BİLİŞİM SİSTEMLERİ DENETİMİ REHBERİ

Haziran 2013
ANKARA

BİLİŞİM SİSTEMLERİ DENETİMİ REHBERİ

Haziran 2013

ANKARA

BELGE ADI:	SDR.4, Bilişim Sistemleri Denetimi Rehberi
VERSİYON NO:	2013/1
VERSİYON TARİHİ	Haziran 2013

Bilişim Sistemleri Denetimi Rehberi, Denetim Planlama ve Koordinasyon Kurulunun 11.06.2013 tarih ve 2013/15 sayılı toplantısında görüşülerek kabul edilmiş ve 24.06.2013 tarihinde Sayıştay Başkanı tarafından onaylanarak yürürlüğe girmiştir.

SUNUŞ

19.12.2010 tarihinde yürürlüğe giren 6085 sayılı Sayıştay Kanunu ve bu Kanun doğrultusunda hazırlanan ikincil mevzuat ile birlikte Sayıştay'ın denetim alanı genişlemiş ve denetim usullerinde de önemli değişimler yaşanmıştır.

Özellikle son yıllarda denetim kapsamındaki kurumların bilgi teknolojilerinden ve bu teknolojilerin sunduğu imkânlardan yararlanmak amacıyla başta mali işlemler olmak üzere her alanda giderek daha yaygın bir şekilde bilişim sistemlerini kullanmaları Sayıştay denetiminin, bu alanı da kapsayacak şekilde yeniden yapılandırılmasını sağlamıştır.

Bilişim sistemlerinin kamu mali yönetiminde kullanılmasında yaşanan gelişmelere paralel olarak, Başkanlığımız da Bilişim Sistemlerinin Denetimi (BSD) alanında birtakım çalışmalarda bulunmuştur. Bu kapsamda; 2005-2007 yılları arasında İngiltere Sayıştayı ile gerçekleştirilen "Sayıştay Denetim Kapasitesinin Güçlendirilmesi Eşleştirme Projesi" kapsamında bir ekip oluşturularak İngiltere Sayıştayı uzmanlarından Bilişim Sistemleri Denetimi konusunda eğitimler alınmıştır. Bu çalışmalar sonucu oluşturulan Taslak Bilişim Sistemleri Denetim Rehberi ile Mali Denetim Rehberinin bilişim sistemlerinin değerlendirilmesine ilişkin bölümleri hazırlanmış ve iki kurumda yapılan pilot denetim çalışmalarıyla test edilmiştir.

Hazırlanan rehberin etkili olması ve bilişim sistemlerinin denetimi konusunda kapasite geliştirilmesi için Sayıştay Başkanlığı ile Türkiye Bilimsel ve Teknolojik Araştırma Kurumu arasında, bilişim sistemleri denetimi, eğitimi, rehber ve yazılım geliştirilmesini de içeren işbirliği protokolü 29.05.2007 tarihinde imzalanmıştır. Bu protokol kapsamında; TÜBİTAK UEKAE uzmanlarından teknik konularda eğitim alınmış ve BSD Rehberinin güncellenmesi çalışması tamamlanmış ve bu rehberin ortaya çıkarılması sağlanmıştır.

Bu rehber ve uygulamalarının Sayıştayın incelediği sistemlere ilişkin duyduğu bilgi güvenliği ve güvenirliliğine ilişkin güvence elde etme ihtiyacını daha iyi karşılaması ve denetlenen kurumların sistemlerinin geliştirilmesi için kurumlara daha fazla katkı sağlamasını dilerim.

Bu vesile ile rehberin hazırlanmasında emeği geçen herkese teşekkür eder, tüm kullanıcılara faydalı olması dileğiyle saygılar sunarım.

Doç. Dr. Recai AKYEL

Sayıştay Başkanı

İÇİNDEKİLER

GİRİŞ VE GENEL METODOLOJİ

GİRİŞ

Bilgisayar teknolojisi hızla gelişmekte ve bu teknolojinin sunduğu imkanlardan yararlanmak amacıyla kurumlarda bilişim sistemleri, başta mali işlemler olmak üzere her alanda giderek daha yaygın bir şekilde kullanılmaktadır. Bilişim sistemlerinin kullanımı bu teknolojiye özgü riskleri de beraberinde getirmektedir.

Riskleri önleyecek etkin kontrol mekanizmalarının oluşturulmaması durumunda sistemlerde üretilen bilginin gizliliği, bütünlüğü ve kullanılabilirliği, dolayısıyla bu bilgiyi işleyen, tutan ve raporlayan sistemlerin güvenliği ve güvenilirliği zarar görebilmektedir. Bu nedenle, bu teknolojilerin yoğun kullanıldığı ortamlarda yürütülecek denetimler sırasında bu risklerin etkilerini dikkate alan yaklaşım, metot ve tekniklerin benimsenmesi gerekmektedir.

Nitekim, Uluslararası Sayıştaylar Birliği (INTOSAI) denetim standartlarına göre, muhasebe veya diğer bilgi sistemlerinin bilgisayarlaştırıldığı ortamlarda denetçi, denetlenen kurumun verilerinin doğruluk, tamlık (bütünlük) ve güvenilirliğini sağlayan iç kontrollerin uygun çalışıp çalışmadığını belirlemelidir.

Bilgi Sistemleri Denetim ve Kontrol Birliği (ISACA) tarafından kabul gören tanıma göre, Bilişim Sistemleri Denetimi; "bir bilgisayar (veya bilgi) sisteminin varlıkları güvence altına alıp almadığı, veri bütünlüğünü sağlayıp sağlamadığı, kurumsal amaçlara etkin biçimde ulaşıp ulaşmadığı ve kaynakları verimli bir şekilde kullanıp kullanmadığını belirlemek amacıyla yapılan kanıt toplama ve değerlendirme sürecidir."

Mali denetim açısından bilişim sistemleri denetiminin amacı, denetlenen kurumlarda kullanılan bilişim sistemlerinin işlem ve uygulamalarının güvenlik ve güvenilirliğini sağlayan iç kontrolleri incelemek ve değerlendirmektir.

Bu rehber kapsamında yapılan bilişim sistemleri denetimi, mali denetim sürecine destek vermeyi, sistemlerin kontrol zayıflıklarının belirlenmesi ve öneriler sunulması yolu ile kuruma katkı sağlamayı ve bilgi sistemleri konusunda kamuoyuna ve parlamentoya bilgi sunmayı amaçlamaktadır.

GENEL METODOLOJİ

Bu rehber, denetçilere bilişim sistemleri denetiminin nasıl planlanacağı, yürütüleceği ve raporlanacağı konusunda yol göstermek amacıyla hazırlanmıştır.

Rehberin hazırlanmasında, başta Bilgi Güvenliği Standartları (ISO 17799, ISO 27001 ..) olmak üzere INTOSAI rehber ve standartları, ISACA rehberleri ile diğer ülke ve ilgili kuruluş rehberlerinden yararlanılmıştır.

Rehber, bilişim sistemleri denetimi konusunda uzmanlaşmış denetçiler tarafından kullanılacağı ve onların da bilişim sistemleri denetimine ilişkin kavramlar konusunda belli düzeyde bilgiye sahip oldukları varsayımı ile hazırlandığından, kavramsal açıklamalara mümkün olduğunca yer verilmemiştir.

Bilişim sistemleri denetimi, denetlenmek istenen her tür bilgi sisteminde yapılabilir. Ancak bu rehber Sayıştay ihtiyaçları da göz önünde bulundurularak mali nitelikteki sistemlerde denetim yapılacağı varsayılarak hazırlanmıştır. Mali nitelikte olmayan bir sistemin denetimine ihtiyaç duyulması durumunda, rehberin mali nitelikteki sistemlerin belirlenmesine ilişkin hususları dışarıda bırakılarak rehberin diğer kısımları kullanılabilir.

Bilişim sistemleri denetimi, bir kurumun bilişim sistemlerinin tamamında yürütülebileceği gibi sadece yüksek riskli olarak görülen sistemler veya kontrol alanlarında da yürütülebilir. Bu durumda denetlenecek sistem veya kontrol alanları, risk değerlendirmesi yoluyla belirlenir. Bu rehberde, bilişim sistemleri denetimi, bir kurumun tüm sistemlerinin değerlendirilmesine imkan sağlayacak şekilde ele alınmıştır.

Rehberde, denetçinin adım adım hangi işleri nasıl yapacağını gösteren süreç odaklı bir yaklaşım benimsenmiş ve ağırlıklı olarak kontrol alanları bazında sistem kontrollerinin nasıl değerlendirileceği düzenlenmiştir.

Bu rehberin hazırlanmasında, Sayıştay ihtiyaçları göz önünde bulundurularak bilgi sistemlerinin güvenlik ve güvenilirliklerinin değerlendirilmesi hususlarına ağırlık verilmiş, sistemlerin verimlilik, etkinlik ve tutumluluklarının değerlendirilmesine daha az yer verilmiştir. Rehberde yer alan kontrol alanları ve buna bağlı kontroller teknolojinin hızlı değişimine paralel olarak değişkendir. Yapılacak denetimler esnasında bu alanlardaki değişikliklere uygun olarak "Denetim Programları" ile "Kontrol Setleri"nin değişeceği unutulmamalıdır. Ayrıca, yapılacak denetimin amacına göre verimlilik, etkinlik ve tutumluluğu değerlendirmeye ilişkin olarak ihtiyaç duyulan kontroller, program ve setlere ilave edilebilir.

Bilişim sistemleri denetimi yürütülürken risk tabanlı denetim yaklaşımına uygun olarak şu genel çerçeve izlenir;

- öncelikle incelenen bilişim sisteminden kaynaklanabilecek riskler belirlenir,
- bu riskleri minimize edecek kontrol mekanizmaları belirlenir,
- bu kontrol mekanizmalarının kurumun yapısı göz önünde tutularak oluşturulup oluşturulmadığı, oluşturulmuş ise etkin çalışıp çalışmadığı incelenir,
- inceleme sonrası, iç kontrollerdeki zayıflıklar değerlendirilir ve
- elde edilen bulgular belli bir prosedüre göre raporlanır.

Bu çerçevede rehber üç ana bölümden oluşturulmuştur:

"Denetimin Planlanması" başlıklı birinci bölümde, bilişim sistemleri denetiminin planlanması sırasında denetçinin yapacağı işler sistematik bir şekilde anlatılmaktadır. Bu işler, kurumun ve kurum bilişim sistemlerinin anlaşılması, sistem risk değerlendirmelerinin yapılması, denetim kapsamının ve uzman ihtiyacının belirlenmesi, denetim stratejisinin oluşturulması ve denetim programlarının hazırlanmasından oluşmaktadır.

"Sistem Kontrollerinin Değerlendirilmesi" başlıklı ikinci bölümde, kontrol değerlendirmeleri kontrol alanı bazında ele alınmaktadır. Her bir kontrol alanı için, kontrol hedefi, o alana ilişkin riskler ve bu riskleri minimize edecek kontrol faaliyetleri açıklanacak şekilde düzenlenmiş ve o alandaki kontrollerin varlığı ve etkinliğinin nasıl değerlendirileceği gösterilmiştir.

Denetim sonuçlarının raporlanması ve izlenmesini konu alan üçüncü bölümde ise, taslak raporun hazırlanması, kurum yöneticileriyle görüşme ve nihai raporun yazılması ve ilgili birimlere sunulması konuları açıklanmaktadır. Ayrıca raporda düzeltilmesi istenen hususların nasıl izleneceği ve denetim kalite kontrolünün nasıl yapılacağı konuları üzerinde durulmaktadır.

BİRİNCİ BÖLÜM
DENETİMİN PLANLANMASI

Denetim faaliyeti, denetimin planlanmasıyla başlar. Planlama, iyi bir denetimin anahtar unsuru olup, denetim süresince takip edilecek yol gösterici bir süreçtir. Planlama, denetçinin, denetlenen kurumun bilişim sistemlerine ilişkin kontrolleri değerlendirmek için denetim kanıtı toplamanın etkin ve verimli metotlarını belirlemesine imkan verir.

Planlama süreci, kurumun ve bilişim sistemlerinin tanınması, sistem risk değerlendirmesinin yapılması, denetim kapsam, yöntem ve stratejisinin oluşturulması, uzman kullanımı ihtiyacının belirlenmesi ve denetim programlarının hazırlanmasından oluşur.

1.1 BİLİŞİM SİSTEMLERİNİN ANLAŞILMASI

Denetçi denetlediği kurumun, mali raporlama ve iş yönetim süreci içerisinde kullanılan bilişim sistemi ve ana faaliyetleri hakkında yeterli düzeyde bilgi sahibi olmalıdır.

Kurumun tanınması ve bilişim sisteminin anlaşılması için denetçi öncelikle kurum ve bilişim sistemi ile ilgili olarak her türlü kaynaktan yararlanmak suretiyle bilgi toplamalıdır. Kurum ve bilişim sistemini tanımaya yönelik olarak aşağıdaki faaliyetler yürütülmelidir:

Bilişim Sistemlerini Oluşturan Unsurların Tanınması

Bilişim sistemleri, bir faaliyeti desteklemek amacıyla kurulan bilgisayar donanımı, yazılımı ile kaynak paylaşımını gerçekleştirmek için bilgisayarları birbirine bağlayan ağlar ve onları kullanan insanlardan oluşur. Bir sistemi anlamak için onu oluşturan unsurların tanınması gerekir. Bunun için kurum bilişim sistemlerinin donanım yapısı, kullanılan yazılımlar ve ağ yapısı incelenmeli sistemi işleten ve kullanan personel ile sisteme veri giriş yöntemleri konusunda bilgi edinilmelidir. Bu kapsamda hazırlanan "Bilişim Sistemleri Bilgi Edinme Formu" (Ek-1) bu amaçla kullanılır.

Denetlenen Kuruma İlişkin Temel Düzenlemelerin Belirlenmesi

Kurumun uyması gereken ve kurum bilişim sistemini etkileyebilecek olan her türlü düzenleme belirlenmeli ve incelenmek üzere not edilmelidir. Bunlar arasında kurumla ilgili mevzuat, stratejik planlar, yıllık programlar, faaliyet raporları ve bütçeler sayılabilir.

Önceki Dönem Denetim Raporlarından Bilgi Toplanması

Önceki dönemlerde yazılmış bağımsız bilişim sistemi denetim raporları, mali denetim raporları, mali denetim sürecinde hazırlanan denetim dosyaları ve iç denetim raporları incelenerek hem kurum bilişim sistemi hem de bilişim sistemine ilişkin kontrol faaliyetleri hakkında bilgi toplanmalıdır.

Kurumda daha önce Sayıştay tarafından bilişim sistemleri denetimi yapılmış ise bu denetim sonucunda hazırlanmış olan İzleme Tabloları elde edilir ve değerlendirilir.

Kurum İş Süreçlerinin Belirlenmesi

İş akış şemaları, iş süreçlerinde; süreç adımlarının, otomatik/manuel kontrollerin, sürecin özel durumlarını da gösteren alternatif akış yollarının, paralel işleyen adımların gösterildiği diyagramlardır.

Denetçinin, bilişim sistemlerindeki veri işleme süreçlerini anlayabilmesi için; kurumun faaliyet gösterdiği alanları, gerçekleştirdiği işleri ve iş akışlarını tanıması gerekir. Bunun için denetçi, kurumun hazırladığı iş akış şemalarından yararlanır. İş akış şemaları mevcut değilse, denetçi bu şemaların hazırlanmasını talep eder ve hazırlık sürecine refakat eder. Gerekiyorsa denetçi, iş akış şemalarını bizzat kendisi çıkararak kurumun iş süreçlerini belirler. Bu belgeler denetimin yürütülmesi için ihtiyaç duyulacak temel kaynaklardandır.

İş akış şemaları, yapılan işlerin her bir aşamasını gösterecek ayrıntıda olmalıdır. Bu şemalar oluşturulurken, bunların anlaşılır olmasına, farklı akış yollarının gösterilmesine ve gerekli yerlerde referansların belirtilmesine özen gösterilmelidir. Ayrıca iş akış şemalarında, yapılan işin kurumun hangi birimi tarafından ve hangi sistem kullanılarak yapıldığı da görülebilmelidir. Şemalarda süreçlerin hangilerinin manuel, hangilerinin bilişim ortamında yürütüldüğü gösterilmelidir.

Denetçi, kurum iş akışlarını incelerken, iş süreçlerinde oluşturulmuş kontrolleri belirleyerek daha sonra sistem kontrollerini incelerken kullanmak üzere not etmelidir.

İş akış şemalarının mevcut olmaması denetim sürecini geciktirebileceğinden, kurumdan mümkün olduğu kadar erken bir safhada talep edilmelidir.

Bilişim Ortamında Gerçekleştirilen İşlerin Belirlenmesi

Kurum iş süreçleri belirlendikten sonra kurum tarafından yürütülen işlerden hangilerinin bilişim ortamında gerçekleştirildiği belirlenmelidir. Ayrıca muhasebeyi ve hesap alanlarını etkileyen sistemlerin de belirlenmesi gerekir. Bu amaçla, "Bilişim Sistemlerinden Etkilenen Hesap Alanlarının Belirlenmesi Formu" (EK-2) kullanılmalıdır.

Üçüncü Taraflarla İlişkilerin Belirlenmesi

Kurumun üçüncü taraflarla, özellikle kamu kurumları ile ilişkisi tanımlanmalıdır. Bu ilişkinin iş süreçleriyle bağlantısı incelenmeli ve bilişim sistemleri bazındaki ilişki üzerinde yoğunlaşılmalıdır.

Servis, bakım ve destek ilişkileri genel hatlarıyla ortaya konmalı, ilgili sözleşmeler temin edilmelidir.

1.2 SİSTEM RİSK DEĞERLENDİRMESİNİN YAPILMASI

Kurumun hangi işlemleri bilişim ortamında yaptığı ve bunların mali tabloları ve hesap alanını etkileyip etkilemediği tespit edildikten sonra, belirlenen sistemlerin risk değerlendirmesi yapılmalıdır. Denetimin planlaması aşamasında yapılacak risk değerlendirmesi, sistemler tek tek ele alınmak suretiyle ve "Sistem Risk Değerlendirme Formu" (EK-3) yardımıyla yapılacaktır.

Sistem Risk Değerlendirme Formu'nda risk faktörleri beş temel kriter altında toplanmış ve toplam risk içerisindeki yüzde ağırlıkları tespit edilmiştir:

- Önemlilik (%36)
- Kritiklik (%20)
- Karmaşıklık (%16)
- Teknik altyapı (%16)
- Kontrol çevresi (%12)

Risk ağırlık yüzdelerinin kriterlere dağılımı sabittir. Ancak risk değerlendirme formu hem objektif hem de subjektif unsurlar içerdiğinden denetçinin bu değerlendirme formu üzerinde

kendi muhakemesiyle, söz konusu denetime münhasır hususiyetleri dikkate alarak birtakım değişikler yapma imkanına sahiptir. Bu çerçevede, toplam ağırlık yüzdesi değişmeyecek şekilde, her bir risk faktörünün ağırlığını yeniden belirleyebileceği gibi yeni risk faktörü ekleyerek de bu ağırlıkları yeniden belirleyebilir.

Risk faktörlerinin risk puanları, belirlenen puan ve ağırlıklara göre tespit edilir. Beş ayrı kriterde ve toplamda risk puanları hesaplanır ve "Risk Değerlendirme Matrisi" (EK-4) yardımıyla sistemin riskinin hangi kriterde yoğunlaştığı tespit edilir ve toplam risk derecesi belirlenir.

Bütün sistemlerin risk değerlendirmesi yapıldıktan sonra, sistemler toplam risk puanları dikkate alınarak "Risk Derecelendirme Formu"nda (EK-5) sıralandırılır.

1.3 DENETİM KAPSAMININ BELİRLENMESİ

Risk Derecelendirme Formu'nda yapılan sıralama, hangi sistemlerin denetim kapsamına alınacağını belirlemede en önemli unsur olacaktır. Denetçi, bu bilgiler ışığında uygulanacak genel kontrollerle birlikte uygulama kontrolleri açısından hangi sistemlerin ayrıntılı incelemeye alınacağına karar verir.

Denetçi, risk değerlendirmesi ile birlikte daha önce kurum ve kurum bilişim sistemlerine ilişkin elde etmiş olduğu bilgiler, denetim amacı ve inceleme yapabileceği zaman gibi unsurları da göz önüne alarak denetimin kapsamını belirler.

1.4 UZMAN İHTİYACININ BELİRLENMESİ

Bilişim sistemlerinin denetiminde aşağıda belirtilen sebeplerle uzman çalıştırılmasına ihtiyaç duyulabilir:

- Bilişim sistemlerinin teknik ve karmaşık unsurlarının değerlendirilmesinde denetim ekibinde yeterli nitelikte denetçinin bulunmaması durumunda uzman desteği alma,
- Özel uzmanlık gerektiren alanlarda kurum dışı uzmanlık ve tecrübelerden yararlanma,
- Yeni yaklaşım ve farklı bakış açılarından yararlanma,
- Kurum dışında geliştirilmiş iyi uygulamaları denetimde kullanma,
- Denetim kanıtlarının, bulguların ve geliştirilen önerilerin ağırlık ve kalitesini arttırma,
- Denetim süresinin sınırlı olması durumunda denetimi zamanında tamamlama

Uzman ihtiyacının belirlenme zamanı

Bilişim sistemleri denetimlerinde uzman çalıştırılıp çalıştırılmayacağı, denetime başlamadan, önceki denetim tecrübelerinden yararlanarak planlanabilir. Bu durumda, uzman çalıştırılmasına ilişkin süreç zaman alabileceğinden, denetim başlamadan önce uzman çalıştırılmasına ilişkin hazırlıklar tamamlanmalıdır.

Uzman çalıştırma ihtiyacı denetim başladıktan sonra bilişim sistemlerinin tanınması aşamasında ortaya çıktı ise, denetim stratejisi hazırlanmadan önce uzman çalıştırılacak şekilde sürecin başlatılmasına dikkat edilmelidir.

Uzman çalıştırılacak alanların kapsamının ve süresinin belirlenmesi

Uzman desteğine ihtiyaç duyulması halinde, uzman desteğinin hangi alanlarda nasıl alınacağı şartnamede açıkça belirtilmelidir.

Şartnamede aşağıda belirtilen hususlara yer verilmelidir:

- Çalışmanın amacı, kapsamı ve süresi,
- Özel çalışma yapılacak alanlar,
- Uzmanın hangi sistemlerde hangi bilgilere erişebileceği,
- Denetim ekibi ile uzmanın birlikte çalışma esasları ve iletişimin nasıl sağlanacağı,
- Denetlenen kurum ile uzman arasındaki ilişkilerin nasıl sağlanacağı,
- Denetlenen kurum bilgilerinin gizliliği ve uyulması gereken kurallar,
- Uzman tarafından kullanılacak metotlar,
- Uzman çalışmalarının sonuçlarının nasıl raporlanacağı

Uzmanda aranacak nitelikler

Uzman çalıştırılırken, uzmanın çalışacağı alandaki yeterliliği değerlendirilmelidir. Uzmanın konusunda yetkin ve tecrübeli olmasına özen gösterilmelidir. Uzmanın çalıştırılacağı alanla ile ilgili uzmanlık sertifikalarının bulunup bulunmadığı ve daha önceki çalışmalarına ilişkin referansları incelenmelidir. Ayrıca uzmanın tarafsız olmasına ve denetlenen kurumla ve bu kurumla bağlantısı olan kuruluşlarla herhangi bir ticari ilişkisinin bulunmamasına dikkat edilmelidir.

Uzman çalışmalarının değerlendirilmesi

Denetçi, uzman tarafından yapılan çalışmaları inceleyerek çalışma sonuçlarını değerlendirmelidir. Değerlendirme yapılırken aşağıdaki hususlar göz önünde bulundurulmalıdır:

- Çalışmanın uzman çalıştırmaya ilişkin şartnameye uygunluğu,
- Uzman tarafından kullanılan kaynak verilerin yeterliliği,
- Kullanılan metotların ve denetim kanıtlarının uygunluğu,
- Çalışma zamanlarının ve sürelerinin uygunluğu,
- Çalışma sonuçlarının ve bulguların diğer çalışmalara uygunluğu,

Uzman çalıştırılırken denetim sürecine göre aşağıdaki hususlara da dikkat edilmelidir.

Planlama aşamasında, denetçi ile uzman, kurumu ve bilişim sistemlerini tanıma, risk değerlendirmesi yapma ve ayrıntılı çalışma alanlarının belirlenmesi çalışmalarını birlikte değerlendirilerek denetim stratejisini oluşturmalı ve uygulanacak test talimatlarını belirlemelidir.

Sistem kontrollerinin değerlendirilmesi aşamasında, uzmanın sistemlerde yapacağı testler ve diğer çalışmalar denetçi refakatinde yerine getirilmelidir.

Raporlama aşamasında, uzman çalışmalarının sonuçları ve raporları uzmanla birlikte değerlendirilerek Bilişim Sistemleri Denetim Raporuna alınacak hususlar belirlenmelidir.

1.5 DENETİM STRATEJİSİNİN OLUŞTURULMASI

Kurumun ve kurum bilişim sistemlerinin tanınması, risk değerlendirmesinin yapılması ve denetim kapsamının belirlenmesi sonrasında denetimin nasıl yürütüleceğini gösteren denetim stratejisinin oluşturulması gerekir. Bu nedenle Denetim Strateji Belgesi hazırlanır.

Kurumu bilgilendirmek ve yapılacak denetimin sağlıklı yürütülmesi için gerekli hazırlıkların kurumca yapılmasını sağlamak amacıyla "Denetim Strateji Belgesi" kurum yönetimine verilir.

Denetim strateji belgesi, aşağıda belirtilen unsurları içerecek şekilde hazırlanmalıdır:

- Denetim sürecini gösteren tarihler
- Denetimin amacı ve metodolojisi
- İncelenecek sistemler
- İncelemeleri yapacak denetçiler ve uzmanlar
- İnceleme yapılacak yerler
- İnceleme süresi
- Erişim yetkileri
- Yerinde yapılacak testlerin ve denetim çalışmalarının kurum faaliyetlerine olası etkileri

Yapılacak incelemelerin kapsamı ve süresi, incelenecek sistemlerin donanımının, kullanıcılarının ve bu sistemleri işleten ve destekleyen kurum personelinin bulunduğu mekanlara göre değişebilir.

Denetim stratejisinin kuruma verilmesi sonrasında, incelenecek her sistemin sorumlusu ve yöneticisinin de içerisinde bulunduğu bir ekip belirlenmeli ve bu ekiple bir çalışma programı oluşturulmalıdır. Bu programda;

- sorumlu personelin isimleri ve iletişim bilgileri,
- katılımcı listesi,
- inceleme tarihleri,
- kapanış toplantılarının tarihleri,
- bulguları tartışma tarihleri ve
- taslak raporun tartışılma tarihleri

belirtilmelidir.

1.6 DENETİM PROGRAMININ HAZIRLANMASI

Denetçi, sistem kontrollerinin incelemesine geçmeden önce hangi kontrol alanlarını inceleyeceğini, inceleme esnasında hangi kontrollerin varlığını arayacağını ve eğer varsa ilgili kontrollerin etkin çalışıp çalışmadığını hangi yöntemleri kullanarak test edeceğini belirlemelidir. Bunu yapabilmek için "Denetim Programı Formu" (EK-11) kullanılarak kuruma özgü denetim programları hazırlanır. Programların hazırlanmasında, rehberin "Sistem Kontrollerinin Değerlendirilmesi" bölümünde yer alan her bir kontrol alanına ilişkin "Kontrollerin Değerlendirilmesi" başlıklı kısımda belirtilen yöntemlerden yararlanılır. Kontrol değerlendirme yöntemleri denetçiyi sınırlayıcı olmayıp sistem kontrollerinin değerlendirilmesi için asgari bir çerçeve sunmaktadır.

İKİNCİ BÖLÜM - SİSTEM KONTROLLERİNİN DEĞERLENDİRİLMESİ

Yapılacak bilişim sistemleri denetiminin planlaması tamamlandıktan sonra, incelenen kurum veya sisteme özgü olarak kontrol alanları itibariyle hazırlanan denetim programları yardımıyla sistem kontrolleri değerlendirilir. Sistem kontrollerinin değerlendirilmesi esnasında sistemin iç kontrol zayıflıklarına ilişkin kanıt toplanır.

Sistem kontrollerinin değerlendirilmesinde üç aşamalı bir süreç izlenmelidir:

- Kontrol varlığının belirlenmesi
- Kontrol etkinliğinin değerlendirilmesi
- Bulguların değerlendirilmesi

Kontrol Varlığının Belirlenmesi

İnceleme faaliyetleri sırasında her bir kontrol alanına ilişkin yapılacak toplantılar öncesinde kurumun ilgili kontroller konusunda bilgilenmesinin ve toplantılara hazırlıklı gelinmesinin sağlanması için denetim programlarında yer alan kontrol değerlendirme sorularını içeren "Kontrol Setleri" hazırlanarak ilgililerine verilir. Bu kontrol setleri olması gereken kontroller, değerlendirme soruları, kurum cevabı ve kurumdan istenen kanıtlayıcı belgeleri içerecek şekilde düzenlenmelidir. Bu amaçla"Kontrol Seti Formu" (EK-12) kullanılır.

Sistem kontrolleri incelenirken öncelikle kontrol alanları itibariyle olması gereken kontrollerin var olup olmadığı araştırılmalıdır. Bunun için yapılan çalışma programına uygun şekilde, her bir kontrol alanına ilişkin olarak hazırlanmış ve kuruma önceden verilmiş olan kontrol setleri temelinde ilgililerle toplantılar yapılmalıdır. Bu toplantılarda kontrollerin varlığına ilişkin kurum cevapları kanıtlayıcı belgelerle birlikte alınmalıdır. Alınan cevaplar ve kanıtlayıcı belgelerin incelenmesi sonrasında ilgili kontrollerin var olup olmadığı, o kontrole ilişkin riskler ve bu risklerin nasıl yönetildiğine ilişkin telafi edici kontrollerin var olup olmadığı da dikkate alınarak belirlenmelidir. Kontrol varlığına ilişkin elde edilen bulgular denetim programı formunda yer alan "Bulgular" sütununda gösterilir. İlgili kontrollerin var olup olmadığını gösteren kanıtlayıcı belgelere ve eğer değerlendirme için ayrı çalışma kağıtları düzenlendiyse bunlara da ilgili "Referans" sütununda yer verilmelidir.

