeki oranının %5'den fazla ve %10'dan az olması	Yerli ve milli ürünlerin işletme BT ürün envanterindeki oranının %10'dan fazla ve %20'dan az olması	Yerli ve milli ürünlerin işletme ürün envanterindeki oranının %20'den fazla olması



SİVİL HAVACILIK
GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(1. Grup Havacılık İşletmeleri)

No	20. İletişim			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	Siber güvenlik yapılanması dahilinde sağlıklı bir iletişim mekanizmasının oluşturulması ve yürütülmesi	Tüm işletme kapsamında sağlıklı bir iletişim mekanizmasının oluşturulması ve yürütülmesi	Kritik BT varlıkları tedarikçi firmaları ile sağlıklı bir iletişim mekanizmasının oluşturulması ve yürütülmesi	İşletme siber güvenlik faaliyetlerini etkileyen tüm iç ve dış paydaşlar ile sağlıklı bir iletişim mekanizmasının oluşturulması ve yürütülmesi



SİVİL HAVACILIK
GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(1. Grup Havacılık İşletmeleri)

Havacılık Sektörü İç Kontrol Metodolojisi 1. Grup Havacılık Sektörü İşletmeleri Kontrol Listesi						
Ana Kontrol Maddesi	Seviye	Kontrol No.	Alt Kontrol Maddesi	U	UD	NA
1. Erişim Yönetimi	1	1.1.1	Erişim Yönetimi Kontrol Prosedürünün Oluşturulması			
		1.1.2	Ayrıcalıklı erişim hakkının belirlenmesi ve yönetilmesi			
		1.1.3	Son kullanıcı erişim hakları matrisinin oluşturulması			
		1.1.4	Ayrıcalıklı erişim hakları matrisinin oluşturulması			
		1.1.5	Varlıkların kritiklik seviyesine uygun bir parola yönetim süreci tesis edilmesi, uygulanması ve denetlenmesi			
	2	1.2.1	Son kullanıcılara verilecek yetkilerin en az yetki prensibine göre verilmesi			
		1.2.2	Çalışan grupları dışında kalan kritik varlıklara usb, harici harddisk vb. cihazlar ile erişimin yönetilmesi			
		1.2.3	Ayrıcalıklı erişim hakkına sahip kullanıcılarda en az yetki prensibinin uygulanması			
		1.2.4	Son kullanıcı erişim haklarının ilgili birim yöneticileri ile gözden geçirilmesi			
		1.2.5	Ayrıcalıklı kullanıcı erişim haklarının ilgili birim yöneticileri ile gözden geçirilmesi			
		1.2.6	Kayıtlı olmayan cihazların networke erişiminin kısıtlanması			
		1.2.7	Tedarikçi firmalara verilen erişim haklarının ilgili süreç bazında ihtiyaç duyulan minimum süre ve minimum yetki bazında verilmesi			
	3	1.3.1	Kritik varlıklara usb, harici harddisk vb. cihazlar ile erişimin kısıtlanması			
		1.3.2	Son kullanıcılara ait bt varlıklarına usb, harici harddisk vb. cihazlar ile erişimin kısıtlanması			
		1.3.3	Erişim yetki tanımlaması yapan personel ve erişim yetki gözden geçirmesini yapan personelin farklı olması			
		1.3.4	İşletme BT varlıklarına erişim sağlaması gereken tedarikçiler için erişim yöntemi ve kontrol mekanizmasının oluşturulması ve yürütülmesi			



SİVİL HAVACILIK
GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(1. Grup Havacılık İşletmeleri)

	4	1.3.5	Tedarikçi firmalar işletme BT varlıklarına erişim sağlaması sürecinde çok faktörlü doğrulama kullanılması			
		1.4.1	Son kullanıcı hakları ve ayrıcalıklı erişim hakları sahiplerinin, sahip oldukları yetkileri kullanımını user behaviour inceleme teknikleri ile analiz et, yetkilerini kullanmıyorsa yetkiyi iptal et.			
		1.4.2	Son kullanıcılara ait BT varlıklarına usb, harici harddisk vb. cihazlar ile erişimin engellenmesi			
		1.4.3	Son kullanıcı hakları ve ayrıcalıklı erişim hakları sahiplerinin, sahip oldukları yetkileri kullanımını kullanıcı davranışları inceleme teknikleri ile analiz edilmesi, yetkilerin kullanılmaması durumunda yetkinin iptal edilmesi			
		1.4.4	Tedarikçi firmalara verilen erişim yetkisinin ihtiyacın bitmesi sonucunda yetkinin ivedilikle sonlandırılması			
2. Varlık Yönetimi	1	2.1.1	Varlık yönetimi prosedürünün hazırlanması			
	2	2.2.1	İşletme BT varlıklarının ve varlık gruplarının gizlilik,bütünlük ve erişilebilirlik kapsamında değerlerinin alan uzmanları ile birlikte belirlenmesi			
		2.2.2	BT varlıklarının kabul edilebilir kullanımlarının belirlenmesi,dokümante edilmesi ve ilgili paydaşların bilgisine sunulması			
		2.2.3	Varlık gruplarının puan ve etki analizinin periyodik olarak gözden geçirilmesi			
	3	2.3.1	Varlık gruplarının puan ve etki analizinin ihtiyaçlar ve güncel siber tehditler kapsamında güncellenmesi			
		2.3.2	Kritik BT süreçlerine yönelik varlıkların imha süreçlerinin belirlenmesi			
		2.3.3	Kritik BT süreçlerine yönelik varlıkların imha süreçlerinin denetlenmesi			
	4	2.4.1	Havacılık kritik data ve sistemlerin imha süreçlerin belirlenmesi			
		2.4.2	Havacılık kritik data ve sistemlerin imha süreçlerinin denetlenmesi			
	1	3.1.1	İz kayıt alınması gereken varlıkların belirlenmesi ve söz konusu bu varlıklardan toplanacak iz kayıt niteliğinin tespit edilip dokümante edilmesi			
		3.1.2	Belirlenen varlıklardan ihtiyaç duyulan iz kayıtlarının alınması			
		3.1.3	NTP server kullanılması			



SİVİL HAVACILIK
GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(1. Grup Havacılık İşletmeleri)

3. İz Kayıt	2	3.1.4	İşletme tarafından alınan iz kayıtları kapsamında toplanan kayıtların nitelik bakımından inkar edilemez olmasının sağlanması			
		3.2.1	İz kayıt toplama sürecinin herhangi bir sebepten ötürü sekteye uğraması durumuna karşı bir alarm mekanizması oluşturulması			
		3.2.2	Herhangi bir sebepten dolayı iz kayıt sağlayamayan sistemlerin tespit edilmesi için bir tespit mekanizmasının oluşturulması			
		3.2.3	İz kayıtlarına erişimin yönetilmesi ve kayıt altına alınması			
		3.2.4	Olası bir siber güvenlik olayına karşı iz kayıtlarının korale edilerek, istenmeyen durumların tespiti için bir süreç oluşturulması			
		3.2.5	İz kayıtlarına yönelik periyodik analiz raporlarının oluşturulması ve gözden geçirilmesi			
		3.2.6	Korelasyonlar sonucunda oluşan alarmların incelenerek ihtiyaç duyulması halinde diğer güvenlik süreçlerinin tetiklenmesi			
	3	3.3.1	Toplanan iz kayıtlarının söz konusu uygulama veya sistemlerden farklı bir serverda tutulması			
		3.3.2	İşletme veya sektör paydaşlarının karşılaştığı siber güvenlik olaylarına yönelik korelasyonların oluşturulması			
		3.3.3	İz kayıtları alarmlarına yönelik yapılan çalışmalar hakkında periyodik olarak analiz yapılması ve söz konusu bu analiz raporunun SGSYY'ye sunulması			
	4	3.4.1	İz kaydı yönetim sürecinde görevlerin ayrılığı ilkesine uygun bir şekilde görevlendirme yapılması			
		3.4.2	Mevcut korelasyon setlerinin periyodik olarak gözden geçirilmesi ve iyileştirilmesi			
		3.4.3	Tehdit istihbarat verilerinden gelen bilgiler kapsamında iz kayıt korelasyon sürecinin geliştirilmesi			
		3.4.4	Alarmların ve olayların incelenmesi sonucunda mevcut korelasyonların değerlendirilerek iyileştirilmesi			
	1	4.1.1	İşletme personellerine etkin bir siber güvenlik farkındalığı eğitiminin sağlanması			
		4.1.2	İşletme tesislerinde görev alan tedarikçi personele için etkin bir siber güvenlik farkındalığı eğitiminin sağlanması			
		4.1.3	Son kullanıcıların siber olay yönetimindeki rollerinin açık bir şekilde dokümente edilmesi ve son kullanıcıların bu süreçteki rollerinin içselleştirilmesi			



SİVİL HAVACILIK
GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(1. Grup Havacılık İşletmeleri)

4. Farkındalık	2	4.2.1	İşletme üst yönetimine özelleştirilmiş bir siber güvenlik farkındalık eğitiminin verilmesi			
		4.2.2	İşletme tarafından hazırlanan siber güvenlik eğitim materyallerinin periyodik olarak gözden geçirilmesi ve ihtiyaçlar ve güncel siber tehditler kapsamında güncellenmesi			
		4.2.3	Siber güvenlik farkındalığı eğitiminin ve sıklığının eğitimi alan personelin icra ettiği görevin kritikliğine uygun olarak verilmesi			
		4.2.4	İşletme personeline verilen siber güvenlik farkındalık eğitimlerinin sonrasında eğitimin yarattığı farkındalık seviyesinin ölçülmesi amacıyla sınavların yapılması			
		4.2.5	İhtiyaç duyulması halinde işletme paydaşlarının söz konusu siber risk ve tehditler kapsamında bilgilendirilmesi			
	3	4.3.1	İşletme personeline en az senede bir siber güvenlik farkındalığı tazeleme eğitimi verilmesi			
		4.3.2	İşletme çalışanlarının siber güvenlik farkındalığı seviyesinin ölçülmesi için işletme çalışanlarının tümünü kapsayacak şekilde en az 6 ayda bir sosyal mühendislik testlerinin yapılması			
		4.3.3	İşletme içi siber güvenlik kültürünün artırılması için bülten, poster vb. materyallerin hazırlanması			
	4	4.4.1	Verilen farkındalık eğitimleri sonrasında yapılan sınav sonuçlarının analiz edilmesi ve hedeflenen farkındalık artışını sağlamaması durumunda eğitim sürecinin (eğitim materyali, eğitmen, eğitim verilme şekli vb.) gözden geçirilerek iyileştirilmesi			
		4.4.2	Yapılan farkındalık sınav ve testlerinde hedeflenen başarı oranının altında kalan personelin farkındalık seviyesini arttırmak amacıyla faaliyetlerde bulunulması			
5. Olay Yönetimi	1	5.1.1	Siber güvenlik ihlal olay yönetim ve müdahale süreçlerini kapsayacak politika veya prosedürlerin oluşturulması			
		5.1.2	Dokümante edilmiş bir siber güvenlik ihlal olay müdahale sürecinin oluşturulması			
	2	5.2.1	Son kullanıcılar ve ilgili paydaşların kullanımına sunulmuş bir siber olay raporlama mekanizmasının oluşturulması			
		5.2.2	İşletmenin yaşadığı siber güvenlik ihlal olaylarını analiz etmesi, kayıt altına alması ve bir daha benzer bir siber güvenlik ihlal olayının yaşanmaması için gerekli önlemleri alması			
		5.2.3	İşletmenin yaşadığı siber güvenlik ihlal olaylarının nedenlerini alınan dersleri ve bir daha yaşanmaması için alınacak önlemleri kayıt altına alması ve ilgili otoriteler ile paylaşması			
	3	5.3.1	Siber güvenlik ihlal olay yönetim süreçlerinde olay inceleme süreçlerinin etkin bir şekilde yürütülmesi			
	4	5.4.1	Siber güvenlik ihlal olay yönetim süreçlerinde tehdit istihbarat hizmetlerinin kullanılarak olası saldırgan gruplarının belirlenmesi, olağan saldırgan gruplarının davranış şekillerinin incelenerek olay yönetim sürecinin yürütülmesi			



SİVİL HAVACILIK
GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(1. Grup Havacılık İşletmeleri)

		5.4.2	Haberli veya habersiz olmak üzere periyodik olarak işletmenin siber güvenlik ihlal olaylarına karşı yanıt verme yetkinliğini test edilmesi			
6. Bakım	1	6.1.1	Bakım amacıyla işletme dışına çıkarılacak sistemlerin içerisinde hiçbir data barındırmamasının sağlanması			
		6.1.2	Bakım süreçlerinde görev alacak personelin izlenmesi			
		6.1.3	BT ve OT süreçlerini etkileyecek varlıkların bakımlarının yetkili işletmeler tarafından görevlendirilen yetkili personel tarafından yapılması			
	2	6.2.1	BT süreçlerini etkileyecek varlıkların bakım sürelerinin dokümanle edilmesi, izlenmesi ve bu sürele uygun olarak bakım çalışmalarının gerçekleştirilmesi			
	3	6.3.1	Bakım verilerin kayıt altında tutulması ve gizliliğinin sağlanması			
	4	6.4.1	Bakım sürecinde yer alan sistemlerin operasyonel süreçlere dahil edilmeden önce güvenlik testlerinin yapılarak söz konusu sistemlerin gizlilik, bütünlük ve erişilebilirlik unsurlarının etkilenmediğinden emin olunması			
7. İnsan Kaynakları Güvenliği	1	7.1.1	İşletme kritik BT varlıklarına erişim sağlayacak personelin işe alım sürecinden önce güvenlik soruşturmalarının yapılması			
		7.1.2	İş sonlandırma süreçlerinde ilgili personelin yetki ve hesap iptaline yönelik mekanizmanın oluşturulması			
		7.1.3	Görev değişikliği süreçlerinde ilgili personelin eski görevine yönelik yetki ve hesap iptali mekanizmanın oluşturulması			
	2	7.2.1	İş sonlandırma süreçlerinde ilgili personelin yetki ve hesap iptaline yönelik oluşturulan mekanizmanın uygulanmasının denetlenmesi			
		7.2.2	Görev değişikliği süreçlerinde ilgili personelin eski görevine yönelik yetki ve hesap iptali mekanizmasının denetlenmesi			
	3	7.3.1	İşletme siber güvenlik politika ve prosedürleri ile belirlenmiş kural setlerine uyulmaması durumunda uygulanmak üzere bir disiplin sürecinin oluşturulması, dokümanle edilmesi ve uygulanması			
	1	8.1.1	Fiziksel güvenlik prosedürünün oluşturulması, periyodik olarak gözden geçirilmesi ve ihtiyaç duyulması halinde güncellenmesi			
		8.1.2	Kritik BT varlıklarını etkileyen fiziksel ortam ve unsurların envanterinin oluşturulması			
	2	8.2.1	Kritik BT varlıklarına fiziksel erişimin yetki kapsamında kısıtlanması			
		8.2.2	Kritik BT varlıklarına fiziksel erişimi izlenmesi ve yetkisiz erişimlerin tespit edilmesi			
8. Fiziksel Güvenlik						