Kanıtlayıcı belgeler kontrol alanları itibariyle numaralandırılarak düzenli bir şekilde arşivlenmelidir.

Kontrol Etkinliğinin Değerlendirilmesi

Olması gereken kontrolün var olup olmadığı belirlendikten sonra, bu kontrolün etkinliği değerlendirilmelidir. Kontrol etkinliğinin değerlendirilmesi, denetim programı formunda yer alan ilgili "Kontrol Etkinliğini Belgeleme ve İnceleme Yöntemi" sütununda belirlenen yöntemlerle yapılır. Bu değerlendirmeler sonucu tespit edilen kontrol zayıflıklarına kanıtlarıyla birlikte denetim programı formunun "Bulgular" sütununda yer verilmelidir. Ayrıca kontrol etkinliğinin değerlendirilmesi sırasında uzman desteğinde yapılacak teknik testlere ilişkin raporların incelenmesi sonrasında elde edilen bulgular da bu bölüme yazılır. İlgili çalışma kağıtları, uzman raporları ve kanıtlayıcı belgeler "Referans" sütununda belirtilmelidir.

Bulguların Değerlendirilmesi

İncelemeler sonunda elde edilen bulgular, denetçi tarafından, yeterli kanıt toplanıp toplanmadığı açısından değerlendirilerek ek incelemeye ihtiyaç olup olmadığı belirlenmeli ve gerekli ek incelemeler yapılarak inceleme süreci tamamlanmalıdır.

Bulgu bir kontrol eksikliğini ya da mevcut bir kontrol zayıflığını ifade etmektedir ve her bir denetim bulgusu kurumun bilgi varlıklarına yönelik bir riski içermektedir. Her bir kontrol alanı itibariyle bulguların risk düzeyleri belirlenerek bulgular arasında derecelendirme yapılmasına ve denetim bulgularının genel değerlendirmesine imkan sağlanır.

Bulguların risk değerlendirmesi, tespit edilen bulgunun ortaya çıkardığı riskin etki düzeyi ile risk gerçekleşme olasılığı birlikte değerlendirilerek yapılmaktadır.

Etki kavramı, aşağıdaki unsurların birini, birkaçını ya da tümünü içerir;

- kurumun bilgi varlıklarının güvenliğine, bütünlüğüne ve kullanılabilirliğine olan etki
- sistemin işleyişine olan etki
- sahteciliğin ve yolsuzluğun meydana gelme ihtimali
- kurumun mali tablolarına olan etki ve ortaya çıkabilecek muhtemel mali kayıplar
- kontrol eksikliğinin ya da zayıflığının ne kadar süre içinde giderilmesi gerektiği (tedbir alma konusundaki aciliyet)

Gerçekleşme olasılığı, belli bir zaman dilimi içerisinde bu riskin gerçekleşmesi ihtimalini ifade eder.

Elde edilen her bir bulguya ilişkin risk düzeyi, yukarıda tanımlanan kriterler ışığında belirlenen etki düzeyi ve gerçekleşme olasılıkları göz önünde bulundurularak ve "Bulgu/Risk Değerlendirme Matrisi" (EK-6) kullanılarak denetçi tarafından belirlenmektedir.

Kontrol alanları itibariyle elde edilen bulgular, olası etkileri, denetçi önerileri ve risk düzeyini de içerecek şekilde "Bulgu Değerlendirme Formu" (EK-7) düzenlenerek ilgili kurum personeliyle görüşülmek üzere kuruma verilmelidir. Daha sonra, ilgili kurum personeli ile kapanış toplantıları yapılarak, bulgulara ilişkin kurum görüşleri alınmalıdır. Kurum görüşleri alındıktan sonra bulgular yeniden gözden geçirilerek rapora alınacaklar belirlenmelidir.

Rapora alınacak bulgular, raporda riski daha iyi belirtmek ve sunum kolaylığı sağlamak için kontrol alanları itibariyle sınıflandırılmalıdır. Bunun için "Bulgu Özet Tablosu Formu" (EK-8) kullanılarak her bir kontrol alanı için elde edilen bulgu sayısı, bunların risk düzeylerine göre sayısı ile mali tabloları doğrudan etkileyenlerin sayısı belirlenmelidir.

Sistem kontrollerinin değerlendirilmesi kontrol alanları itibariyle yapılır. Kontrol alanları, genel ve uygulama kontrolleri olmak üzere iki ana başlık altında gruplandırılır.

2.1 GENEL KONTROLLERİN DEĞERLENDİRİLMESİ

Genel Kontroller, kuruma ait tüm bilişim sistemleri faaliyetlerinin sürekliliğinin sağlanmasına yönelik yapı, yöntem ve prosedürlere ilişkin kontrollerdir. Bu kontroller uygulama yazılımları ve bunlara ilişkin kontroller için güvenli bir ortam oluşturur. Genel kontroller aşağıda yazılı kontrol alanlarından oluşur:

- Yönetim Kontrolleri
- Fiziksel ve Çevresel Kontroller
- Ağ Yönetimi ve Güvenliği Kontrolleri
- Mantıksal Erişim Kontrolleri
- İşletim Kontrolleri
- Sistem Geliştirme ve Değişim Yönetimi Kontrolleri
- Acil Durum ve İş Sürekliliği Planlaması Kontrolleri

2.1.1 YÖNETİM KONTROLLERİ

Kurum yönetimi, bilişim sisteminin kurum amaçlarına uygun çalışmasını ve işlevlerini doğru bir şekilde yerine getirmesini sağlayacak tedbirleri almakla yükümlüdür. Yönetim kontrollerinin amacı güvenli ve yeterli bir bilişim ortamının sağlanması için uygun politika ve prosedürler oluşturmaktır. Bu kontroller denetçiye alt düzeydeki ayrıntılı kontrollerin varlığı ve etkinliği konusunda makul bir güvence sağlar. Yönetim kontrolleri, stratejik planlama, güvenlik politikaları, organizasyon, varlık yönetimi, personel ve eğitim politikaları ile yasal düzenlemelere uygunluk alanlarından oluşur.

2.1.1.1 STRATEJİK PLANLAMA

Kontrol Hedefi	Bilişim sistemlerine ilişkin tüm faaliyetlerin, kurumun stratejik amaç ve hedefleri doğrultusunda ve risk değerlendirmesi çerçevesinde yürütülmesini sağlamaktır.
Riskler	Kurumun bilişim sistemlerine ilişkin stratejik planlama yapamaması şu riskleri ortaya çıkarır: ▪ Bilişim sistemleri ihtiyaçlarının, kurumsal amaç ve hedeflere uygun olarak karşılanmaması ▪ Kurum ihtiyaçlarının BS yönetimi tarafından anlaşılamaması veya yeterli düzeyde karşılanamaması ▪ İş önceliklerinin doğru tanımlanamaması ve kaynakların yanlış tahsis edilmesi ▪ BS yetkinliğine ilişkin yeni fırsatların fark edilemeyerek kaçırılması ▪ Kurumun karşı karşıya kalacağı tehlikelerin belirlenememesi, etkilerinin ölçülememesi ve riskin yönetilememesi ▪ Her riskin etkisinin sadece bir güvenlik olayı gibi algılanması nedeniyle BS varlıklarının bütünlük veya güvenilirliğine zarar gelmesi

- Tesis edilmiş olan zayıf kontrollere aşırı güven
- Kaynakların riskleri karşılamak için etkin kullanılamaması
- Risklerin azaltılmasına yönelik kontrollerin amaçlandığı gibi işlememesi
- Üst yönetimin, kurumun bilişim sistemlerine ilişkin alınacak önemli kararlarda etkin bir rol alamaması
- Bilişim sistemlerine ilişkin faaliyetlerde koordinasyon sorunlarının ortaya çıkması
- BS bütçesi üzerinde zayıf kontrol

Temel Kontroller

Bilişim sistemlerinin stratejik planlamasının yapılamaması durumunda ortaya çıkacak riskleri minimize edecek temel kontroller şunlardır:

- Kurumun bilişim sistemlerine ilişkin yazılı bir stratejisi ve bu stratejinin uygulanmasına ilişkin planları olmalıdır.
- Bilişim sistemlerinin stratejik planlamasının yapılması ve koordinasyonun sağlanması için bir bilişim sistemleri yönlendirme kurulu olmalıdır.
- Bilişim sistemine ilişkin düzenli olarak risk değerlendirilmesi yapılmalıdır.

Kontrollerin Değerlendirilmesi

Risk değerlendirmesi

Kontrol

SP-1 Bilişim sistemine ilişkin riskler düzenli olarak değerlendirilmeli ve stratejik planlama çerçevesinde dikkate alınmalıdır.

Kontrol varlığını değerlendirme soruları

- Görevli bir birim tarafından düzenli olarak risk değerlendirmesi yapılıyor mu?
- Bilişim sistemleri güvenliğine ilişkin risk kütüğü tutuluyor mu?
- Risk değerlendirmeleri ve yönetim tarafından alınan kararlar/tedbirler bilişim sistemleri stratejisi ve kısa dönemli planlara yansıtılmış mı?

Kontrol etkinliğini inceleme yöntemi

- Risk değerlendirmesine ilişkin faaliyetler ve risk kütüğünün genel risk kütüğü kayıtlarıyla uyumluluk, önceliklendirme ve risk sorumluları itibariyle incelenmesi
- Yapılan risk değerlendirmelerinin bilişim sistemleri stratejisinin hazırlanmasında ve uygulanmasında dikkate alınıp alınmadığının değerlendirilmesi

Bilişim sistemleri stratejisi

Kontrol

SP-2 Kurumun bilişim sistemlerine ilişkin yazılı bir stratejisi olmalıdır.

Kontrol varlığını değerlendirme soruları

- Kurumun, üst yönetim tarafından onaylanmış bilişim sistemlerini de kapsayan yazılı bir strateji bildirimi var mı?
- Düzenli aralıklarla gözden geçiriliyor mu?

- Hazırlanması ve uygulamaya geçirilmesine ilişkin prosedürler var mı?
- Strateji, kısa dönemli planlar ile uygulamaya geçirilebilecek detayda tasarlanarak eylem planları yapılmış mı?

Kontrol etkinliğini inceleme yöntemi

- Kurum strateji planı ve bilişim sistemleri strateji planının incelenerek kurum bilişim sistemlerinin kurum amaçları doğrultusunda, gerçekleştirilecek faaliyetleri ve başarı göstergelerini de içerecek şekilde planlı olarak geliştirilip geliştirilmediğinin incelenmesi
- Bilişim Sistemleri Stratejisinin kısa dönem planlar ve bütçeyle ilişkilendirilip ilişkilendirilmediğinin incelenmesi
- Stratejide ortaya konulan eylem planına uyulup uyulmadığının incelenmesi
- Bilişim sistemleri stratejisinde bilgi güvenliğine ilişkin hususlara yer verilip verilmediğinin incelenmesi

Bilişim sistemleri yönlendirme kurulu

Kontrol

SP-3 Kurumun bilişim sistemlerine ilişkin stratejik planlamanın yapılması için bilişim sistemleri yönlendirme kurulu olmalıdır.

Kontrol varlığını değerlendirme soruları

- Kurumun bilişim sistemleri yönlendirme kurulu var mı?
- Yönlendirme kurulunun oluşumuna ve faaliyetlerini icra etmesine ilişkin düzenlemeler var mı?

Kontrol etkinliğini inceleme yöntemi

- Üst yönetim ve önemli birimlerin yöneticilerinin bilişim sistemleri yönlendirme kuruluna katılımının ve toplantı tutanaklarının incelenmesi
- Kurulun, teknik konulara ilişkin olarak teknik düzeyde bilgi sahibi kişilerden oluşan ayrı kurul ya da komisyonlardan destek alıp almadığının incelenmesi
- Kurulun, kurumun stratejik planlarının bilişim sistemlerini ilgilendiren kısımlarının ve bilişim sistemleri stratejisinin hazırlanmasında oynadığı rolün değerlendirilmesi

2.1.1.2 GÜVENLİK POLİTİKALARI

Kontrol Hedefi

Kurumun iş gerekleri ve ilgili mevzuatına uygun şekilde, bilgi güvenliğini destekleyecek politika ve prosedürleri belirlemek ve uygulanmasını sağlamaktır.

Riskler

Kurum yönetiminin bilişim sistemi güvenliği ile ilgili kurumsal politikaları ve düzenlemeleri yapmaması durumunda karşılaşılabilecek temel riskler şunlardır:

- Güvenliğe ilişkin olaylara zamanında ve uygun karşılık verilememesi
- Kontrol ve güvenlik kültürünün zayıflayarak aksaklıklara neden olması
- Tehditlerin zamanında belirlenememesi ve ihlallerin artması

- Güvenlik Politikasının gereklerinin aşırı maliyetli olması
- Personelin bilgi güvenliği bilincine sahip olmaması
- Güvenlik politikalarının sahipsiz kalması, güncellikten uzaklaşması ve yazılı hale getirilememesi

Temel Kontroller

Bilgi güvenliği politikalarına ilişkin riskleri minimize edecek temel kontrol faaliyetleri şunlardır:

- Kurum bilişim sistemine ilişkin yazılı bir bilgi güvenliği politikasına sahip olmalıdır.
- Yazılı güvenlik politikası üst yönetim tarafından onaylanmış ve basılıp tüm personele dağıtılmış olmalıdır.
- Güvenlik politikasının amacı ve kapsamı açıkça ifade edilmiş, politikaları uygulayacak personel ve sorumlulukları belirlenmiş ve diğer destekleyici düzenlemelerle ilgileri kurulmuş olmalıdır.
- Güvenlik politikaları belirli aralıklarla güncellenmelidir.

Kontrollerin Değerlendirilmesi

Bilgi güvenliği politika belgesi

Kontrol

GP-1 Kurum, bilişim sistemine ilişkin yazılı bir bilgi güvenliği politikasına sahip olmalıdır.

Kontrol varlığını değerlendirme soruları

- Kurumun yazılı bir bilgi güvenliği politikası var mı?
- Yazılı güvenlik politikası üst yönetim tarafından onaylanmış mı?
- Güvenlik politika belgesi basılıp tüm personele dağıtılmış mı?

Kontrol etkinliğini inceleme yöntemi

- Kurumun yazılı bilgi güvenliği politika belgesinin aşağıdaki hususlar dikkate alınarak incelenmesi:
  - Güvenlik politika belgesinin tüm personel tarafından anlaşılır bir dille yazılıp yazılmadığı
  - Güvenlik politikalarının amacının, kapsamının ve hangi birimlerin uygulayacağının açık bir şekilde ifade edilip edilmediği
  - İlgili güvenlik tedbirlerine uyulmaması durumunda, karşılaşılabilecek risklerin açıkça belirtilip belirtilmediği
  - Güvenlik politikalarını destekleyen diğer politika ve prosedürlere atıfta bulunulup bulunulmadığı
- Bilgi Güvenliği politika belgesinin aşağıdaki konuları da içerip içermediğinin incelenmesi:
  - E-posta politikası
  - Şifre politikası
  - Kötü niyetli yazılımlardan korunma politikası
  - İnternet erişim ve kullanım politikası

- Sunucu güvenlik politikası
- Güvenlik açıkları tespit etme politikası
- Ağ cihazları güvenlik politikası
- Ağ yönetimi politikası
- Uzaktan erişim politikası
- Sanal özel ağ (VPN) politikası
- Risk değerlendirme politikası
- Kablosuz iletişim politikası
- İnternet DMZ cihazları politikası
- Bilgi sistemlerinin genel kullanım politikası
- Donanım ve yazılım envanteri oluşturma politikası
- Kriz/acil durum yönetimi politikası
- Fiziksel güvenlik politikası
- Kimlik doğrulama ve yetkilendirme politikası
- Veri tabanı güvenlik politikası
- Değişim yönetimi politikası
- Bilgi sistemleri yedekleme politikası
- Personel güvenliği politikası
- Bakım politikası
- Kişisel kayıtların güvenliği politikası

▪ Personelin politika belgesine kolayca ulaşmasını sağlayacak bir dağıtım ve duyuru prosedürünün bulunup bulunmadığının incelenmesi

▪ Örnekleme yoluyla seçilecek personelle, güvenlik politikalarından haberdar olup olmadıkları konusunda görüşme yapılması

Üst yönetim

Kontrol	**GP-2** Üst yönetim bilgi güvenliği politikalarını sahiplenmelidir.
Kontrol varlığını değerlendirme soruları	▪ Bilgi güvenliğine ilişkin politikaların uygulanmasından sorumlu bir üst düzey yönetici var mı?
Kontrol etkinliğini inceleme yöntemi	▪ Bilgi güvenliği politikalarından sorumlu üst düzey bir yöneticinin bulunup bulunmadığının organizasyon şeması ve görev dağılımı yazıları incelenerek tespit edilmesi

Güncelleme

Kontrol	**GP-3** Bilgi güvenliği politikaları belirli aralıklarla güncellenmelidir.
Kontrol varlığını değerlendirme soruları	▪ Bilgi güvenliği politikaları belirli aralıklarla güncelleniyor mu?
Kontrol etkinliğini	▪ Bilgi güvenliği politika belgesinin en son ne zaman

inceleme yöntemi	güncellendiğinin bir önceki belge ile karşılaştırılarak kontrol edilmesi ▪ Mevzuatta bilgi güvenliğini ilgilendiren bir değişiklik varsa, bunun politika belgesine yansıtılıp yansıtılmadığının incelenmesi

Uygulama

Kontrol	**GP-4** Bilgi güvenliği politikaları uygulanmalıdır.
Kontrol varlığını değerlendirme soruları	▪ Bilgi güvenliğine ilişkin politikaların personel tarafından yerinde uygulanmasını sağlayacak süreç ve prosedürler oluşturulmuş mu?
Kontrol etkinliğini inceleme yöntemi	▪ Personelin uyması gereken bazı prosedürlerin seçilip, bunlara uyulup uyulmadığının gözlemlenmesi

2.1.1.3 ORGANİZASYON

Kontrol Hedefi	Kurum içinde bilgi güvenliğini sağlayacak bir organizasyon yapısının kurulmasını ve etkin yönetilmesini sağlamaktır.
Riskler	Bilgi güvenliği konusunda yetersiz örgütlenmeden kaynaklanabilecek temel riskler şunlardır: ▪ Sorumluluklarda karmaşa, aşırı yetki verme veya hiç yetki vermeme durumlarının oluşması ▪ Kurumun karşı karşıya kalacağı tehlikelerin belirlenememesi, etkilerinin ölçülememesi ve riskin yönetilememesi ▪ Prosedür ve süreçlerin aksaması ve faaliyetlerde karmaşa yaşanması ▪ Yönetimin amaçları ile kontrol kültürlerinin örtüşmemesi ▪ Personelin iş tatmininin yönetim zafiyeti ve yetersiz gözetimden kaynaklanan nedenlerle sağlanamaması ▪ Kurum tarafından belirlenen politikaların anlaşılamaması veya kabul görmemesi ▪ Esnek olmayan bir BS organizasyon yapısı ▪ Yapılan işlemlerde mükerrerliklerin ve boşlukların meydana gelmesi ▪ İhtiyaçların belirlenmesinde etkin ve verimli bir yapının tesis edilememesi ▪ Yetersiz personel istihdamı ▪ Uygun olmayan görev ayrımlarının yapılması ▪ Zayıf hizmet sunumu ▪ Zayıf bilişim sistemleri güvenliği
Temel Kontroller	Kurum bilişim sistemlerine ilişkin organizasyonun yeterli düzeyde kurulamaması sonucu meydana gelecek riskleri minimize edecek temel

kontrol faaliyetleri şunlardır:

- Kurum, bilişim sistemlerinin etkin bir şekilde yönetilmesini sağlayacak organizasyon yapısına sahip olmalıdır.
- Bilgi güvenliğine ilişkin faaliyetler iyi bir şekilde koordine edilmelidir.
- Bilgi güvenliğine ilişkin görev ve sorumluluklar açıkça belirlenmelidir.
- Bilgi işlem sürecinde, yönetici yetkisi prosedürü belirlenmiş olmalıdır.
- Bilişim sistemleri bağımsız bir şekilde denetlenmelidir.
- Bilişim sistemleri ile ilgili üçüncü kişilerden mal ve hizmet alımlarında, ilgili sözleşmelerine bilgi güvenliğine ilişkin hükümler konulmalıdır.
- Diğer kurum ve kuruluşlarla işbirliği yapılması halinde bilgi güvenliğini sağlayacak tedbirler alınmalıdır.

Kontrollerin Değerlendirilmesi

Organizasyon yapısı

Kontrol	**BSO-1** Kurum, bilişim sistemlerinin etkin bir şekilde yönetilmesini sağlayacak organizasyon yapısına sahip olmalıdır.
Kontrol varlığını değerlendirme soruları	▪ Kurumun bir bilgi işlem birimi var mı? ▪ Bilgi işlem birimi, bilgi güvenliğini sağlayacak şekilde örgütlenmiş mi?
Kontrol etkinliğini inceleme yöntemi	▪ Bilgi işlem biriminin, işlevlerini (genel yönetim, ağ yönetimi, sistem yönetim ve güvenliği, program yönetimi, yazılım geliştirme, teknik destek vb.) yerine getirecek şekilde iyi örgütlenip örgütlenmediğinin incelenmesi ▪ Bilgi işlem biriminin, işlerini iş akışlarına uygun şekilde yapıp yapmadığının incelenmesi ▪ Bilgi işlem biriminin organizasyon şemasının incelenmesi

Bilgi güvenliği koordinasyonu

Kontrol	**BSO-2** Bilgi güvenliğine ilişkin faaliyetler iyi bir şekilde koordine edilmelidir.
Kontrol varlığını değerlendirme soruları	▪ Kurumun bilgi güvenliğinin sağlanması konusunda koordinasyonu sağlayacak bir bilgi güvenliği koordinasyon kurulu var mı? ▪ Bilgi güvenliği koordinasyon kurulu oluşumuna ve faaliyetlerini icra etmesine ilişkin düzenlemeler var mı? ▪ Bilgi güvenliği koordinasyonuna ilişki görev ve sorumluluklarla ilgili ayrı bir birim görevlendirilmiş mi?
Kontrol etkinliğini	▪ Bilgi güvenliği koordinasyon kurulunun toplantı tutanaklarının

inceleme yöntemi	incelenmesi ▪ Bilgi güvenliğine ilişkin ayrı bir birim var ise bu birimin görev ve sorumluluklarının incelenmesi
	Görev ve sorumluluklar
Kontrol	**BSO-3** Bilişim sistemleri güvenliğine ilişkin görev ve sorumluluklar yazılı olarak ve anlaşılır şekilde belirlenmelidir.
Kontrol varlığını değerlendirme soruları	▪ Bilgi güvenliğine ilişkin görev ve sorumluluklar belirlenmiş mi?
Kontrol etkinliğini inceleme yöntemi	▪ İlgili belgeler incelenerek bilgi güvenliğinden tüm kurum personelinin sorumlu tutulup tutulmadığının tespit edilmesi ▪ Personel iş tanımlarının incelenmesi ▪ Görevlerin ayrılığı prensibine uyulup uyulmadığının belirlenmesi
	Yetkilendirme süreci
Kontrol	**BSO-4** Bilgi işlem araç ve faaliyetleri için, bir yönetim yetkilendirme süreci tanımlanmalı ve uygulanmalıdır.
Kontrol varlığını değerlendirme soruları	▪ Bilgi işlem araçlarının uygulamaya konulmasından ve bilişim faaliyetlerinin yürütülmesinden önce ilgili yöneticilerin gerekli yetkilendirmeleri yapmasına ilişkin süreçler tanımlanmış mı? ▪ İlgili tüm güvenlik politikalarının gereklerinin karşılanması için, bilişim sistemlerinin güvenliğini sağlamaktan sorumlu olan yönetici tarafından da yetkilendirme yapılmasına ilişkin süreçler var mı?
Kontrol etkinliğini inceleme yöntemi	▪ Bilgi güvenliği politika belgesi incelenerek kullanıcı yetkilendirme süreçlerine ilişkin prosedürlerin oluşturulup oluşturulmadığının belirlenmesi
	Bağımsız denetim
Kontrol	**BSO-5** Bilişim sistemleri bağımsız bir şekilde denetlenmelidir.
Kontrol varlığını değerlendirme soruları	▪ Kurum bilişim sistemi, bağımsız bir birim tarafından düzenli olarak denetleniyor mu? ▪ Bu denetim sistemde önemli değişiklikler olduğunda da yapılıyor mu?
Kontrol etkinliğini inceleme yöntemi	▪ Bilişim sistemleri denetimi, iç denetim birimi tarafından yapılıyorsa, yapılan denetimin etkinliğinin aşağıdaki hususlar dikkate alınarak incelenmesi: o İç denetim raporlarının tamamın üst yönetime sunulup sunulmadığı o İç denetim raporlarında önerilere yer verilip verilmediği o Bu öneriler üzerine uygulamada gerekli değişiklik ve düzenlemelerin yapılıp yapılmadığı (Raporlarda yer alan

önerilerin yüzde kaçının uygulamaya geçirildiği)

- İç denetim çalışmalarının planlama, inceleme ve belgeleme açısından yeterli kalitede olmasını sağlayacak gözetim ve kalite kontrol mekanizmalarının kurulup kurulmadığı
- İç denetim biriminde çalışan personele bilişim sistemlerinin denetimi konusunda eğitim verilip verilmediği

- Bilişim sistemleri denetimi bağımsız kurum ve kuruluşlar tarafından yapılıyorsa, uluslararası bilişim sistemleri denetim standartlarına uygun denetim yapılıp yapılmadığının incelenmesi

Mal ve hizmet alımlarında güvenlik ve iş garantisi

Kontrol

BSO-6 Bilişim sistemleri ile ilgili üçüncü kişilerden mal ve hizmet alımlarında, ilgili sözleşmelerine bilgi güvenliğine ilişkin hükümler konulmalı ve iş garantisi istenmelidir.

Kontrol varlığını değerlendirme soruları

- Bilişim sistemleri ile ilgili üçüncü kişilerle yapılan mal ve hizmet alımları sözleşmelerinde bilgi güvenliğine ilişkin hükümler var mı?
- Üçüncü kişilerin verdikleri mal ve hizmete ilişkin olarak iş garanti isteniyor mu?

Kontrol etkinliğini inceleme yöntemi

- Üçüncü kişilerle yapılan sözleşmeler ve ekleri incelenerek bilgi güvenliğine ilişkin hükümlerin konulup konulmadığının incelenmesi
- Sözleşmede, kurumun üçüncü kişileri denetim yetkisi olduğu hükmünün yer alıp almadığının incelenmesi (veya bu yetkiyi kısıtlayan hükümler olup olmadığının incelenmesi)
- İşin gereğine göre üçüncü kişilerin sertifikalı elemanlar eliyle işi göreceğine ilişkin hüküm olup olmadığının incelenmesi
- Verilen garanti belgeleri incelenerek garantinin iş yapılan üçüncü kişi tarafından mı yoksa başka bir kurum veya kişi tarafından mı verildiğinin incelenmesi
- Garanti kapsamının önemli açıklar bulunup bulunmadığı açısından incelenmesi

Diğer kamu kurumları ile işbirliği

Kontrol

BSO-7 Diğer kamu kurum ve kuruluşlarla işbirliği yapılması halinde bilgi güvenliğinin gerekleri, taraflar arasında anlaşma sağlanmış bir güvenlik yönetimi planı içersinde yerine getirilmelidir.

Kontrol varlığını değerlendirme soruları

- Diğer kamu kurum ve kuruluşlarla işbirliği yapılması durumunda kurumun bilgi varlıklarının korunmasını sağlayacak tedbirleri içeren prosedürler var mı?

Kontrol etkinliğini inceleme yöntemi

- Diğer kamu kurum ve kuruluşları ile olan işbirliği faaliyetlerinin ve bunları bilgi güvenliği yönünden düzenleyen prosedürlerin incelenmesi

2.1.1.4 VARLIK YÖNETİMİ

Kontrol Hedefi

Bilişim sistemlerine ilişkin tüm bilgi ve varlıkları koruyacak, işlevlerini düzenli ve sürekli bir şekilde yerine getirmelerini sağlayacak etkin bir varlık yönetimi için Kurum gerekli tedbirleri almalıdır..

Riskler

Etkin bir varlık yönetiminin olmaması aşağıdaki risklerin ortaya çıkmasına sebep olabilir:

- Varlıklar üzerindeki kontrolün kaybedilmesi
- Varlıklara ilişkin denetim izinin kaybedilmesi
- Varlıkların maliyet, getiri ve risklerine ilişkin kontrolün kaybedilmesi
- Lisanssız yazılımdan kaynaklanabilecek yazılım hataları veya varlık kayıp ve zararların meydana gelmesi
- Elden çıkarılacak varlıkların yetersiz kontrolü dolayısıyla veri kaybı
- İşin aksaması ve mali kayıplara yol açması
- Hesap verilebilirliğin ve sorumlulukların tanımlanamaması veya karıştırılması
- BS yatırımlarının karar alma süreçlerinin verimsiz işletilmesi sonucu yatırımların kuruma olumsuz etkide bulunması ya da beklenen getiriyi sağlayamaması
- Varlık yönetimine ilişkin üst yönetim desteğinin sağlanamaması

Temel Kontroller

Varlık yönetiminden kaynaklanabilecek riskleri minimize edecek temel kontrol faaliyetleri şunlardır:

- Bilişim sisteminde kullanılan varlıkların envanteri yapılmış olmalıdır.
- Varlıkların kullanım kuralları belirlenmiş olmalıdır.
- Varlıkların kullanımdan çıkartılması veya imhası belirli bir prosedüre bağlanmış olmalıdır.
- Kurum verileri uygun bir şekilde sınıflandırılmalıdır.
- Varlıkların kullanım kuralları belirlenmiş olmalıdır.
- Bilişim sistemlerinin bütün iş ve işlemleri belgelendirilmelidir.

Kontrollerin Değerlendirilmesi

Varlık envanteri

Kontrol

VY-1 Bilişim sisteminde kullanılan varlıkların envanteri yapılmış olmalıdır.

Kontrol varlığını değerlendirme soruları

- Kurumun bilişim sistemlerine ilişkin tüm varlıkların açık ve anlaşılır şekilde tanımlanmış bir envanteri çıkarılmış mı?
- Varlık envanterine yeni alınan varlıklar ile yeri değiştirilen ya da elden çıkarılan varlıkların kayıtlarının düzenli bir şekilde yapılmasını sağlayacak bir prosedür var mı?

Kontrol etkinliğini inceleme yöntemi	▪ Bilişim sistemleri varlık envanterinin, kurumun tüm donanım ve yazılımlarını tür, kullanan kişi ve kullanıldığı yer bilgilerini de içerecek şekilde tutulup tutulmadığının incelenmesi ▪ Risk değerlendirmesi çalışmaları çerçevesinde varlıklar için yapılan değerlendirmelerin belirlenmesi ve alınan tedbirlerin incelenmesi ▪ Örnekleme yoluyla seçilen varlıklar ile envanter bilgilerinin karşılaştırılması ▪ Envanterde, önemli varlıkların özelliklerinin ayrıntılı bir şekilde yazılıp yazılmadığının kontrol edilmesi

Sorumluların belirlenmesi

Kontrol	**VY-2** Bilişim sistemlerine ilişkin tüm varlıkların kullanımları dikkate alınarak sorumluları belirlenmelidir.
Kontrol varlığını değerlendirme soruları	▪ Bilişim sistemlerine ilişkin tüm varlıkların elde edilmesi, geliştirilmesi, bakımının yapılması, kullanımı ve güvenliğinin sağlanması amacıyla belli bir bireyin ve birimin yönetim sorumluluğuna verilmesini öngören prosedürler var mı?
Kontrol etkinliğini inceleme yöntemi	▪ Örnekleme yoluyla seçilen varlıklara ilişkin olarak yönetim sorumluluklarının, özellikle güvenlik kontrollerinin tespit edilmesi

Kullanımı ve kullanımdan çıkarılması

Kontrol	**VY-3** Varlıkların kabul edilebilir kullanımı ve kullanımdan çıkartılması veya imhası belirli bir prosedüre bağlanmış olmalıdır.
Kontrol varlığını değerlendirme soruları	▪ Varlıkların kabul edilebilir kullanımına ilişkin kurallar yazılı şekilde tanımlanmış mı? ▪ Kullanımdan çıkartılacak veya imha edilecek varlıklar için uygun bir prosedür belirlenmiş mi?
Kontrol etkinliğini inceleme yöntemi	▪ Varlıkların kabul edilebilir kullanımına ilişkin kuralların incelenmesi ▪ Varlıkların kullanımdan çıkarılmasına ilişkin prosedürün incelenmesi ▪ Varlıkların kullanımdan çıkarılmasına ilişkin prosedürlerde aşağıdaki hususların yer alıp almadığının incelenmesi: o Bu varlıklarda yer alan bilgilerin belgeye bağlanması ve elden çıkarılmasına ilişkin üst yönetimin onayının aranması o Üzerindeki bilgilerin silinmesi veya teknik olarak yapılacak diğer düzenlemeler o Varlıkların fiziksel imhası için gerekli düzenlemeler ▪ Örnekleme yapılarak kullanımdan çıkarılacak bir varlık ile ilgili olarak belirtilen düzenlemelerin uygulanıp uygulanmadığının izlenmesi

Veri (Bilgi) sınıflandırması

Kontrol

VY-4 Kurum verileri uygun bir şekilde sınıflandırılmalı ve korunmalıdır.

Kontrol varlığını değerlendirme soruları

- Verilerin uygun şekilde sınıflandırılmasını ve güvenliğini sağlayacak prosedürler var mı?
- Verileri güvenlik gereksinimlerine göre sınıflandıran bir sınıflandırma cetveli var mı? (değerlerine, gizlilik derecelerine, işteki önemlerine ve yasal düzenlemelere göre)
- Bilginin nasıl yönetileceği ve korunacağına karar verilmesinde yardımcı olan bilgi sınıflandırma planı ya da rehberi var mı?
- Kurumun benimsediği bilgi sınıflandırma planına göre bilgi etiketlemesi ve yönetilme prosedürleri tanımlanmış mı?

Kontrol etkinliğini inceleme yöntemi

- Örnekleme yoluyla seçilecek bazı verilerin doğru sınıflandırılıp sınıflandırılmadığının incelenmesi
- Örnekleme yoluyla seçilen verilerin güvenlik derecelerine uygun şekilde sınıflandırılıp sınıflandırılmadığının incelenmesi
- Örnekleme yoluyla seçilen verilerin güvenlik derecelerine uygun ortamlarda kullanılıp kullanılmadığının ve uygun depolama alanlarında muhafaza edilip edilmediğinin belirlenmesi

2.1.1.5 PERSONEL VE EĞİTİM POLİTİKALARI

Kontrol Hedefi

Bilişim sistemlerine zarar verebilecek insan kaynaklı hata, ihmal ve suiistimalleri önleyecek tedbirleri almaktır.

Riskler

Personel ve eğitim politikalarındaki zayıflıklar, aşağıdaki risklerin ortaya çıkmasına sebep olabilir;

- Güvenilir ve gerekli bilgi ve beceriye sahip olmayan personelin istihdamı
- Belli bir konu üzerinde uzmanlığı olan personelden her konuda yararlanmak zorunda kalma
- Bilgi varlıklarının korunmasına yönelik Kurum politikalarına bağlılık konusunda sözleşmeli personelin kendinden beklenen sorumlulukları yerine getirememesi
- Sözleşmeli personelden beklenen sorumluluk üstlenme ve hesap verebilme konularında uyuşmazlığa düşülmesi durumunda başlayacak olan adli sürecin Kuruma olan olumsuz ve mali etkileri
- Personelde güvenlik bilincinin oluşturulamaması sonucu meydana gelen güvenlik olayları ve sistem hataları
- Hassas noktalarda çalışan kilit personelin yokluğunda güvenlik olaylarının etkilerinin ve sayılarının artması
- Personelin kariyer gelişimi açısından tatmin edilememesi
- Personelin Kurumun kritik ihtiyaçlarının karşılanabilmesi için gerekli yetenek ve bilgi düzeyine yükseltilememesi

- Kurumun kritik iş süreçlerinin kesintisiz ve düzenli bir şekilde sürdürülememesi
- Eğitim politikalarının yeterli ve etkin olmaması
- Karşılaşılan problemlerin çözüm süreçlerinin etkin işleyememesi
- İşten ayrılan veya işine son verilen personelin sisteme yetkisiz erişebilmesi

Temel Kontroller

Personelden kaynaklanabilecek riskleri minimize edecek temel kontrol faaliyetleri şunlardır:

- Bilişim sistemlerine yönelik güvenlik politikalarına uygun şekilde personelin rol ve sorumlulukları yazılı olarak belirlenmiş olmalıdır.
- Bilişim sistemlerinde hassas noktalarda çalıştırılacak personelin seçiminde gereken özen gösterilmelidir.
- Personelle bilgi güvenliğine ilişkin hususların da yer aldığı sözleşmeler yapılmalıdır.
- Yönetim, personele ilişkin gözetim görevini yerine getirmelidir.
- Personelin düzenli olarak bilgi güvenliğine ilişkin eğitim ve bilgi güncelleme programlarına katılması sağlanmalıdır.
- İşten ayrılan personelin, kullanımında olan varlıkları kuruma teslim etmesi ve kurum bilgilerine ulaşma yetkilerinin derhal kaldırılması sağlanmalıdır.

Kontrollerin Değerlendirilmesi

Görev tanımları

Kontrol

PEP-1 Bilgi güvenliği politikalarına uygun şekilde personelin rol ve sorumlulukları belirlenmelidir.

Kontrol varlığını değerlendirme soruları

- Personelin görev tanımları yazılı olarak yapılmış ve onaylanmış mı?

Kontrol etkinliğini inceleme yöntemi

- Personel görev tanımlarının bilgi güvenliği politika belgesine uygunluğunun incelenmesi
- Örnekleme yoluyla seçilen personelle görev tanımlarından haberinin olup olmadığına ilişkin olarak görüşme yapılması

Personel istihdam koşulları

Kontrol

PEP-2 Bilişim sistemlerinde hassas noktalarda çalıştırılacak personelin seçiminde gereken özen gösterilmelidir.

Kontrol varlığını değerlendirme soruları

- Personel politikaları, personelin, çalıştırılacakları işe uygun bilgi ve beceriye sahip olmasına ilişkin bir düzenleme içeriyor mu?
- Personel politikaları, bilgi işlem hizmetlerinde istihdam edilecek personelin güvenilir olmasına ilişkin bir düzenleme içeriyor mu?

Kontrol etkinliğini inceleme yöntemi	▪ Yeni personel alım prosedürünün incelenmesi ▪ Örnekleme yoluyla seçilen yeni bir personel için personel kayıtlarından işe uygun bilgi ve beceriye sahip olup olmadığının incelenmesi ▪ Personelle yapılan sözleşmelerden örnek seçilip incelenmesi

Personel sözleşmeleri

Kontrol	**PEP-3** Personelle bilgi güvenliğine ilişkin hususların da yer aldığı sözleşmeler yapılmalıdır.
Kontrol varlığını değerlendirme soruları	▪ Personelle yapılan sözleşmeler, bilgi güvenliği ile ilgili hükümler içeriyor mu?
Kontrol etkinliğini inceleme yöntemi	▪ Örnekleme yoluyla seçilen personel sözleşme dosyalarının incelenerek bilgi güvenliğine ilişkin hükümler içerip içermediğinin belirlenmesi

Gözetim

Kontrol	**PEP-4** Yönetim, personel üzerinde bilgi güvenliğine ilişkin gözetim görevini yerine getirmelidir.
Kontrol varlığını değerlendirme soruları	▪ Yönetimin, personelin güvenlik politikalarına uyup uymadığını izlemesine ve gerekli tedbirlerin alınmasına ilişkin bir prosedür belirlenmiş mi?
Kontrol etkinliğini inceleme yöntemi	▪ Örnekleme yoluyla seçilen personel ile yönetici gözetimi konusunda görüşme yapılması ▪ Varsa yönetici raporlarının veya toplantı tutanaklarının incelenmesi ▪ Bilgi güvenliği politikalarını ihlal eden personele uygulanan yaptırımların incelenmesi

Personel eğitimi

Kontrol	**PEP-5** Personelin düzenli olarak bilgi teknolojilerine ve güvenliğine ilişkin eğitim ve bilgi güncelleme programlarına katılması sağlanmalıdır.
Kontrol varlığını değerlendirme soruları	▪ Personel için düzenli olarak bilgi güvenliğine ilişkin eğitim programları yapılıyor mu? ▪ Personelin bu programlara katılımı sağlanıyor mu?
Kontrol etkinliğini inceleme yöntemi	▪ Eğitim programlarının incelenmesi ▪ Örnekleme yoluyla seçilen personelle aldıkları eğitimler konusunda görüşme yapılması

İşten ayrılma

Kontrol

PEP-6 İşten ayrılan bütün personelin, bilişim sistemlerine olan tüm erişim yetkileri derhal kaldırılmalı ve uhdesinde bulunan cihazlar geri alınmalıdır.

Kontrol varlığını değerlendirme soruları

- İşten ayrılan veya işine son verilen bütün personelden, kullandıkları kuruma ait varlıklar geri alınıyor mu?
- İşten ayrılan veya işine son verilen personelin kurum bilgilerine ulaşma yetkilerinin derhal kaldırılmasına ilişkin bir düzenleme var mı?

Kontrol etkinliğini inceleme yöntemi

- Varlık iade işlemlerine ilişkin ayniyat kayıtlarının incelenmesi
- Örnekleme yoluyla seçilen işten ayrılan personelin erişim şifre ve e-posta adreslerinin işten ayrılma tarihinden sonra kullanılıp kullanılmadığının günlük kayıtlarından incelenmesi

2.1.1.6 UYGUNLUK

Kontrol Hedefi

Kurum bilişim sistemlerinin yasalar ve diğer düzenlemelere uygun şekilde işletilmesini sağlamaktır.

Riskler

Yasalar ve diğer düzenlemelere uyulmaması, aşağıda belirtilen risklerin ortaya çıkmasına neden olabilir:

- Maddi zararların meydana gelmesi
- Kurumu zor duruma düşürecek, itibar kaybetmesine neden olacak olayların meydana gelmesi
- Sistemi kötü amaçlarla kullanan personelin tespit edilememesi
- Kurum kayıtlarının yargı tarafından kabul edilmemesi
- Mevzuata uymama sonucu Kurumun karşılaşacağı maddi yaptırımlar ve cezalar
- Suç teşkil eden fiillerin ortaya çıkması
- Güncel mevzuatın takip edilmemesi

Temel Kontroller

Kurum bilişim sistemlerinin yasalar ve diğer düzenlemelere uygun şekilde işletilmesini sağlayacak temel kontrol faaliyetleri şunlardır:

- Kurum bilişim sistemlerini ilgilendiren yasal düzenlemelerin gereklerini yerine getirmelidir.
- Bilgi güvenliğine ilişkin düzenlemelerin geliştirilmesi ve yenileme ihtiyacının belirlenmesi için bilgi güvenliğine ilişkin uygulama sonuçları düzenli bir şekilde üst yönetime raporlanmalıdır.
- Bilişim sistemleri mevzuata uygunluk açısından denetlenmelidir.

Kontrollerin Değerlendirilmesi

Yasal düzenlemeler

Kontrol

BSU-1 Kurum bilişim sistemlerini ilgilendiren yasal düzenlemelerin gereklerini yerine getirmelidir.

Kontrol varlığını değerlendirme soruları

- Kurum, bilişim sistemlerinin kurulması, işletimi ve kullanımı ile ilgili var olan düzenleyici mevzuatı belirlemiş, derleyip belgelendirmiş mi?
- Bilişim sistemlerini ilgilendiren konularda yapılan yasal düzenlemelerin gereklerini yerine getirecek şekilde yazılı prosedürler geliştirilmiş mi?
  - Fikri Mülkiyet Hakları,
  - Kurum kayıtlarının korunması
  - Kişisel bilgilerin gizliliği ve verilerin korunması
  - Bilgi işlem araçlarının kötü niyetli kullanımının önlenmesi
  - Kriptografi kullanımı

Kontrol etkinliğini inceleme yöntemi

- Kurumun, ilgili mevzuatı karşılayacak şekilde düzenlemeler yapıp yapmadığının incelenmesi
- Yazılımların lisanslı olup olmadığının örnekleme yapılarak incelenmesi
- Önemli kurum kayıtlarının (muhasebe kayıtları, veri tabanı kayıtları, işlem kayıtları, denetim kayıtları vb.) türlerine göre, tutulacak asgari süre ve tutulma şekli ve yeri de belirtilecek şekilde sınıflandırılıp sınıflandırılmadığının incelenmesi
- Örnekleme yoluyla seçilen arşiv kayıtlarının yasaların öngördüğü süre kadar arşivde muhafaza edilip edilmediğinin tespit edilmesi
- Arşiv kayıtlarından yararlanma prosedürlerinin kayıtlara zarar verilmeden gerçekleştirilmesini sağlayacak mekanizmaların kurulup kurulmadığının incelenmesi

Bilgi güvenliği politikalarına ilişkin uygulama sonuçlarının raporlanması

Kontrol

BSU-2 Bilgi güvenliğine ilişkin düzenlemelerin geliştirilmesi ve yenileme ihtiyacının belirlenmesi için bilgi güvenliğine ilişkin uygulama sonuçları düzenli bir şekilde üst yönetime raporlanmalıdır.

Kontrol varlığını değerlendirme soruları

- Bilgi güvenliği kontrollerinin uygulamasına ilişkin her türlü husus sorumluları tarafından raporlanıyor mu?
- Bu raporlar üst yönetime düzenli olarak sunuluyor mu?

Kontrol etkinliğini inceleme yöntemi

- Üst yönetime iletilen bilgi güvenliğine ilişkin raporların incelenerek güvenlik ihlallerine ilişkin olaylara, kullanıcı şifreleri yenileme sayılarına ilişkin matrislere, hizmet verilememe sürelerine, uygulama programlarında karşılaşılan sorunlara ilişkin yeterli bilgi içerip içermediğinin incelenmesi

Mevzuata uygunluk denetimi

Kontrol	**BSU-3** Bilişim sistemleri mevzuata uygunluk açısından denetlenmelidir.
Kontrol varlığını değerlendirme soruları	▪ Bilişim sistemlerini yürürlükteki düzenlemelere uygunluğu açısından denetlenmesine ilişkin prosedür oluşturulmuş mu?
Kontrol etkinliğini inceleme yöntemi	▪ Mevzuata uygunluk denetimine ilişkin prosedürlerinin aşağıdaki hususları içerip içermediğinin incelenmesi: o Görevli birim o Yapılacak denetimin sıklığı o Raporlamanın formatı o Raporların sunulacağı yer o Bulguların değerlendirilmesi ▪ En son ne zaman mevzuata uygunluk denetimi yapıldığının tespit edilmesi ▪ Denetimin kapsamının yeterli olup olmadığının incelenmesi ▪ Denetim bulgularının raporlanıp raporlanmadığının bu bulgular ışığında belirlenen faaliyetlerin ve bu faaliyetlerin ne ölçüde gerçekleştirildiğinin incelenmesi

2.1.2 FİZİKSEL VE ÇEVRESEL KONTROLLER

Fiziksel ve çevresel kontrollerin amacı, bilişim sistemleri donanımın ve yazılımının kasten ya da kazaen oluşan hasarlara, izinsiz erişim sonucu bozulma veya çalınma ile her türlü çevresel tehlikelere karşı korunmasıdır. Bilişim sistemleri, bu sistemlere erişme yetkisi olmayan kişilerin yol açabilecekleri hasarlara ve müdahalelere karşı fiziksel engeller konulmak suretiyle korunurken; yangın, su (ya da aşırı nem), elektrik, voltaj dalgalanmaları veya güç yetersizlikleri gibi çevresel tehlikelere karşı ise, bunlara ilişkin uygun önlemler alınarak korunmalıdır.

Kontrol Hedefi

Kurum bilişim sistemlerine yetkisiz erişimi engelleyecek ve kurum varlıklarını koruyacak her türlü fiziksel ve çevresel tehlikelere karşı önlemler alınmalıdır.

Riskler

Fiziksel ve çevresel korumaya yönelik kontrollerin hiç veya yeterli düzeyde kurulamaması durumunda aşağıda belirtilen risklerle karşılaşılabilir:

- Bilişim sisteminin, personelin isteyerek veya istemeyerek verebileceği zararlara açık hale gelmesi
- Kritik veya gizli bilginin görülmesi, kopyalanması veya kaybedilmesi
- Bilgisayar donanımının veya üzerinde yazılım ve bilgi bulunduran parçaların çalınması veya bozulması
- Sistemin yetkisiz kişilerin izinsiz erişimi sonucu bozulması veya hasar görmesi
- Bilişim sisteminin yangın, sel, elektrik kesintileri veya voltaj düzensizlikleri, sıcaklık ve nem gibi çevresel tehlikelerle kısmen veya tamamen çalışamaz duruma gelmesi ve hizmette aksaklıklara veya veri kayıplarına neden olması
- İş ihtiyaçlarına uygun fiziksel ve çevresel güvenliğin tanımlanmaması
- Donanımın yetkisiz kişiler tarafından çalınması
- BS bölümüne yetkisiz kişilerin fiziksel müdahalesi
- Ziyaretçilerin BS bölümünde hassas bölgelere yetkisiz erişimi
- Kullanılan donanımın bulunduğu ortamlarda sağlıklı işleyebilmesi için gereken koşulların sağlanmamış olması

Temel Kontroller

Fiziksel ve çevresel kontroller, sadece yönetim tarafından yetkilendirilenlerin bilişim sistemlerine fiziksel erişim sağlamasını ve yangın, su, elektrik gibi çevresel tehlikelere karşı önlemlerin alınmasını hedeflemektedir.

Sistemlere yetkisiz fiziksel erişimi engellemek ve çevresel tehlikelerden kaynaklanabilecek riskleri kabul edilebilir düzeye indirmek için oluşturulabilecek kontroller aşağıda belirtilmiştir:

- Kurum, yetkisiz fiziksel erişime ve çevresel tehlikelere ilişkin yazılı güvenlik politikasına ve prosedürlerine sahip olmalıdır.
- Kurum, ana bilişim sistemlerinin bulunduğu binalara yetkisiz fiziksel erişimi önlemelidir.

- Kurum, bilgisayar odalarına ve çalışma alanlarına fiziksel erişimin yetki dahilinde gerçekleştirilmesini sağlamalıdır.
- Yangın belirleme ve söndürme sistemleri kurulmuş olmalıdır.
- Bilişim sistemleri su basması riskinin yüksek olduğu yerlerde zemin veya zemin altı katlarda kurulmuş olmamalıdır.
- Bilişim sistemleri donanımı yerden yüksekte konumlandırılmalı ve su boruları veya su tanklarının etrafında veya ıslak zeminlerin (Lavabo, mutfak, banyo…) bitişiklerinde bulundurulmamalıdır.
- Olası su sızıntılarına karşı bilişim sistemleri personelini uyarmak amacıyla otomatik su veya nem detektörleri kullanılmalıdır.
- Bilişim sistemlerini elektrik kaynaklı zararlardan korumak amacıyla kesintisiz güç kaynakları, jeneratörler, alternatif güç kablolaması ve diğer düzenleyiciler kurulmuş olmalıdır.
- Ana bilişim sistemlerini toz, nem ve sıcaklıktan kaynaklanacak zararlardan korumak amacıyla uygun havalandırma ve soğutma sistemleri kurulmalıdır.
- Ana bilişim sistemlerinin bulunduğu alanların anti-statik zemin kaplaması yapılmalıdır.
- Çatı, su ve kanalizasyon borularının düzenli bakımı yapılmalıdır.
- Bilişim sistemlerinin bulunduğu alanlarda sigara içme, yiyecek ve içecek tüketimine yönelik düzenlemeler yapılmış olmalıdır.
- Bilgisayar odalarında bulunan çöpler kaldırılmalı ve düzenli olarak temizlenmelidir.

Kontrollerin Değerlendirilmesi

Politika ve Prosedürler

Kontrol

FÇK-1 Kurum yetkisiz fiziksel erişime ve çevresel tehlikelere ilişkin yazılı güvenlik politikasına ve prosedürlerine sahip olmalıdır.

Kontrol varlığını değerlendirme soruları

- Kurum, bilişim sistemlerine ilişkin teçhizatın, yazılımın ve verinin fiziksel güvenliğine yönelik politika belgesine sahip mi?
- Kurum kabul edilen politikalarla uyumu sağlamak için prosedürlere sahip mi?
- Prosedürler ve politika düzenli olarak gözden geçiriliyor mu?

Kontrol etkinliğini inceleme yöntemi

- Mevcut fiziksel ve çevresel güvenlik politika belgesi ve prosedürlerinin aşağıda belirtilen hususları içerip içermediğinin incelenmesi:
  - Fiziksel güvenlik politikaları için hedeflerin belirlenmesi
  - Temel işlevlerin ayrılması (örneğin, yetkilendirme, koruma ve kaydetme)
  - Donanımın konumu

- Bilgisayar alanlarına ve ilgili binalara erişim yöntemleri
- Giriş çıkış kontrolleri ve personel güvenliği
- Güvenlik görevlilerin yerleştirilmesi
- Geçici personel ve ziyaretçilerle ilgili prosedürler
- Alarmların ve diğer sızma tespit araçlarının kullanımı
- Hassas bilişim ortamlarında her türlü sıvı ve katı gıda tüketimi
- Olağanüstü durumlarda tahliye prosedürleri
- Su, yangın, elektrik, sıcaklık ve nem gibi problemlere ilişkin kontrol düzenlemeleri
- Her türlü çıktıya ilişkin güvenlik ve kontrol
- Kablolar ve iletişim teçhizatının konumu, isimlendirmesi ve korunması
- İhlal prosedürleri

Binalara erişim

Kontrol

FÇK-2 Kurum, ana bilişim sistemlerinin bulunduğu binalara yetkisiz fiziksel erişimi önlemelidir.

Kontrol varlığını değerlendirme soruları

- Binalara erişimi kontrol altına alacak önlemler var mı?
- Binalar göze çarpmayan ve kullanılma amaçlarıyla ilgili en az göstergelerle belirlenmiş mi?
- Uygun sızma tespit sistemleri (hırsız alarmı, kamera, projektör vs.) kurulmuş mu?
- Stratejik noktaları izlemek üzere video kameralar konulmuş mu ve giriş çıkışlar kaydediliyor mu?
- Kurumun binalarına girişlerde güvenlik görevlileri konumlandırılmış mı?
- Bina girişlerinde personel kimlik kartlarının kullanımına ilişkin uygulama var mı?
- Gelen ziyaretçiler izleniyor ve ziyaretçi defterine kaydediliyor ve güvenlik durumuna göre gidecekleri yere refakatçi eşliğinde götürülüp getirilmeleri sağlanıyor mu?
- İşten ayrılan personelin kurum kaynaklarına fiziksel erişimini engelleyen prosedürler var mı?

Kontrol etkinliğini inceleme yöntemi

- Bütün güvenlik kapılarının ve diğer erişim kontrol özelliklerinin tam olarak çalışıp çalışmadığının kontrol edilmesi (özellikle zemin katta olan kapı ve pencerelerin kilitli ve parmaklık konmuş veya kapatılmış olup olmadığının tespit edilmesi)
- Sızma tespit sistemlerinin düzenli testlerine ilişkin sonuçların elde edilmesi (bu sistemlerin gerektiği çalışıp çalışmadığının doğrudan test edilebilir)
- Ziyaretçi defterlerinde şu hususların yer alıp almadığının tespit edilmesi: tarih, giriş-çıkış saati, imza, nereye gittiği, kiminle

görüşeceği, hassas alanlara giriş yetkisi verilmiş olup olmadığı, bu alanlarla ilgili güvenlik bilgilerinin kendilerine anlatılıp anlatılmadığı, güvenlik görevlisi refakatinin gerekip gerekmediği

- Denetçi kendini tanıtmadan binaya ve hassas alanlara erişim denemesi yapması ve buna ilişkin uygulamaları yerinde izlenmesi
- Ayrılan personelin bilişim sistemlerinin bulunduğu alanlara erişim hakları kaldırılıp, güvenlik görevlilerinin bilgilendirilmesi veya anahtarlarının ve diğer giriş kimliklerinin iptalinin sağlanıp sağlanmadığının tespit edilmesi
- Video kameralarıyla izleme yapılıyorsa, kayıt sisteminin incelenmesi
- Giriş yerlerinde görevli güvenlik görevlileri ile güvenlik sorunları hakkında görüşme yapılması
- Kurum binalarının konumuna ilişkin güvenlik açısından gözlem yapılması
- Uygulama alanında çalışan bütün personelin resmi ve geçerli geçiş kartlarını takıp takmadığının belirli bir periyotta gözlenmesi
- Kabloların güvenlik gerekleri dikkate alınarak düzenli şekilde döşenmiş olup olmadığının ve periyodik olarak gözden geçirilip geçirilmediğinin incelenmesi

Bilgisayar odalarına erişim

Kontrol

FÇK-3 Kurum bilgisayar odalarına ve çalışma alanlarına fiziksel erişimin yetki dahilinde gerçekleştirilmesini sağlamalıdır.

Kontrol varlığını değerlendirme soruları

- Ana bilgisayar ve bağlantı noktaları özel olarak belirlenmiş odalarda tutuluyor mu?
- Bu odalar binaların çalışma yoğunluğu az ve tecridi yapılmış iç kısımlarında yer alıyor mu?
- Bilgisayar odasına erişim sadece burada çalışanlarla sınırlandırılmış mı?
- Bilgisayar odalarına erişim hakları düzenli olarak gözden geçiriliyor ve güncelleniyor mu?
- Kurum tarafından yönetilen bilişim sistemleri, üçüncü tarafların yönettiği sistemlerden fiziksel olarak ayrılmış mı?
- Kuruma mal ve hizmet sağlayanların güvenli veya hassas bilgi işleme alanlarına erişimi sadece gerektiğinde, yetki dahilinde ve izlenmek kaydıyla sınırlandırılmış mı?
- Bilişim sistemlerinin bulunduğu alanlara geçişlerin yetki dahilinde yapılıp yapılmadığı kontrol ediliyor mu?
- Bilişim sistemlerinin bulunduğu odaların kapıları sağlam yapıda mı ve fiziksel olarak korunuyor mu?
- Sık kullanılmayan alanlar (arşiv, depo alanları, yedekleme merkezleri…) fiziksel olarak kilitli tutuluyor ve periyodik olarak kontrol ediliyor mu?

- Bilişim sistemlerinin bulunduğu alanlarda çalışan personel bu yerler için alınan güvenlik önlemleri hakkında bilgilendirilmiş mi?
- Hassas ve önemli iş bilgilerinin bulunduğu belgeler veya ortam araçlarının bulunduğu mekanlar, mesai saatleri dışında veya kullanılmadığı zamanlarda kilitleniyor mu?
- Kişisel bilgisayarların ve yazıcıların, kullanılmadıkları zamanlarda açık olarak bırakılmamasına ve anahtar, şifre veya diğer araçlarla korunmasına yönelik prosedürler var mı?
- Bilişim sistemleri teçhizatlarının düzenli olarak bakımına ilişkin prosedürler var mı?
- Bilişim sistemleri kabloları güvenlik gerekleri çerçevesinde düzenli şekilde döşenmiş mi?
- Fotoğraf, video veya diğer kayıt cihazlarına yetki dahilinde izin veriliyor mu?