SİVİL HAVACILIK
GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(1. Grup Havacılık İşletmeleri)

		8.2.3	Kritik BT varlıklarının bulunduğu alanlarda, yaka kartı takılmasının zorunlu olması ve kritik BT varlıklarına erişimde kişi yaka kartı eşleştirmesinin yapılması			
	3	8.3.1	Kritik BT varlıklarının bulunduğu alanlara erişim yetkisine sahip olmayan iç ve dış kaynaklı çalışanlara ve ziyaretçilere söz konusu kritik bu alanlara erişimlerinde eşlik edilmesi, bu kişilerin aktivitelerinin izlenmesi			
	4	8.4.1	İşletmenin ISO 27001 Ek.A.11 kapsamında senede en az 2 kere denetim faaliyeti gerçekleştirilmesi			
9. Yedekleme	1	9.1.1	İşletmenin süreç kritikliğinde göz önüne alarak bir yedekleme politika veya prosedürü oluşturması			
		9.1.2	İşletme yedekleme politika ve prosedürüne uygun şekilde düzenli olarak backup alınması.			
	2	9.2.1	Periyodik olarak yedekten geri dönme test çalışmalarının gerçekleştirilmesi			
	3	9.3.1	Alınan yedeklerin farklı bir sunucuda yer alması			
	4	9.4.1	Farklı bir risk bölgesinde işletme kritik dataların hepsini içerecek bir FKM yapısının kurulması			
		9.4.2	Bilgi işleme olanaklarının, erişilebilirlik gereksinimlerini karşılamak için yeterli fazlalık ile gerçekleştirilmesi			
10. Risk Yönetimi	1	10.1.1	Siber Güvenlik Risk Değerlendirme Metodolojisinin belirlenmesi, dokümanite edilmesi			
		10.1.2	Siber Güvenlik Etki Değerlendirme Metodolojisinin belirlenmesi, dokümanite edilmesi			
		10.1.3	Siber Güvenlik Risk Değerlendirme çalışmasının periyodik olarak gözden geçirilmesi ve güncellenmesi			
	2	10.2.1	Varlık envanteri kapsamında belirlenmiş varlıkları 27001 Ek.A maddeleri kapsamında her bir madde ayrı ayrı olacak şekilde değerlendirilmesi			
		10.2.2	İşletmenin üretici veya tedarikçi bağımlılığı kapsamında siber güvenlik risklerinin belirlenmesi ve dokümanite edilmesi			
		10.2.3	Siber Güvenlik risk değerlendirme çalışmasının işletme iç ve dış kaynaklar tarafından yapılan sızma testi, zafiyet taraması, kırmızı takım vb. çalışmaların sonuçlarına göre güncellenmesi ve iyileştirilmesi			
	3	10.3.1	Risk indirgeme çalışmalarının ilgili birimler ile koordine edilerek yürütülmesi, takip edilmesi ve dokümanite edilmesi			
		10.3.2	Risk kabulü ile ilgili sürecin aktif bir şekilde yürütülmesi ve dokümanite edilmesi			



SİVİL HAVACILIK
GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(1. Grup Havacılık İşletmeleri)

	4	10.3.3	Siber Güvenlik risk değerlendirme çalışmasının işletme iç ve dış kaynaklar tarafından yapılan denetim faaliyetlerinin sonuçlarına göre güncellenmesi ve iyileştirilmesi			
		10.4.1	Siber Güvenlik sigortası bulunması			
		10.4.2	Siber güvenlik risk değerlendirme çalışmasının tehdit istihbarat çalışmaları çıktıları sonucuna göre güncellenmesi ve iyileştirilmesi			
		10.4.3	Siber Güvenlik Risk Değerlendirme faaliyetlerinin yeterliliğinin ölçülmesi ve iyileştirilmesi			
11. Durumsal Farkındalık ve Sistem Test	1	11.1.1	Mevcut güvenlik mimarisinin güncelliğinin ve işletme ihtiyaçlarını karşılayıp karşılamadığının değerlendirmesinin yapılması			
		11.1.2	Mesai saatleri içerisinde siber tehdit veya siber güvenlik ihlal olayı tespit görevini icra edecek bir mekanizmanın kurulması			
		11.1.3	Mesai saatleri içerisinde siber olay müdahale görevini icra edecek bir mekanizma kurulması			
	2	11.2.1	Havacılık Sektörü İç Kontrol Metodolojisine uygun olarak en üst seviyeye erişmek için gerekli olan aksiyonların belirlenmesi			
		11.2.2	7x24 prensibine göre siber tehdit veya siber güvenlik ihlal olayı tespit görevini icra edecek bir mekanizmanın kurulması			
		11.2.3	Siber tehdit veya siber güvenlik ihlal olayı tespit yapılanmasının yeterliliğinin ölçülmesi ve iyileştirilmesi			
		11.2.4	Siber olay müdahale yapılanmasının yeterliliğinin ölçülmesi ve iyileştirilmesi			
		11.2.5	Periyodik zafiyet taraması yapılması			
	3	11.3.1	İşletmenin tabi olduğu yasal düzenlemelere uygun hale gelmek için gerekli aksiyonların belirlenmesi			
		11.3.2	TSE akredite firmalar tarafından en az senede bir geniş kapsamlı sızma testi faaliyetinin gerçekleştirilmesi			
		11.3.3	Siber güvenlik alanında icra edilen iç ve dış kaynaklı test, denetim, zafiyet taraması vb. çalışmalar sonucu tespit edilen bulguların ve risklerin giderilmesi amacıyla bir bulgu yönetim sürecinin tesis edilmesi ve uygulanması			
	4	11.4.1	7x24 prensibine göre siber tehdit veya siber güvenlik ihlal olayı müdahale görevini icra edecek bir mekanizmanın kurulması			
		11.4.2	Tehdit avcılığı mekanizmasının oluşturulması ve kullanılması			



SİVİL HAVACILIK
GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(1. Grup Havacılık İşletmeleri)

		11.4.3	Kırmızı takım çalışmalarının yapılması			
		11.4.4	Bug bounty çalışmalarının gerçekleştirilmesi			
	1	12.1.1	Genel Müdürlük ve taşra teşkilatı bazında ağ segmentasyonun yapılması			
		12.1.2	İşletme iç ağındaki internete çıkış noktasına yerleştirilmiş bir güvenlik duvarı cihazının bulunması			
		12.1.3	Port, protokol ve servis kısıtlamasının minimum yetki prensibine uygun olarak uygulanması			
		12.1.4	Network cihazlarının fiziksel güvenliğinin sağlanarak yetkisiz erişiminin engellenmesi			
		12.1.5	Mac filtreleme metodu ile kayıtdışı cihazların işletme iç ağına erişiminin engellenmesi			
		12.1.6	İnaktif oturumların belirli bir süre sonrasında otomatik kilitlenmesi			
		12.1.7	İşletme BT sistemleri ile ilgili konfigürasyon envanterlerinin ve temel konfigürasyon setlerinin oluşturulması ve doküman edilmesi			
		12.1.8	Mobil cihazlar, sunucular ve son kullanıcılara ait BT varlıklarında antivirüs yazılımı kullanılması			
		12.1.9	DDoS saldırılarına karşı önlem alınması ve alınan bu önlemlerin yeterliliğini periyodik olarak test edilmesi			
		12.2.1	Birim bazında ağ segmentasyonunun yapılması			
		12.2.2	Her bir ağ segmentasyonu için ayrı ayrı güvenlik duvarı yapılanmasının oluşturulması			
		12.2.3	Dıştan içe veya içten içe iletilen medyanın taranması için sandbox uygulamalarının kullanılması			
		12.2.4	Firewall kurallarının periyodik olarak gözden geçirilmesi ve iyileştirilmesi			
		12.2.5	Ağ güvenlik cihazlarının ve sunucu güvenlik konfigürasyon setlerinin USOM,SHGM gibi üst kuruluşlardan gelen talimatlara göre sıkılaştırılması			
		12.2.6	İşletme siber güvenlik kabiliyetinin artırılması amacı ile siber istihbarat hizmetlerinin kullanılması			



SİVİL HAVACILIK
GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(1. Grup Havacılık İşletmeleri)

12. Sistem ve Haberleşme Güvenliği	2	12.2.7	Network cihazlarının yönetiminde şifrelenmiş oturumlar kullanılması			
		12.2.8	802.1x metodu ile kayıtdışı cihazların veya kullanıcıların networke erişiminin engellenmesi			
		12.2.9	DNS filtreleme çalışmasının gerçekleştirilmesi			
		12.2.10	URL filtreleme çalışmasının gerçekleştirilmesi			
		12.2.11	Son kullanıcılar tarafından ziyaret edilen web sitelerinin zararlı bir bileşen(exploit kit vb.) içermediğinin doğrulanması			
		12.2.12	İhtiyaç duyulduğu kadar yetki prensibine bağlı kalarak güvenlik kontrollerinin uygulanması			
		12.2.13	Eposta hizmetlerinin güvenliğini sağlamak üzere spam koruma ve email gateway kullanılması			
		12.2.14	Network trafiğinde şüpheli hareket analizinin yapılması			
		12.2.15	Kullanıcı bazında şüpheli hareket analizinin yapılması			
		12.2.16	İşletme bünyesinde NAC çözümlerinin kullanılması			
		12.2.17	İşletme bünyesinde load balancer çözümlerinin kullanılması			
		12.2.18	İşletme bünyesinde WAF çözümlerinin kullanılması			
		12.2.19	İşletme bünyesinde IDS ve IPS çözümlerinin kullanılması			
		12.2.20	İşletme iç paydaşlarının kullanımına yönelik olan sistemlerin uzaktan erişiminin ipsec vpn üzerinden olması			
		12.3.1	Görev ve kritiklik bazında ağ segmentasyonunun yapılması			
		12.3.2	Firewall trafiğinin izlenmesi, analiz edilmesi ve yapılan analiz sonucunda riskli görülen trafiğin engellenmesi			
		12.3.3	DMZ yapılanmasının oluşturulması ve efektif bir şekilde kullanımının sağlanması			



SİVİL HAVACILIK
GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(1. Grup Havacılık İşletmeleri)

	3	12.3.4	Kritik bilgi akışının şifreli bir şekilde yapılması			
		12.3.5	Kritik operasyonlarda erişim yönetim süreçlerinde kullanılmak üzere kriptografik şifreler oluşturma ve bu şifrelerin kullanımının yönetilmesi			
		12.3.6	VOİP teknolojileri kullanılıyorsa, söz konusu bu teknolojiye yönelik sıkılaştırmaların yapılması			
		12.3.7	Ağ güvenlik cihazlarının ve sunucu güvenlik konfigürasyon setlerinin siber tehdit istihbarat hizmeti verilerine göre sıkılaştırılması			
		12.3.8	Tüm son kullanıcı gruplarının yükleme izni olan uygulamaların belirlenmesi amacıyla whitelist ve blacklist uygulanması ve söz konusu sistemin 7x24 izlenmesi			
		12.3.9	Sanallaştırma sistemlerinde kullanılacak olan imajların sıkılaştırılmasının yapılması ve sürecin denetlenmesi			
		12.3.10	İşletme bünyesinde DLP çözümlerinin kullanılması			
		12.3.11	Son kullanıcılara yönelik cihazlarda EDR çözümlerinin kullanılması			
	4	12.4.1	Risk teşkil eden BT varlıklarına yönelik disk şifreleme çözümlerinin kullanılması			
		12.4.2	Mevcut DNS filtreleme çalışmalarının KamuDNS projesi ile entegrasyonunun sağlanması			
		12.4.3	İşletme mobil cihazlarının tek bir merkezden güvenlik operasyonlarının yürütülmesi amacıyla MDM kullanılması			
		12.4.4	Network ve sunucu mimarisinin görevler ayrılığı ilkesi gözetilerek değerlendirilmesi, dokümanite edilmesi ve iyileştirilmesi			
		12.4.5	Güvenlik sıkılaştırmalarının yeterliliğinin görevler ayrılığı ilkesi gözetilerek değerlendirilmesi, dokümanite edilmesi ve iyileştirilmesi			
		12.4.6	Network güvenlik cihazlarının konumlandırılmasının ve konfigürasyonlarının görevler ayrılığı ilkesi gözetilerek değerlendirilmesi, dokümanite edilmesi ve iyileştirilmesi			
		12.4.7	İşletme bilgi teknolojileri altyapısını korumak için honeypot çözümlerinin kullanılması			
		12.4.8	İşletme bünyesinde kullanılan EKS, SCADA ve IOT teknolojileri için özelleştirilmiş firewall çözümlerinin kullanılması			
		12.4.9	Veri aktarımı için diyet ürünlerinin kullanılması			