Kontrol etkinliğini inceleme yöntemi

- Veri merkezlerinin bilişim sistemlerinin bulunduğu ortamı ve erişim noktalarının, donanım ve çevresel teçhizatların ve personelin konumunu gösteren kat planlarının incelenmesi
- Sunucuların, terminallerin ve ağ teçhizatlarının fiziksel olarak sınırlandırılmış alanlarda korunduğunun ve sadece yetkili personel tarafından erişilebildiğinin gözlem, mülakat ve belge incelemesiyle tespit edilmesi
- Hassas alanlara yetkili erişim hakkı bulunanların listesinin elde edilmesi ve erişim uygunluklarının belirlenmesi
- Denetçi olarak kendinizi tanıtmadan, refakatçi olmadan veya kimlik kartsız hassas alanlara erişmeye çalışılması
- Normal iş saatlerinde ve bunların dışında bilişim sistemleri imkanlarının bulunduğu yerlere giriş ve çıkışların izlenmesi
- Personelin, bilgisayarının başında olmadığı zamanlarda sisteme izinsiz girişi engellemek üzere gerekli önlemleri alıp almadığının gözlenmesi
- Güvenlik biriminden, uygulama birimlerine erişimi bulunan bütün personelin listesinin elde edilmesi ve örnekleme yoluyla seçilen personelin sorumluluklarına uygun olarak mevcut geçişlerle karşılaştırılması
- Eşlik edilmeyen yabancıların ve görsel kimlik tanıma araçları taşımayanların güvenliğe bildirilmesine ilişkin prosedürlerin işleyip işlemediğinin gözlemlenmesi veya personel ile görüşme yapılarak belirlenmesi
- Bilgisayar odalarının kapıların sağlamlığının ve kilitlenebilir olup olmadığının tespit edilmesi
- Teçhizat bakım prosedürlerinin incelenmesi ve örnekleme yoluyla seçilen örnek teçhizatların bakımlarına ilişkin inceleme yapılması
- Çalışma alanlarında bulunan önemli donanım parçalarının kilitlenip kilitlenmediği, bakım ve temizliğine dikkat edilip edilmediğinin gözlenmesi

- Genel kablolama şemalarının güvenlik açısından incelenmesi

Çevresel Tehlikeler (Yangın)	
Kontrol	**FÇK-4** Kurum, bilişim sistemlerini yangın tehlikesine karşı koruması gerektiğini bilmeli, gerekli önlemleri almalı ve alınan önlemler düzenli olarak test edilmelidir.
Kontrol varlığını değerlendirme soruları	▪ Bilişim sistemlerinin bulunduğu binalarda ve odalarda yangına karşı önlemler alınmış mı? ▪ Yangından kurtarmaya ilişkin olarak belirli bir prosedür veya görevli kişiler belirlenmiş mi?
Kontrol etkinliğini inceleme yöntemi	▪ Yangın tehlikesine karşı aşağıdaki önlemlerin alınıp alınmadığının incelenmesi: o Bilişim sistemleri alanlarının yanmayan maddeler kullanılarak inşa edilmesi o Yangın ve/veya duman detektörlerinin konulması o Uygun yangın söndürme araçlarının tesis edilmesi o Bina kullanılmadığı zamanlarda bilgisayar odalarında otomatik yangın belirleme ve söndürme sistemlerinin kurulması o Yangın ve/veya duman detektörlerinin, bilgisayar odalarının yakınındaki hassas donanım parçalarının bulunduğu odalarda da kurulması o Yanıcı maddelerin bilgisayar teçhizatlarından uzakta tutulması (atık kağıt, kimyasallar, kırtasiye, temizlik sıvıları) o Yangını söndürme ve önleme aletlerinin çalışıyor olduğunun test edilmesi o Binada sigara içilmeme veya belirli bir alanda içme politikasının yerleştirilmesi o Elektrik yangınlarında kullanılmak üzere uygun yangın söndürme teçhizatlarının bulundurulması o Yangın söndürme teçhizatlarının düzenli olarak bakımının yapılması o Personelin yangın söndürme teçhizatının uygun şekilde kullanılması konusunda eğitilmesi o İşletim personelinin yangın alarmının, yangın detektörlerinin, elektrik anahtarlarının, su kesme vanalarının ve acil bir durumda kullanılabilir olan diğer araçların var olduğu konusunda bilgilendirilmesi

Çevresel Tehlikeler (Su)	
Kontrol	**FÇK-5** Kurum, bilişim sistemlerini su tehlikesine karşı koruması gerektiğini bilmeli, gerekli önlemleri almalı ve alınan önlemler düzenli olarak test edilmelidir.

Kontrol varlığını değerlendirme soruları	▪ Bilişim sistemlerinin sudan kaynaklanacak felaketlere karşı korunması için önlemler alınmış mı?
Kontrol etkinliğini inceleme yöntemi	▪ Su tehlikesine karşı aşağıdaki önlemlerin alınıp alınmadığının incelenmesi: o Bilişim sistemleri su basması riskinin yüksek olduğu yerlerde zemin veya zemin altı katlarda kurulmaması o Bilişim sistemleri donanımı yerden yüksekte konumlandırılması ve su boruları veya su tanklarının etrafında veya ıslak zeminlerin (Lavabo, mutfak, banyo…) bitişiklerinde kurulmaması o Olası su sızıntılarına karşı bilişim sistemleri personelini uyarmak amacıyla otomatik su veya nem detektörleri kullanılması

Çevresel Tehlikeler (Elektrik)

Kontrol	**FÇK-6** Bilişim sistemlerini elektrik kaynaklı zararlardan korumak amacıyla kesintisiz güç kaynakları, jeneratörler, alternatif güç kablolaması ve diğer düzenleyiciler kurulmuş olmalıdır.
Kontrol varlığını değerlendirme soruları	▪ Bilişim sistemlerinin elektrik kaynaklı tehlikelere karşı koruması sağlanmış mı? ▪ Kesintisiz güç kaynakları, jeneratörler ve diğer düzenleyicilerin bakımı mutat aralıklarla yapılmış mı?
Kontrol etkinliğini inceleme yöntemi	▪ Elektrik kaynaklı tehlikelere karşı aşağıdaki önlemlerin alınıp alınmadığının incelenmesi: o Bilgisayar teçhizatlarına uygun elektrik sağlanması o Güç kaynaklarında, jeneratörlerde ve yedekleme jeneratörlerinde gücün devamlılığını sağlamak için alternatifli çoklu besleyicilerin bulundurulması o Kesintisiz güç kaynakları ve jeneratörlerin bakımlarının yapıldığına ilişkin dokümanların incelenmesi

Çevresel Tehlikeler (Havalandırma ve soğutma)

Kontrol	**FÇK-7** Bilişim sistemlerini toz, nem ve sıcaklıktan kaynaklanacak zararlardan korumak amacıyla uygun havalandırma ve soğutma sistemleri kurulmalıdır.
Kontrol varlığını değerlendirme soruları	▪ Bilgisayar odaları ve çalışan teçhizatlar için uygun hava koşulları sağlanıyor mu? ▪ Bilgisayarların etrafında yeterli havalandırma var mı?
Kontrol etkinliğini inceleme yöntemi	▪ Hava soğutma sistemlerinin işletilmesi, konumu, bakımı ve erişiminin izlenmesi

Çevresel Tehlikeler (Temizlik)

Kontrol	**FÇK-8** Kurum, bilişim sistemleri teçhizatının ve bulundukları alanların temiz tutulmasını sağlamalıdır.
Kontrol varlığını değerlendirme soruları	▪ Kurum, bilişim sistemleri teçhizatının ve bulundukları alanların temiz tutulmasını sağlamak için kontrollere sahip mi?
Kontrol etkinliğini inceleme yöntemi	▪ Bilişim sistemlerinin bulunduğu alanlarda yeme, içme hususlarının belirli bir prosedüre dayalı olarak işletilip işletilmediğinin incelenmesi ▪ Bilgisayar odasının çöpleri ve atıklarının düzenli olarak toplanması ve uygun şekilde temizlenip temizlenmediğinin gözlenmesi ▪ Bilişim sistemleri teçhizatlarının temiz tutulmasına yönelik prosedürlerin işleyip işlemediğinin izlenmesi

2.1.3 AĞ YÖNETİMİ VE GÜVENLİĞİ KONTROLLERİ

Ağ yönetimi ve güvenliği kontrollerinin amacı, ağ sistemini oluşturan tüm varlıkların korunması, ağ hizmetlerinin güvenli bir şekilde yürütülmesi ve ağ aracılığıyla gerçekleşebilecek yetkisiz erişim ve bunlar dolayısıyla oluşabilecek tehlikelerin önlenmesidir.

Ağ, veri paylaşımı amacıyla iki ya da daha fazla cihazın birbiriyle bağlantılı hale getirilmesiyle oluşturulan bir yapıdır. Yüzlerce iş istasyonu veya kişisel bilgisayardan oluşabileceği gibi iki bilgisayarın birbirine bağlanmasıyla da elde edilebilir. Bu ağ ortamıyla iletişim, bilgiye ulaşım, kaynak paylaşımı, yedekleme gibi hizmetler sağlanabilmektedir.

Riskler

Ağı oluşturan sistemler tasarlanırken veya devreye alınırken güvenlik unsuru hesaba katılmadığında, bu sistemlerin çeşitli zayıflıkları nedeniyle kötü niyetli veya meraklı kişiler tarafından sistemler ve hizmetler kullanılamaz hale getirilebilir ya da kurumlar için çok önem taşıyan bilgilerin öğrenilmesi/değiştirilmesi mümkün olabilir. Bu nedenle, ağlar, yetkisiz erişimlerin engellenerek sadece yetkili kullanıcıların erişebilmesi için kontrol edilmelidir.

Bilişim sistemlerinin ağ nedeniyle karşı karşıya olduğu riskler şunlardır:

- Verilerin bozulması, kaybolması ve/veya çalınması, kötüye kullanılması
- Yetkisiz işlem tesis edilmesi, ağ anahtarlarının yetkisiz kişiler tarafından kullanılması
- Gizli bilgilerin tutulduğu uygulamaların ağa bağlı olduğu yerlerde hem kazaen hem de isteyerek yetkisiz kişiler tarafından ifşa edilmesi
- Ağ üzerinden gerçekleştirilen hizmetin gerçekleştirilmemiş gibi gösterilmesi
- Ağ bağlantıları ve sunucuların kolaylıkla zarar görebilmesi nedeniyle kurulan sistemin işlememesi
- Ağ sisteminin tasarımındaki uygunsuzluklar nedeniyle ilerleyen zamanlarda ağ performansında azalma, işlemlerde yavaşlama
- Güvenliği zayıflatacak ve sistemde açıklıkların meydana gelmesine sebebiyet verecek virüs gibi kötü niyetli yazılımların bulaşması, sistemin yavaş çalışması nedeniyle işin yürütülmesinde çeşitli aksamaların meydana gelmesi
- Fikri mülkiyet hakları ve Ceza Kanunu gibi yürürlükteki yasal mevzuatın ihlal edilmesi, kullanılan yazılımların kanuni gereklilikleri karşılayamaması

Temel Kontroller

Ağ güvenliği, yönetilen hizmetlerin devamının sağlanmasını, bilginin gizliliği ve başka kişiler tarafından değiştirilmemesini sağlamaya yönelik çalışmaların bütünü olarak özetlenebilir. Etkin risk yönetimi ile var olan güvenlik riskleri azaltılarak kabul edilebilir bir seviyeye indirilmelidir.

Fiziksel güvenliği sağlanmayan cihaz üzerinde alınacak yazılımsal yöntemlerin hiç bir değeri bulunmadığından ağın fiziksel unsurlarının (kablolar, sunucular, iletişim araçları vs.) güvenliği fiziksel ve çevresel kontroller altında sağlanmalıdır. Bununla birlikte ağ ve internet güvenliğinin sağlanması için başka kontrollerin de kurulması gerekmektedir. Bu kontroller şunlardır:

- Bilişim sistemleri güvenlik politikasının bir parçası olarak ağ ve internet kullanımına ilişkin güvenlik politikası olmalıdır.
- Bilgi güvenliği politika belgesine ve ağ güvenlik politikasına bağlı olarak yazılı halde ağ ve internet kullanımına ilişkin standartlar, prosedürler ve işletim talimatları bulunmalıdır.
- Kurum, ağ kablolama diyagramları gibi ağın fiziksel yerleşimini tanımlayan belgelere sahip olmalı, güncellemeli ve güvenli bir şekilde saklamalıdır.
- Şifre seçiminden e-posta eklentileri kullanımına kadar güvenlik konularında kullanıcıların ve bilgi işlem yöneticilerinin bilinçlendirilmesi sağlanmalıdır.
- Kurum oturum açmaların, şifrelerin ve kaynak erişim izinlerinin "Mantıksal Erişim Kontrolleri" politika ve prosedürlerine uygun olarak yürütüldüğünden emin olmalıdır. (Parola temelli kullanıcı doğrulama mekanizması genellikle bir çok sistem için en zayıf noktalardan birisidir. Kullanıcılar tarafından seçilen parolaların genellikle kolayca tahmin edilebilir olması, saldırganların bu sistemlere daha kolay bir biçimde sızabilmesi ile sonuçlanmaktadır. Parolalar yerine kullanılabilecek diğer kullanıcı doğrulama mekanizmaları arasından kurum bütçesi için uygun olan bir diğer alternatifin seçilmesi ve uygulanması güvenliği önemli ölçüde arttırabilecektir. Akıllı kartların, biyometrik denetimlerin ya da salt-yazılım ile gerçekleştirilebilen S/KEY gibi yalnız bir sefer kullanılabilen parola düzeneklerinin uygulanması parola güvenliğini arttırmak için uygun bir yaklaşım olabilir. Bunların herhangi bir gerekçe ile uygulanamıyor olması durumunda, parolalar için yaşlandırma mekanizmasının kullanılması ile parolaların belirli aralıklar ile değiştirilmesinin zorunlu hale getirilmesi ve parolaları sınayarak kolay tahmin edilebilir olanlarını belirlemek için kullanılabilecek yazılımların belirli aralıklar ile çalıştırılması uygun olacaktır)
- Ağların işletim sorumluluğu, mümkün olan yerlerde bilgisayar işletmenlerinden alınarak, uygun eğitim almış ve tecrübeli olan personel tarafından yönetilmeli ve yönetim tarafından izlenmelidir
- Belli ağ olayları otomatik olarak ağ işletim sistemi tarafından kaydedilmelidir. Kayıtlar periyodik olarak yetkisiz faaliyetler için gözden geçirilmelidir.
- Ağda kurulu tüm sistemlerin ve ağ aktif cihazlarının üzerlerinde kurulu olan yazılımlarda, güvenlik sorunu olup olmadığı düzenli olarak takip edilmeli, yazılım güncellemeleri ve güncel yamalar uygulanmalı ve bunlar için gerekli önlemler alınmalıdır.
- Ağ hizmet sunucuları üzerinde işleyen sunucu yazılımları incelenmeli ve çalışması gerekli olmayan yazılımların durdurulması sağlanmalıdır. Ayrıca bilgisayar sistemlerinin üzerinde kullanılması zorunlu olanlar dışında yazılımlar kurulmamalı, bu tür yazılımlar varsa kaldırılmalıdır.
- Kötü niyetli yazılımların hızla tespit edilmesi ve yok edilmesi için kişisel bilgisayar sistemleri ve sunucu sistemler üzerinde ağ tabanlı anti-virüs sistemleri kurulmalı ve kurulu sisteme özgü olarak düzenli şekilde güncellenmelidir.

- Kurumun yazılım sağlayıcılara, bakım ve yazılım boşluklarını belirlemek için bir uzak erişim bağlantısı vermesi durumunda, sadece Yazılım sağlayıcı talep ettiğinde ve onaylandığında bu erişim verilmeli ve izlenmelidir.
- Belli durumlarda ağ üzerindeki verilerin iletimi gerçekleştirilirken kriptolama yapılmalıdır.
- İletişim kurma veya veri iletiminde kesilme veya hata olma riskini azaltmak için özel hatların kullanılması sağlanmalıdır.

İnternet Kullanımı

Kurumda internet kullanımı kurum bilişim sistemleri için ilave riskler anlamına geldiğinden, güvenlik açısından bu riskleri makul seviyeye indirecek kontrollerin kurulması gerekmektedir. Yukarıda belirtilen kontrollere ilave olarak oluşturulması gereken kontroller şunlardır:

- Öncelikle kurum personeline internet dolayısıyla karşılaşılacak risklerin iyi anlatılması gerekir. Kullanıcılara güçlü şifre seçiminin önemi, internetten program indirilmesinin tehlikeleri, elektronik postaların başkaları tarafından okunabileceği, diğer internet kullanıcılarının iddia edilen kişiler olmayabilecekleri, elektronik posta okuma, dosya ve program yüklenmesi esnasında virüs gibi kötü niyetli yazılımları da sisteme bulaştırabilecekleri konularında eğitim verilmelidir.
- İnternet açısından en iyi koruma politikası, kurumun ana bilişim sistemi ile internet arasında fiziksel bağlantı kurulmamasıdır. Kurum bütün risklerine rağmen her kullanıcının internete doğrudan açılmasını tercih ettiği durumlarda kurum ağ sistemi ve internet arasındaki trafiği kontrol etmek için "güvenlik duvarı" ile başlayan bir dizi önlem alınmalıdır. Bunlar arasında, dış ağlara açık olan cihazların özel güvenlik duvarlarıyla korunan bir alana konması, hizmet grupları veya kullanıcılar itibariyle ağ içersinde alt ağ grupları oluşturulması, sızma tespit ve saldırı önleme sistemlerinin kurulması, uygun kriptolama ve güvenlik protokollerinin uygulanması ve anti virüs programlarının sistemde etkin kullanılması sayılabilir.
- Kurumun internet üzerinden dış dünyaya hizmet vermesi söz konusu ise ilgili cihazların da yine özel güvenlik duvarlarıyla korunan bir alanda bulunması gerekir.
- Üçüncü kişilerden servis sağlayıcılık hizmeti alınması durumunda bu kişilerin sağladığı hizmetler incelenip güvenilirlikleri araştırılmalı ve düzenli olarak denetlenmelidir.

Kontrollerin Değerlendirilmesi

Politika ve prosedürler

Kontrol

AYGK-1 Kurum bilgi güvenliği politikasının bir parçası olarak uygun bir ağ güvenlik politikasına sahip olmalı ve bu belgelere dayanılarak ağ ve internet kullanımına ilişkin standartlar, prosedürler ve işletim talimatları ve ağ hizmetlerinin sürekliliğine ilişkin acil durum planı yazılı olarak hazırlanmış olmalıdır.

Kontrol varlığını değerlendirme soruları

- Kurum ağ ve ağ hizmetlerinin kullanımına ve güvenliğine ilişkin önceden yapılan risk değerlendirmesine dayalı yazılı bir politika belgesine sahip mi?

- Ağ ve internet kullanımına ilişkin olarak kullanıcılara ve bilgi işlem yöneticilerine yönelik standartlar, prosedürler ve talimatlar belirlenmiş mi?
- Eğer varsa, kullanıcıların ve bilgi işlem yöneticilerinin politika içeriği ile standartlardan, prosedürlerden ve talimatlardan haberdar olması sağlanmış mı?
- Ağ hizmetlerinin sürekliliğinin sağlanmasında acil durum planı oluşturulmuş mu?

Kontrol etkinliğini inceleme yöntemi

- Kurum ağ güvenlik politikasının aşağıdaki hususları içerip içermediğinin incelenmesi:
  - İsim ve unvan bazında görev ve sorumluluklar
  - Güvenliğin sağlanması gereken ortamlar (bilgisayar, ağ vb.)
  - Uzaktan erişim dahil genel erişim düzenlemeleri
  - Kablosuz iletişim
  - Sanal özel ağ (VPN) politikası
  - Ağ cihazlarının güvenliği ve yönetimi
  - Yönetim protokolleri ve kriptolama
  - İnternet ve e-posta kullanımı
  - İnternet DMZ cihazları politikası
  - Şifre politikası
  - Web sayfası uygulamaları
  - Kullanıcı güvenliği ve bilgi koruma
  - Kullanıcı ve ayrıcalıklı kullanıcı sorumlulukları
  - Kötü niyetli yazılımlardan korunma
  - Ağın tüm uygulamalarına yönelik belgeleme
  - Ağın ve ağ üzerinden sunulan hizmetlerin izlenmesine yönelik düzenlemeler
  - Anti-virus politikası
  - Sunucu güvenlik politikası
  - Güvenlik açıkları tespit etme politikası
  - Kriz/acil durum yönetimi politikası
  - Kimlik doğrulama ve yetkilendirme politikası
  - Bakım politikası
  - Kişisel kayıtların güvenliği politikası
- Bu politika belgelerinin aşağıdaki hususları gözeterek oluşturulup oluşturulmadığının incelenmesi:
  - Tüm çalışanların anlayabileceği düzeyde detaylı ve açık yazılmış olması
  - Yasal ve düzenleyici mevzuata uygun olması
  - Görev ve sorumlulukların somut şekilde belirlenmesi
  - Uygulamaların ve aykırı uygulamaların sonuçlarını, karşılaşılabilecek riskleri açıkça gösteren işletim talimatları ve prosedürlerin yayımlanması

- Tüm çalışmaların belgelendirilmesi
- Kolay ulaşılabilmesi ve düzenli olarak güncellenmesi
- Ağ güvenlik politikalarını destekleyen diğer politika ve prosedürlere atıfta bulunulup bulunulmadığı

- Ağ güvenliği politika belgesinin ekinde aşağıdaki hususların da elde edilmesi ve incelenmesi:
  - Sistemde kullanılan işletim sistemi
  - Kullanıcı yerleri, kurum kaynaklarına erişim yöntemleri
  - Sistem yönetimi altında olan ve olmayan hizmet sağlayan sunucu makinelerinin listesi
  - Ağ ve kablolama diyagramları (Ağ topolojisi, alt ağlar, kullanılan servisler)
  - Güvenlik duvarı aracılığıyla izin verilen sistem güvenlik politikası tarafından tanımlanan yetkili trafik tanımı
  - Uzaktan erişimle yetkili kullanıcıların kimliklerini doğrulamaya yönelik kullanılan teknikler (şifre, önceden tanımlanmış tahsis edilmiş hatlar, önceden tanımlanmış kullanıcı adresleri, geri çevirme veya geri arama yöntemleri vs.)
  - Geniş sistemlerde iş gerekleri ve farklı güvenlik gereksinimlerine göre, ağların hizmet grupları veya kullanıcılar itibariyle ayrılmasını gösteren diyagramlar ve erişim ilkeleri [iç ağ-dış ağ, sanal özel ağ (vpn), kablosuz-kablolu ağlar vs.]
  - Sızma tespit raporları ve hangi düzensizliklerin raporlanacağına ilişkin düzenlemeler ve yönetimce gözden geçirme prosedürleri
  - Güvenlik yazılım değişim kontrol prosedürleri
  - Kriptolama standartları
  - Sistem kaynaklarına erişim hakkı olan üçüncü kişilerin listesi ile birlikte erişim sağlama amaçları ve ilgili portların listesi
  - Kullanıcıların ağa erişim haklarını kısıtlamada kullanılan yöntemler (elektronik mesaj, tek yönlü dosya aktarımı, çift yönlü dosya aktarımı, etkileşimli erişim, zaman ve tarih sınırlamalı ağ erişimi)
  - Veri iletiminde kullanılan servis sağlayıcıların listesi
  - Veri iletimi hizmet sağlayıcılarla yapılan sözleşmelerin kopyaları
  - Kullanıcı güvenlik ve farkındalık belgelerinin imzalı kopyaları
- Ağ ve internet kullanımına ilişkin olarak kullanıcılara ve bilgi işlem yöneticilerine yönelik hazırlanmış standartların, prosedürlerin ve talimatların incelenmesi;
- Kullanıcılarda ve bilgi işlem yöneticilerinde güvenlik farkındalığının oluşturulması için yapılan çalışmaların incelenmesi
- Kurum genel iş sürekliliği planlamasında ağ hizmetlerinin sürekliliğine ilişkin hususlara yer verilip verilmediğinin belirlenmesi
- Ağ hizmetlerinin sürekliliğinin sağlanmasına yönelik acil durum planının incelenmesi.

Ağ Yönetimi

Kontrol

AYGK-2 Ağ ve ağ hizmetleri yönetimi, uygun eğitim almış ve yeterli bilgi birikimine sahip, tecrübeli görevliler eliyle yürütmeli ve ağ faaliyetleri düzenli olarak izlenmelidir.

Kontrol varlığını değerlendirme soruları

- Kurumda ağ ve ağ hizmetlerinin güvenlik politikasına uygun olarak yönetilmesine ilişkin prosedür var mı?
- Ağın kullanımı ve kapasitesinin sürekli olarak izlenmesine ve sonuçların raporlanmasına ilişkin prosedür var mı?

Kontrol etkinliğini inceleme yöntemi

- Ağ ve ağ hizmetlerinin yönetimine ilişkin prosedürlerin aşağıdaki hususları içerip içermediğinin incelenmesi:
  - Ağ işletim sorumluluğunun bilgisayar işletimlerinden ayrılması
  - Ağın gerekli eğitimleri almış ve tecrübeli uzmanlar tarafından yönetilmesi (Web Uygulamaları dahil)
  - Kullanıcı ve ayrıcalıklı kullanıcıların sorumluluklarının belirlenmesi
  - Ağa uzaktan erişimin düzenlenmesi (Yöneticilerin veya hizmet sağlayan üçüncü kişilerin uzaktan ağa erişim hakkına sahip olması ve bu hakların kullanımının izlenmesi)
  - Kullanıcılara ait olanlar dahil, uzaktan erişimle donanım yönetimi için sorumlulukların belirlenmesi,
  - Gerekli durumlarda kullanıcı doğrulama ve şifreleme yöntemlerinin belirlenmesi.
- Yerinde izleyerek, birim personeliyle görüşme yaparak ve bilgi işlem birimi görevlendirme belgelerini inceleyerek uygulamaların bu prosedürlere uygun şekilde yürütülüp yürütülmediğinin incelenmesi
- Ağın kullanımının izlenmesine yönelik prosedürlerin aşağıdaki hususları içerip içermediğinin incelenmesi:
  - Ağ cihazları ve sunucularından gerekli bilgileri alabilmek için SNMP(Simple Network Management Protokol) gibi ağ izleme protokollerinin / yazılımların kullanılması ve güncel versiyonlarının takip edilmesi
  - Ağ trafiğine ilişkin istatistikleri toplayacak, gerekli ayarları yapılmış bir veya birden fazla bilgisayar atanması
  - Yardımcı bir yazılım (Linux-MRTG ve NeTraMet gibi yazılımlar) ile ağ performansının analizinin yapılması ve kimin, nereye, ne kadar trafik oluşturduğunun gözlenmesi
  - SNMP ile cihazlara erişim ve sorgulamanın sadece erişimin kısıtlandığı ve gerekli güvenlik önlemlerinin alındığı belirli güvenilir bilgisayarlar tarafından yapılabilmesi için erişim listesi düzenlenmesi
  - SNMP erişiminin zor bir iletişim parametresi tanımlanarak yapılması ve iletişim TCP protokolü temelli veya yönlendirici /sunucu destekli ise kriptolu veri trafiği üzerinden yapılması
  - İnternete açık sistemlerde yönlendirici/sunucu üzerinde bulunan paket filtreleme seçenekleri ve erişim denetim kuralları aracılığıyla sadece bağlanması istenen sistemlere izin verilmesi

- Ağın dış ağa bağlantı noktasında protokol tabanlı analiz yapılması için bütün trafiği inceleyebilecek bir ağ dinleyicisi (sniffer) ve/veya Saldırı Tespit Sistemi kullanılması
- Ağdaki faaliyetlerin farklı bir noktada mümkünse sadece yazılabilir bir medyaya otomatik olarak kaydedilmesi ve bu kayıtların periyodik olarak yetkisiz faaliyetler, saldırılar için gözden geçirilmesi
- Ağ güvenliğine yapılan ve otomatik olarak kaydedilen saldırıların belgelendirilerek üst birimlere raporlanması

Ağ cihazları ve yazılımlarının güvenliği

Kontrol

AYGK-3 Ağ cihazlarının ve bu cihazlar üzerinde çalışan yazılımların güvenliği sağlanmalıdır.

Kontrol varlığını değerlendirme soruları

- Ağ hizmetlerini sağlayan cihazların güvenliği ve bu cihazların yönetimi konusunda prosedür var mı?

Kontrol etkinliğini inceleme yöntemi

- Ağ hizmetlerini sağlayan cihazların güvenliği ve yönetimine ilişkin prosedürlerin aşağıdaki hususlar yönünden incelenmesi:
  - Alternatifi olmayan ve bir sorun olduğunda sisteme büyük zarar verebilecek yazılım ve donanım sorunlarına ilişkin risk değerlendirmesi yapılması
  - İşletim merkezleri mimarisinin, tek nokta hatalarına (single point of failure) karşı esnek olması, yeterli yedekleme yapılması, ağ cihazları ve sunucuların yedekli ve yük paylaşımlı çalışabilmesi
  - Ağın, sadece dışarıya açık sistemler (web sunucular), hem dışarıya hem içeriye açık sistemler (e-posta sunucuları), sadece içeriye açık sistemler (bazı veritabanı sunucuları) şeklinde birbirlerinden güvenlik duvarlarıyla ayrılarak konumlandırılması (DMZ)
  - Ağda kurulu tüm sistemlerin ve ağ aktif cihazlarının işletim sistemlerinde ve üzerlerinde kurulu olan yazılımların güvenlik durumunun düzenli olarak takip edilmesi, bu yazılımların güncellenmelerinin ve güncel yamalarının uygulanması
  - Ağ hizmet sunucuları üzerinde işleyen sunucu yazılımlarından sadece gerekli olanlarının çalışması, çalışması gerekli olmayan yazılımların durdurulması
  - Bilgisayar sistemlerinin üzerinde kullanılması zorunlu olanlar dışında yazılımların kurulmaması ve varsa kaldırılması
  - Ağ hizmetlerinin sağlanmasında kabloların gerekli standartları sağlamasına özen gösterilmesi ve mümkünse UTP/STP kabloların veya fiber optik kabloların kullanılması
  - Mümkün olan durumlarda özel uygulamalar için veri iletiminde sanal özel ağ (VPN) gibi özel veya belirlenmiş hatların kullanılması
  - İnternet üzerinden kriptolama yapılarak özel, güvenli bir veri iletimi tüneli oluşturulması

Kontrol varlığını değerlendirme soruları

- Ağ cihazlarına ilişkin fiziksel ve çevresel güvenlik önlemleri alınmış mı?