SİVİL HAVACILIK
GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(1. Grup Havacılık İşletmeleri)

		12.4.10	İşletme bünyesinde kullanılan EKS,SCADA ve IOT teknolojileri için veri aktarımı şifreleme çözümlerinin kullanılması			
		12.4.11	İşletme bünyesinde bulunan sunucularda EDR çözümlerinin kullanılması			
13. Siber Güvenlik Yapılanması	1	13.1.1	SOME'nin kurulmuş olması			
		13.1.2	SOME birimi personelinin kapsam ve görev tanımlarının belirlenmiş ve dokümente edilmiş olması			
	2	13.2.1	SOME'nin BT birim ve süreçlerinden görevlerin ayrılığı ilkesi kapsamında ayrılması			
		13.2.2	SOME biriminin en az Genel Müdür Yrd. seviyesine bağlanması			
		13.2.3	SGSYY'nin en az lisans derecesine sahip olması ve siber güvenlik konusunda uzmanlaşmış olması			
		13.2.4	Some personeli işe alım sürecinden önce güvenlik soruşturmasının yapılması (adli sicil kaydı, şahıs güvenlik belgesi v.b.)			
		13.2.5	Some'de görev alan personelin ön lisans veya lisans programlarından mezun olması ve en az iki yıl bilgi işlem tecrübesine sahip olması veya bilgi güvenliği/siber güvenlik konularında bilgi ve tecrübeye sahip olması			
	3	13.3.1	SGSYY'nin SHT-Siber EK-5'de yer alan sertifikalara sahip olması			
		13.3.2	İstihdam devam ederken rastgele güvenlik soruşturması araştırmalarının yapılması(adli sicil kaydı, şahıs güvenlik belgesi v.b.)			
		13.3.3	Görevlendirilecek personelin some kapsamındaki görev ve sorumluluklarını yerine getirebilmesi için sorumlu olduğu konuda uzman olması			
	4	13.4.1	Siber Güvenlik Stratejik Planı'nın oluşturulması, gözden geçirilmesi ve güncellenmesi			
		13.4.2	SOME personeli memnuniyetinin ölçülerek birim bazında personel değişiklik oranının düşürülmesi için faaliyetlerde bulunulması			
	1	14.1.1	BT varlıklarının iş sürekliliğine yönelik bir politika veya prosedürün oluşturulması			
	2	14.2.1	BT varlıklarına yönelik iş sürekliliği etki analizinin yapılması			
		14.3.1	İş sürekliliği risk ve etki analizinin periyodik olarak gözden geçirilmesi ve ihtiyaç duyulması halinde güncellenmesi			



SİVİL HAVACILIK
GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(1. Grup Havacılık İşletmeleri)

14. İş Sürekliliği	3	14.3.2	İş sürekliliği planlarının oluşturulması, gözden geçirilmesi ve güncel tutulması			
		14.3.3	İş sürekliliği çalışmalarının, görevler ayrılığı ilkesinde gözetilerek, objektif bir şekilde değerlendirilmesi			
	4	14.4.1	BT süreçlerini etkileyen tüm varlıklara yönelik iş sürekliliği yedekliliğinin sağlanması			
		14.4.2	İş sürekliliği planlarına yönelik tüm hususların tatbikatının senede en az bir kere yapılması			
		14.4.3	İş sürekliliği planı iyileştirme çalışmalarının gerçekleştirilmesi			
15. Tedarikçi Yönetimi	1	15.1.1	Tedarikçi yönetimi politikası veya prosedürünün oluşturulması			
		15.1.2	Dış kaynaklı olarak alınan hizmet ve ürünlerin işletmeye olan etkisine göre kritik tedarikçilerinin belirlenmesi			
	2	15.2.1	Tedarik ihtiyacı olan süreçle ilgili tedarikçi bilgi güvenliği gereksinim seviyelerinin belirlenmesi			
		15.2.2	Tedarikçi çıkış stratejilerinin oluşturulması			
	3	15.3.1	Tedarikçi yönetim sürecinin değerlendirilmesi ve iyileştirilmesi			
		15.3.2	Kritik tedarikçilerin sözleşmelerinde bilgi güvenliği unsurlarının yer alması			
		15.3.3	Kritik tedarikçilerin denetim sonuçlarına göre ihtiyaç duyulması halinde çıkış stratejilerinin uygulanması			
	4	15.4.1	Kritik tedarikçilerin bilgi güvenliği kapsamında denetlenmesi			
16. Yasal Uyum	1	16.1.1	İşletmenin ISO 27001 Sertifika belgesine sahip olması			
	2	16.2.1	ISO 27001 Ek.A.18.2.1 kapsamında yasal uyum süreci envanterinin oluşturulması			
	3	16.3.1	İşletmenin yasal sorumluluğunun olduğu alanlarda yeni çıkan regülasyonlar ile ilgili takip mekanizması oluşturması			
	4	16.4.1	Yasal uyum süreci ile alakalı boşluk analizinin yapılması			



SİVİL HAVACILIK
GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(1. Grup Havacılık İşletmeleri)

17. İşletim Güvenliği	1	17.1.1	Yama yönetiminin uygulanması				
		17.1.2	Lisanssız yazılımların kullanılmaması				
	2	17.2.1	Değişiklik yönetiminin uygulanması				
		17.2.2	Kapasite yönetiminin uygulanması				
	3	17.3.1	Kullanıcının yükleme izni olan uygulamalar için whitelist ve blacklist uygulanması ve sürecin izlenmesi				
	1	18.1.1	Sistem temini geliştirme ve bakımı süreçlerini ele alan bir politika veya prosedürün oluşturulması				
		18.1.2	Geliştirilecek veya temin edilecek sistemin güvenliğini sağlamak amacıyla analizin yapılması ve siber güvenlik gereksinimlerinin belirlenmesi				
	2	18.2.1	Geliştirilecek veya temin edilecek sistemin güvenliğini sağlamak amacıyla siber güvenlik test süreçlerinin gerçekleştirilmesi				
		18.2.2	İç veya dış kaynaklı sistem temini, geliştirme veya güncelleme süreçlerinde değişiklik yönetimi süreçlerinin etkin bir şekilde yürütülmesi				
		18.2.3	Test ve geliştirme ortamlarının ayrıştırılması				
3	18.3.1	Test verisinin kişisel veri veya operasyonel kritik veri içermemesi					
18. Sistem Temini, Geliştirme ve Bakım	4	18.4.1	Temin edilecek, geliştirilecek veya güncellenecek sistemlerin güvenliğini sağlamak amacıyla SHT-Siber Ek-10'da yer alan Havacılık Sektörü Güvenli Yazılım Yazılım Geliştirme Rehberi içerisinde bulunan kontrol listesinin kullanılması ve bu sürecin SOME tarafından denetlenmesi				
	19. Yerli Milli Ürün Kullanılması	1	19.1.1	Yerli ve milli ürünlerin işletme BT ürün envanterindeki oranının %5'den az olması			
		2	19.2.1	Yerli ve milli ürünlerin işletme BT ürün envanterindeki oranının %5'den fazla ve %10'dan az olması			
		3	19.3.1	Yerli ve milli ürünlerin işletme BT ürün envanterindeki oranının %10'den fazla ve %20'dan az olması			
		4	19.4.1	Yerli ve milli ürünlerin işletme ürün envanterindeki oranının %20'den fazla olması			
	19. Yerli Milli Ürün Kullanılması	1	20.1.1	Siber güvenlik yapılanması dahilinde sağlıklı bir iletişim mekanizmasının oluşturulması ve yürütülmesi			



SİVİL HAVACILIK
GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(1. Grup Havacılık İşletmeleri)

20. İletişim	2	20.2.1	Tüm işletme kapsamında sağlıklı bir iletişim mekanizmasının oluşturulması ve yürütülmesi			
	3	20.3.1	Kritik BT varlıkları tedarikçi firmaları ile sağlıklı bir iletişim mekanizmasının oluşturulması ve yürütülmesi			
	4	20.4.1	İşletme siber güvenlik faaliyetlerini etkileyen tüm iç ve dış paydaşlar ile sağlıklı bir iletişim mekanizmasının oluşturulması ve yürütülmesi			

U: Uygun

UD:Uygun Değil

NA:Uygulanamaz



T.C. ULAřTIRMA VE ALTYAPI BAKANLIđI
SİVİL HAVACILIK GENEL MÜDÜRLÜđÜ

2. GRUP HAVACILIK SEKTÖRÜ İřLETMELERİ

HAVACILIK GÜVENLİđİ DAİRE BAřKANLIđI-SİBER GÜVENLİK KOORDİNATÖRLÜđÜ



SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(2. Grup Havacılık İşletmeleri)

Sıra	Kontrol Maddesi	Seviye 1	Seviye 2	Seviye 3	Seviye 4	Toplam
1	Erişim Yönetimi	2	4	8	2	16
2	Varlık Yönetimi	1	1	2	3	7
3	İz Kayıt	3	6	2	3	14
4	Farkındalık	2	3	3	2	10
5	Olay Yönetimi	1	2	2	1	6
6	Bakım	2	1	1	1	5
7	İnsan Kaynakları Güvenliği	2	3	1	0	6
8	Fiziksel Güvenlik	1	2	1	2	6
9	Yedekleme	1	1	2	1	5
10	Risk Yönetimi	2	2	4	2	10
11	Durumsal Farkındalık ve Sistem Test	3	2	5	1	11
12	Sistem ve Haberleşme Güvenliği	6	13	11	7	37
13	Siber Güvenlik Yapılanması	2	3	1	2	8
14	İş Sürekliliği	1	1	0	3	5
15	Tedarikçi Yönetimi	1	1	1	3	6
16	Yasal Uyum	1	0	1	1	3
17	İşletim Güvenliği	1	1	2	1	5
18	Sistem Temini, Geliştirme ve Bakım	1	1	4	1	7
19	Yerli Milli Ürün Kullanması	0	0	1	1	2
20	İletişim	1	1	1	1	4
Seviye Toplam		34	48	53	38	173



SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi (2. Grup Havacılık İşletmeleri)

No	1. Erişim Yönetimi			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	Erişim Yönetimi Kontrol Prosedürünün Oluşturulması	Son kullanıcılara verilecek yetkilerin en az yetki prensibine göre verilmesi	Çalışan grupları dışında kalan kritik varlıklara usb, harici harddisk vb. cihazlar ile erişimin yönetilmesi	Kritik varlıklara usb, harici harddisk vb. cihazlar ile erişimin kısıtlanması
2	Varlıkların kritiklik seviyesine uygun bir parola yönetim süreci tesis edilmesi, uygulanması ve denetlenmesi	Ayrıcalıklı erişim hakkının belirlenmesi ve yönetilmesi	Son kullanıcılara ait bt varlıklarına usb, harici harddisk vb. cihazlar ile erişimin yönetilmesi	Erişim yetki tanımlaması yapan personel ve erişim yetki gözden geçirmesini yapan personel/personellerin farklı olması
3		Son kullanıcı erişim hakları matrisinin oluşturulması	Ayrıcalıklı erişim hakkına sahip kullanıcılarda en az yetki prensibinin uygulanması	
4		Ayrıcalıklı erişim hakları matrisinin oluşturulması	Son kullanıcı erişim haklarının ilgili birim yöneticileri ile gözden gözden geçirilmesi	
5			Ayrıcalıklı kullanıcı erişim haklarının ilgili birim yöneticileri ile gözden geçirilmesi	
6			Kayıtlı olmayan cihazların networke erişiminin kısıtlanması	
7			İşletme BT varlıklarına erişim sağlaması gereken tedarikçiler için erişim yöntemi ve kontrol mekanizmasının oluşturulması ve yürütülmesi	
8			Tedarikçi firmalara verilen erişim haklarının ilgili süreç bazında ihtiyaç duyulan minimum süre ve minimum yetki bazında verilmesi	



SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(2. Grup Havacılık İşletmeleri)

No	2. Varlık Yönetimi			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	Varlık yönetimi prosedürünün hazırlanması	İşletme BT varlıklarının ve varlık gruplarının gizlilik, bütünlük ve erişilebilirlik kapsamında değerlerinin alan uzmanları ile birlikte belirlenmesi	BT varlıklarının kabul edilebilir kullanımlarının belirlenmesi, dokümente edilmesi ve ilgili paydaşların bilgisine sunması	Varlık gruplarının puan ve etki analizinin ihtiyaçlar ve güncel siber tehditler kapsamında güncellenmesi
2			Varlık gruplarının puan ve etki analizinin periyodik olarak gözden geçirilmesi	Kritik BT süreçlerine yönelik varlıkların imha süreçlerinin belirlenmesi
3				Kritik BT süreçlerine yönelik varlıkların imha süreçlerinin denetlenmesi



SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi (2. Grup Havacılık İşletmeleri)