Kontrol etkinliğini inceleme yöntemi

- Sunucular, kablolar, yönlendiriciler, modemler ile anahtarların içinde bulunduğu ağ cihazlarının fiziksel ve çevresel tehditlere karşı korunması için alınan önlemlerin aşağıdaki hususları da içerip içermediğinin incelenmesi:
  - Cihazların sadece ağ yöneticisinin veya onun yardımcısının açabileceği kilitli, ayrı odalarda, oda ayırmanın mümkün olmadığı yerlerde özel kilitli dolaplarda tutulması
  - Cihazlara fiziksel olarak kimin ve ne zaman eriştiğini belirten erişim listelerinin tutulması ve bu listelerin güncellenmesi
  - Kabloların tek tek etiketlenmesi ve kayıtlarının tutulması
  - Kullanılmayan kabloların sökülmesi
  - Cihazların yakınına (şifre, IP adresi) gibi güvenlik bilgilerinin yapıştırılmaması ve gizli tutulması
  - Cihazlara erişim listesi hazırlanarak sadece belirli IP adreslerinin ulaşmasına izin verilmesi

(Daha ayrıntılı güvenlik önlemleri için; Bkz 2.1.2 Fiziksel ve Çevresel Kontroller)

Ağ Cihazları Güvenliği (Güvenlik Duvarı)

Kontrol varlığını değerlendirme soruları

- Kurumda güvenlik politikasına uygun şekilde konfigüre edilmiş güvenlik duvarı var mı?
- Bu güvenlik duvarı uygulamaları zafiyetleri dikkate alınarak düzenli şekilde test ediliyor mu?
- Güvenlik duvarındaki olaylar kaydediliyor, kayıtların değiştirilmesi veya silinmesine karşı korunuyor ve düzenli olarak gözden geçiriliyor mu?

Kontrol etkinliğini inceleme yöntemi

- Varolan güvenlik duvarının sahip olması gereken minimum özelliklerin aşağıdaki gibi olup olmadığının incelenmesi:
  - İç ağdan dış ağa giden ya da dış ağdan iç ağa gelen bütün trafik güvenlik duvarından geçmelidir.
  - Güvenlik politikasında tanımlandığı gibi sadece yetkili trafiğe izin verilmeli, istenmeyen paketlerin ağa girmesi veya ağdan çıkması engellenmelidir.
  - Güvenlik duvarı mimarisi iç ağın yapısını saklayacak şekilde yapılandırılmalı, bu amaçla;
    - Dış ağa hizmet veren sunucuların bulunduğu mimari topolojilerde iç ağda bulunan sunucular ve kullanıcı bilgisayarları sadece iç ağdaki kullanıcılara ve istemcilere hizmet vermeli, dış ağa servis vermemeli ve güvenlik derecesi en yüksek bölümde tutulmalıdır. İç ağa ve dış ağa hizmet veren sunucular DMZ ağında yer almalı, güvenlik duvarı bu farklı güvenlik seviyesine sahip ağlar arasındaki trafiği düzenleyerek ağın güvenli ve yüksek performanslı çalışmasını sağlamalıdır.

- İç ağda bulunan sunucuların ve istemcilerin IP adresleri gerçek IP adresleri olmamalı, iç ağda kullanılan sanal IP adresleri olmalıdır. İç ağdaki herhangi bir bileşen geniş alan ağıyla (internet) haberleşmek istediğinde iç ağdaki IP adresleri güvenlik duvarı üzerinde adres dönüşümüne tabi tutularak dönüştürülmüş IP adresleri ile internete açılmalıdır. İç ağdan geniş alan ağına olan adres dönüşümü dinamik adres dönüşümü olmalı, bu sayede iç ağın IP adres bloğu gizlenmelidir.
- Genel ağdan gelen hizmet istekleri için destek sağlayan kurum konakları (hostları) güvenlik duvarının dışında olmalıdır.

- Güvenlik duvarı ağ üzerinde ve kendi üzerinde çalışan servisleri kontrol etmelidir.
- Güvenlik duvarı mimarisi kendisini kayıtlı saldırı imzaları ile doğrudan saldırılara karşı savunmalıdır.
- Güvenlik duvarı özellikle ağdaki sunucuları dışarıdan veya içeriden görünmez kılabilecek bir koruma şemsiyesine sahip olmalıdır.
- Trafik sadece uygulama katmanındaki güvenlik duvarı ile gerçekleşmelidir.
- Güvenlik duvarı mimarisi hem uygulama hem de ağ katmanındaki kontrol önlemlerini birleştirmelidir.
- Güvenlik duvarı bütün ve/veya önemli kurallara ilişkin kural tablosunu ve servislere ilişkin önemli olayların kayıtlarını kendi üzerinde veya ayrı bir bilgisayarda tutarak ağa ait önemli olayların sonradan incelenebilmesi için gerekli olan denetim kayıtlarını tutmalıdır.
- Güvenlik duvarının kural tablosunun oluşturulmasında bilgi güvenliği politika belgesi ve ağ güvenliği belgesi ile kurum ihtiyaçları göz önünde bulundurulmalıdır.
- Belirlenmiş herhangi bir ağ trafiğine rastlandığında güvenlik duvarı alarm üretebilmeli ve e-posta yoluyla sistem yöneticilerine bilgi vermelidir.
- Merkezi bir noktadan tüm kullanıcı iş istasyonlarının kullanıcı bilgisayarlarının korunmasına olanak tanımalı ve her bir güvenlik duvarı kurulumunu izleme, sorun giderme ve yönetme imkânına sahip olmalıdır.
- Merkezi bir noktadan güvenlik duvarı yapılandırma ayarlarının istemci bilgisayarlar üzerine kurulması ve güncellenebilmesi gibi özelliklere sahip olmalıdır.
- Güvenlik duvarı mimarisi unsurlarının yönetimi için güçlü yetkilendirme prosedürü olmalı, güvenlik duvarının konfigürasyonu yetkisiz olarak değiştirilememelidir.
- Güvenlik duvarı yazılımları/cihazları güvenliğin yapı taşları olup sistem içerisindeki diğer güvenlik yazılım/cihazları ile uyumlu çalışmalıdır.
- Güvenlik duvarı mimarisi minimal geçişe izin verecek şekilde konfigüre edilmeli, bu amaçla öncelikle tüm hizmetler bloklanmalı, daha sonra gerekli olanlar açılmalıdır.

- Ağ bilgi akışı sürekliliğinin ya da performansın önemli olduğu durumlarda "yedekli yapıda güvenlik duvarı" kullanılmalı, aktif-pasif (master-slave; failover mimari) yapıda, çalışmayan güvenlik duvarının diğer çalışan güvenlik duvarını sürekli kontrol etmesi ve çalışmadığında otomatik olarak devreye girmesi sağlanmalıdır. Aktif-aktif yedekli yapıda her iki güvenlik duvarının da sürekli olarak aktif olması, bir tanesi devre dışı kaldığında diğerinin otomatik olarak tüm bağlantıları üzerine alıp ağ iletişimini sürdürmesi sağlanmalıdır.
- Çok sıkı güvenlik gereksinimi olan ve ardışık iki güvenlik duvarının kullanıldığı sistemlerde bu güvenlik duvarları farklı üreticilerden, modellerden seçilmeli ve bunlar birbirini tamamlayıcı nitelikte olmalıdır.
- Tek güvenlik duvarının kullanıldığı mimari topolojilerde ağ trafiği yüksek seviyelerde ise kullanılacak güvenlik duvarı "durumsal güvenlik duvarı" olarak seçilmelidir. Durumsal güvenlik duvarı OSI referans modelinin oturum katmanında hizmet verdiğinden uygulama seviyesinde güvenliğin sağlanması amacıyla mümkünse güvenlik duvarı ile birlikte vekil sunucular da kullanılmalıdır.

- Kurumda bulunan güvenlik duvarının düzenli şekilde aşağıdaki başlıklar altında sıkılaştırmalarının yapılıp yapılmadığının incelenmesi
  - Yönetim Konsolu için;
    - Yönetim konsolu güvenli bir ağda konumlandırılmış olmalı, tek güvenlik duvarı olan topolojilerde güvenlik duvarı iç ağdan yönetilmelidir.
    - Yönetim konsolunun işletim sistemi sıkılaştırılmalıdır.
    - Bilinen açıklıklar kapatılmalıdır.
    - Yönetim konsolu ile güvenlik duvarı arasındaki iletişimin şifreli olması sağlanmalıdır.
    - Tahmin edilmesi zor yönetici/kullanıcı şifreleri seçilmelidir.
    - Gereksiz yere tanımlanmış yöneticiler/kullanıcılar silinmelidir.
    - Tanımlı yöneticilere/kullanıcılara sadece ihtiyaç duydukları kadar erişim hakkı verilmelidir.
    - Yönetim konsolu, belirli bir süre boyunca işlem yapılmadığı takdirde, güvenlik duvarı ile bağlantısını koparmalıdır.
  - Güvenlik Duvarı için;
    - Güvenlik duvarı ağ topolojisi içerisinde doğru bir şekilde konumlandırılmalıdır.
    - Güvenlik duvarını yönetecek yönetim konsolları kısıtlanmalıdır.
    - Kural tablosu sıkılaştırılmalı, bu amaçla;

- Gereksiz kurallar silinmeli, mümkün olduğunca sade tutulmalıdır.
- Sadece ihtiyaç duyulan bağlantılara izin verilmelidir.
- Güvenlik duvarına doğrudan erişimi engelleyen kural bulunmalıdır.
- İzin verilmeyen bağlantılara ilişkin geriye cevap döndürülmemeli, ağ paketlerinin sessizce düşürülmesi sağlanmalıdır.
- Kritik bağlantılara ilişkin kayıtlar tutulmalıdır.
- Erişimler mümkün olduğunca kısıtlanmalıdır.
  - ⇒ Kaynak bilgisayar
  - ⇒ Hedef bilgisayar
  - ⇒ Kullanılan servis

♦ Yamalar takip edilerek yazılım güncel tutulmalıdır.

♦ Bilinen açıklıklar kapatılmalıdır.

♦ Saldırı önleme imzaları güncel tutulmalıdır.

♦ Önemli saldırı tiplerine karşı imzalar aktif hale getirilmelidir.

♦ Ağ adres çevrimi yapılarak iç ağa ait IP adresleri dış ağdan gizlenmelidir.

♦ Bağlantı sayısı (İç ağdan dış ağa yapılan bağlantı sayıları) sınırlandırılmalıdır.

♦ Tutulan tüm olay, ağ trafiği, denetim vs. kayıtlarının güvenliği sağlanmalıdır.

o Prosedüre ilişkin güvenlik için;

♦ Kural tablosu güncel tutulmalı, düzenli olmalı ve dokümante edilmelidir.

♦ Güvenlik kayıtları geriye dönük olarak düzenli bir şekilde yedeklenmeli, incelenmeli ve raporlanmalıdır.

♦ Tutulan kayıtların silinmesi belirli bir prosedüre göre yapılmalıdır.

♦ İlgili personel düzenli eğitimlerden geçirilmelidir.

♦ Güvenlik duvarı periyodik güvenlik denetimlerinden geçirilmelidir. (Başka kurum ve kuruluşlar tarafından ve/veya iç denetim)

♦ Güvenlik duvarının birebir yedeği önceden alınmış olmalıdır.

♦ Güvenlik duvarı üzerinde yapılan tüm değişiklikler raporlanmalıdır.

▪ Sistem yöneticisiyle yukarıda belirtilen sıkılaştırmalarının yerindeliğine ilişkin görüşme yapılması ve güvenlik duvarına sızma denemelerinin yapılması

- Sistem yöneticisiyle görüşülerek güvenlik duvarı konfigürasyonunun yetkisiz değişimlerinin takip edilip edilmediğinin belirlenmesi

Ağ Cihazları Güvenliği (İçerik Kontrolcüsü)

Kontrol varlığını değerlendirme soruları

- Kurum güvenlik politikasına uygun olarak kurumun iç ağı ile dış ağ arasındaki trafikte yer alabilecek zararlı içeriklere karşı kontroller yapılıyor mu?

Kontrol etkinliğini inceleme yöntemi

- İçerik kontrolüne ilişkin olarak aşağıdaki hususları düzenleyen yazılı bir politikanın bulunması ve bu politika belgesinin düzenli olarak güncellenip güncellenmediğinin incelenmesi
  - Filtrelenecek zararlı içerikler (Virüs ve trojanlar, aktif nesneler, spyware/adware, macro, logic bombs trap doors, worms, exploit, keyloggers, rootkit vb…)
  - Filtrelenecek dosya türleri (*.exe, *.zip, *.rar, vb…)
  - Yapılacak URL filtreleme
  - Filtreleme yapılacak anahtar kelimeler
  - Göndericiler ve/veya alıcılara göre filtreleme
  - İç ağ ile dış ağ arasında akan her bir ağ paketinin filtreden geçmeden iç ağa ulaşmasına izin vermeyecek şekilde içerik kontrolcüsünün ağ mimarisindeki yeri
  - Bu politikaların uygulama noktalarının belirlenmesi (sunucu veya ağ geçidi tabanlı)
  - Zararlı içerik tespiti halinde uygulanacak prosedür
  - Zararlı içeriklerin güncel tutulmasına ilişkin prosedür
- Politikaların güncellenmesinin aşağıdaki hususlar çerçevesinde yapılıp yapılmadığının tespit edilmesi
  - Gerekli ve gereksiz filtreleme kurallarının belirlenmesi
  - Gereksiz filtreleme kurallarının o anki geçerli politikadan çıkarılması
  - İhtiyaç duyulan yeni filtreleme kurallarının geçerli politikaya eklenmesi
  - Böylece bir önceki politikanın ihtiyaçlara cevap verebilecek hale getirilmesi
- İçerik kontrolcüsüne ilişkin sıkılaştırmaların aşağıdaki hususlar kapsamında düzenli olarak yapılıp yapılmadığının belirlenmesi
  - Yönetim konsolunun güvenliğinin sağlanması
    - Yönetim konsolu güvenli bir ağda konumlandırılmalı
    - Yönetim konsolunun işletim sistemi sıkılaştırılmalı
    - Bilinen açıklıklar kapatılmalı
    - Yönetim konsolu ile içerik kontrolcüsü arasındaki iletişimin şifreli olması sağlanmalı

- Tahmin edilmesi zor yönetici/kullanıcı şifreleri seçilmeli
- Gereksiz yere tanımlı yöneticiler/kullanıcılar silinmeli
- Tanımlı yöneticilere/kullanıcılara sadece ihtiyaç duydukları kadar erişim hakkı verilmeli
- Yönetim konsolu, belirli bir süre boyunca işlem yapılmadığı takdirde, içerik kontrolcüsü ile bağlantısını koparmalı

o İçerik kontrolcüsünün güvenliğinin sağlanması

- Mümkünse içerik kontrolcüsü güvenlik duvarının bacaklarının birinde konumlandırılmalı ve güvenlik duvarıyla entegre bir şekilde çalışmalıdır.
- İçerik kontrolcüsünü yönetecek yönetim konsolları kısıtlanmalı
- Filtreleme ayarları aşağıdaki gibi yapılmalı:
  - Zararlı olduğu bilinen içerikler bloklanmalı, zararlı olduğu tespit edilen ağ trafiğine ilişkin paketler düşürülüp bu ağ trafiğine ilişkin temiz olan paketlerin geçişine izin verilmeli
  - Zararlı olduğu tespit edilen ancak temizlenemeyen ağ trafiğine ilişkin bütün paketler reddedilerek düşürülmeli
  - Düşürülen bütün paketlerin bir kopyası alınarak izole bir yerde saklanmalı, karantinaya alınan bu kopyalar sonradan incelenerek zararlı içerikler hakkında bilgi edinilmeli
  - Sıkıştırılmış içeriklerin taranması sağlanmalı (örneğin seviye 10'a kadar, üstü reddedilmeli)
  - Sıkıştırılmış dosya boyutu belirlenen miktara (örneğin 50MB) kadar incelenmeli, bunun üstü bloklanmalı
  - Şifre korumalı dosyalar, şifreli mesajlar reddedilmeli
  - Uzantısı değiştirilmiş dosyaların gerçek dosya tipini belirlenmesi için taranması sağlanmalı
  - Aktif içerikler (ActiveX/Javascript) bloklanmalı
  - Şüpheli Macro'lar taranmalı
  - Tespit edilen Spyware/Adware'ler bloklanmalı
  - Spam e-postalar bloklanmalı
  - Zararlı içerik gönderdiği tespit edilen sunucular ve/veya kişiler "YASAKLI" listesine alınmalı
  - Yasaklı yerlerden gelen dosyaların otomatik olarak taranması veya bloklanması sağlanmalı
  - URL filtreleme gerçekleştirilmeli
  - Anahtar kelimelere göre tarama yapmalı
  - Kritik olayların sistem yöneticilerine e-posta ile gönderilmesi sağlanmalı

- Bloklanan, geçişine izin verilmeyen, reddedilen veya karantinaya alınan ağ paketlerine ilişkin geriye cevap döndürülmemeli

♦ Yamalar takip edilerek güncel tutulmalı

♦ Bilinen açıklıklar kapatılmalı

♦ Zararlı içerik imzaları güncel tutulmalı

♦ Filtrelenen zararlı içeriklere ilişkin kayıtlar tutulmalı, periyodik olarak gözden geçirilmeli

o Prosedüre ilişkin güvenliğin sağlanması

♦ Filtreleme politikaları belirli aralıklarla güncellenmeli ve dokümante edilmeli

♦ Filtreleme kayıtları düzenli aralıklarla gözden geçirilmeli ve karşılaşılan güvenlik ihlalleri raporlanmalı

♦ Tutulan kayıtların silinmesi belirli bir prosedüre göre yapılmalıdır.

♦ Personel düzenli eğitimlerden geçirilmeli

♦ İçerik kontrolcüsü periyodik güvenlik denetimlerinden geçirilmeli (Başka kurum ve kuruluşlar tarafından veya iç denetim)

♦ İçerik kontrolcüsünün birebir yedeği önceden alınmış olmalı

♦ İçerik kontrolcüsü üzerinde yapılan tüm değişiklikler raporlanmalıdır.

▪ İçerik kontrolcüsü tarafından tutulan kayıt ve alarmlar incelenerek filtrelenmesi gereken zararlı içeriklerin gerçekten filtrelenip filtrelenmediğine ve üretilen alarmların politikalara uygunluğuna bakılması

▪ Yapılan raporlarda kurumun karşı karşıya kaldığı ve/veya ortaya çıkan yeni tehditlere yer verilip verilmediğinin incelenmesi

Ağ Cihazları Güvenliği (Saldırı Tespit ve Önleme Sistemleri)

Kontrol varlığını değerlendirme soruları	▪ Kurumda ağ güvenliğinin sağlanmasında saldırı tespit ve önleme sistemleri bulunmakta mı?
Kontrol etkinliğini inceleme yöntemi	▪ Sistem yöneticisi ile görüşme yapılarak Saldırı Tespit ve Önleme Sistemlerinin özellikleri dikkate alınarak ağ mimarisi içerisinde doğru şekilde konumlandırılmasının sağlanıp sağlanmadığının belirlenmesi (yönetim konsolu dahil) ▪ Sistem yöneticisi ile görüşme yapılarak, ilgili belgeler incelenerek ve yerinde gözlem ve testler yapılarak saldırı tespit ve önleme sisteminde aşağıdaki hususların dikkate alınıp alınmadığının incelenmesi o Kuralların etkinliği düzenli olarak kontrol edilmeli (gereksiz olan kurallar kaldırılmalı, yakalanan trafiğe göre belirlenebilecek ek kurallar da gözden geçirilmeli, saldırıya göre değil açıklığa göre kural yazılmalı)

- Saldırı imzası veritabanı düzenli olarak güncellenmeli (örneğin, haftada bir toplu güncelleme veya çok önemli bir saldırı olduğu anda özel güncelleme)
- Sadece sistemde yer alan bileşenlerle ilgili saldırı imzalarını aktif hale getirmeli
- Güvenlik duvarının bloke edeceği saldırılarla ilgili imzalar aktif olmamalı
- Saldırı tespit sistemi (STS) bileşenleri (yönetim konsolu, veritabanı ve sensör) arasında alarm alışverişinin şifreli yapıldığı kontrol edilmeli (Örneğin sensörün veritabanına gönderdiği alarm bilgilerinin şifreli olması, aynı şekilde veritabanından çekilen bilgilerin de şifreli ulaştırılması gerekmektedir. Alarm bilgilerinin hassas bilgiler olduğu unutulmamalı, ağ saldırıları hakkında bilgi veren bu ağ paketleri buna göre şifrelenerek korunmalıdır)
- STS yönetim konsoluna politikalara uygun bir şekilde erişim kontrolü yapılıp yapılmadığı kontrol edilmeli (Alarmların kimler tarafından gözlenip raporlanabileceği, kimler tarafından silinip değiştirilebileceği belirlenmeli ve her personel ayrı hesaplar kullanarak oturum açmalıdır)
- STS'ye özel konfigürasyon dosyaları (örneğin *Snort*'ta *"snort.conf"* dosyası) gözden geçirilmeli ve bir aksaklık olup olmadığı kontrol edilmeli
- Alarm miktarı kontrol edilebilecek miktarda olmalı
- STS alarmlarının ne kadar sıklıkla ve kim tarafından izlendiği, ne kadar sıklıkla raporlama gibi faaliyetlerde bulunulduğu kontrol edilmeli
- STS yanlış alarmlar üretmesi durumunda gerekli önlemler alınmalı (kural değiştirilmeli, kural değiştirilemeyecek gibi görünüyorsa, o zaman kaynak IP adresine özel olarak bir ihmal etme kuralı konulmalı, kaynak IP adres çok fazla ise yanlış alarm üreten kural görmezden gelinerek bir şey yapılmamalıdır.)

- Saldırı tespit ve önleme sisteminin aşağıdaki hususları içerip içermediğinin incelenmesi:
  - Geniş çeşitlilikte sızmaları tespit etmeli
    - İçeriden veya dışarıdan gelebilecek sızmaları belirlemeli
    - Daha önceden bilinen ve bilinmeyen saldırıları belirlemeli
    - Daha önceden bilinmeyen saldırıları belirlemek için bir uyum veya öğrenme düzeneğine sahip olmalı
  - Yapılan çözümlemeyi en kolay anlaşılabilecek şekilde sunabilmeli
  - Bilgisayar sistemleri ve ağlar arasındaki trafiği dikkat çekmeden analiz edebilmeli
  - Sisteme yapılan saldırılara karşı koyabilmeli ve ağ yöneticisine bildirebilmeli
  - Gerçek zamanlı veya zaman aralıklı saldırı tespiti yapabilmeli
  - Saldırı tespitlerini ağ ve işletim sistemlerini inceleyerek yapabilmeli

- Ağda dolaşan paketleri görüntüleyebilmeli ve saldırı içerikli olup olmadığını tespit edebilmeli
- Bütün ağ protokollerini analiz edebilmeli
- İşletim sisteminin kayıtlarına bakarak belli bir sisteme yapılan izinsiz erişimleri ve sistemde uygulanan izinsiz aktiviteleri kontrol edebilmeli
- Sistem yöneticisi tarafından grafik ara yüzü ile kolayca yönetilebilmeli
- Sistem yöneticisi grafik ara yüzü ile olası uyarıları görüntüleyebilmeli, algılayıcıların konfigürasyonlarını kontrol edebilmeli, verileri toplayabilmeli, bu veriler veritabanı ortamında saklanabilmeli ve ağ veya sistem aktivitelerini raporlayabilmeli
- Saldırılara karşı nasıl tespit yapılacağı ve nasıl karşı koyulacağı konularında var olan veri tabanını internet aracılığı ile güncelleyebilmeli ve bu teknikleri kullanıcı tanımları ile kontrol edebilmeli
- Saldırı durumunda konsola uyarı gönderebilmeli (SNMP), e-posta atabilmeli, aktif oturumu görüntüleyebilmeli, raporlama yapabilmeli, saldırı tehdidi içeren bağlantıları kesebilmeli, durdurabilmeli, kullanıcı tarafından kontrol edilebilmeli ve gerekirse güvenlik duvarı üzerinde belirlenmiş olan ağ güvenlik politikasını değiştirebilmeli ve güvenlik duvarı ile entegre çalışabilmeli
- Tespit edilen saldırılara kontrolsüz tepkiler verilmemeli

- Sistem yönetici ve diğer yetkili görevliler ile görüşme yapılarak belirlenen saldırılara karşı sistemi en az hasarla eski durumuna getirmek için kullanılan metotların (engelleme, hapsetme, çağrılara geciktirilerek cevap verme…) belirlenmesi ve bu metotların belgelendirilerek saklanması ve birim yöneticisine raporlanıp raporlanmadığının incelenmesi

Ağ Cihazları Güvenliği (Web Sunucuları)

Kontrol varlığını değerlendirme soruları

- Kurumda bulunan web sunucusunun güvenliğine ilişkin yazılı prosedürlere uygun olarak belirlenmiş kontroller var mı?

Kontrol etkinliğini inceleme yöntemi

- Web sunucularının ve sitenin güvenliğine ilişkin prosedürlerin aşağıdaki hususları içerip içermediğinin incelenmesi:
  - Güvenli bir web hizmeti için güvenli yazılım esaslarına göre tasarlanmış ve kodlanmış bir web sunucusunun bulundurulması
  - Web sunucu yazılımlarının düzenli olarak güncellenmesi (Web sunucuda yapılacak sürüm değişikliği veya güncellemeler, ürün firması tarafından desteğin kesilmesine neden olabileceğinden hizmet alımındaki sözleşmelerde bu hususların yer alması gerekir.)
  - Gerekli olmayan tüm bileşenlerin (WebDAV, HTTP Trace, Frontpage Uzantıları, Yazıcı desteği, Index oluşturma desteği ve örnek CGI uygulamaları) sistemden çıkarılması

- Sunucu üzerindeki uygulamanın tüm bileşenlerinde kullanılan değişkenler için kontroller oluşturulması ve değişkene atanması beklenen veri türü ile kullanıcı girdisinin karşılaştırılması
- Beklenen girdi türünden farklı karakterler (örn. <>/;()) saptanması durumunda, karakterler anlam ifade etmeyecek biçimde değiştirilmesi, silinmesi veya kullanıcıya uyarı mesajı döndürülmesi
- Sunucuya erişim seviyelerinin belirlenmesi:
  - Herkese açık (/private (özel) dizini hariç tüm URL`lere salt-okunur erişim)
  - Kurum çalışanları (private dizini dahil tüm URL`lere salt-okunur erişim)
  - HTML yazarları(Doküman ağacında HTML dosyaları yaratma, değiştirme ve silme hakları olan kişiler)
  - Site yöneticileri (Web sunucusunun konfigürasyon dosyalarını değiştirme, CGI script`leri kurma ve Web sunucusunun kapatılıp açılması hakkına sahip olanlar)
  - Sistem yöneticileri (Web sunucusu makinesinin konfigürasyonunu değiştirme ve makineyi kapatıp açma hakkına sahip olan kişiler)
- Yetkilendirme prosedürünün düzenlenmesi (HTML yazarları, site yöneticileri ve sistem yöneticileri erişim seviyeleri için bilgi işlem birimi yöneticisi ya da yardımcısından yazılı izin alınmalı)
- Yetkilerin iptaline ilişkin prosedürün oluşturulması (Tüm erişim seviyeleri için yetkilerin, bilgi işlem birimi yöneticisi veya yardımcısı uygun gördüğünde herhangi bir uyarı yapılmadan kaldırılmalı)
- Erişim haklarının sağlanması:
  - Web sunucusu makinesine yerel konsoldan login sadece sistem ve site yöneticileri için sağlanmalı, Login`lerin amacı sadece site bakımı için olmalı
  - Dosya paylaşımı dahil olmak üzere ağ login`lerinin her şekli yasaklanmalı
  - Tüm sunucu yönetimi yerel olarak yapılmalı, uzaktan erişime izin verilmemeli
  - CGI script`leri, site yöneticilerinden en az ikisi tarafından gözden geçirilip onaylandıktan sonra site yöneticileri tarafından kurulmalı, Kaynak kodu mevcut olmayan CGI script`leri bilgi işlem birimi yöneticisi veya yardımcısının izni olmadan kurulmamalı
- Ağ hizmetlerinin düzenlenmesi:
  - Web sunucusu LAN`daki diğer veritabanları, dosya sistemleri veya servisler ile, bilgi işlem birimi yöneticisinin yazılı izni olmadan bağlantı kurmamalı
  - Gelen ve giden FTP bağlantıları sadece web sayfalarını güncelleme amaçlı olmalı ve FTP erişimi, web yazarlarına,

site ve sistem yöneticilerine olacak şekilde sınırlandırılmalı; anonim FTP ve kurum domain alanı dışarısından her türlü FTP erişimi yasaklanmalı

- ♦ Web makinesi tarafından başka hiçbir ağ servisi sağlanmamalı

- Çalışma, yedekleme ve izlemeye ilişkin bakım prosedürlerinin belirlenmesi

Ağ Cihazları Güvenliği (Mobil bilgi işlem araçları)

Kontrol varlığını değerlendirme soruları	▪ Kurumda güvenlik politikasına ve risk değerlendirmesine dayalı mobil bilgi işlem araçlarının kullanımına yönelik prosedürler var mı?
Kontrol etkinliğini inceleme yöntemi	▪ Mobil bilgi işlem araçlarının kullanımına yönelik prosedürlerin aşağıdaki hususları içerip içermediğinin incelenmesi: o Kabul edilebilir kullanım kuralları o Hangi amaçlar için kullanılacağı o Çalışma ortamları o Kullanılan yazılım ve donanım teknolojisi o Anahtar süreçlerin belgelendirilmesi o Fiziksel ve çevresel güvenlik önlemlerinin alınması o Kullanıcıların bilinçlendirilmesi o Kullanım kurallarının ihlal edilmesi sonrası yaptırımlar o Ağa uzak erişim sağlanmasına yönelik kriptolama ve şifre kuralları (iki unsurlu doğrulama, sanal özel ağ..)