No	3. İz Kayıt			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	İz kayıt alınması gereken varlıkların belirlenmesi ve söz konusu bu varlıklardan toplanacak iz kayıt niteliğinin tespit edilip dokümanite edilmesi	Belirlenen varlıklardan ihtiyaç duyulan iz kayıtlarının alınması	Herhangi bir sebepten dolayı iz kayıt sağlayamayan sistemlerin tespit edilmesi için bir tespit mekanizmasının oluşturulması	Toplanan iz kayıtlarının söz konusu uygulama veya sistemlerden farklı bir serverda tutulması
2	NTP server kullanılması	İz kayıt toplama sürecinin herhangi bir sebepten ötürü sekteye uğraması durumuna karşı bir alarm mekanizması oluşturulması	İz kayıtları alarmlarına yönelik yapılan çalışmalar hakkında periyodik olarak analiz yapılması ve söz konusu bu analiz raporunun SOME birimi yöneticisine sunulması	İşletme veya sektör paydaşlarının karşılaştığı siber güvenlik olaylarına yönelik korelasyonların oluşturulması
3	İşletme tarafından alınan iz kayıtları kapsamında toplanan kayıtların nitelik bakımından inkar edilemez olmasının sağlanması	İz kayıtlarına erişimin yönetilmesi ve kayıt altına alınması		Mevcut korelasyon setlerinin periyodik olarak gözden geçirilmesi ve iyileştirilmesi
4		Olası bir siber güvenlik olayına karşı iz kayıtlarının korele edilerek, istenmeyen durumların tespiti için bir süreç oluşturulması		
5		İz kayıtlarına yönelik periyodik analiz raporlarının oluşturulması ve gözden geçirilmesi		
6		Korelasyonlar sonucunda oluşan alarmların incelenerek ihtiyaç duyulması halinde diğer güvenlik süreçlerinin tetiklenmesi		



SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi (2. Grup Havacılık İşletmeleri)

No	4. Farkındalık			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	İşletme personellerine etkin bir siber güvenlik farkındalığı eğitiminin sağlanması	İşletme tesislerinde görev alan tedarikçi personele için etkin bir siber güvenlik farkındalığı eğitiminin sağlanması	Siber güvenlik farkındalığı eğitiminin ve sıklığının eğitimi alan personelin icra ettiği görevin kritikliğine uygun olarak verilmesi	İşletme çalışanlarının siber güvenlik farkındalığı seviyesinin ölçülmesi için işletme çalışanlarının tümünü kapsayacak şekilde en az senede bir sosyal mühendislik testlerinin yapılması
2	Son kullanıcıların siber olay yönetimindeki rollerinin açık bir şekilde dokümente edilmesi ve son kullanıcıların bu süreçteki rollerinin içselleştirilmesi	İşletme tarafından hazırlanan siber güvenlik eğitim materyallerinin periyodik olarak gözden geçirilmesi ve ihtiyaçlar ve güncel siber tehditler kapsamında güncellenmesi	İşletme personeline en az senede bir siber güvenlik farkındalığı tazeleme eğitimi verilmesi	Yapılan farkındalık sınav ve testlerinde hedeflenen başarı oranının altında kalan personelin farkındalık seviyesini arttırmak amacıyla faaliyetlerde bulunulması
3		İşletme personeline verilen siber güvenlik farkındalık eğitimlerinin sonrasında eğitimin yarattığı farkındalık seviyesinin ölçülmesi amacı ile sınavların yapılması	İhtiyaç duyulması halinde işletme paydaşlarının söz konusu siber risk ve tehditler kapsamında bilgilendirilmesi	



SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(2. Grup Havacılık İşletmeleri)

No	5. Olay Yönetimi			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	Siber güvenlik ihlal olay yönetim ve müdahale süreçlerini kapsayacak politika veya prosedürlerin oluşturulması	Son kullanıcılar ve ilgili paydaşların kullanımına sunulmuş bir siber olay raporlama mekanizmasının oluşturulması	Dokümanite edilmiş bir siber güvenlik ihlal olay müdahale sürecinin oluşturulması	Siber güvenlik ihlal olay yönetim süreçlerinde adli bilişim süreçlerinin etkin bir şekilde yürütülmesi
2		İşletmenin yaşadığı siber güvenlik ihlal olaylarının nedenlerini alınan dersleri ve bir daha yaşanmaması için alınacak önlemleri kayıt altına alması ve ilgili otoriteler ile paylaşması	İşletmenin yaşadığı siber güvenlik ihlal olaylarını analiz etmesi, kayıt altına alması ve bir daha benzer bir siber güvenlik ihlal olayının yaşanmaması için gerekli önlemleri alması	



SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(2. Grup Havacılık İşletmeleri)

No	6. Bakım			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	Bakım amacıyla işletme dışına çıkarılacak sistemlerin içerisinde hiçbir data barındırmamasının sağlanması	Bakım süreçlerinde görev alacak personelin izlenmesi	BT süreçlerini etkileyecek varlıkların bakım sürelerinin dokümente edilmesi, izlenmesi ve bu sürelerle uygun olarak bakım çalışmalarının gerçekleştirilmesi	Bakım verilerin kayıt altında tutulması ve gizliliğinin sağlanması
2	BT ve OT süreçlerini etkileyecek varlıkların bakımlarının yetkili işletmeler tarafından görevlendirilen yetkili personel tarafından yapılması			



SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(2. Grup Havacılık İşletmeleri)

No	7. İnsan Kaynakları Güvenliği			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	İşletme kritik BT varlıklarına erişim sağlayacak personelin işe alım sürecinden önce güvenlik soruşturmalarının yapılması	İş sonlandırma süreçlerinde ilgili personelin yetki ve hesap iptaline yönelik oluşturulan mekanizmanın uygulanmasının denetlenmesi	İşletme siber güvenlik politika ve prosedürleri ile belirlenmiş kural setlerine uyulmaması durumunda uygulanmak üzere bir disiplin sürecinin oluşturulması, dokümente edilmesi ve uygulanması	
2	İş sonlandırma süreçlerinde ilgili personelin yetki ve hesap iptaline yönelik mekanizmanın oluşturulması	Görev değişikliği süreçlerinde ilgili personelin eski görevine yönelik yetki ve hesap iptali mekanizmanın oluşturulması		
3		Görev değişikliği süreçlerinde ilgili personelin eski görevine yönelik yetki ve hesap iptali mekanizmasının denetlenmesi		



SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(2. Grup Havacılık İşletmeleri)

No	8. Fiziksel Güvenlik			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	Fiziksel güvenlik prosedürünün oluşturulması, periyodik olarak gözden geçirilmesi ve ihtiyaç duyulması halinde güncellenmesi	Kritik BT varlıklarını etkileyen fiziksel ortam ve unsurların envanterinin oluşturulması	Kritik BT varlıklarına fiziksel erişimi izlenmesi ve yetkisiz erişimlerin tespit edilmesi	Kritik BT varlıklarının bulunduğu alanlara erişim yetkisine sahip olmayan iç ve dış kaynaklı çalışanlara ve ziyaretçilere söz konusu kritik bu alanlara erişimlerinde eşlik edilmesi, bu kişilerin aktivitelerinin izlenmesi
2		Kritik BT varlıklarına fiziksel erişimin yetki kapsamında kısıtlanması		Kritik BT varlıklarının bulunduğu alanlarda, yaka kartı takılmasının zorunlu olması ve kritik BT varlıklarına erişimde kişi yaka kartı eşleştirmesinin yapılması



SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(2. Grup Havacılık İşletmeleri)

No	9. Yedekleme			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	İşletmenin süreç kritikliğinde göz önüne alarak bir yedekleme politika veya prosedürü oluşturması	İşletme yedekleme politika ve prosedürüne uygun şekilde düzenli olarak backup alınması	Periyodik olarak yedekten geri dönme test çalışmalarının gerçekleştirilmesi	Farklı bir risk bölgesinde işletme kritik dataların hepsini içerecek bir FKM yapısının kurulması
2			Backupların farklı bir sunucuda yer alması	



SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi (2. Grup Havacılık İşletmeleri)

No	10. Risk Yönetimi			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	Siber Güvenlik Risk Değerlendirme Metodolojisinin belirlenmesi, dokümanite edilmesi	Siber güvenlik risk değerlendirme çalışmasının periyodik olarak gözden geçirilmesi ve güncellenmesi	Varlık envanteri kapsamında belirlenmiş varlıkları ISO 27001 Ek.A maddeleri kapsamında her bir madde ayrı ayrı olacak şekilde değerlendirilmesi	Risk indirgeme çalışmalarının ilgili birimler ile koordine edilerek yürütülmesi, takip edilmesi ve dokümanite edilmesi
2	Siber Güvenlik Etki Değerlendirme Metodolojisinin belirlenmesi, dokümanite edilmesi	Siber güvenlik risk değerlendirme çalışmasının işletme iç ve dış kaynaklar tarafından yapılan sızma testi, zafiyet taraması, kırmızı takım vb. çalışmaların sonuçlarına göre güncellenmesi ve iyileştirilmesi	İşletmenin üretici veya tedarikçi bağımlılığı kapsamında siber güvenlik risklerinin belirlenmesi ve dokümanite etmesi	Siber güvenlik risk değerlendirme faaliyetlerinin yeterliliğinin ölçülmesi ve iyileştirilmesi
3			Risk kabulü ile ilgili sürecin aktif bir şekilde yürütülmesi ve dokümanite edilmesi	
4			Siber güvenlik risk değerlendirme çalışmasının işletme iç ve dış kaynaklar tarafından yapılan denetim faaliyetlerinin sonuçlarına göre güncellenmesi ve iyileştirilmesi	



SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi (2. Grup Havacılık İşletmeleri)

No	11. Durumsal Farkındalık ve Sistem Test			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	Mevcut güvenlik mimarisinin güncelliğinin ve işletme ihtiyaçlarını karşılayıp karşılamadığının değerlendirilmesinin yapılması	Havacılık Sektörü İç Kontrol Metodolojisine uygun olarak en üst seviyeye erişmek için gerekli olan aksiyonların belirlenmesi	İşletmenin tabi olduğu yasal düzenlemelere uygun hale gelmek için gerekli aksiyonların belirlenmesi	7x24 prensibine göre siber tehdit veya siber güvenlik ihlal olayı müdahale görevini icra edecek bir mekanizmanın kurulması
2	Mesai saatleri içerisinde siber tehdit veya siber güvenlik ihlal olayı tespit görevini icra edecek bir mekanizmanın kurulması	Periyodik zafiyet taraması yapılması	7x24 prensibine göre siber tehdit veya siber güvenlik ihlal olayı tespit görevini icra edecek bir mekanizmanın kurulması	
3	Mesai saatleri içerisinde siber olay müdahale görevini icra edecek bir mekanizma kurulması		Siber tehdit veya siber güvenlik ihlal olayı tespit yapılanmasının yeterliliğinin ölçülmesi ve iyileştirilmesi	
4			Siber olay müdahale yapılanmasının yeterliliğinin ölçülmesi ve iyileştirilmesi	
5			TSE akredite firmalar tarafından en az senede bir geniş kapsamlı sızma testi faaliyetinin gerçekleştirilmesi	



SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi (2. Grup Havacılık İşletmeleri)

No	12. Sistem ve Haberleşme Güvenliği			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	Genel Müdürlük ve taşra teşkilatı bazında ağ segmentasyonunun yapılması	Birim bazında ağ segmentasyonunun yapılması	Her bir ağ segmentasyonu için ayrı ayrı güvenlik duvarı yapılanmasının oluşturulması	Görev ve kritiklik bazında ağ segmentasyonunun yapılması
2	İşletme iç ağında internete çıkış noktasına yerleştirilmiş bir güvenlik duvarı cihazının bulunması	Port, protokol ve servis kısıtlamasının minimum yetki prensibine uygun olarak uygulanması	Dıştan içe veya içten içe iletilen medyanın taranması için sandbox uygulamalarının kullanılması	DMZ yapılanmasının oluşturulması ve efektif bir şekilde kullanımının sağlanması
3	Network cihazlarının fiziksel güvenliğinin sağlanarak yetkisiz erişiminin engellenmesi	Firewall kurallarının periyodik olarak gözden geçirilmesi ve iyileştirilmesi	Firewall trafiğinin izlenmesi, analiz edilmesi ve yapılan analiz sonucunda riskli görülen trafiğin engellenmesi	İşletme siber güvenlik kabiliyetinin artırılması amacı ile siber istihbarat hizmetlerinin kullanılması
4	İnaktif oturumların belirli bir süre sonrasında otomatik kilitlenmesi	Ağ güvenlik cihazlarının ve sunucu güvenlik konfigürasyon setlerinin USOM,SHGM gibi üst kuruluşlardan gelen talimatlara göre sıkılaştırılması	Kritik bilgi akışının şifreli bir şekilde yapılması	Tüm son kullanıcı gruplarının yükleme izni olan uygulamaların belirlenmesi amacıyla whitelist ve blacklist uygulanması ve söz konusu sistemin 7x24 izlenmesi
5	İşletme BT sistemleri ile ilgili konfigürasyon envanterlerinin ve temel konfigürasyon setlerinin oluşturulması ve dokümante edilmesi	Network cihazlarının yönetiminde şifrelenmiş oturumlar kullanılması	Kritik operasyonlarda erişim yönetim süreçlerinde kullanılmak üzere kriptografik şifreler oluşturulması ve bu şifrelerin kullanımının yönetilmesi	İşletme bünyesinde load balancer çözümlerinin kullanılması
6	Mobil cihazlar, sunucular ve son kullanıcılara ait BT varlıklarında antivirüs yazılımı kullanılması	Mac filtreleme metodu ile kayıtdışı cihazların işletme iç ağına erişiminin engellenmesi	802.1x metodu ile kayıtdışı cihazların veya kullanıcıların networke erişiminin engellenmesi	İşletme bünyesinde WAF çözümlerinin kullanılması
7		DNS filtreleme çalışmasının gerçekleştirilmesi	VOIP teknolojileri kullanılıyorsa, söz konusu bu teknolojiye yönelik sıkılaştırmaların yapılması	Son kullanıcılara yönelik cihazlarda EDR çözümlerinin kullanılması
8		URL filtreleme çalışmasının gerçekleştirilmesi	Son kullanıcılar tarafından ziyaret edilen web sitelerinin zararlı bir bileşen(exploit kit vb.) içermediğinin doğrulanması	
9		İhtiyaç duyulduğu kadar yetki prensibine bağlı kalarak güvenlik kontrollerinin uygulanması	Kullanıcı bazında şüpheli hareket analizinin yapılması	
10		Eposta hizmetlerinin güvenliğini sağlamak üzere spam koruma ve email gateway kullanılması	İşletme bünyesinde IDS ve IPS çözümlerinin kullanılması	
11		DDoS saldırılarına karşı önlem alınması ve alınan bu önlemlerin yeterliliğini periyodik olarak test edilmesi	İşletme iç paydaşlarının kullanımına yönelik olan sistemlerin uzaktan erişiminin ipsec vpn üzerinden olması	
12		Network trafiğinde şüpheli hareket analizinin yapılması		
13		İşletme bünyesinde NAC çözümlerinin kullanılması		



SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(2. Grup Havacılık İşletmeleri)

No	13. Siber Güvenlik Yapılanması			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	SOME'nin kurulmuş olması	SOME Yöneticisi'nin en az lisans derecesine sahip olması ve siber güvenlik konusunda uzmanlaşmış olması	SOME biriminin en az Genel Müdür Yrd. seviyesine bağlanması	SOME'nin BT birim ve süreçlerinden görevlerin ayrılığı ilkesi kapsamında ayrılması
2	SOME birimi personelinin kapsam ve görev tanımlarının belirlenmiş ve dokümante edilmiş olması	SOME personeli işe alım sürecinden önce güvenlik soruşturmasının yapılması (adli sicil kaydı, şahıs güvenlik belgesi v.b.)		Görevlendirilecek personelin some kapsamındaki görev ve sorumluluklarını yerine getirebilmesi için sorumlu olduğu konuda uzman olması
3		Some'de görev alan personelin ön lisans veya lisans programlarından mezun olması ve en az iki yıl bilgi işlem tecrübesine sahip olması veya bilgi güvenliği/siber güvenlik konularında bilgi ve tecrübeye sahip olması		



SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(2. Grup Havacılık İşletmeleri)

No	14. İş Sürekliliği			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	BT varlıklarının iş sürekliliğine yönelik bir politika veya prosedürün oluşturulması	BT varlıklarına yönelik iş sürekliliği etki analizinin yapılması		İş sürekliliği risk ve etki analizinin periyodik olarak gözden geçirilmesi ve ihtiyaç duyulması halinde güncellenmesi
2				İş sürekliliği planlarının oluşturulması, gözden geçirilmesi ve güncel tutulması
3				İş sürekliliği çalışmalarının, görevler ayrılığı ilkesinde gözetilerek, objektif bir şekilde değerlendirilmesi



SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(2. Grup Havacılık İşletmeleri)

No	15. Tedarikçi Yönetimi			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	Tedarikçi yönetimi politikası veya prosedürünün oluşturulması	Dış kaynaklı olarak alınan hizmet ve ürünlerin işletmeye olan etkisine göre kritik tedarikçilerinin belirlenmesi	Tedarik ihtiyacı olan süreçle ilgili tedarikçi bilgi güvenliği gereksinim seviyelerinin belirlenmesi	Tedarikçi yönetim sürecinin değerlendirilmesi ve iyileştirilmesi
2				Kritik tedarikçilerin sözleşmelerinde bilgi güvenliği unsurlarının yer alması
3				Kritik tedarikçilerin bilgi güvenliği kapsamında denetlenmesi



SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(2. Grup Havacılık İşletmeleri)

No	16. Yasal Uyum			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	İşletmenin ISO 27001 Sertifika belgesine sahip olması		ISO 27001 Ek.A.18.2.1 kapsamında yasal uyum süreci envanterinin oluşturulması	İşletmenin yasal sorumluluğunun olduğu alanlarda yeni çıkan regülasyonlar ile ilgili takip mekanizması oluşturması



SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(2. Grup Havacılık İşletmeleri)

No	17. İşletim Güvenliği			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	Lisanssız yazılımların kullanılmaması	Yama yönetiminin uygulanması	Değişiklik yönetiminin uygulanması	Kullanıcının yükleme izni olan uygulamalar için whitelist ve blacklist uygulanması ve sürecin izlenmesi
2			Kapasite yönetiminin uygulanması	



SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(2. Grup Havacılık İşletmeleri)

No	18. Sistem Temini, Geliştirme ve Bakım			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	Sistem temini geliştirme ve bakımı süreçlerini ele alan bir politika veya prosedürün oluşturulması	Geliştirilecek veya temin edilecek sistemin güvenliğini sağlamak amacıyla analizin yapılması ve siber güvenlik gereksinimlerinin belirlenmesi	Geliştirilecek veya temin edilecek sistemin güvenliğini sağlamak amacıyla siber güvenlik test süreçlerinin gerçekleştirilmesi	Temin edilecek, geliştirilecek veya güncellenecek sistemlerin güvenliğini sağlamak amacıyla SHT-Siber Ek-10'da yer alan Havacılık Sektörü Güvenli Yazılım Yazılım Geliştirme Rehberi içerisinde bulunan kontrol listesinin kullanılması ve bu sürecin SOME tarafından denetlenmesi
2			İç veya dış kaynaklı sistem temini, geliştirme veya güncelleme süreçlerinde değişiklik yönetimi süreçlerinin etkin bir şekilde yürütülmesi	
3			Test ve geliştirme ortamlarının ayrıştırılması	
4			Test verisinin kişisel veri veya operasyonel kritik veri içermemesi	



SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(2. Grup Havacılık İşletmeleri)

No	19. Yerli Milli Ürün Kullanılması			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1			Yerli ve milli ürünlerin işletme BT ürün envanterindeki oranının %5'den az olması	Yerli ve milli ürünlerin işletme BT ürün envanterindeki oranının %5'den fazla ve %10'dan az olması



SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(2. Grup Havacılık İşletmeleri)

No	20. İletişim			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	Siber güvenlik yapılanması dahilinde sağlıklı bir iletişim mekanizmasının oluşturulması ve yürütülmesi	Tüm işletme kapsamında sağlıklı bir iletişim mekanizmasının oluşturulması ve yürütülmesi	Kritik BT varlıkları tedarikçi firmaları ile sağlıklı bir iletişim mekanizmasının oluşturulması ve yürütülmesi	İşletme siber güvenlik faaliyetlerini etkileyen tüm iç ve dış paydaşlar ile sağlıklı bir iletişim mekanizmasının oluşturulması ve yürütülmesi



SİVİL HAVACILIK
GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(2. Grup Havacılık İşletmeleri)

Havacılık Sektörü İç Kontrol Metodolojisi						
2. Grup Havacılık Sektörü İşletmeleri Kontrol Listesi						
Kontrol Başlığı	Seviye	Kontrol No.	Kontrol Maddesi	U	UD	NA
1. Erişim Yönetimi	1	1.1.1	Erişim Yönetimi Kontrol Prosedürünün Oluşturulması			
		1.1.2	Varlıkların kritiklik seviyesine uygun bir parola yönetim süreci tesis edilmesi, uygulanması ve denetlenmesi			
	2	1.2.1	Son kullanıcılara verilecek yetkilerin en az yetki prensibine göre verilmesi			
		1.2.2	Ayrıcalıklı erişim hakkının belirlenmesi ve yönetilmesi			
		1.2.3	Son kullanıcı erişim hakları matrisinin oluşturulması			
		1.2.4	Ayrıcalıklı erişim hakları matrisinin oluşturulması			
	3	1.3.1	Çalışan grupları dışında kalan kritik varlıklara usb, harici harddisk vb. cihazlar ile erişimin yönetilmesi			
		1.3.2	Son kullanıcılara ait bt varlıklarına usb, harici harddisk vb. cihazlar ile erişimin yönetilmesi			
		1.3.3	Ayrıcalıklı erişim hakkına sahip kullanıcılarda en az yetki prensibinin uygulanması			
		1.3.4	Son kullanıcı erişim haklarının ilgili birim yöneticileri ile gözden gözden geçirilmesi			
		1.3.5	Ayrıcalıklı kullanıcı erişim haklarının ilgili birim yöneticileri ile gözden geçirilmesi			
		1.3.6	Kayıtlı olmayan cihazların networke erişiminin kısıtlanması			
		1.3.7	İşletme BT varlıklarına erişim sağlaması gereken tedarikçiler için erişim yöntemi ve kontrol mekanizmasının oluşturulması ve yürütülmesi			
		1.3.8	Tedarikçi firmalara verilen erişim haklarının ilgili süreç bazında ihtiyaç duyulan minimum süre ve minimum yetki bazında verilmesi			
	4	1.4.1	Kritik varlıklara usb, harici harddisk vb. cihazlar ile erişimin kısıtlanması			
		1.4.2	Erişim yetki tanımlaması yapan personel ve erişim yetki gözden geçirmesini yapan personel/personellerin farklı olması			
	1	2.1.1	Varlık yönetimi prosedürünün hazırlanması			
	2	2.2.1	İşletme BT varlıklarının ve varlık gruplarının gizlilik,bütünlük ve erişilebilirlik kapsamında değerlerinin alan uzmanları ile birlikte belirlenmesi			



SİVİL HAVACILIK
GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(2. Grup Havacılık İşletmeleri)

2. Varlık Yönetimi	3	2.3.1	BT varlıklarının kabul edilebilir kullanımlarının belirlenmesi, dokümanite edilmesi ve ilgili paydaşların bilgisine sunması			
		2.3.2	Varlık gruplarının puan ve etki analizinin periyodik olarak gözden geçirilmesi			
	4	2.4.1	Varlık gruplarının puan ve etki analizinin ihtiyaçlar ve güncel siber tehditler kapsamında güncellenmesi			
		2.4.2	Kritik BT süreçlerine yönelik varlıkların imha süreçlerinin belirlenmesi			
		2.4.3	Kritik BT süreçlerine yönelik varlıkların imha süreçlerinin denetlenmesi			
3. İz Kayıt	1	3.1.1	İz kayıt alınması gereken varlıkların belirlenmesi ve söz konusu bu varlıklardan toplanacak iz kayıtlarının tespiti edilip dokümanite edilmesi			
		3.1.2	NTP server kullanılması			
		3.1.3	İşletme tarafından alınan iz kayıtları kapsamında toplanan kayıtların nitelik bakımından inkar edilemez olmasının sağlanması			
	2	3.2.1	Belirlenen varlıklardan ihtiyaç duyulan iz kayıtlarının alınması			
		3.2.2	İz kayıt toplama sürecinin herhangi bir sebepten ötürü sektöre uğraması durumuna karşı bir alarm mekanizması oluşturulması			
		3.2.3	İz kayıtlarına erişimin yönetilmesi ve kayıt altına alınması			
		3.2.4	Olası bir siber güvenlik olayına karşı iz kayıtlarının korele edilerek, istenmeyen durumların tespiti için bir süreç oluşturulması			
		3.2.5	İz kayıtlarına yönelik periyodik analiz raporlarının oluşturulması ve gözden geçirilmesi			
		3.2.6	Korelasyonlar sonucunda oluşan alarmların incelenerek ihtiyaç duyulması halinde diğer güvenlik süreçlerinin tetiklenmesi			
	3	3.3.1	Herhangi bir sebepten dolayı iz kayıt sağlayamayan sistemlerin tespiti edilmesi için bir tespit mekanizmasının oluşturulması			
		3.3.2	İz kayıtları alarmlarına yönelik yapılan çalışmalar hakkında periyodik olarak analiz yapılması ve söz konusu bu analiz raporunun SOME birimi yöneticisine sunulması			
	4	3.4.1	Toplanan iz kayıtlarının söz konusu uygulama veya sistemlerden farklı bir serverda tutulması			
		3.4.2	İşletme veya sektör paydaşlarının karşılaştığı siber güvenlik olaylarına yönelik korelasyonların oluşturulması			
		3.4.3	Mevcut korelasyon setlerinin periyodik olarak gözden geçirilmesi ve iyileştirilmesi			



SİVİL HAVACILIK
GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(2. Grup Havacılık İşletmeleri)

4. Farkındalık	1	4.1.1	İşletme personellerine etkin bir siber güvenlik farkındalığı eğitiminin sağlanması			
		4.1.2	Son kullanıcıların siber olay yönetimindeki rollerinin açık bir şekilde dokümanle edilmesi ve son kullanıcıların bu süreçteki rollerinin içselleştirilmesi			
	2	4.2.1	İşletme tesislerinde görev alan tedarikçi personele için etkin bir siber güvenlik farkındalığı eğitiminin sağlanması			
		4.2.2	İşletme tarafından hazırlanan siber güvenlik eğitim materyallerinin periyodik olarak gözden geçirilmesi ve ihtiyaçlar ve güncel siber tehditler kapsamında güncellenmesi			
		4.2.3	İşletme personeline verilen siber güvenlik farkındalık eğitimlerinin sonrasında eğitimin yarattığı farkındalık seviyesinin ölçülmesi amacı ile sınavların yapılması			
	3	4.3.1	Siber güvenlik farkındalığı eğitiminin ve sıklığının eğitimi alan personelin icra ettiği görevin kritikliğine uygun olarak verilmesi			
		4.3.2	İşletme personeline en az senede bir siber güvenlik farkındalığı tazeleme eğitimi verilmesi			
		4.3.3	İhtiyaç duyulması halinde işletme paydaşlarının söz konusu siber risk ve tehditler kapsamında bilgilendirilmesi			
	4	4.4.1	İşletme çalışanlarının siber güvenlik farkındalığı seviyesinin ölçülmesi için işletme çalışanlarının tümünü kapsayacak şekilde en az senede bir sosyal mühendislik testlerinin yapılması			
		4.4.2	Yapılan farkındalık sınav ve testlerinde hedeflenen başarı oranının altında kalan personelin farkındalık seviyesini arttırmak amacıyla faaliyetlerde bulunulması			
5. Olay Yönetimi	1	5.1.1	Siber güvenlik ihlal olay yönetim ve müdahale süreçlerini kapsayacak politika veya prosedürlerin oluşturulması			
	2	5.2.1	Son kullanıcılar ve ilgili paydaşların kullanımına sunulmuş bir siber olay raporlama mekanizmasının oluşturulması			
		5.2.2	İşletmenin yaşadığı siber güvenlik ihlal olaylarının nedenlerini alınan dersleri ve bir daha yaşanmaması için alınacak önlemleri kayıt altına alması ve ilgili otoriteler ile paylaşması			
	3	5.3.1	Dokümanle edilmiş bir siber güvenlik ihlal olay müdahale sürecinin oluşturulması			
		5.3.2	İşletmenin yaşadığı siber güvenlik ihlal olaylarını analiz etmesi, kayıt altına alması ve bir daha benzer bir siber güvenlik ihlal olayının yaşanmaması için gerekli önlemleri alması			
	4	5.4.1	Siber güvenlik ihlal olay yönetim süreçlerinde adli bilişim süreçlerinin etkin bir şekilde yürütülmesi			
6. Bakım	1	6.1.1	Bakım amacıyla işletme dışına çıkarılacak sistemlerin içerisinde hiçbir data barındırmamasının sağlanması			
		6.1.2	BT ve OT süreçlerini etkileyecek varlıkların bakımlarının yetkili işletmeler tarafından görevlendirilen yetkili personel tarafından yapılması			
	2	6.2.1	Bakım süreçlerinde görev alacak personelin izlenmesi			