Kötü Niyetli Yazılımlar

Kontrol	**AYGK-4** Kötü niyetli yazılımların hızla tespit edilmesi ve yok edilmesi için kişisel bilgisayar sistemleri ve sunucu sistemler üzerinde ağ tabanlı anti-virüs sistemleri kurulmalı ve kurulu sisteme özgü olarak düzenli şekilde güncellenmelidir.
Kontrol varlığını değerlendirme soruları	▪ Ağ sistemi içinde her noktanın kötü niyetli yazılımlara karşı korunması için alınmış önlemler var mı? ▪ Kötü niyetli yazılımlara karşı alınan önlemler düzenli olarak izleniyor mu?
Kontrol etkinliğini inceleme yöntemi	▪ Kötü niyetli yazılımlardan korunma prosedürlerinin aşağıdaki hususları içerip içermediğinin incelenmesi: o Kötü niyetli yazılımlara ilişkin risklerin bir değerlendirmesinin yapılması o Yapılan bu risk değerlendirmesine dayalı olarak kötü niyetli yazılımlara karşı alınacak tedbirlere ilişkin bir politika oluşturulması o Bu politikaların detaylı uygulamalarıyla birlikte belgelendirilmesi

- Kullanıcıların bu politika konusunda eğitim, e-posta duyuruları, web sayfası güvenlik uyarıları gibi yollarla bilinçlendirilmesi
- Önemli veri tutan sunucularda veri yedeğinin düzenli olarak alınması
- Kötü niyetli yazılımlara karşı kullanılan yazılımların belgelendirilmesi ve sürekli güncel tutulması için düzenli güncellemelerinin yapılması
- Sistem yöneticilerinin ve kullanıcıların lisanssız yazılım kullanmalarına izin verilmemesi
- Kullanıcılara belirli yazılımları yükleme konusunda sınırlama getirilmesi
- Tüm yazılımların kurulumu ve kullanımından önce virüs taraması yapılması
- Serbest veya kopyalanabilir programların indirilmesi, kabulü ve kullanımı konusunda yazılı bir politikanın olması ve bu politikaya bağlı kalınması
- İnternetten belirli dosya türlerinin indirilmesi ve kurulmasının yasaklanması
- Kritik uygulama yazılımların mesaj doğrulama kodu veya digital imza ile korunması ve doğrulamanın başarısız olması durumunda yazılımın kullanılmasına engel olunması
- Kullanıcıların performans yavaşlaması ve dosya büyüklüklerindeki garip artış gibi durumlarda virüslerin belirlenmesi ve raporlanmasına ilişkin talimatlar alması
- Kurumun dışardan satın alınan programla gelen disketlerin kontrol edilmesine yönelik politika ve prosedürlerin olması ve buna bağlı kalınması

- Kötü niyetli yazılımların önlenmesi için Kurum tarafından kullanılan yazılımların aşağıdaki hususları yerine getirip getirmediğinin belirlenmesi:
  - SMTP, HTTP, FTP data paketlerinde tarama yapabilmeli
  - Güvenlik duvarına entegre çalışabilmeli
  - E-posta trafiğini görüntüleyebilmeli
  - Olası virüs özelliği taşıyabilecek dosyaları algılamalı
  - Kötü niyetli JavaScript, VBScript ve Applet'leri sezmeli ve istenirse sınırlamalı
  - Ağ yöneticisinin isteği doğrultusunda mesajlardaki ekleri (attachment) tarayabilmeli
  - Olası virüs tespitinde ağ yöneticisine, gönderen kişiye ve alıcıya uyarı postası atmalı
  - İçerik denetleme özelliğine sahip olmalı ve bu özelliği sağlayan ürünlerle entegre çalışabilmeli
  - Spam postalarını engellemeli, dosya uzunluğunu sınırlamalı ve e-postaları arşivlemeli

- Gönderilen postanın metninde geçen bir kelimeye kadar filtreleme özelliği olmalı ve bu özelliği sağlayan ürünlerle entegre çalışabilmeli
- Hem kullanıcı hem de domain bazında e-postaları bloklayabilmeli
- Sıkıştırılmış dosyalar üzerinde virus taraması yapabilmeli
- Posta kutusuna düşmeden tarama işlemi yapabilmeli ve istenildiğinde posta kutusu bazında tarama yapabilmeli
- Kullanıcıları ve sunucuları disk, disket, cd .vs gibi çevre birimlerinden bulaşabilecek virüslere karşı koruyabilmeli
- Kullanıcılara istenirse uzaktan tek merkezden otomatik olarak yüklenebilmeli
- Kullanıcı yetkilendirme hakkı şifreli olarak verilebilmeli
- Tüm kullanıcılar görüntülenebilmeli ve üzerlerindeki virüs aktivitesi kontrol edilebilmeli

▪ Kötü niyetli yazılımlardan korunmaya yönelik programların yönetiminin aşağıdaki hususları içermesi:
  - Bir merkezden yönetilmesi
  - Görüntülenmesi, kayıt dosyalarının incelenmesi
  - Uzaktan kontrol edilmesi ve çalıştırılması
  - Güncel bilgilerini aldığı ' Virus Pattern ' dosyasını internet aracılığı ile istenilen zaman aralıklarında otomatik olarak güncellemesi ve ilgili programlara dağıtabilmesi
  - İşletim sistemlerince desteklenmesi

▪ Örnekleme yoluyla seçilen sunucularda kötü niyetli yazılımlara karşı çalıştırılan bir yazılım olup olmadığının görülmesi için yüklü yazılımın çalıştırılması, en son güncelleme tarihinin tespit edilmesi ve herhangi bir bulgu sonrası yapılan faaliyetlerin izlenmesi

▪ Örnekleme yoluyla seçilen kullanıcıların bilgisayarlarında kötü niyetli yazılımlara ilişkin programların doğru şekilde kurulup kurulmadığı ve yeterli düzeyde çalışıp çalışmadığının belirlenmesi

▪ Örnekleme yoluyla seçilen kullanıcılarla görüşme yapılarak kötü niyetli yazılımlara karşı bilinçlendirilip bilinçlendirilmediğinin izlenmesi

Kriptolama ve güvenli iletişim kontrolleri

Kontrol

AYGK-5 Kurumda hassas bilgilerin saklanması ve iletiminde kriptolama yapılmalı ve ağ hizmetlerinin güvenli bir şekilde yerine getirilmesi için kullanılacak güvenlik çözümleri düzenli olarak takip edilmelidir.

Kontrol varlığını değerlendirme soruları

▪ Kurum hangi bilgilerinin ne düzeyde korunması gerektiğine ilişkin bir risk değerlendirmesi yapıyor mu?

▪ Kurum hangi bilgilerinin ne düzeyde kriptolanacağına ve bu bilginin kim tarafından hangi metotlarla açılacağına ilişkin prosedürlere sahip mi?

- Kurum kriptolama sistemine ilişkin olarak algoritma seçiminden başlayan değişimleri ve güncellemeleri de içeren prosedürlere sahip mi?

Kontrol etkinliğini inceleme yöntemi

- Kriptolamaya yönelik prosedürlerde belirlenen ve açıkça tanımlanmış olan görev sorumlulukların aşağıdaki hususları içerip içermediğinin belirlenmesi:
  - Anahtar yönetimi (anahtar oluşturma ve üretme dahil)
  - Yükleme (değişiklikler için kontrollü yükseltmeler dahil)
  - Taşıma
  - Depolama
  - Kurtarma
  - İhtiyaç dışına çıkarma ve imha
  - Hırsızlık ve kullanım sıklığı
- Kriptolamaya ilişkin prosedürlerde aşağıdaki hususların açıkça belirlenip belirlenmediğinin incelenmesi:
  - Kriptolamayı gerektiren hassas verilen hangileri olduğu
  - Kriptolamanın ne zaman ve nasıl uygulanacağı
  - Kriptolamanın ana dosyalarda bulunan verilere mi yoksa sadece bu verilerin internet üzerinden iletilmesinde mi yapılacağı
- Kriptolamaya yönelik prosedürlerde aşağıdaki hususlarda kontrollerin kurulup kurulmadığının incelenmesi:
  - Anahtarların iki ayrı kilit unsurlardan oluşturulması ve ayrı bilgi ve ikili kontrol kavramları altında bilinmesi
  - Anahtarların hiçbir kullanıcı ve programcının erişemeyeceği güçlü mantıksal ve fiziksel kontrollerle sağlamlaştırılmış ortamlardaki bilgisayarlarda tutulması
- Kriptolama sistemindeki değişiklik ve güncellemelere ilişkin prosedürlerin aşağıdaki hususları içerip içermediğinin incelenmesi:
  - Anahtarların ihtiyaç dışına çıkarma zamanının belirlenen standartlara uygun olması
  - Uygulamaya yeni anahtarların konması güvenlik zafiyetlerini ortaya çıkarabileceğinden dikkatli kullanılması (özellikle anahtarlar sadece özel modüllerde saklanmalı, işletim sistemi ve uygulama programlarının açık metinlerinde tutulmamalıdır)
  - Kullanılmakta olan anahtarların yükseltilmesi sadece seçilen güvenlik elemanları tarafından belirli bir zaman içerisinde yapılması
  - Anahtarların kopyalarının test ortamında veya herhangi bir programcı veya kullanıcının erişebileceği ortamlarda bırakılmaması

Kriptolama standartları

Kontrol varlığını değerlendirme soruları	▪ Kurumda uygulamalarını dikkate alan genel kriptolama standartları kullanılmakta mı?
Kontrol etkinliğini inceleme yöntemi	▪ Bilgi işlem birimi ve ilgili yetkililerle görüşme yapılarak kurum amaçlarına uygun olan hangi kriptolama standartlarının etkin şekilde kullandığının tespit edilmesi (IPSec, SSL, TLS…)

Elektronik imza

Kontrol	Elektronik imzanın kullanımı durumunda kullanımı ve izlenmesi belirli kurallara bağlı olmalıdır.
Kontrol varlığını değerlendirme soruları	▪ Kurumda elektronik imza kullanılmakta mı? ▪ Elektronik imza için anahtar sertifikasının kullanımı izleniyor ve kayıtları tutuluyor mu?
Kontrol etkinliğini inceleme yöntemi	▪ Kamu kurumları için elektronik imzaya ilişkin sertifika verme TÜBİTAK'ın yetkisindedir. Verilen bu yetkinin yerinde kullanıldığının örnekleme yoluyla seçilen bazı işlemler üzerinden tespit edilmesi

Sanal Özel Ağlar (VPN)

Kontrol	Kurum veri iletiminde sanal özel ağların (VPN) oluşturulması durumunda bu bağlantılar izlenmeli, kayıtları tutulmalı ve belgelenmelidir.
Kontrol varlığını değerlendirme soruları	▪ Kurumda veri iletiminin güvenli şekilde yapılabilmesi için sanal özel ağlar (VPN) oluşturuluyor mu? ▪ Bu bağlantılar izleniyor, kayıtları tutuluyor ve belgelendiriliyor mu?
Kontrol etkinliğini inceleme yöntemi	▪ Sanal özel ağın oluşturulmasına ilişkin olarak belirlenen politika belgesinde aşağıdaki hususların dikkate alınıp alınmadığının incelenmesi: o Hizmetten kimin yararlanacağı o Kullanım kuralları o Kullanımın güvenlik politika ve prosedürlerine uygun olması o Bu hizmet üzerinden başka hizmetin (Proxy, DHCP, BOOTP, DNS vb.) verilip verilmeyeceği o Hizmet alanların kurallara uyması ve yaptırımların uygulanması o Kullanıcıların alması gereken güvenlik önlemleri o Konfigürasyon değişikliklerinin işlenmesi ve duyurulması o Kullanılan teknolojiye ilişkin standart ve protokoller ve güncellemelerin takip edilmesi ▪ Sanal özel ağın güvenliğinin sağlanmasına yönelik kontrollerde aşağıdaki hususların yer alıp almadığının belirlenmesi: o Sunucuların kendilerine ayrılmış bir DMZ bölümü oluşturulması ve güvenlik duvarı aracılığıyla yerel ağa bağlanması

- Sunucularda sayısal sertifika veya tek seferlik şifre gibi harici kimlik doğrulama sistemleri kullanılması
- İnternet kullanımı ile sanal özel ağ kullanımı arasında izolasyon yapılması ve istemcilerin İnternet'te farklı kaynaklara erişiminin kısıtlaması
- Güçlü kriptolama algoritmalarının seçilmesi
- Uzak erişimlerde sahip olunan yetkilerin, yerel ağda sahip olunan yetkilerden çok daha az olacak şekilde yapılandırılması

Kablosuz ağlar

Kontrol

- Kurumda kablosuz ağların güvenli ve güvenilir şekilde kullanılmasına yönelik önlemler alınmış olmalıdır.

Kontrol varlığını değerlendirme soruları

- Kurumda kablosuz ağların güvenli kullanımına yönelik prosedürler var mı?

Kontrol etkinliğini inceleme yöntemi

- Kablosuz ağlara ilişkin oluşturulan prosedürlerde aşağıdaki hususların dikkate alınıp alınmadığının belirlenmesi:
  - Güçlü kimlik doğrulama mekanizması
  - Rogue EN'lere yönelik sürekli tarama (Denetleme yazılımları)
  - İstemci konfigürasyonu (Group Policy)
  - Uygun Erişim Noktası Yerleşim Planı hazırlanması
  - Güç seviyesinin gerekli minimum seviyede tutulması
  - Güçlü şifreleme
  - Kriptografik veri bütünlüğü kontrolü
  - Kapsama alanının taranarak gürültüye sebep olan cihazlara müdahale edilmesi
  - AP fiziksel konumu doğru seçilmeli, veya fiziksel erişim riskine karşı koruyucu önlemler alınmalı
  - Kablosuz ağın kurulması, erişim kontrolleri, çevresel güvenlik önlemleri ve uygulama düzeyinde güvenlik önlemlerini içeren kullanım politika ve prosedürlerinin bulunması
  - Kablosuz ağ tasarımı yapılırken yeterli kapsama alanını içeren erişim noktalarının sayısının minimum düzeyde tutulması
  - Erişim noktalarının kendisinden beklenen işleri yapabilecek en az güçle çalıştırılması
  - Yayın kapsama alanının test edilmesi
  - RSN veya WPA gibi en son standartların ve protokollerin ve bunlara uygun çalışan donanımların bulundurulması ve yeni gelişmelerin düzenli şekilde izlenmesi
  - Kablosuz ağı kullanacakların ve bu ağ üzerinde gönderilecek veri türünün tespit edilmesi
  - Erişim noktalarının ve diğer aletlerin kullanımı, korunması ve bakımının yapılması için sorumluların belirlenmesi
  - İstemcilerden ayrıca sayısal sertifika veya tek seferlik şifre gibi harici doğrulama yöntemlerinin de istenmesi

- Ağ üzerine saldırı tespit sistemi ve kablosuz güvenlik duvarı kurulması ve erişimin buradan yapılmasının sağlanması, tercihen sanal özel ağ oluşturulması
- Uygulama düzeyinde de kullanıcı doğrulamasının istenmesi
- Kablosuz ağın güvenli şekilde işletilmesine yardım edecek kapsamlı yazılımların bulundurulması
- Kullanıcıların ve diğer sorumluların eğitilmesi

▪ Kurum güvenlik politikası dahilinde hareketli kullanıcıların kablolu yerel ağa bağlı olması durumunda bilgisayarlarındaki kablosuz bağlantı araçlarının engellenmesi

E-posta güvenliği

Kontrol varlığını değerlendirme soruları

▪ Kurumda e-posta hizmetinin güvenli şekilde yapılmasına yönelik prosedürler var mı?

Kontrol etkinliğini inceleme yöntemi

▪ Kurum e-posta hizmetinin sunulması prosedürlerinin aşağıdaki hususları içerip içermediğinin incelenmesi:

- E-posta sistem yönetici kullanıcılarının sadece e-posta hizmeti verebilmek için gerekli olan minimum erişim haklarına sahip olması
- Servis Dışı Bırakma (DoS) saldırılarına karşı e-posta eklentilerine belirli bir büyüklükle sınırlama getirilerek büyük boyutta e-postaların gönderilmesi veya alınmasının engellenmesi, kullanıcı e-posta kutularının bulundurabileceği dosyaların boyutuna bir sınırlandırma getirilmesi
- Denetim amaçlı olarak kullanıcılardan gönderilen ve kullanıcılara gelen e-postaların geriye dönerek takip edilmesi.
- Gerektiği durumlarda geriye yönelik kullanıcı bağlantı isteklerine erişilebilmesi
- E-posta takip kayıtlarına erişimin sadece e-posta takibi yapması düşünülen sistem yöneticileri veya gruplarına tanınması
- Kullanıcı iş başında olmadığı zamanlarda otomatik olarak gönderilmesi amacıyla Ofis Dışı e-postasıyla istenmeyen kullanıcılara gereksiz bilginin gönderilmesinin engellenmesi
- E-posta sunumcusunun, sunumcu üzerinde hesabı olmayan kullanıcılara internet üzerinden e-posta gönderilmesine (E-Posta Relay) izin vermemesi
- Geçerli bir kullanıcı adı ve şifresi sağlanmadığı sürece, e-posta sunumcusuna anonim SMTP bağlantı kurulmasının engellenmesi
- Kullanılan Kimlik Doğrulama Metodunun (SMTP, POP3, IMAP4) güvenli olması; kullanıcı adı ve parolasının açık metin olarak görünmesini engellemesi
- Başarılı ve başarısız SMTP bağlantısı kayıtlarının tutulması
- OWA (Outlook Web Access) kullanılıyorsa internet sitesi girişinde kullanıcı adı ve parolası sorularak geçerli bir kullanıcı adı ve parolası girmeden sisteme erişimin engellenmesi

- Bir OWA kullanıcısının, belirlenen bir sayıdan daha fazla yanlış parola girmesi durumunda kullanıcı hesabının otomatik olarak OWA kullanımından devre dışı bırakılması
- OWA kullanıcısının adı, parolası ve e-posta bilgilerinin internet üzerinden açık olarak taşınmaması
- OWA erişiminde kullanılan HTTP (TCP Port 80) ve SSL (TCP Port 443) portları dışındaki portların erişiminin engellenmiş olması
- Kurum personeli tarafından internet ortamı aracılığı ile iletilen her türlü kişisel e-posta mesajının altında, kurum tarafından belirlenen "gizlilik notu" ve "sorumluluk notu" bilgileri yer alması (Bu bilgiler, e-posta iletisinin içeriğinden ve niteliğinden kurumun sorumlu tutulamayacağı gibi açıklamalar içermelidir.)
- Gizli ve hassas bilgi içeren e-postaların kriptolanarak iletilmesi (Sayısal Sertifika, e-imza kullanımı da dahil)
- Güvenli e-posta iletimi için sunucu (SMTP) ve istemci (POP3s, IMAPs) protokollerinin takip edilmesi ve sunucu ve yazılımlarda gerekli güncellemelerin yapılması

- Kurum e-posta kullanımı prosedürlerinin aşağıdaki hususları içerip içermediğinin incelenmesi:
  - Kurumun e-posta sistemi aracılığıyla, taciz, suistimal veya herhangi bir şekilde alıcının haklarına zarar verecek öğeleri içeren mesajların gönderilmemesi konusunda kullanıcıların bilgilendirilmesi
  - Bu tür özelliklere sahip bir mesaj alındığında hemen ilgili birim yöneticisine haber verilmesi ve daha sonra bu mesajın tamamen silinmesi
  - Mesajların gönderilen kişi dışında başkalarına ulaşmaması için gönderilen adrese ve içerdiği bilgilere azami biçimde özen gösterilmesi
  - Kurum ile ilgili olan hiçbir gizli bilginin, gönderilen mesajlarda yer almaması
  - Zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında hemen silinmesi ve kesinlikle başkalarına iletilmemesi
  - Kurum işlevleri dışında, kişisel kullanım için Internet'teki listelere üye olunması durumunda kurum e-posta adreslerinin kullanılmaması
  - Spam, zincir e-posta, sahte e-posta vb. zararlı e-postalara yanıt yazılmaması ve bilgi işlem birimine bilgi verilmesi
  - Kullanıcıların kullanıcı kodu/şifresini girmesini isteyen e-postaların sahte e-posta olabileceği dikkate alınarak, herhangi bir işlem yapılmaksızın derhal bilgi işlem birimine bilgi verilmesi
  - Çalışanların e-posta ile uygun olmayan içerik (pornografi, ırkçılık, siyasi propaganda, fikri mülkiyet içeren malzeme, vb) göndermemesi
  - Kurumda kişisel amaçlar için e-posta kullanımının mümkün olduğunca makul sayıda olması

- Alınan e-postaların arşivlenmesi ve silinmesine yönelik kuralların bulunması
- Çalışanlar mesajlarının yetkisiz kişiler tarafından görülmesinin engellenmesi konusunda sorumlu tutulması

- Kurum yönetimi ile görüşme yapılarak yukarıdaki uygulamaları hangi ölçüde ve ne sıklıkla izlediklerinin belirlenmesi

İnternet kullanımı

Kontrol

AYGK-6 Kurumda internet kullanımının güvenli şekilde yapılmasına ilişkin kontroller olmalıdır.

Kontrol varlığını değerlendirme soruları

- Doğru ve güvenli internet kullanımına ilişkin kullanım rehberi var mı?
- Kullanıcılar rehberin içeriğinden haberdar edilmiş mi?
- İnternet bağlantısı ve izlenmesine yönelik yazılı prosedürler var mı?
- Sistem yöneticileri ve kullanıcıların sorumluluklarını düzenleyen yazılı prosedürler var mı?

Kontrol etkinliğini inceleme yöntemi

- İnternet kullanımına ilişkin rehberin aşağıdaki hususları içerip içermediğinin incelenmesi:
  - Güvenlik politikası ile ilgisinin kurulması
  - Kullanıcı, bilişim sistemleri ve güvenlik yönetimi sorumlulukları
  - İzin verilen hizmetler
  - Bu hizmetlerin kabul edilebilir kullanım kuralları ve kuralların ihlali durumunda yaptırımlar
  - Yürürlükteki mevzuata uygun ağ izleme prosedürleri
  - Ahlaki tutumlar
  - E-posta gönderme ve tutma kuralları
  - Kullanıcı eğitim gereksinimleri
  - İşbirliği yapılabilecek ortaklar arasında anlaşma kuralları
- Tüm kullanıcıların rehberi okuduklarını, anladıklarını ve izleyeceklerini gösteren imzalarının olup olmadığının belirlenmesi
- İnternet bağlantısını gösteren belgelerin aşağıdaki hususları içerip içermediğinin tespit edilmesi:
  - Ağ çevre elemanlarının tanımlanması
  - Erişim noktalarının tanımları
  - Bütün modem bağlantılarının tanımlanması
  - Yönlendiriciler ve varsa proxy sunucularının konfigürasyonu
  - Günlük kayıtlarının güvenli depolanmasının tanımlanması
- İzleme faaliyetlerine ilişkin belgelerin aşağıdaki hususları içerip içermediğinin belirlenmesi:
  - Yedekleme kaynakları da dahil internet bağlantısının yönetimi ve bakım sorumluluklarının tanımlanması

- Güvenlik duvarı günlük kayıtlarının gözden geçirilmesi
- Mevcut sunuculardan işlemlerin gözden geçirilmesi
- Kullanıcı faaliyetleri günlük kayıtlarının gözden geçirilmesi
- Ağ istatistiklerinin gözden geçirilmesi
- Güvenlik olayları veya girişimlerinin izlenmesi

- Kullanıcıların sorumluluklarına yönelik prosedürlerin aşağıdaki hususları içerip içermediğinin incelenmesi:
  - Bilişim sistemleri güvenlik politikalarına, kullanım rehberlerine ve diğer mevzuata bağlı kalması
  - Telefon veya e-posta yoluyla kullanıcı şifrelerinin kimseye verilmemesi
  - Ağa erişim için kullanılan şifrelerin aynılarının internet ortamında asla kullanılmaması
  - İnternetten indirilen verilerin kullanılmadan önce kötü niyetli yazılımlara karşı taranması
- Sistem yöneticilerinin sorumluluklarına ilişkin prosedürlerin aşağıdaki hususları içerip içermediğinin incelenmesi:
  - İnternet güvenlik duvarları, yönlendiriciler, sunucular ve diğer teçhizatın kullanımda tutulması
  - Kullanımda olan sistem ve uygulamaların tehdit ve zaaflarının izlenerek güncellenmesi
  - Bilgi güvenliğinde görevli personelin işletmenlik, sistem çözümleyicisi veya programcı gibi ilave işlerin verilmesine yönelik sınırlama getirilmesi
  - Kullanıcılara internet kullanımına yönelik rehber konusunda bilgi verilmesi
  - Tüm günlük kayıtların izlenmesi ve gerekenlerin üst yönetime raporlanması
  - Üst düzey yöneticilerin de internet politikasını düzenlemesi, politika ve ilgili süreçleri izlemesi, yeterli kaynakları tahsis etmesi ve Bilgi İşlem Birimini bu politikaların uygulanması için yetkilendirmesi

Kontrol varlığını değerlendirme soruları

- Kurum çalışanların internet erişiminin (ziyaret edilen siteler, indirilen programlar, gerçekleştirilen anlık görüşme ve yazışmalar…) sisteme olası etkileri konusunda bilgi verilmiş mi?
- Çalışanların internete erişiminden kaynaklanabilecek riskleri önleyecek kontroller oluşturulmuş mu?

Kontrol etkinliğini inceleme yöntemi

- İnternet erişiminin sisteme olumsuz etkilerini önlemek için oluşturulan kontrollerin aşağıdaki hususları içerip içermediğinin incelenmesi:
  - Çalışanlara internetten elde edilen bilginin kalitesine güvenilmemesi, bilginin güncellenememe ihtimali olduğu bilincinin verilmesi

- Kurum ihtiyacı doğrultusunda içerik filitreleme sistemleri kullanılarak istenilmeyen sitelere (pornografi, oyun, kumar, şiddet içeren vs) erişimin engellenmesi
- İnternet tarayıcılarının güvenlik zaaflarının takip edilmesi ve güncellemelerinin yapılması
- Çok kullanılan tarayıcıların ekinde sunulan program yazılımları saldırganlar için açıklar ihtiva ettiğinden sadece güvenli tarayıcıların kullanılmasının sağlanması ve bu tür ek yazılımların kurulması ve konfigürasyon değişikliklerinin yapılmasına izin verilmemesi
- Ziyaret edilen siteleri ve bu sitelerde yapılan faaliyetleri gösteren ve kullanıcı için kolaylıklar içeren çerezler (cookies), şifrelere ilişkin bilgileri de içerebildikleri için güvenli olmadıklarından bunlardan yararlanma ve gerektiğinde silmeye ilişkin prosedürlerin belirlenmesi.
- Program indirmelerin belirli bir kurala bağlı olması ve uzantısı ".exe .lnk .dll .shs .hta .com .vbs .vbe .js .jse .bat .cmd .vxd .scr .shm .pif .chm" gibi dosyaların indirilmesine veya e-posta ile alınmasına izin verilmemesi
- İnternet üzerinden indirilen tüm dosyaların kullanılmadan önce kötü niyetli yazılımlara karşı taranması (spyware dahil)
- İnternet üzerinden kurum tarafından onaylanmamış ve korsan yazılımların indirilmesinin engellenmesi
- İnternet aracılığıyla sohbet (IRC) uygulamalarına kurumda izin verilmemesi; gerekli olduğu durumlarda önemli uygulama programlarının olmadığı ve sisteme bağlı olmayan yalnız bir bilgisayardan uygulamanın yapılması ve şifre veya herhangi bir gizli bilginin verilmemesi için önlem alınması
- Tüm faaliyetlerin izlenmesi ve gerektiğinde üst birimlere kural ihlallerinin bildirilmesi

2.1.4 MANTIKSAL ERİŞİM KONTROLLERİ

Mantıksal erişim kontrollerinin amacı, işletim sistemine, ağa, veri tabanına ve uygulama programlarına yetkisiz erişimin önlenmesi ve bilginin değiştirilmesi, açığa çıkarılması ve kaybına karşı korunmasıdır.

Mantıksal erişim kontrolleri, hem sistem hem de uygulama düzeyinde ortaya çıkabilir. Bilişim sistemi ortamındaki erişim kontrolleri ağa, işletim sistemine, sistem kaynaklarına, veri tabanına ve uygulama programlarına erişimi sınırlandırırken, uygulama düzeyindeki kontroller, tek tek uygulamalar bünyesindeki kullanıcı faaliyetlerini kısıtlar.

2.1.4.1 MANTIKSAL ERİŞİM POLİTİKALARI

Kontrol Hedefi

Kurum bilişim sistemlerine yetkisiz mantıksal erişimi önleyecek politika ve prosedürleri belirlemektir.

Riskler

Mantıksal erişim kontrollerinde kurumca politika ve prosedürlerin tanımlanmamış olması durumunda ortaya çıkabilecek riskler aşağıda belirtilmiştir:

- Kurum varlıklarına erişimde yetki karmaşıklığına, sorumluların belirlenememesine, kullanıcıların yeterli düzeyde bilgilenememelerine yol açması
- Yetersiz şifre uygulamalarının, sisteme ve uygulama programlarına yetkisiz erişimi kolaylaştırması
- Kullanıcıların kim olduklarının ve erişim seviyelerinin belirlenememesi, ayrıcalıklı kullanıcıların izlenememesi, yetki ve sorumlulukların işin gereğine uygun tespit edilememesi (yetersiz veya aşırı yetkilendirme)
- Kullanıcı şifrelerinin çalınması ve kullanılması
- İşten ayrılan personelin sisteme yetkisiz erişebilmesi
- Erişim politikasından sapmaların tespit edilememesi
- Yetkisiz erişim teşebbüslerinin ve etkilerinin belirlenememesi
- Yönetimce gerekli önlemlerin alınamaması

Temel Kontroller

Kurum bilişim sistemlerinde mantıksal erişim kontrollerine ilişkin politika ve prosedürlerin olmaması veya yetersiz olması sonucu meydana gelecek riskleri minimize edecek temel kontrol faaliyetleri şunlardır:

- Sistem ve uygulama programlarına erişimin güvenli olmasını sağlayan bir mantıksal erişim politikası olmalıdır.
- Kurumun şifre politikası olmalıdır.
- Kullanıcı erişim yönetimine ilişkin prosedürler tanımlanmış olmalıdır.
- Sistem ve uygulama programlarına erişimler kayıt altına alınmalı ve izlenmelidir.
- Yetkisiz erişimler raporlanmalı ve yönetimce gereken işlemler süratle yapılmalıdır.