SİVİL HAVACILIK
GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(2. Grup Havacılık İşletmeleri)

	3	6.3.1	BT süreçlerini etkileyecek varlıkların bakım sürelerinin dokümente edilmesi, izlenmesi ve bu sürelerle uygun olarak bakım çalışmalarının gerçekleştirilmesi			
	4	6.4.1	Bakım verilerin kayıt altında tutulması ve gizliliğinin sağlanması			
<u>7. İnsan Kaynakları Güvenliği</u>	1	7.1.1	İşletme kritik BT varlıklarına erişim sağlayacak personelin işe alım sürecinden önce güvenlik soruşturmalarının yapılması			
		7.1.2	İş sonlandırma süreçlerinde ilgili personelin yetki ve hesap iptaline yönelik mekanizmanın oluşturulması			
	2	7.2.1	İş sonlandırma süreçlerinde ilgili personelin yetki ve hesap iptaline yönelik oluşturulan mekanizmanın uygulanmasının denetlenmesi			
		7.2.2	Görev değişikliği süreçlerinde ilgili personelin eski görevine yönelik yetki ve hesap iptali mekanizmanın oluşturulması			
		7.2.3	Görev değişikliği süreçlerinde ilgili personelin eski görevine yönelik yetki ve hesap iptali mekanizmasının denetlenmesi			
	3	7.3.1	İşletme siber güvenlik politika ve prosedürleri ile belirlenmiş kural setlerine uyulmaması durumunda uygulanmak üzere bir disiplin sürecinin oluşturulması, dokümente edilmesi ve uygulanması			
<u>8. Fiziksel Güvenlik</u>	1	8.1.1	Fiziksel güvenlik prosedürünün oluşturulması, periyodik olarak gözden geçirilmesi ve ihtiyaç duyulması halinde güncellenmesi			
	2	8.2.1	Kritik BT varlıklarını etkileyen fiziksel ortam ve unsurların envanterinin oluşturulması			
		8.2.2	Kritik BT varlıklarına fiziksel erişimin yetki kapsamında kısıtlanması			
	3	8.3.1	Kritik BT varlıklarına fiziksel erişimi izlenmesi ve yetkisiz erişimlerin tespit edilmesi			
	4	8.4.1	Kritik BT varlıklarının bulunduğu alanlara erişim yetkisine sahip olmayan iç ve dış kaynaklı çalışanlara ve ziyaretçilere söz konusu kritik bu alanlara erişimlerinde eşlik edilmesi, bu kişilerin aktivitelerinin izlenmesi			
		8.4.2	Kritik BT varlıklarının bulunduğu alanlarda, yaka kartı takılmasının zorunlu olması ve kritik BT varlıklarına erişimde kişi yaka kartı eşleştirmesinin yapılması			
<u>9. Yedekleme</u>	1	9.1.1	İşletmenin süreç kritikliğinde göz önüne alarak bir yedekleme politika veya prosedürü oluşturması			
	2	9.2.1	İşletme yedekleme politika ve prosedürüne uygun şekilde düzenli olarak backup alınması.			
	3	9.3.1	Periyodik olarak yedekten geri dönme test çalışmalarının gerçekleştirilmesi			
		9.3.2	Backupların farklı bir sunucuda yer alması			
	4	9.4.1	Farklı bir risk bölgesinde işletme kritik dataların hepsini içerecek bir FKM yapısının kurulması			



SİVİL HAVACILIK
GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(2. Grup Havacılık İşletmeleri)

10. Risk Yönetimi	1	10.1.1	Siber Güvenlik Risk Değerlendirme Metodolojisinin belirlenmesi, dokümanle edilmesi			
		10.1.2	Siber Güvenlik Etki Değerlendirme Metodolojisinin belirlenmesi, dokümanle edilmesi			
	2	10.2.1	Siber güvenlik risk değerlendirme çalışmasının periyodik olarak gözden geçirilmesi ve güncellenmesi			
		10.2.2	Siber güvenlik risk değerlendirme çalışmasının işletme iç ve dış kaynaklar tarafından yapılan sızma testi, zafiyet taraması, kırmızı takım vb. çalışmaların sonuçlarına göre güncellenmesi ve iyileştirilmesi			
	3	10.3.1	Varlık envanteri kapsamında belirlenmiş varlıkları ISO 27001 Ek.A maddeleri kapsamında her bir madde ayrı ayrı olacak şekilde değerlendirilmesi			
		10.3.2	İşletmenin üretici veya tedarikçi bağımlılığı kapsamında siber güvenlik risklerinin belirlenmesi ve dokümanle etmesi			
		10.3.3	Risk kabulü ile ilgili sürecin aktif bir şekilde yürütülmesi ve dokümanle edilmesi			
		10.3.4	Siber güvenlik risk değerlendirme çalışmasının işletme iç ve dış kaynaklar tarafından yapılan denetim faaliyetlerinin sonuçlarına göre güncellenmesi ve iyileştirilmesi			
	4	10.4.1	Risk indirgeme çalışmalarının ilgili birimler ile koordine edilerek yürütülmesi, takip edilmesi ve dokümanle edilmesi			
		10.4.2	Siber güvenlik risk değerlendirme faaliyetlerinin yeterliliğinin ölçülmesi ve iyileştirilmesi			
11. Durumsal Farkındalık	1	11.1.1	Mevcut güvenlik mimarisinin güncelliğinin ve işletme ihtiyaçlarını karşılayıp karşılamadığının değerlendirmesinin yapılması			
		11.1.2	Mesai saatleri içerisinde siber tehdit veya siber güvenlik ihlal olayı tespit görevini icra edecek bir mekanizmanın kurulması			
		11.1.3	Mesai saatleri içerisinde siber olay müdahale görevini icra edecek bir mekanizma kurulması			
	2	11.2.1	Havacılık Sektörü İç Kontrol Metodolojisine uygun olarak en üst seviyeye erişmek için gerekli olan aksiyonların belirlenmesi			
		11.2.2	Periyodik zafiyet taraması yapılması			
	3	11.3.1	İşletmenin tabi olduğu yasal düzenlemelere uygun hale gelmek için gerekli aksiyonların belirlenmesi			
		11.3.2	7x24 prensibine göre siber tehdit veya siber güvenlik ihlal olayı tespit görevini icra edecek bir mekanizmanın kurulması			
		11.3.3	Siber tehdit veya siber güvenlik ihlal olayı tespit yapılanmasının yeterliliğinin ölçülmesi ve iyileştirilmesi			
		11.3.4	Siber olay müdahale yapılanmasının yeterliliğinin ölçülmesi ve iyileştirilmesi			



SİVİL HAVACILIK
GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(2. Grup Havacılık İşletmeleri)

		11.3.5	TSE akredite firmalar tarafından en az senede bir geniş kapsamlı sızma testi faaliyetinin gerçekleştirilmesi			
	4	11.4.1	7x24 prensibine göre siber tehdit veya siber güvenlik ihlal olayı müdahale görevini icra edecek bir mekanizmanın kurulması			
	1	12.1.1	Genel Müdürlük ve taşra teşkilatı bazında ağ segmentasyonun yapılması			
		12.1.2	İşletme iç ağında internete çıkış noktasına yerleştirilmiş bir güvenlik duvarı cihazının bulunması			
		12.1.3	Network cihazlarının fiziksel güvenliğinin sağlanarak yetkisiz erişiminin engellenmesi			
		12.1.4	İnaktif oturumların belirli bir süre sonrasında otomatik kilitlenmesi			
		12.1.5	İşletme BT sistemleri ile ilgili konfigürasyon envanterlerinin ve temel konfigürasyon setlerinin oluşturulması ve dokümanite edilmesi			
		12.1.6	Mobil cihazlar, sunucular ve son kullanıcılara ait BT varlıklarında antivirüs yazılımı kullanılması			
	2	12.2.1	Birim bazında ağ segmentasyonunun yapılması			
		12.2.2	Port, protokol ve servis kısıtlamasının minimum yetki prensibine uygun olarak uygulanması			
		12.2.3	Firewall kurallarının periyodik olarak gözden geçirilmesi ve iyileştirilmesi			
		12.2.4	Ağ güvenlik cihazlarının ve sunucu güvenlik konfigürasyon setlerinin USOM,SHGM gibi üst kuruluşlardan gelen talimatlara göre sıkılaştırılması			
		12.2.5	Network cihazlarının yönetiminde şifrelenmiş oturumlar kullanılması			
		12.2.6	Mac filtreleme metodu ile kayıtdışı cihazların işletme iç ağına erişiminin engellenmesi			
		12.2.7	DNS filtreleme çalışmasının gerçekleştirilmesi			
		12.2.8	URL filtreleme çalışmasının gerçekleştirilmesi			
		12.2.9	İhtiyaç duyulduğu kadar yetki prensibine bağlı kalarak güvenlik kontrollerinin uygulanması			
		12.2.10	Eposta hizmetlerinin güvenliğini sağlamak üzere spam koruma ve email gateway kullanılması			
		12.2.11	DDoS saldırılarına karşı önlem alınması ve alınan bu önlemlerin yeterliliğini periyodik olarak test edilmesi			



SİVİL HAVACILIK
GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(2. Grup Havacılık İşletmeleri)

12. Sistem ve Haberleşme Güvenliği		12.2.12	Network trafiğinde şüpheli hareket analizinin yapılması			
		12.2.13	İşletme bünyesinde NAC çözümlerinin kullanılması			
	3	12.3.1	Her bir ağ segmentasyonu için ayrı ayrı güvenlik duvarı yapılanmasının oluşturulması			
		12.3.2	Dıştan içe veya içten içe iletilen medyanın taranması için sandbox uygulamalarının kullanılması			
		12.3.3	Firewall trafiğinin izlenmesi, analiz edilmesi ve yapılan analiz sonucunda riskli görülen trafiğin engellenmesi			
		12.3.4	Kritik bilgi akışının şifreli bir şekilde yapılması			
		12.3.5	Kritik operasyonlarda erişim yönetim süreçlerinde kullanılmak üzere kriptografik şifreler oluşturma ve bu şifrelerin kullanımının yönetilmesi			
		12.3.6	802.1x metodu ile kayıtdışı cihazların veya kullanıcıların networke erişiminin engellenmesi			
		12.3.7	VOIP teknolojileri kullanılıyorsa, söz konusu bu teknolojiye yönelik sıkılaştırmaların yapılması			
		12.3.8	Son kullanıcılar tarafından ziyaret edilen web sitelerinin zararlı bir bileşen(exploit kit vb.) içermediğinin doğrulanması			
		12.3.9	Kullanıcı bazında şüpheli hareket analizinin yapılması			
		12.3.10	İşletme bünyesinde IDS ve IPS çözümlerinin kullanılması			
		12.3.11	İşletme iç paydaşlarının kullanımına yönelik olan sistemlerin uzaktan erişiminin ipsec vpn üzerinden olması			
	4	12.4.1	Görev ve kritiklik bazında ağ segmentasyonunun yapılması			
		12.4.2	DMZ yapılanmasının oluşturulması ve efektif bir şekilde kullanımının sağlanması			
		12.4.3	İşletme siber güvenlik kabiliyetinin artırılması amacı ile siber istihbarat hizmetlerinin kullanılması			
		12.4.4	Tüm son kullanıcı gruplarının yükleme izni olan uygulamaların belirlenmesi amacıyla whitelist ve blacklist uygulanması ve söz konusu sistemin 7x24 izlenmesi			
		12.4.5	İşletme bünyesinde load balancer çözümlerinin kullanılması			
		12.4.6	İşletme bünyesinde WAF çözümlerinin kullanılması			



SİVİL HAVACILIK
GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(2. Grup Havacılık İşletmeleri)