Kontrollerin Değerlendirilmesi

Erişim politikası

Kontrol	**EP-1** Kurumun etkin bir mantıksal erişim politikası olmalıdır.
Kontrol varlığını değerlendirme soruları	▪ Kurumun işletim sistemine, ağa ve uygulama programlarına yetkili ve güvenli erişimi içeren yazılı mantıksal erişim politikası var mı?
Kontrol etkinliğini inceleme yöntemi	▪ Yazılı mantıksal erişim politika belgelerinde aşağıdaki hususlara yer verilip verilmediğinin incelenmesi: o Kullanıcıların hak ve sorumlulukları o Sistem yöneticilerinin hak ve sorumlulukları o Erişim verilmesine ilişkin esaslar, bunların gözden geçirilmesi veya bu hakların kaldırılması o Hassas bilgi ile yapılabileceklerin belirlenmesi ve yanlış kullanımının yol açacağı problemler o Kullanıcılara erişim hak ve sorumluluklarıyla ilgili yazılı bir bildirge verilmesi ve bunun personele imzalatılması o Politikaların güncellenmesine ilişkin esaslar

Şifre politikası

Kontrol	**EP-2** Kurumun yazılı bir şifre politikası olmalıdır.
Kontrol varlığını değerlendirme soruları	▪ Kurumun güçlü şifre oluşturma, oluşturulan şifrelerin korunması ve değiştirilmesine ilişkin politikası var mı?
Kontrol etkinliğini inceleme yöntemi	▪ Kurumun yazılı şifre politikasının aşağıdaki hususları içerip içermediğinin incelenmesi: o Temel güçlü şifre oluşturma kuralları ♦ Altıdan aşağı olmamak üzere minimum karakter uzunluğunun belirlenmesi ♦ Alfabetik ve sayısal karakterlerin karışık kullanılması ♦ Şifrede alfabetik karakterlerde büyük ve küçük harflerin karışık kullanılması ♦ Her sistem kullanıcısının kendine özel ve kendisi tarafından tanımlanmış bir şifre kullanması ♦ Kullanıcıların basit ve kolay tahmin edilebilir şifre seçiminin engellenmesi ve bu konularda kullanıcıların bilgilendirilmesi ♦ Değişik sistemler için farklı şifrelerin kullanılma zorunluluğu o Temel şifre koruma kuralları ♦ Kullanıcı şifrelerinin kodlanarak şifre dosyalarında saklanması

- Şifre dosyalarına yetkisiz erişim denemelerinin raporlanması
- Kullanıcı şifresinin başkasıyla paylaşılmaması, kağıtlara yada elektronik ortamlara kaydedilmemesi
- Görevden ayrılan personele ait şifrelerin hemen iptal edilmesi

o Temel şifre değiştirme kuralları

- Belirli periyotlarla şifre değiştirme zorunluluğu getirilmesi
- Önceden kullanılan kullanıcı şifrelerinin kayıtları belli bir süre (örneğin geçen 12 ay boyunca) saklanması ve yeniden kullanımının engellenmesi
- Şifre değişikliklerinde önceki şifrenin kullanılamaması
- Uygulama programlarının kurulumunu takiben varsayılan satıcı şifrelerinin hemen değiştirilmesi
- Şifre unutulması durumunda izlenecek prosedürlerin belirlenmesi

- Örnekleme yoluyla seçilen uygulamalarda bu kurallara uyulup uyulmadığının incelenmesi
- Kullanıcılardan kişisel şifrelerini gizli tutma ve çalışma grubu şifrelerini sadece grup üyelerinin içinde tutmaları için bir bildirge imzalamalarının istenip istenmediğinin tespit edilmesi

Kullanıcı erişim yönetimi

Kontrol

EP-3 Kullanıcıların erişim haklarının tanınmasına ve kullanılmasına ilişkin kurallar belirlenmiş olmalıdır.

Kontrol varlığını değerlendirme soruları

- Kullanıcıların yetki ve sorumluluklarına bağlı olarak sisteme erişim haklarının tanınmasına ve kullanılmasına ilişkin kurallar belirlenmiş mi?
- Ayrıcalıklı erişim haklarının tanınmasına ve kullanılmasına ilişkin kurallar belirlenmiş mi?
- Sistem yöneticilerinin ayrıcalıklı yetkilerini nasıl kullandıkları izleniyor mu?
- Bu düzenlemeler düzenli olarak gözden geçiriliyor mu?

Kontrol etkinliğini inceleme yöntemi

- Kullanıcı erişim yönetimine ilişkin düzenlemelerin aşağıdaki konuları içerecek şekilde oluşturulup oluşturulmadığının incelenmesi:
  - Yapılan işin yetki itibariyle tanımlanması
  - İş amaçları, güvenlik politikaları ve daha önce yapılan kaynak tasnifi (veri dosyaları, uygulama programları, şifre dosyaları, sistem yazılımları ve araçları, günlük kayıtları…) dikkate alınarak uygun erişim seviyesinin belirlenmesi
  - Kullanıcı kimliklerinin tanımlanması ve bu kimliklerin hesap ve şifrelerinin belirlenmesi

- Kullanıcıların sadece kendi hesap ve şifrelerinin kullanılması konusundaki sorumluluklarının belirlenmesi
- Kullanıcı kayıtlarının düzenli olarak gözden geçirilmesi ve güncellenmesi
- Erişim yetkilerinin, sistem sahibi veya yönetim tarafından onaylanması
- Kullanıcı kayıtlarının saklanması
- Görev yeri değişen veya işten ayrılan kullanıcıların erişim haklarının hemen kaldırılması
- Kullanıcıların erişim hakları belirli aralıklarla örneğin 6 aylık zaman diliminde ve her değişiklikten sonra gözden geçirilmesi
- Özel ayrıcalıklı erişim hakları için yetkilendirmeler daha sık aralıklarla örneğin 3 aylık zaman dilimi içinde gözden geçirilmesi

- Örnekleme yoluyla seçilen kullanıcılar ile görüşme yapılması ve yaptıkları işlemlerin günlük kayıtları aracılığıyla incelenmesi
- Ayrıcalıklı kullanıcıların yaptıkları işlemlerin günlüklerde kayıt altına alınıp alınmadığının ve üst yönetime raporlanıp raporlanmadığının incelenmesi

Erişim kayıtlarının tutulması ve izlenmesi

Kontrol

EP-4 Sistem (işletim sistemi, ağ, uygulama programı) erişimleri günlük tutularak kayıt altına alınmalıdır.

Kontrol varlığını değerlendirme soruları

- Yapılan işlemlerin takibine imkan veren günlük kayıtları tutuluyor mu?
- Günlük kayıtları arşivleniyor mu?
- Günlük kayıtlarının devre dışı bırakılamaması ve değiştirilememesi için önlem alınmış mı?

Kontrol etkinliğini inceleme yöntemi

- Sistem yöneticileri ve kullanıcılar ile görüşme yapılarak, sistemle ilgili kayıtlar incelenerek ve günlük analiz yöntemleri kullanılarak yapılan faaliyetlerin denetim veya güvenlik günlüklerinde aşağıdaki bilgileri içerecek şekilde kaydedilip kaydedilmediğinin belirlenmesi:
  - Kullanıcı kimlikleri
  - Oturum açma ve kapama tarihleri ve zamanları
  - Eğer mümkünse terminal kimliği veya yerleşimi
  - Başarılı veya reddedilmiş sistem erişim denemelerine ilişkin kayıtlar
  - Başarılı veya reddedilmiş veri ve diğer kaynak erişim denemelerine ilişkin kayıtlar
- Örnekleme yoluyla seçilen günlük kayıtlarının arşivlenip arşivlenmediğinin belirlenmesi

- Günlük kayıtlarının devre dışı bırakılıp bırakılmadığının veya değiştirilip değiştirilmediğinin tutulan günlük kayıtları üzerinden sistem ve yardımcı sistem araçları yardımıyla incelenmesi

Yetkisiz erişimlerin raporlanması

Kontrol

EP-5 Yetkisiz erişimler raporlanmalı ve yönetimce gereken işlemler süratle yapılmalıdır.

Kontrol varlığını değerlendirme soruları

- Yetkisiz erişim teşebbüsleri ve işlemlerine ilişkin günlükler düzenli olarak yönetime raporlanıyor mu?
- Bu raporların gereği yapılmasını sağlayacak prosedürler var mı?
- Raporlar arşivleniyor mu?

Kontrol etkinliğini inceleme yöntemi

- Yetkisiz erişim teşebbüslerine ilişkin yönetime sunulan raporların istenerek incelenmesi ve bu raporlarda belirtilen hususlara ilişkin olarak işlem yapılıp yapılmadığının tespit edilmesi

2.1.4.2 İŞLETİM SİSTEMİ ERİŞİM KONTROLLERİ

Kontrol Hedefi

Yetkisiz erişimin kontrol edilmesi suretiyle işletim sisteminin güvenli bir ortamda çalışmasını sağlamaktır.

Riskler

Erişim kontrollerindeki zayıflık nedeniyle sistemde karşılaşılabilecek riskler aşağıda belirtilmiştir:

- Sistem kaynaklarına ve uygulama programlarına yetkisiz erişim
- Sistemdeki güvenlik yazılımlarına ulaşılabilmesi
- Kullanıcı hesaplarına izinsiz girilmesi ve bu hesapların yetkisiz kullanımı
- Sistem yapılandırmalarında kullanılan yardımcı programlarının kullanımının kısıtlanmaması sonucu önceden tanımlanmış erişim kısıtlamalarının ortadan kalkması

Temel Kontroller

İşletim sistemine yetkisiz erişimin önlenmesi için uygulanabilecek erişim kontrollerinin bazıları aşağıda belirtilmiştir.

- Belirli yerlere ve taşınabilir teçhizatlara bağlantıları doğrulamak için otomatik terminal tanımlaması olmalıdır.
- Oturum açma uygulamaları sisteme yetkisiz erişimleri en aza indirecek şekilde tasarlanmalıdır.
- Sisteme giriş onaylanmadan önce kullanıcı kimlikleri doğrulanmalıdır.
- Sistem yapılandırmalarında kullanılan yardımcı programların kullanımı kısıtlanmalı ve sıkı bir şekilde kontrol edilmelidir.
- Sisteme giriş yapıldıktan sonra, belirli bir süre kullanılmadıklarında sistem otomatik olarak kapanmalıdır.
- Sisteme bağlı kalma sürelerini sınırlayan bir kontrol sistemi olmalıdır.

Kontrollerin Değerlendirilmesi

Terminal doğrulaması

Kontrol

İSEK-1 Belirli yerlere ve taşınabilir teçhizatlara bağlantıları doğrulamak için otomatik terminal tanımlaması olmalıdır.

Kontrol varlığını değerlendirme soruları

- Oturumun sadece belirli yerlerden veya bilgisayar terminallerinden başlamasını sağlayan otomatik terminal (uç birim) doğrulaması tekniği kullanılmakta mı?

Kontrol etkinliğini inceleme yöntemi

- Sisteme erişim yetkisi olan terminallerin listesinin elde edilmesi ve hangi işlemleri başlatmaya veya almaya izinli olduğunun sistem yöneticisi ile görüşme yapılarak belirlenmesi
- Sisteme erişim yetkisi olan terminallerin dışında erişim sağlanıp sağlanmadığının günlük kayıtlarından tespit edilmesi

Oturum açma

Kontrol

İSEK-2 Oturum açma uygulamaları sisteme yetkisiz erişimi en aza indirecek şekilde tasarlanmalıdır.

Kontrol varlığını değerlendirme soruları

- Sisteme erişmek için güvenli oturum açma (logon) uygulamaları var mı?

Kontrol etkinliğini inceleme yöntemi

- Güvenli oturum açma uygulamalarının sağlanabilmesi için sisteme tanıtılan otomatik kontrol mekanizmasının aşağıdaki hususları içerip içermediğinin belirlenmesi:
  - Oturum açma süreci tamamlanmadan sistem ve uygulama tanımlayıcılarının görüntülenmemesi
  - Bilgisayarın yalnızca yetkili kişiler tarafından kullanılacağını gösteren bir uyarı mesajının görüntülenmesi
  - Oturum açma esnasında yetkisiz kullanıcıya yardım edecek şekilde yardım mesajlarının sağlanmaması
  - Oturum açma bilgisini sadece tüm girdi bilgilerinin girilmesiyle geçerli kılınması
  - Bir hata söz konusuysa sistem bilgisinin hangi kısmının doğru veya yanlış olduğunu göstermemesi
  - Başarısız oturum açma girişimlerinin sınırlandırılması
  - Sınırlandırılma varsa aşağıdaki hususların tespit edilmesi
    - Başarısız girişimlerin kaydedilmesi
    - Daha sonraki oturum açma denemelerine izin vermeden önce zamanın geciktirilmesi veya belli yetkilendirmeler olmadan sonraki denemelerin reddedilmesi
    - Veri bağlantılarının kesilmesi
  - Oturum açma için izin verilmiş zaman sınırlaması ve eğer bu zamanlar aşılırsa sistemin oturumu sona erdirmesi
  - Başarılı bir oturum açma sürecinin tamamlanması sonrasında, başarılı oturum açma işleminin tarih ve saati ve

son başarılı oturum açma işleminden bu yana başarısız logon işlemlerinin ayrıntılarına ilişkin bilgilerin görüntülenmesi

- Kullanılmayan sistemin otomatik olarak kendini sonlandırması
- Eş zamanlı olarak birden fazla oturumun açılmasının sınırlandırılması

- Örnekleme yoluyla seçilen kullanıcılar ile görüşme yapılması ve bu kuralların etkin çalışıp çalışmadığının incelenmesi

Kimlik tanıma ve doğrulama

Kontrol

İSEK-3 Sisteme giriş onaylanmadan önce kullanıcı kimlikleri doğrulanmalıdır.

Kontrol varlığını değerlendirme soruları

- Kullanıcı kimlik doğrulaması yapılmakta mı?
- Kullanıcı kimliklerinin doğrulanması için ilave önlemler var mı? (Şifre, pin kodu; akıllı kart, manyetik kart veya anahtar vs.; kullanıcının fiziksel karakteristiğini taşıyan parmak izi, avuç içi izi, retina izi, ses; imza)

Kontrol etkinliğini inceleme yöntemi

- Örnekleme yoluyla seçilen kullanıcıların kimlik doğrulama denetimi yapılarak sistemin kimlik doğrulama yapıp yapmadığının incelenmesi

Sistem yapılandırma yardımcı programlarının kullanımı

Kontrol

İSEK-4 Sistem yapılandırmalarında kullanılan yardımcı programların kullanımı kısıtlanmalı ve sıkı bir şekilde kontrol edilmelidir.

Kontrol varlığını değerlendirme soruları

- Sistem yapılandırmalarında kullanılan yardımcı programların kullanılmasına ilişkin bir prosedür tanımlanmış mı?

Kontrol etkinliğini inceleme yöntemi

- Sistem ve uygulama kontrollerini geçersiz hale getirebilen sistem yardımcı programlarının kullanımı ve sıkı bir şekilde kontrolüne ilişkin prosedürlerin aşağıdakileri içerip içermediğinin incelenmesi:
  - Kimlik doğrulama prosedürlerinin sistem yardımcı programları için de kullanılması
  - Sistem araçlarının uygulama yazılımlarından ayrı tutulması
  - Sistem yardımcı programlarının kullanımının az sayıda yetkili kişilerle sınırlandırılması
  - Sistem yardımcı programlarının kullanabilirliğinin kısıtlanması, örneğin araçlara erişimin yetki verilen değişim süresi boyunca kullanılması ve bu sürenin sonunda kaldırılması
  - Sistem yardımcı programlarının her kullanımının kaydının tutulması
  - Sistem yardımcı programlarının tüm bağlantılarının kesilmesi

- Sistem yardımcı programları için yetki düzeylerinin tanımlanması ve belgelenmesi
- Tüm gereksiz yazılımların kaldırılması

Terminal zaman aşımı

Kontrol	**İSEK-5** Sisteme giriş yapıldıktan sonra, belirli bir süre kullanılmadığında sistem otomatik olarak kapanmalıdır.
Kontrol varlığını değerlendirme soruları	▪ Belirli bir süre kullanılmadığında sistemin otomatik olarak kapanmasını sağlayacak mekanizmalar oluşturulmuş mu?
Kontrol etkinliğini inceleme yöntemi	▪ Örnekleme yoluyla seçilen terminallerde sisteme şifre ile giriş yapıldıktan sonra, sistem açık bırakılarak belirli bir süre kullanılmadığında sistemin otomatik olarak kapanıp kapanmadığının incelenmesi

Bağlantı süresinin sınırlanması

Kontrol	**İSEK-6** Kurum hassas bilgilerinin /uygulamalarının bulunduğu sisteme bağlı kalma süreleri sınırlandırılmalıdır.
Kontrol varlığını değerlendirme soruları	▪ Kurum hassas bilgilerinin /uygulamalarının bulunduğu sistemlere bağlanan terminallerin sisteme bağlı kalma sürelerini sınırlayan bir uygulama var mı?
Kontrol etkinliğini inceleme yöntemi	▪ Özellikle, yüksek riskli alanlarda bulunan terminallerde, yığın dosya transferleri veya kısa süreli ve düzenli interaktif oturumlar için önceden belirlenmiş bağlantı sürelerine uyulup uyulmadığının test edilmesi ▪ Fazla çalışma gereği yoksa normal çalışma saatlerine göre belirlenmiş bağlantı sürelerine uyulup uyulmadığının günlük kayıtları incelenerek veya bu süreler dışında sisteme girme denemelerinde bulunularak test edilmesi

2.1.4.3 UYGULAMA PROGRAMLARINA ERİŞİM KONTROLLERİ

Kontrol Hedefi	Uygulama programlarını ve bunların veri dosyalarını izinsiz erişime, değiştirmeye ve silmeye karşı korumaktır.
Riskler	Bu alanda karşılaşılabilecek risklerin bir kısmı aşağıda belirtilmiştir. ▪ Uygulama programlarından üretilecek bilgilerin güvenirliliğinin zedelenmesi ▪ Hatalı işlem yapılması ▪ Verilerin değiştirilmesi ▪ Program ve verilerin kaybolması ▪ Verilerin çalınması

Temel Kontroller

Uygulama programlarına yetkisiz erişimin önlenmesi için uygulanabilecek kontroller aşağıda belirtilmiştir:

- Erişim politikalarına uygun olarak uygulama programlarına erişim kısıtlanmalıdır.
- Ana dosyalara erişim sınırlandırılmalıdır.

Kontrollerin Değerlendirilmesi

Erişim kısıtlaması

Kontrol

UPEK-1 Belirlenmiş erişim politikalarına uygun olarak uygulama programlarına erişim kısıtlanmalıdır.

Kontrol varlığını değerlendirme soruları

- Uygulama programlarının erişimine, belirlenmiş erişim politikalarına göre kısıtlama getirilmiş mi?

Kontrol etkinliğini inceleme yöntemi

- İncelemeye alınan uygulama programları ile ilgili görüşme yapılarak ve sistem dokümanları ve belgeleri incelenerek aşağıda yazılı kısıtlamaların uygulanıp uygulanmadığının belirlenmesi:
  - Uygulamaya özgü şifrelerin kullanılması
  - Kısıtlı uygulama menülerinin oluşturulması
  - Her uygulama için kullanıcı ve grup profilleri oluşturulması
  - Kullanıcıların erişim haklarının sınırlandırılması, örneğin sadece okuma, yazma, silme veya yürütme yetkisi verilmesi
- Hassas bilgiler barındıran uygulama programlarının diğer programlardan izole edilip edilmediğinin incelenmesi
- Bu programlar eğer paylaştırılmış bir ortamda çalışmak zorunda ise, kaynakları paylaşacak olduğu uygulama sistemleri tanımlanmış ve duyarlı uygulamanın sahibi tarafından onaylanmış olup olmadığının incelenmesi

Ana dosyalara erişim

Kontrol

UPEK-2 Ana dosyalara erişim sınırlandırılmalıdır

Kontrol varlığını değerlendirme soruları

- Ana dosyalara erişimin yetki dahilinde yapılması için yazılı bir kontrol prosedürü oluşturulmuş mu?

Kontrol etkinliğini inceleme yöntemi

- Oluşturulmuş yazılı kontrol prosedürünün aşağıdaki hususları içerip içermediğinin incelenmesi:
  - Değiştirme yetkisi
  - Giriş yetkisi
  - Yapılan değişikliklerin bağımsız birimce gözden geçirilmesi
  - Yapılan değişikliklerin günlük kayıtlarının tutulması
  - Yapılacak değişiklikleri için terminal tahsis edilmesi
- Ana dosyadaki kalıcı verilerde yapılan değişiklerin kanıtlayıcı belgelerle kayıt altına alınıp alınmadığının tespit edilmesi

- Bu kayıtların aşağıdaki hususları kapsayıp kapsamadığının belirlenmesi:
  - Değişikliğin haklı gerekçesi
  - Uygulanacak yeni değerlerin özellikleri, hangi tarihten itibaren geçerli oldukları
  - Uygun seviyede, yetkili kişiler tarafından değişikliklerin yapıldığına dair onaylar
  - Talep edilen değişikliklerin doğru bir şekilde gerçekleştiğini gösteren uygulama sonrası kontrol kayıtları
  - Sistem sahipleri ve kullanıcıları için değişen veri elemanlarının değişiklik öncesi ve sonrasına ait birer kopyası

2.1.5 İŞLETİM KONTROLLERİ

İşletim kontrollerinin amacı bilişim sisteminin kendinden beklenen faaliyetlerin sürekliliğini ve güvenliğini sağlayacak şekilde işletilmesidir.

İşletim kontrolleri aşağıdaki alanlara göre incelenir:

- *İşletim sistemi ve bilgisayar işlemleri kontrolleri:* Uygulama yazılımların üzerinde çalıştığı işletim sisteminin kurulum ve işletilmesi ile bakım işlemlerinin sorunsuz yürütülmesini ve tüm bilgisayar işlemlerinin güvenli bir şekilde gerçekleştirilmesini sağlamaya yönelik her türlü kontrollerdir.
- *Veri tabanı güvenlik kontrolleri:* Birbirleriyle ilişkili verilerin güvenli bir şekilde kaydedilip depolanmasını, belgelendirilmesini ve gerektiğinde de güvenli ve çok amaçlı kullanılmasını sağlayacak her türlü kontrollerdir.

2.1.5.1 İŞLETİM SİSTEMİ VE BİLGİSAYAR İŞLEMLERİ KONTROLLERİ

Kontrol Hedefi

Kurumun ana faaliyetlerine yönelik olarak kullanmakta olduğu işletim sisteminin gerektiği gibi çalışmasını ve bunlar üzerindeki bilgisayar işlemlerinin sorunsuz yürütülmesini sağlamaktır.

Riskler

İşletim sistemi kontrollerinin yeterli düzeyde kurulamaması durumunda karşılaşılabilecek riskler şunlardır:

- İhtiyaca uygun olmayan sistem temini
- Yetkisiz erişim
- Sistem çökmesi
- İşlemlerin zorlaşması
- Hizmetin gerçekleşmemesi
- Ortam araçlarının çalınması, bozulması veya bunlara ihtiyaç olduğunda erişilememesi
- Kaynak yetersizlikleri
- Kullanıcıların karışması
- Aktif olmayan hesapların askıya alınamaması, silinememesi
- Program ve verilerin bozulması, kaybolması, değiştirilmesi
- Program ve verilerin çalınması
- Olay ve problem yönetimine ilişkin yetkili birim ve prosedürlerin oluşturulmaması sonucunda olayların ve problemlerin çözümünün gerçekleştirilememesi veya çözümde gecikmeler meydana gelmesi ve bunlardan dolayı iş süreçlerinde aksama meydana gelerek hizmet kalitesinin düşmesi
- Problem Yönetiminin bir birim veya ekip tarafından üstlenilip yerine getirilmemesi

Temel Kontroller

İşletim siteminin düzenli çalışmasını ve güvenli veri üretmesini sağlayacak kontroller aşağıda yer almaktadır:

- İşletim sisteminin seçimi ve kurulumuna ilişkin prosedürler tanımlanmalı ve kurum sistem ihtiyaçlarının giderilmesinde bu prosedürlere uygun hareket edilmelidir.

- İşletim sisteminin güvenli yönetilmesine yönelik tüm süreçler ve bunlara ilişkin görev ve sorumluluklar ve onay işlemleri yazılı prosedürlere bağlanmalıdır.
- Güvenlik amacıyla konsollara erişim sadece yetkili kişilerle sınırlandırılmalıdır.
- Sisteme ilişkin güncel yamaların takip ve kontrol edilerek gerektiğinde kullanılmasını sağlayacak prosedürler bulunmalıdır.
- İşletim sisteminin güçlendirilmesine yönelik kontrol listeleri hazırlanmalı ve bu listelere göre gereksiz servisler devre dışı bırakılmak suretiyle minimum özelliklerle konfigürasyon yapılmalı, böylece sistemin performansı artırılmalıdır.
- Yeniden çalıştırma, yedekleme, sistem ve geçici dosya temizlemeleri, disk birleştirmesi ve kapasite kontrolleri gibi işlemlerle sistemin düzenli bakım ve kontrolünün yapılması sağlanmalıdır.
- Olası sistem başarısızlıklarını önleme amacıyla belli aralıklarla geri yükleme noktası oluşturulmalıdır.
- Sistem kapasite ve performans durumunun düzenli olarak izlenmesi sağlanarak gelecekte gerekli olacağı düşünülen kapasite tahminleri ve planları yapılmalıdır.
- Çalışma saatleri dışında veya ilgili personelin yokluğu durumunda sistemin çalışmasında ortaya çıkabilecek sorunlara müdahale edilmesini sağlama amacıyla bilgi işlem biriminde devamlı personel bulundurulmalıdır.
- Bilgi ortamı araçlarının (kasetler, manyetik ve optik diskler vs) oluşturulma, transfer, korunma ve saklanma gibi işlemleri etkin bir şekilde yönetilmelidir.
- Bilişim sisteminden sorumlu birimin diğer birimlere sağlayacağı hizmetler yazılı olarak tanımlanmış olmalıdır.
- Olay yönetimine ilişkin önceden belirlenmiş prosedürler olmalıdır. Olayların takip ve çözümü için bunların tanımlanması, kaydının tutulması, analiz ve destek hizmetlerinin sağlanmasına yönelik prosedürler belirlenmeli, olayın işe etkisi değerlendirilmeli ve bir daha olmasını önleyecek çarelere ilişkin planlar yapılmalıdır. Ayrıca olayların istatistiklerinin çıkarılarak yönetime bildirilmesi sağlanmalıdır.
- Yine olay yönetimi ile işbirliği içerisinde bulunmak kaydıyla problemlerin yönetimine ilişkin prosedürler belirlenerek ve yardım masası kurularak problemlerin uzman personele aktarılmasını sağlayacak yapı oluşturulmalıdır.

Kontrollerin Değerlendirilmesi

Seçim ve kurulum

Kontrol

İSBİK-1 İşletim sisteminin seçimi ve kurulmasına ilişkin prosedürler bulunmalıdır.

Kontrol varlığını değerlendirme soruları

- İşletim sistemi seçimi için belirlenmiş bir prosedür var mı?
- Sistem kurulumunda güvenlik seçenekleri belirlenmiş mi (güvenlik seçenekleri aktif mi)?

- İşletim sisteminde güvenlikle ilgili varsayılan değerleri değiştirmede kullanılacak bir prosedür var mı?
- Sistem araçlarını korumaya yönelik prosedür var mı?

Kontrol etkinliğini inceleme yöntemi

- Kurum ihtiyaçlarına uygun işletim sistemi seçim kriterlerinin oluşturulup oluşturulmadığının belirlenmesi
- Örnekleme yoluyla seçilecek ana bilgisayarlar ile kullanıcı bilgisayarlarındaki güvenlik parametrelerinin belirlenip belirlenmediğinin incelenmesi
- Özellikle kullanıcı bilgisayarlarındaki güvenlik seçeneklerinin yönetici yetkili mi ya da kullanıcı yetkili mi ayarlandığının incelenmesi
- Sistem araçlarına her türlü müdahaleyi engelleyen koruma uygulanıp uygulanmadığının belirlenmesi ve virüslerden korunma amacıyla gerçek zamanlı virüs tanımlama ve korunma sistemi kurulması
- Sistem bilgisayarlarına uzaktan erişim söz konusu ise sadece yetkili yönetici ve kullanıcıların erişimine izin verilecek şekilde düzenleme yapılması

İşletim sistemi yönetimi

Kontrol

İSBİK-2 İşletim sisteminin yönetimine ilişkin süreçler tanımlanmış olmalıdır.

Kontrol varlığını değerlendirme soruları

- İşletim sisteminin yönetimine ilişkin bir yazılı prosedür var mı?