		12.4.7	Son kullanıcılara yönelik cihazlarda EDR çözümlerinin kullanılması			
13. Siber Güvenlik Yapılanması	1	13.1.1	SOME'nin kurulmuş olması			
		13.1.2	SOME birimi personelinin kapsam ve görev tanımlarının belirlenmiş ve dokümante edilmiş olması			
	2	13.2.1	SOME Yöneticisi'nin en az lisans derecesine sahip olması ve siber güvenlik konusunda uzmanlaşmış olması			
		13.2.2	SOME personeli işe alım sürecinden önce güvenlik soruşturmasının yapılması (adli sicil kaydı, şahıs güvenlik belgesi v.b.)			
		13.2.3	Some'de görev alan personelin ön lisans veya lisans programlarından mezun olması ve en az iki yıl bilgi işlem tecrübesine sahip olması veya bilgi güvenliği/siber güvenlik konularında bilgi ve tecrübeye sahip olması			
	3	13.3.1	SOME biriminin en az Genel Müdür Yrd. seviyesine bağlanması			
	4	13.4.1	SOME'nin BT birim ve süreçlerinden görevlerin ayrılığı ilkesi kapsamında ayrılması			
		13.4.2	Görevlendirilecek personelin some kapsamındaki görev ve sorumluluklarını yerine getirebilmesi için sorumlu olduğu konuda uzman olması			
14. İş Sürekliliği	1	14.1.1	BT varlıklarının iş sürekliliğine yönelik bir politika veya prosedürün oluşturulması			
	2	14.2.1	BT varlıklarına yönelik iş sürekliliği etki analizinin yapılması			
	4	14.4.1	İş sürekliliği risk ve etki analizinin periyodik olarak gözden geçirilmesi ve ihtiyaç duyulması halinde güncellenmesi			
		14.4.2	İş sürekliliği planlarının oluşturulması, gözden geçirilmesi ve güncel tutulması			
		14.4.3	İş sürekliliği çalışmalarının, görevler ayrılığı ilkesinde gözetilerek, objektif bir şekilde değerlendirilmesi			
15. Tedarikçi Yönetimi	1	15.1.1	Tedarikçi yönetimi politikası veya prosedürünün oluşturulması			
	2	15.2.1	Dış kaynaklı olarak alınan hizmet ve ürünlerin işletmeye olan etkisine göre kritik tedarikçilerinin belirlenmesi			
	3	15.3.1	Tedarik ihtiyacı olan süreçle ilgili tedarikçi bilgi güvenliği gereksinim seviyelerinin belirlenmesi			
	4	15.4.1	Tedarikçi yönetim sürecinin değerlendirilmesi ve iyileştirilmesi			
		15.4.2	Kritik tedarikçilerin sözleşmelerinde bilgi güvenliği unsurlarının yer alması			



SİVİL HAVACILIK
GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(2. Grup Havacılık İşletmeleri)

		15.4.3	Kritik tedarikçilerin bilgi güvenliği kapsamında denetlenmesi			
<u>16. Yasal Uyum</u>	1	16.1.1	İşletmenin ISO 27001 Sertifika belgesine sahip olması			
	3	16.3.1	ISO 27001 Ek.A.18.2.1 kapsamında yasal uyum süreci envanterinin oluşturulması			
	4	16.4.1	İşletmenin yasal sorumluluğunun olduğu alanlarda yeni çıkan regülasyonlar ile ilgili takip mekanizması oluşturması			
<u>17. İşletim Güvenliği</u>	1	17.1.1	Lisanssız yazılımların kullanılmaması			
	2	17.2.1	Yama yönetiminin uygulanması			
	3	17.3.1	Değişiklik yönetiminin uygulanması			
		17.3.2	Kapasite yönetiminin uygulanması			
	4	17.4.1	Kullanıcının yükleme izni olan uygulamalar için whitelist ve blacklist uygulanması ve sürecin izlenmesi			
<u>18. Sistem Temini, Geliştirme ve Bakım</u>	1	18.1.1	Sistem temini geliştirme ve bakımı süreçlerini ele alan bir politika veya prosedürün oluşturulması			
	2	18.2.1	Geliştirilecek veya temin edilecek sistemin güvenliğini sağlamak amacıyla analizin yapılması ve siber güvenlik gereksinimlerinin belirlenmesi			
	3	18.3.1	Geliştirilecek veya temin edilecek sistemin güvenliğini sağlamak amacıyla siber güvenlik test süreçlerinin gerçekleştirilmesi			
		18.3.2	İç veya dış kaynaklı sistem temini, geliştirme veya güncelleme süreçlerinde değişiklik yönetimi süreçlerinin etkin bir şekilde yürütülmesi			
		18.3.3	Test ve geliştirme ortamlarının ayrıştırılması			
		18.3.4	Test verisinin kişisel veri veya operasyonel kritik veri içermemesi			
	4	18.4.1	Temin edilecek, geliştirilecek veya güncellenecek sistemlerin güvenliğini sağlamak amacıyla SHT-Siber Ek-10'da yer alan Havacılık Sektörü Güvenli Yazılım Yazılım Geliştirme Rehberi içerisinde bulunan kontrol listesinin kullanılması ve bu sürecin SOME tarafından denetlenmesi			
<u>19. Yerli Milli Ürün Kullanılması</u>	3	19.3.1	Yerli ve milli ürünlerin işletme BT ürün envanterindeki oranının %5'den az olması			
	4	19.4.1	Yerli ve milli ürünlerin işletme BT ürün envanterindeki oranının %5'den fazla ve %10'dan az olması			
	1	20.1.1	Siber güvenlik yapılması dahilinde sağlıklı bir iletişim mekanizmasının oluşturulması ve yürütülmesi			



SİVİL HAVACILIK
GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(2. Grup Havacılık İşletmeleri)

20. İletişim	2	20.2.1	Tüm işletme kapsamında sağlıklı bir iletişim mekanizmasının oluşturulması ve yürütülmesi			
	3	20.3.1	Kritik BT varlıkları tedarikçi firmaları ile sağlıklı bir iletişim mekanizmasının oluşturulması ve yürütülmesi			
	4	20.4.1	İşletme siber güvenlik faaliyetlerini etkileyen tüm iç ve dış paydaşlar ile sağlıklı bir iletişim mekanizmasının oluşturulması ve yürütülmesi			

U: Uygun

UD:Uygun Değil

NA:Uygulanamaz



T.C. ULAřTIRMA VE ALTYAPI BAKANLIđI
SİVİL HAVACILIK GENEL MÜDÜRLÜđÜ

3. GRUP HAVACILIK SEKTÖRÜ İřLETMELERİ

HAVACILIK GÜVENLİđİ DAİRE BAřKANLIđI-SİBER GÜVENLİK KOORDİNATÖRLÜđÜ



SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi (3. Grup Havacılık İşletmeleri)

Sıra	Kontrol Maddesi	Seviye 1	Seviye 2	Seviye 3	Seviye 4	Toplam
1	Erişim Yönetimi	0	1	1	2	4
2	Varlık Yönetimi	0	0	1	1	2
3	İz Kayıt	1	1	1	1	4
4	Farkındalık	1	0	1	2	4
5	Olay Yönetimi	0	1	0	1	2
6	Bakım	2	0	0	1	3
7	İnsan Kaynakları Güvenliği	1	2	2	1	6
8	Fiziksel Güvenlik	0	1	0	1	2
9	Yedekleme	0	0	1	1	2
10	Risk Yönetimi	0	0	3	1	4
11	Durumsal Farkındalık ve Sistem Test	0	0	2	3	5
12	Sistem ve Haberleşme Güvenliği	1	2	7	3	13
13	Siber Güvenlik Yapılanması	0	1	0	0	1
14	İş Sürekliliği	0	0	0	0	0
15	Tedarikçi Yönetimi	0	0	1	1	2
16	Yasal Uyum	0	0	0	1	1
17	İşletim Güvenliği	1	0	0	0	1
18	Sistem Temini, Geliştirme ve Bakım	0	1	0	1	2
19	Yerli Milli Ürün Kullanımı	0	0	0	0	0
20	İletişim	1	1	1	1	4
Seviye Toplam		8	11	21	22	62



SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi (3. Grup Havacılık İşletmeleri)

No	1. Erişim Yönetimi			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1		Erişim Yönetimi Kontrol Prosedürünün Oluşturulması	Son kullanıcılara verilecek yetkilerin en az yetki prensibine göre verilmesi	Ayrıcalıklı erişim hakkının belirlenmesi ve yönetilmesi
2				Son kullanıcı erişim haklarının ilgili birim yöneticileri ile gözden gözden geçirilmesi



SİVİL HAVACILIK
GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(3. Grup Havacılık İşletmeleri)

No	2. Varlık Yönetimi			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1			Varlık yönetimi prosedürünün hazırlanması	İşletme BT varlıklarının ve varlık gruplarının gizlilik,bütünlük ve erişilebilirlik kapsamında değerlerinin alan uzmanları ile birlikte belirlenmesi



SİVİL HAVACILIK
GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(3. Grup Havacılık İşletmeleri)

No	3. İz Kayıt			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	NTP server kullanılması	İz kayıt alınması gereken varlıkların belirlenmesi ve söz konusu bu varlıklardan toplanacak iz kayıt niteliğinin tespit edilip dokümante edilmesi	Belirlenen varlıklardan ihtiyaç duyulan iz kayıtlarının alınması	Olası bir siber güvenlik olayına karşı iz kayıtlarının korale edilerek, istenmeyen durumların tespiti için bir süreç oluşturulması



SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi (3. Grup Havacılık İşletmeleri)

No	4. Farkındalık			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	İşletme personellerine etkin bir siber güvenlik farkındalığı eğitiminin sağlanması		Son kullanıcıların siber olay yönetimindeki rollerinin açık bir şekilde dokümente edilmesi ve son kullanıcıların bu süreçteki rollerinin içselleştirilmesi	İşletme tarafından hazırlanan siber güvenlik eğitim materyallerinin periyodik olarak gözden geçirilmesi ve ihtiyaçlar ve güncel siber tehditler kapsamında güncellenmesi
2				İşletme personeline en az senede bir siber güvenlik farkındalığı tazeleme eğitimi verilmesi



SİVİL HAVACILIK
GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(3. Grup Havacılık İşletmeleri)

No	5. Olay Yönetimi			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1		Siber güvenlik ihlal olay yönetim ve müdahale süreçlerini kapsayacak politika veya prosedürlerin oluşturulması		Son kullanıcılar ve ilgili paydaşların kullanımına sunulmuş bir siber olay raporlama mekanizmasının oluşturulması



SİVİL HAVACILIK
GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(3. Grup Havacılık İşletmeleri)

No	6. Bakım			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	Bakım amacıyla işletme dışına çıkarılacak sistemlerin içerisinde hiçbir data barındırmamasının sağlanması			BT süreçlerini etkileyecek varlıkların bakım sürelerinin dokümente edilmesi, izlenmesi ve bu sürelerle uygun olarak bakım çalışmalarının gerçekleştirilmesi
2	BT ve OT süreçlerini etkileyecek varlıkların bakımlarının yetkili işletmeler tarafından görevlendirilen yetkili personel tarafından yapılması			



SİVİL HAVACILIK
GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(3. Grup Havacılık İşletmeleri)

No	7. İnsan Kaynakları Güvenliği			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	İşletme kritik BT varlıklarına erişim sağlayacak personelin işe alım sürecinden önce güvenlik soruşturmalarının yapılması	İş sonlandırma süreçlerinde ilgili personelin yetki ve hesap iptaline yönelik mekanizmanın oluşturulması	Görev değişikliği süreçlerinde ilgili personelin eski görevine yönelik yetki ve hesap iptali mekanizmanın oluşturulması	İşletme siber güvenlik politika ve prosedürleri ile belirlenmiş kural setlerine uyulmaması durumunda uygulanmak üzere bir disiplin sürecinin oluşturulması, dokümente edilmesi ve uygulanması
2		İş sonlandırma süreçlerinde ilgili personelin yetki ve hesap iptaline yönelik oluşturulan mekanizmanın uygulanmasının denetlenmesi	Görev değişikliği süreçlerinde ilgili personelin eski görevine yönelik yetki ve hesap iptali mekanizmasının denetlenmesi	



SİVİL HAVACILIK
GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(3. Grup Havacılık İşletmeleri)

No	8. Fiziksel Güvenlik			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1		Fiziksel güvenlik prosedürünün oluşturulması, periyodik olarak gözden geçirilmesi ve ihtiyaç duyulması halinde güncellenmesi		Kritik BT varlıklarının bulunduğu alanlarda, yaka kartı takılmasının zorunlu olması ve kritik BT varlıklarına erişimde kişi yaka kartı eşleştirmesinin yapılması



SİVİL HAVACILIK
GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(3. Grup Havacılık İşletmeleri)

No	9. Yedekleme			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1			İşletmenin süreç kritikliğinde göz önüne alarak bir yedekleme politika veya prosedürü oluşturması	İşletme yedekleme politika ve prosedürüne uygun şekilde düzenli olarak backup alınması



SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi (3. Grup Havacılık İşletmeleri)

No	10. Risk Yönetimi			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1			Siber Güvenlik Risk Değerlendirme Metodolojisinin belirlenmesi, dokümanite edilmesi	Siber güvenlik risk değerlendirme faaliyetlerinin yeterliliğinin ölçülmesi ve iyileştirilmesi
2			Siber Güvenlik Etki Değerlendirme Metodolojisinin belirlenmesi, dokümanite edilmesi	
3			Siber güvenlik risk değerlendirme çalışmasının periyodik olarak gözden geçirilmesi ve güncellenmesi	



SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi (3. Grup Havacılık İşletmeleri)

No	11. Durumsal Farkındalık ve Sistem Test			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1			Mevcut güvenlik mimarisinin güncelliğinin ve işletme ihtiyaçlarını karşılayıp karşılamadığının değerlendirilmesinin yapılması	Mesai saatleri içerisinde siber tehdit veya siber güvenlik ihlal olayı tespit görevini icra edecek bir mekanizmanın kurulması
2			Periyodik zafiyet taraması yapılması	Mesai saatleri içerisinde siber olay müdahale görevini icra edecek bir mekanizma kurulması
3				TSE akredite firmalar tarafından en az senede bir geniş kapsamlı sızma testi faaliyetinin gerçekleştirilmesi



SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi (3. Grup Havacılık İşletmeleri)

No	12. Sistem ve Haberleşme Güvenliği			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	Mobil cihazlar, sunucular ve son kullanıcılara ait BT varlıklarında antivirüs yazılımı kullanılması	İşletme iç ağında internete çıkış noktasına yerleştirilmiş bir güvenlik duvarı cihazının bulunması	Genel Müdürlük ve taşra teşkilatı bazında ağ segmentasyonunun yapılması	Birim bazında ağ segmentasyonunun yapılması
2		Network cihazlarının fiziksel güvenliğinin sağlanarak yetkisiz erişiminin engellenmesi	Mac filtreleme metodu ile kayıtdışı cihazların işletme iç ağına erişiminin engellenmesi	Port, protokol ve servis kısıtlamasının minimum yetki prensibine uygun olarak uygulanması
3			İnaktif oturumların belirli bir süre sonrasında otomatik kilitlenmesi	Eposta hizmetlerinin güvenliğini sağlamak üzere spam koruma ve email gateway kullanılması
4			DNS filtreleme çalışmasının gerçekleştirilmesi	
5			URL filtreleme çalışmasının gerçekleştirilmesi	
6			İşletme BT sistemleri ile ilgili konfigürasyon envanterlerinin ve temel konfigürasyon setlerinin oluşturulması ve dokümanite edilmesi	
7			Network trafiğinde şüpheli hareket analizinin yapılması	



SİVİL HAVACILIK
GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(3. Grup Havacılık İşletmeleri)

No	13. Siber Güvenlik Yapılanması			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1		İşletmenin siber güvenliğini sağlamak için en az 1 adet görevlendirilmiş uzman personelin olması		



SİVİL HAVACILIK
GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(3. Grup Havacılık İşletmeleri)

14. İş Sürekliliği			
Seviye 1	Seviye 2	Seviye 3	Seviye 4
Kontrol maddesi ile alakalı bu grup işletmeler için alınması gereken tedbir yoktur.			



SİVİL HAVACILIK
GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(3. Grup Havacılık İşletmeleri)

No	15. Tedarikçi Yönetimi			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1			Tedarikçi yönetimi politikası veya prosedürünün oluşturulması	Dış kaynaklı olarak alınan hizmet ve ürünlerin işletmeye olan etkisine göre kritik tedarikçilerinin belirlenmesi



SİVİL HAVACILIK
GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(3. Grup Havacılık İşletmeleri)

No	16. Yasal Uyum			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1				İşletmenin ISO 27001 Sertifika belgesine sahip olması



SİVİL HAVACILIK
GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(3. Grup Havacılık İşletmeleri)

No	17. İşletim Güvenliği			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	Lisanssız yazılımların kullanılmaması			



SİVİL HAVACILIK
GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(3. Grup Havacılık İşletmeleri)

No	18. Sistem Temini, Geliştirme ve Bakım			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1		Sistem temini geliştirme ve bakımı süreçlerini ele alan bir politika veya prosedürün oluşturulması		Geliştirilecek veya temin edilecek sistemin güvenliğini sağlamak amacıyla siber güvenlik test süreçlerinin gerçekleştirilmesi



SİVİL HAVACILIK
GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(3. Grup Havacılık İşletmeleri)

19. Yerli Milli Ürün Kullanılması			
Seviye 1	Seviye 2	Seviye 3	Seviye 4
Kontrol maddesi ile alakalı bu grup işletmeler için alınması gereken tedbir yoktur.			



SİVİL HAVACILIK
GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(3. Grup Havacılık İşletmeleri)

No	20. İletişim			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	Siber güvenlik yapılanması dahilinde sağlıklı bir iletişim mekanizmasının oluşturulması ve yürütülmesi	Tüm işletme kapsamında sağlıklı bir iletişim mekanizmasının oluşturulması ve yürütülmesi	Kritik BT varlıkları tedarikçi firmaları ile sağlıklı bir iletişim mekanizmasının oluşturulması ve yürütülmesi	İşletme siber güvenlik faaliyetlerini etkileyen tüm iç ve dış paydaşlar ile sağlıklı bir iletişim mekanizmasının oluşturulması ve yürütülmesi

Havacılık Sektörü İç Kontrol Metodolojisi
3. Grup Havacılık Sektörü İşletmeleri Kontrol Listesi

Kontrol Başlığı	Seviye	Kontrol No.	Kontrol Maddesi	U	UD	NA
1. Erişim Yönetimi	2	1.2.1	Erişim Yönetimi Kontrol Prosedürünün Oluşturulması			
	3	1.3.1	Son kullanıcılara verilecek yetkilerin en az yetki prensibine göre verilmesi			
	4	1.4.1	Ayrıcalıklı erişim hakkının belirlenmesi ve yönetilmesi			
		1.4.2	Son kullanıcı erişim haklarının ilgili birim yöneticileri ile gözden gözden geçirilmesi			
2. Varlık Yönetimi	3	2.3.1	Varlık yönetimi prosedürünün hazırlanması			
	4	2.4.1	İşletme BT varlıklarının ve varlık gruplarının gizlilik,bütünlük ve erişilebilirlik kapsamında değerlerinin alan uzmanları ile birlikte belirlenmesi			
3. İz Kayıt	1	3.1.1	NTP server kullanılması			
	2	3.2.1	İz kayıt alınması gereken varlıkların belirlenmesi ve söz konusu bu varlıklardan toplanacak iz kayıtlarının tespiti edilip dokümanite edilmesi			
	3	3.3.1	Belirlenen varlıklardan ihtiyaç duyulan iz kayıtlarının alınması			
	4	3.4.1	Olası bir siber güvenlik olayına karşı iz kayıtlarının korale edilerek, istenmeyen durumların tespiti için bir süreç oluşturulması			
4. Farkındalık	1	4.1.1	İşletme personellerine etkin bir siber güvenlik farkındalığı eğitiminin sağlanması			
	3	4.3.1	Son kullanıcıların siber olay yönetimindeki rollerinin açık bir şekilde dokümanite edilmesi ve son kullanıcıların bu süreçteki rollerinin içselleştirilmesi			
	4	4.4.1	İşletme tarafından hazırlanan siber güvenlik eğitim materyallerinin periyodik olarak gözden geçirilmesi ve ihtiyaçlar ve güncel siber tehditler kapsamında güncellenmesi			
		4.4.2	İşletme personeline en az senede bir siber güvenlik farkındalığı tazeleme eğitimi verilmesi			
5. Olay Yönetimi	2	5.2.1	Siber güvenlik ihlal olay yönetim ve müdahale süreçlerini kapsayacak politika veya prosedürlerin oluşturulması			
	4	5.4.1	Son kullanıcılar ve ilgili paydaşların kullanımına sunulmuş bir siber olay raporlama mekanizmasının oluşturulması			
6. Bakım	1	6.1.1	Bakım amacıyla işletme dışına çıkarılacak sistemlerin içerisinde hiçbir data barındırmamasının sağlanması			
		6.1.2	BT ve OT süreçlerini etkileyecek varlıkların bakımlarının yetkili işletmeler tarafından görevlendirilen yetkili personel tarafından yapılması			

	4	6.4.1	BT süreçlerini etkileyecek varlıkların bakım sürelerinin dokümente edilmesi, izlenmesi ve bu sürelerle uygun olarak bakım çalışmalarının gerçekleştirilmesi			
7. İnsan Kaynakları Güvenliği	1	7.1.1	İşletme kritik BT varlıklarına erişim sağlayacak personelin işe alım sürecinden önce güvenlik soruşturmasının yapılması			
	2	7.2.1	İş sonlandırma süreçlerinde ilgili personelin yetki ve hesap iptaline yönelik mekanizmanın oluşturulması			
		7.2.2	İş sonlandırma süreçlerinde ilgili personelin yetki ve hesap iptaline yönelik oluşturulan mekanizmanın uygulanmasının denetlenmesi			
	3	7.3.1	Görev değişikliği süreçlerinde ilgili personelin eski görevine yönelik yetki ve hesap iptali mekanizmanın oluşturulması			
		7.3.2	Görev değişikliği süreçlerinde ilgili personelin eski görevine yönelik yetki ve hesap iptali mekanizmasının denetlenmesi			
	4	7.4.1	İşletme siber güvenlik politika ve prosedürleri ile belirlenmiş kural setlerine uyulmaması durumunda uygulanmak üzere bir disiplin sürecinin oluşturulması, dokümente edilmesi ve uygulanması			
8. Fiziksel Güvenlik	2	8.2.1	Fiziksel güvenlik prosedürünün oluşturulması, periyodik olarak gözden geçirilmesi ve ihtiyaç duyulması halinde güncellenmesi			
	4	8.4.1	Kritik BT varlıklarının bulunduğu alanlarda, yaka kartı takılmasının zorunlu olması ve kritik BT varlıklarına erişimde kişi yaka kartı eşleştirmesinin yapılması			
9. Yedekleme	3	9.3.1	İşletmenin süreç kritikliğinde göz önüne alarak bir yedekleme politika veya prosedürü oluşturması			
	4	9.4.1	İşletme yedekleme politika ve prosedürüne uygun şekilde düzenli olarak backup alınması			
10. Risk Yönetimi	3	10.3.1	Siber Güvenlik Risk Değerlendirme Metodolojisinin belirlenmesi, dokümente edilmesi			
		10.3.2	Siber Güvenlik Etki Değerlendirme Metodolojisinin belirlenmesi, dokümente edilmesi			
		10.3.3	Siber güvenlik risk değerlendirme çalışmasının periyodik olarak gözden geçirilmesi ve güncellenmesi			
	4	10.4.1	Siber güvenlik risk değerlendirme faaliyetlerinin yeterliliğinin ölçülmesi ve iyileştirilmesi			
11. Durumsal Farkındalık ve Sistem Test	3	11.3.1	Mevcut güvenlik mimarisinin güncelliğinin ve işletme ihtiyaçlarını karşılayıp karşılamadığının değerlendirmesinin yapılması			
		11.3.2	Periyodik zafiyet taraması yapılması			
	4	11.4.1	Mesai saatleri içerisinde siber tehdit veya siber güvenlik ihlal olayı tespit görevini icra edecek bir mekanizmanın kurulması			
		11.4.2	Mesai saatleri içerisinde siber olay müdahale görevini icra edecek bir mekanizma kurulması			
		11.4.3	TSE akredite firmalar tarafından en az senede bir geniş kapsamlı sızma testi faaliyetinin gerçekleştirilmesi			



**SİVİL HAVACILIK
GENEL MÜDÜRLÜĞÜ**

Havacılık Sektörü İç Kontrol Metodolojisi
(3. Grup Havacılık İşletmeleri)

12. Sistem ve Haberleşme Güvenliği	1	12.1.1	Mobil cihazlar, sunucular ve son kullanıcılara ait BT varlıklarında antivirüs yazılımı kullanılması			
	2	12.2.1	İşletme iç ağında internete çıkış noktasına yerleştirilmiş bir güvenlik duvarı cihazının bulunması			
		12.2.2	Network cihazlarının fiziksel güvenliğinin sağlanarak yetkisiz erişiminin engellenmesi			
	3	12.3.1	Genel Müdürlük ve taşra teşkilatı bazında ağ segmentasyonunun yapılması			
		12.3.2	Mac filtreleme metodu ile kayıtdışı cihazların işletme iç ağına erişiminin engellenmesi			
		12.3.3	İnaktif oturumların belirli bir süre sonrasında otomatik kilitlenmesi			
		12.3.4	DNS filtreleme çalışmasının gerçekleştirilmesi			
		12.3.5	URL filtreleme çalışmasının gerçekleştirilmesi			
		12.3.6	İşletme BT sistemleri ile ilgili konfigürasyon envanterlerinin ve temel konfigürasyon setlerinin oluşturulması ve dokümante edilmesi			
		12.3.7	Network trafiğinde şüpheli hareket analizinin yapılması			
	4	12.4.1	Birim bazında ağ segmentasyonunun yapılması			
		12.4.2	Port, protokol ve servis kısıtlamasının minimum yetki prensibine uygun olarak uygulanması			
		12.4.3	Eposta hizmetlerinin güvenliğini sağlamak üzere spam koruma ve email gateway kullanılması			
13. Siber Güvenlik Yapılanması	2	13.2.1	İşletmenin siber güvenliğini sağlamak için en az 1 adet görevlendirilmiş uzman personelin olması			
15. Tedarikçi Yönetimi	3	15.3.1	Tedarikçi yönetimi politikası veya prosedürünün oluşturulması			
	4	15.4.1	Dış kaynaklı olarak alınan hizmet ve ürünlerin işletmeye olan etkisine göre kritik tedarikçilerinin belirlenmesi			
16. Yasal Uyum	4	16.4.1	İşletmenin ISO 27001 Sertifika belgesine sahip olması			
17. İşletim Güvenliği	1	17.1.1	Lisanssız yazılımların kullanılmaması			
18. Sistem Temini, Geliştirme ve Bakım	2	18.2.1	Sistem temini geliştirme ve bakımı süreçlerini ele alan bir politika veya prosedürün oluşturulması			
	4	18.4.1	Geliştirilecek veya temin edilecek sistemin güvenliğini sağlamak amacıyla siber güvenlik test süreçlerinin gerçekleştirilmesi			



SİVİL HAVACILIK
GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(3. Grup Havacılık İşletmeleri)

20. İletişim	1	20.1.1	Siber güvenlik yapılanması dahilinde sağlıklı bir iletişim mekanizmasının oluşturulması ve yürütülmesi			
	2	20.2.1	Tüm işletme kapsamında sağlıklı bir iletişim mekanizmasının oluşturulması ve yürütülmesi			
	3	20.3.1	Kritik BT varlıkları tedarikçi firmaları ile sağlıklı bir iletişim mekanizmasının oluşturulması ve yürütülmesi			
	4	20.4.1	İşletme siber güvenlik faaliyetlerini etkileyen tüm iç ve dış paydaşlar ile sağlıklı bir iletişim mekanizmasının oluşturulması ve yürütülmesi			

U: Uygun

UD:Uygun Değil

NA:Uygulanamaz