Kontrol etkinliğini inceleme yöntemi

- İşletim sisteminin yönetimine ilişkin prosedürlerin aşağıdaki hususları içerip içermediğinin belirlenmesi:
  - Sistemin işletilmesine ilişkin görev ve sorumlulukların tanımlanması
  - Sistem açma ve kapama
  - Bellek kullanımının düzenlenmesi
  - Yedekleme ve yeniden kurma
  - Yedekleri uzak yerlere transfer
  - Yığın işlemleri planlama ve planları düzenleme
  - Bilgisayar ve ağ hatalarını çözme
  - Yeni ve değiştirilmiş yazılımın hayata geçirilmesi gibi işlemlerin onaydan geçirilmesi
- Örnekleme yoluyla seçilen personele ilişkin iş tanımları ile yaptıkları işler karşılaştırılarak, bu tanımların bilgisayar işlemlerinin sorunsuz yürütülmesini sağlayacak şekilde belirlenip belirlenmediğinin araştırılması

Konsollara erişim

Kontrol	**İSBİK-3** Konsollara erişim kısıtlanmalıdır.
Kontrol varlığını değerlendirme soruları	▪ Konsollara erişimde kısıtlama uygulamaları var mı?
Kontrol etkinliğini inceleme yöntemi	▪ Konsolların nerelerde bulunduğunun kontrol edilmesi ve bunlara erişimin yeterince güvence altına alınıp alınmadığının incelenmesi

Güncel yama kullanımı

Kontrol	**İSBİK-4** Güncel yamaların kullanılmasını sağlayacak prosedürler bulunmalıdır.
Kontrol varlığını değerlendirme soruları	▪ İşletim sistemine güncel yamaların uygulanmasını sağlayacak prosedürler var mı?
Kontrol etkinliğini inceleme yöntemi	▪ İşletim sistemine güncel yamaların uygulanmasını sağlayan prosedürlerin görüşme, belge incelemesi test prosedürleri uygulanarak aşağıdaki hususları içerip içermediğinin belirlenmesi: o Sistem yöneticilerinin açıklıkları kapatacak güvenlik güncelleştirme ve yamaları takip ve kontrol etmesi o En son yamaların uygulanıp uygulanmadığının belirlenmesi o Güvenlik yamalarının uygun bir şekilde tüm bilgisdayarlara dağıtılması o Yamaların tüm kuruma dağıtılmadan önce test ortamında uyumsuzluklara karşı test edilmesi o Gerektiğinde sisteme ilişkin yama programlarının otomatik olarak kullanılabilmesi o Yama uygulanmadan önce yedekleme yapılması o Uygulanan yamaların kaydının tutulması o Merkezi olarak güncelleştirme yamalarını uygulamayan bilgisayarlar takip edilerek gerekirse bunların da elle yüklenmesnin sağlanması ▪ İşletim sistemi kurulum planının, sistem kayıtlarının temin edilip incelenmesi ve işletim sistemi ve diğer sistem yazılımlarında yapılan değişikliklerin prosedürlere uygunluk açısından incelenmesi

Sistem güçlendirmesi

Kontrol	**İSBİK -5** İşletim sisteminin güçlendirilmesine ilişkin kontrol listeleri kullanılmalıdır.
Kontrol varlığını değerlendirme soruları	▪ İşletim sisteminin güçlendirilmesine ilişkin kontrol listeleri kullanılıyor mu?

- Standart güçlendirmesi yapılmış bir sistemde yapılan farklılaştırmalar yetkilendiriliyor mu?

Kontrol etkinliğini inceleme yöntemi

- İşletim sisteminin güçlendirilmesine ilişkin kontrol listesinin aşağıdaki hususları içerip içermediğinin incelenmesi:
  - Gerek sunucu gerekse kulanıcı bilgisayarlarında görevle ilgili servislerin açık olması ve faaliyeti etkilemiyorsa gereksiz servislerin durdurulması veya devre dışı bırakılması
  - İşletim sisteminin minimum özellikler ile konfigüre edilmesi
  - Kullanıcıların yetkilerinin ve uygulamaların sadece temel görevlerin yerine getirilebilmesine yetecek şekilde düzenlenmesi, yönetici ve kullanıcı dışındaki gereksiz kullanıcıların ve hesapların bulunmaması ve bu kullanıcıların yazma özelliği olan sürücüleri (Disket Sürücü, USB Disk, CD Yazıcı vb.) kullanamaması
  - Bilgisayarlarda gereksiz yere açık bulunan ve hangi amaçla açık olduğu bilinmeyen gereksiz servis portlarının kapatılması
  - Sistemle birlikte varsayılan olarak gelen "Administrator" hesabının kapatılarak bunun yerine yönetici yetkili hesap açılması ayrıca tuzak "adminstrator" hesabının açılması
  - İhtiyaç olmayan "guest" hesaplarının kapatılması ve boş oturumlara izin verilmemesi
  - Bilgisayar açılışında sabit disk bölmeleri dışındaki sürücü ve ortamların (Floppy Disket, CD, Ağ vb.) kullanılamaması
  - Sunucu bilgisayarda ve gerekli olan kullanıcı bilgisayarlarında BIOS giriş şifresinin etkin olması
  - Sunuculara yönelik olası servis ataklarına (DoS) karşı önem alınması
- Örnek bir sistem seçip söz konusu güçlendirme listesinin kullanılıp kullanılmadığının test edilmesi
- Standart güçlendirmesi yapılmış sistemin kontrol listesinden istisnalara yetki verilip verilmediğinin incelenmesi

Düzenli bakım

Kontrol

İSBİK-6 Sistemin düzenli bakım ve kontrolü yapılmalıdır.

Kontrol varlığını değerlendirme soruları

- Sistemin düzenli bakım ve kontrolünün yapılmasına ilişkin bir prosedür var mı?

Kontrol etkinliğini inceleme yöntemi

- Sistem bakım ve kontrolüne ilişkin prosedürlerin aşağıdaki hususları içerip içermediğinin incelenmesi:
  - Her bir sunucu için düzenli bakım uygulaması (yeniden çalıştırma, yedekleme, geçici dosya temizlemeleri, disk birleştirmesi, kapasite kontrolleri)
  - Bakım uygulamalarının kontrol ve değerlendirmesinin yapılması

	Geri yükleme
Kontrol	**İSBİK-7** Geri yükleme noktası oluşturulmalıdır.
Kontrol varlığını değerlendirme soruları	▪ Belli dönemlerde sistem geri yükleme noktası oluşturulmasına ilişkin bir uygulama var mı?
Kontrol etkinliğini inceleme yöntemi	▪ Sistem yöneticisi ile görüşme yapılması ve geri yükleme noktası oluşturulma tarihlerinin incelenmesi ▪ Sistem başarısızlıklarından sonra geri yükleme noktasının kullanılmasına ilişkin bir talimatın bulunup bulunmadığının tespit edilmesi
	Kapasite planlaması
Kontrol	**İSBİK-8** Kapasite planlaması yapılmalıdır.
Kontrol varlığını değerlendirme soruları	▪ Düzenli aralıklarla kapasite planlamasının yapıldığı bir uygulama var mı?
Kontrol etkinliğini inceleme yöntemi	▪ Görüşme yapılmak suretiyle kapasite planlamasının aşağıdaki hususlar dikkate alınarak yapılıp yapılmadığının incelenmesi: o Kapasite ve performans durumunun düzenli olarak izlenmesi o Gelecekte gerekli olacağı düşünülen kapasite tahminlerinin yapılması o Bu tahminlerin yapılmasında işlem hacmi, veri kayıtları, işlemci, bellek ve disk kullanımı gibi hususların dikkate alınması
	Personel bulundurma
Kontrol	**İSBİK-9** Bilgi işlem biriminde devamlı personel bulundurulmalıdır.
Kontrol varlığını değerlendirme soruları	▪ Çalışma saatleri dışında veya ilgili personelin yokluğu durumunda sistemin çalışmasında ortaya çıkabilecek sorunlara müdahale edilmesini sağlayacak bir personel istihdam politikası var mı?
Kontrol etkinliğini inceleme yöntemi	▪ Personel vardiya listesinin ve acil durum çağrı listesinin incelenmesi ▪ Bu acil durum çağrı listesinin güncelliğinin örnekleme yöntemiyle kontrol edilmesi
	Bilgi ortam araçları
Kontrol	**İSBİK -10** Bilgi ortamı araçları (kasetler, manyetik ve optik diskler vs) etkin bir şekilde yönetilmelidir.

Kontrol varlığını değerlendirme soruları

- Bilgi ortam araçlarının yönetimine ilişkin tanımlanmış bir prosedür var mı?

Kontrol etkinliğini inceleme yöntemi

- Bilgi ortam araçlarına ilişkin prosedürlerin incelenerek aşağıdaki hususları içerip içermediğinin belirlenmesi:
  - Bilgi ortam araçlarının yönetimine ilişkin görev, sorumluluk ve erişim yetkisinin tanımlanması
  - Bilgi ortam araçlarının sınıflandırılması (barkot, etiketleme vb.)
  - Bilgi ortam araçlarının envanter işlemlerinin belgeli olarak yapılması ve düzenli envanter kontrolü (sayımı)
  - Ortam araçlarının fiziksel ve çevresel güvenliği sağlanmış ortamlarda saklanması
  - Hizmet süresince ortam araçlarının teslim, kullanılma ve iade uygulaması
  - Gizli bilgi içeren ortam araçlarının kullanılması
  - Kaybolan ortam araçlarının yeniden temini
  - Ömrünü tamamlayan ya da ihtiyaç kalmayan ortam araçlarının takibi ve imha prosedürleri
  - Uygulama ortamı dışında tutulan araçlarının kullanılabilir olmasına ilişkin testlerin yapılması

Hizmet sunum taahhüdü

Kontrol

İSBİK-11 Bilişim sisteminden sorumlu birimin diğer birimlere sağlayacağı hizmetler yazılı olarak tanımlanmış olmalıdır.

Kontrol varlığını değerlendirme soruları

- Diğer birimlere sunulacak hizmetler yazılı olarak tanımlanmış mı?

Kontrol etkinliğini inceleme yöntemi

- Sunumu taahhüt edilmiş bilgi işlem hizmetlerine ilişkin belgelerin aşağıdaki hususları içerip içermediğinin incelenmesi:
  - Hizmetin kapsamı, taraflar
  - Gözden geçirme tarihi
  - Hizmetlere ilişkin kısa tanımlamalar
  - Hizmetin hazır olması ve sürekliliği
  - Hizmet talebine cevap süresi
  - Çözüm bulunamama süresi
  - Yardım masası hizmetleri
  - Sınırlamalar (zaman, işlem sayısı, kullanıcı,…..)
- Örnekleme yoluyla seçilen kullanıcılarla görüşme yapılarak sunumu taahhüt edilmiş hizmetlerin iş ihtiyaçlarına uygun olup olmadığının belirlenmesi

Olay ve problem yönetimi

Kontrol

İSBİK-12 Olay ve problem yönetimine ilişkin önceden belirlenmiş prosedürler olmalıdır.

Kontrol varlığını değerlendirme soruları

- Hizmetin aksamasına neden olabilecek olayların (sistem arızaları, hizmet reddi, verilerden kaynaklanan hatalar, gizliliğin ihlali, ..) takip ve yönetimine ilişkin yazılı bir prosedür var mı?
- Olayların istatistiği çıkarılıyor mu?
- Problemlerin ve bunların çözümünün kaydedilmesine ilişkin bir prosedür var mı?
- Problem ve olay yönetimi arasında işbirliği var mı?
- Problemlerin çözümünü hızlandıracak yardım masası kurulmuş mu?
- Yardım masası için bir eğitim programı uygulanmış mı?

Kontrol etkinliğini inceleme yöntemi

- Olay yönetimi için tanımlanmış prosedürlerin aşağıdaki hususları içerip içermediğinin incelenmesi:
  - Olayların tanımlanması, kaydının alınması, önceliklendirilmesi ve ilk desteğin sağlanması
  - Çözüm sürecinde olayı takibe alan uyarı ve bilgilendirme sistemlerinin varlığı
  - Olayın analizi ve bilgi bankasında var olup olmadığı
  - Olayın işe etkisi
  - Olayın yeniden olmasını önleyecek çarelerin planlarının yapılması
  - Olayın yönetime bildirilmesi
- Olay istatistiklerinin çıkarılıp çıkarılmadığının tespiti ve eğer çıkarılıyorlarsa bilgi bankasında bunların değerlendirilip değerlendirilmediğinin belirlenmesi
- Yardım masasında görev alan personelin almış oldukları eğitim, sertifikaları ve iş tecrübeleri dikkate alınarak yeterliliklerinin değerlendirilmesi
- Sık tekrar eden sorunların nedenlerinin araştırılmasında olay yönetimi veri tabanındaki bilgi bankasından yararlanılıp yararlanılmadığının araştırılması
- Yardım masasının sorunların çözülmesi veya bunun başarılamaması durumunda ilgili uzman personele yönlendirilebilecek şekilde yapılandırılıp yapılandırılmadığının incelenmesi
- Örnekleme yoluyla seçilen kullanıcılarla görüşme yapılarak yardım masasından alınan desteğin yeterliliğinin değerlendirilmesi

2.1.5.2 VERİ TABANI GÜVENLİK KONTROLLERİ

Kontrol Hedefi

Kurumdaki veri tabanı için güvenilir bir çevre oluşturmaktır.

Riskler

Zayıf veri tabanı güvenliğinden kaynaklanan riskler şunlardır:

- Kullanıcı kimliklerinin çalınması
- Kullanıcı kimliklerinin karışması
- Veri tabanındaki açıklıklardan yararlanarak yapılabilecek yetkisiz erişim
- Sorumluluğun kaybı
- Faaliyetlerin baskı altında yürütülmesi
- Kullanılmayan hesapların askıya alınmaması/silinmemesi
- Verinin yok olması/bozulması
- Verinin çalınması
- Hizmetin kabul edilmemesi
- Güvenlirliği zayıf veritabanı uygulamalarına dayanarak işlem yapılması, rapor üretilmesi

Temel Kontroller

Zayıf bir veri tabanı çevresi ve uygulamalarından dolayı olası riskleri minimize etmeye yardımcı olabilecek temel kontroller aşağıda sıralanmıştır:

- Veri tabanı yönetimine ilişkin politika ve prosedürler tanımlanmış olmalıdır.
- Veri tabanının yeterli bir şekilde belgelendirilmesi sağlanmalıdır. Veri tabanının varlığı doğrulanabilmelidir. İlişkiler önemli ve tutarlı isimlere sahip olmalı ve iş kuralları diyagramda gösterilebilmelidir. Nihayetinde kurum ilişki modeli veri tabanı fiziki şemasıyla eş güdümlü olmalıdır.
- Veri tabanı ve uygulama arasında uyumluluk sağlanmalıdır. Fiziki şemalar, tablolar, günlük kayıtları, indeksler ve geçici alanlar için başlangıç ve uzantı boşlukları tahsisinin uygunluğu incelenmelidir. Eğer veri tabanı düzeltilmediyse gerekçesi bulunmalıdır.
- Veri tabanının bütünlüğü sağlanabilmelidir. Verinin bütünlük ve güvenliğini sağlamak için bilgi alma ve çıkarma prosedürleri diğer sistemlerle doğrulanmalıdır.
- Veritabanının yoğun bir şekilde kullanılmasından sonra bazı hataların ortaya çıkması olasılığına karşı çıkarılan yeni versiyonların kurulumu suretiyle gerekli güncellemeler yapılmalıdır.
- Veri tabanı üzerinde çalışmaları hızlandırmaya yönelik olarak veri tabanı belli aralıklarla derlenmelidir.
- Zaman içinde veri tabanı üzerinde kullanıcı sayısının ya da veri giriş/çıkışının artmasıyla birlikte kullanılan kaynaklar da artacağından veri tabanın eski hızında çalışması mümkün olmayabilir. Bu durumda yeni gelişmelere göre veri tabanının performansı izlenmeli, gerekiyorsa performans analizleri

kullanılmalı ve bu yeniliklere göre veri tabanı üzerinde gerekli parametre değişikliklerine gidilebilmelidir.

- Veri tabanında değişik nedenlerle olası kayıpları önlemek amacıyla, belli aralıklarla yedekleme ve geri yüklemeye ilişkin tanımlanmış prosedürler bulunmalıdır.
- Önemli veriye sahip tabloların denetim izleri sağlanmalı ve verinin içeriği denetime uygun olmalıdır.

Kontrollerin Değerlendirilmesi

Yönetim

Kontrol

VTK-1 Veri tabanı yönetimine ilişkin politika ve prosedürler tanımlanmış olmalıdır.

Kontrol varlığını değerlendirme soruları

- Veri tabanı yönetimine ilişkin tanımlanmış yazılı politika ve prosedür var mı?

Kontrol etkinliğini inceleme yöntemi

- Veri tabanı yönetimine ilişkin söz konusu politika ve prosedürlerin incelenerek aşağıdaki konuları kapsayıp kapsamadığının tespit edilmesi:
  - Görevler, sorumluluklar, kimlik denetimi ve yetkilendirme
  - Veri tabanı kayıt ve kontrol yerleri ile bu dosyalara (yazma ve okuma) erişim hakları
  - Veri tabanı kullanıcıları ve kullanıcı şemaları
  - Depolama ayarları
  - Kullanıcı profil ve kaynak kullanım limitleri
  - Veri tabanı uygulamaları üzerindeki kullanıcı hareketlerinin izlenmesi
  - Gerek görülüyorsa external kullanıcı hakları
  - Veri tabanı sunucusuna uzaktan erişime ilişkin tanımlanmış prosedürler

Belgeleme

Kontrol

VTK-2 Veri tabanının kurulumundan uygulama anına kadar "varsayılan" haricindeki tüm işlemleri yeterli bir şekilde belgelendirilmelidir.

Kontrol varlığını değerlendirme soruları

- Veri tabanının yeterli bir şekilde belgelendirilmesini sağlayacak kontroller var mı?

Kontrol etkinliğini inceleme yöntemi

- Veri tabanı için mantıksal veri yapısı ve veri sözlüğü bulunup bulunmadığının belirlenmesi
- Veri sözlüğünün incelenmesi ve bilişim sistemlerinden yeterince verim alabilmek için veri birimlerinin yeterince tanımlanıp tanımlanmadığının incelenmesi
- Bilişim sistemlerinden yeterince destek alabilmek için veri birimleri arasındaki birincil/ikincil ve birden çok ilişkiyi yeterince gösterip göstermediğini tespit için mantıksal veri yapısının incelenmesi

	Uyumluluk
Kontrol	**VTK-3** Veri tabanı ve uygulama arasında uyumluluk sağlanmalıdır.
Kontrol varlığını değerlendirme soruları	▪ Veri tabanı yapısında düşünülen değişikliklerin veritabanı yöneticilerine bildirilmesini ve uygulamada da bu değişikliklerin yapılmasını sağlayan prosedürler var mı? (örneğin, bir alana girilen verinin uzunluğunda bir artış olması durumunda veriyi kullanan uygulama içerisindeki tüm programların içerisindeki veri tabanı tablolarının uzunluklarının artırılmasında olduğu gibi)
Kontrol etkinliğini inceleme yöntemi	▪ Veri tabanı yöneticilerine bildirilen değişiklik talebinin yerine getirilip getirilmediğinin incelenmesi ▪ Örnekleme yoluyla seçilen veri tabanında yapılan değişikliklerin değişim yönetimi prosedürlerine göre gerçekleştirilip gerçekleştirilmediğinin belirlenmesi ▪ Veri tabanı kayıtlarının uygunluğu ile redo kayıtlarının yeterliliğinin test edilmesi
	Bütünlük
Kontrol	**VTK-4** Veri tabanının bütünlüğü sağlanabilmelidir.
Kontrol varlığını değerlendirme soruları	▪ Veri tabanının bozulmasını önleyecek kontroller var mı?
Kontrol etkinliğini inceleme yöntemi	▪ Veri tabanının bütünlüğünü sağlayacak kontrollerin aşağıdaki hususları kapsayıp kapsamadığının incelenmesi: o Tabloların, oluşturulan veya yerleştirilen satırların ikinci kez yazımının önlenmesini sağlayan anahtar (primary key) istenmesi o Sınırlamaların kullanılması ve ikincil kayıtlar oluşturulduğunda birincil kayıtların silinmesinin engellenmesi o Doldurulması zorunlu alanların (not-null) boş bırakılmasının engellenmesi o Uygulamayla güncellenip değiştirilebilecek tüm tabloların iki aşamalı işlem süreciyle kontrol edilmesi ve eski duruma dönmek istendiğinde eski tabloyla uyumun sağlanabilmesi o Veri tabanının bütünlük kontrollerine yönelik toparlama işlemlerinin varolması
	Güncelleme
Kontrol	**VTK-5** Veri tabanı ve veri tabanı ile bütünleşik çalışan uygulamaların güncel olması sağlanmalıdır.
Kontrol varlığını değerlendirme soruları	▪ Veri tabanının yeni gelişmeler karşısında güncellenmesine ilişkin prosedür oluşturulmuş mu?
Kontrol etkinliğini inceleme yöntemi	▪ Veri tabanının güncel versiyonlarının yüklenip yüklenmediğinin tespit edilmesi

	Derleme
Kontrol	**VTK-6** Veri tabanı belli aralıklarla derlenmelidir.
Kontrol varlığını değerlendirme soruları	▪ Veri tabanının düzenli aralıklarla derlenmesini sağlayacak prosedürler var mı?
Kontrol etkinliğini inceleme yöntemi	▪ Derlemenin prosedür ve rutinlerinin reindexing, tablo boşluğu izleme ve tahsis, disk boşluğu izleme ve tahsis, veri bütünlüğü kontrolleri, tablo kilit ve sorun giderme gibi fonksiyonları içerip içermediğinin incelenmesi
	Performans
Kontrol	**VTK-7** Veritabanı performansı izlenebilmelidir.
Kontrol varlığını değerlendirme soruları	▪ Kurum tarafından kabul edilen uygulama geliştirme standartları, performansı artırmaya yönelik talimatlar içeriyor mu?
Kontrol etkinliğini inceleme yöntemi	▪ Performansı artırmaya yönelik tekniklerin kullanılıp kullanılmadığının belirlenmesi
	Yedekleme
Kontrol	**VTK-8** Veri tabanı yedekleme ve geri yüklemeye ilişkin tanımlanmış prosedürler bulunmalıdır.
Kontrol varlığını değerlendirme soruları	▪ Veri tabanının yedeklenmesi ve yeniden geri yüklenebilmesine ilişkin prosedürler var mı?
Kontrol etkinliğini inceleme yöntemi	▪ Veri tabanının yedeklenmesi ve yeniden geri yüklenebilmesine ilişkin prosedürlerin aşağıdaki hususları içerip içermediğinin incelenmesi: o Yedeklemenin yapılma sıklığı o Redo loglarının veri tabanı tablolarından ayrı yerde yedeklenmesi o Veri tabanı tablolarının bozulmalara karşı daha güvenli disklerde (RAID gibi) depolanması o Veri tabanı tablolarının uygulama esnasında yeniden geri yüklemede bekleme zamanını (recovery time) ve olağanüstü durumlarda veri kaybını önlemek amacıyla ikizlerinin çıkarılması ve bu işlemin yapılma sıklığı ▪ Veri tabanının geri yüklemesinin en son ne zaman yapıldığının ve sonuçlarının araştırılması
	Denetim
Kontrol	**VTK-9** Veri tabanı denetlenebilmelidir.
Kontrol varlığını değerlendirme soruları	▪ Denetim izinin takip edilmesini sağlayacak prosedürler var mı?

Kontrol etkinliğini inceleme yöntemi

- Denetim izinin takibini sağlayacak prosedürlerin aşağıdaki hususları kapsayıp kapsamadığının tespit edilmesi:
  - Önemli verileri içeren tabloların içeriklerinin denetime uygun olarak tasarlanması
  - Denetlenecek verinin belirlenmesi
  - Bu verinin oluşturulmasına yönelik işlemlerinin istendiğinde denetim raporlarının üretilebilmesi
  - Üretilen raporların yönetim tarafından gözden geçirilmesi
- Tablolardaki güncellemelerden ya da yapılan değişikliklerden bir örneğin alınarak denetim izinin sağlanmasına uygun olup olmadığının incelenmesi

2.1.6 SİSTEM GELİŞTİRME VE DEĞİŞİM YÖNETİMİ KONTROLLERİ

Bu kontrollerin amacı sistem geliştirme üzerindeki tüm proje yönetimi ve kontrollerinin tatmin edici olmasını, kalıcı ve yeterli iç kontrol ve denetim izine sahip olmasını, sistem geliştirme kalitesinin artırılmasını ve sistemin kullanıcıların ihtiyaçlarını karşıladığı kadar kurumun stratejik amaçlarını da desteklemesini sağlamaktır.

2.1.6.1 SİSTEM GELİŞTİRME KONTROLLERİ

Kontrol Hedefi

Bilişim sistemlerinin geliştirilmesine ilişkin çalışmaların proje yönetimi yaklaşımıyla kontrollü bir çerçevede yürütülmesini sağlamaktır.

Riskler

Sistem geliştirme kontrollerinin yeterli düzeyde kurulamaması durumunda karşılaşılabilecek riskler şunlardır:

- Sistem geliştirme projesinin yetersiz hazırlanması, politika ve prosedürlerinin standartlara uymaması
- Proje yönetim ekibinin yeterli nitelik ve deneyime sahip olmaması
- Planın kurum ihtiyaçlarına cevap vermemesi
- Kaynak problemlerinin oluşması
- Fizibilite çalışmasında yeterli analizin yapılmaması
- Uygun sistem seçim kriterlerinin tesis edilememesi
- Seçilen yapının kurum üzerindeki etki değerlendirmesinde hata yapılması
- Sistem temin sözleşmesinde sistemin gerektiği gibi teslimine ilişkin yeterli ayrıntıların bulunmaması

Temel Kontroller

Bilişim sistemlerinin geliştirilmesinde olası riskleri minimize edecek temel kontrol faaliyetleri şunlardır:

- Sistem geliştirme projesi için standart hale getirilmiş politika ve prosedürler bulunmalıdır. Önceden belirlenmiş standartlar yeni bir sistemin geliştirilmesine yönelik süreç esaslı kontroller sağlar ve bu sürecin uyulması gereken aşamalarını gösterir. Sistem geliştirmenin söz konusu aşamalarına ilişkin olarak uygulama ve standartların, başlangıç, sistem analizi ve tespiti, sistem tasarımı, sistem geliştirme, kabul testi, uygulama ve uygulama sonrası kabul ve inceleme konuları itibariyle tutarlılığı sağlanmalıdır.
- Yeterli tecrübe ve birikime sahip proje yönetimi olmalıdır. Sistem geliştirme süresince benimsenen iyi bir yönetim sistemi projenin başarısı üzerinde olumlu yönde etkileyecektir. Bu nedenle proje yönetim metodolojisi kapsamında değerlendirilebilecek olan yetki ve sorumlukların yapısı, yönetim ekibinin deneyim ve nitelikleri değerlendirilmelidir.
- Yeterli mali ve insan kaynağı sağlanmalıdır. Bütün projelerin maliyet fayda analizlerinin yapılabilmesi için bütçelenmesine ihtiyaç vardır. Bu nedenle doğru bir bütçeleme gerçekçi bir plan için önemlidir. Ayrıca proje yetkililerinin gerek

hazırlamada gerekse bütçelemede aktif katılımı önemlidir. Bu çalışmalara katılanlara gerekli bilgileri elde edebilmeleri ve gerçekçi tahminlerde (keşiflerde) bulunabilmeleri için yetki ve destek verilmelidir.

- Projenin düzenli olarak izlenmesi ve bütçe ve zaman hedeferinin gerçekleşme düzeyini takip için iş programları ve çizelgeler hazırlanmalıdır.
- Proje yönetimi tarafından izleme ve değerlendirme faaliyetlerinin yapılması ve bunların yazılı hale getirilmelidir. Projenin ayrıntılı planı olmalıdır. Planın başarılı olabilmesi için, projenin tüm aşamalarının ve ayrıntılarının tanımlaması, belgeye dayandırılması ve bunların takvime bağlaması, olasılıklarıyla birlikte projede olabilecek her türlü gecikmelerin dikkate alınmış olması gerekir.
- Risk değerlendirmesi yapılmalıdır. Geliştirilmekte olan sistemin tatmin edici sonuç vermesini temin için projenin risk yönetimi oluşturulmalı ve kurumun varlıkları, tehditleri ve hassas noktaları belirlenmek suretiyle riskler tanımlanmalıdır.
- Her proje için kapsamlı proje teklif belgesi hazırlanmalıdır.
- Projeye ilişkin fizibilite raporu hazırlanmış olmalıdır. Bu belge ikna edici kanıtlarla desteklenmiş olabilirlik incelemesi içermelidir. Sistemin verimsiz çalışmasını önlemeye yönelik ihtiyaçların analizi ile her türlü teknik, performans, mali ve sosyal analizler yapılmalıdır.
- Talep edilecek paketin teminine ilişkin ihale süreci mevcut yasal düzenlemelere uygun olmalı, uygun seçim kriterlerini kapsamalıdır.
- Paket seçiminin mevcut altyapı ve destek kaynaklarına etkisi ve ilave yatırımlar (yeni donanım alımı gibi) gerektirip gerektirmediği gibi hususlar değerlendirilmiş olmalıdır.
- Sistem, kullanılabilirlik, yönetim, destek ve bakım açısından yeterince belgelendirilmelidir.
- Sözleşme, sistemin tatmin edici düzeyde teslimini sağlayacak tüm ayrıntıları içermeli ve buna ilişkin tanımlanan prosedürler yasal düzenlemelere uygun olmalıdır.

Kontrollerin Değerlendirilmesi

Politika ve prosedürler

Kontrol

SGK-1 Sistem geliştirme projeleri için belirlenmiş politika ve prosedürler olmalıdır.

Kontrol varlığını değerlendirme soruları

- Üst yönetimin sistem geliştirme projelerine ilişkin kabul ettiği standart ve politikaları var mı?

Kontrol etkinliğini inceleme yöntemi

- Belirlenen politika ve standartların aşağıdaki hususları kapsayıp kapsamadığının incelenmesi:
  - Proje görev ve sorumlulukları
  - İlgili yasal düzenlemeler ve esas alınan standartlar

	o Proje teklifi, fizibilite, uygunluk vb hususlara ilişkin düzenlemeler o Teknik ve işlevsel ihtiyaçların proje gerekleriyle bağdaştırılması o Satınalma, kurulum, yapılandırma, test o Uygulama, veri transferi o İzleme
	Proje Yönetimi
Kontrol	**SGK -2** Proje, sistematik bir proje yönetim süreci çerçevesinde yönetilmelidir.
Kontrol varlığını değerlendirme soruları	▪ Projenin yürütülmesinden sorumlu bir yönetim birimi var mı?
Kontrol etkinliğini inceleme yöntemi	▪ Kurumun bilişim sistemlerinden sorumlu üst yönetimle görüşülmesi ve bir projenin nasıl yürütüldüğüne ve projeden sorumluluğa ilişkin ayrıntılı bilgilerin elde edilmesi ▪ Proje yönetiminden sorumlu olanların yeterli nitelik ve deneyime sahip olup olmadıklarının tespit edilmesi
	Kaynak tahsisi
Kontrol	**SGK -3** Projenin yeterince kaynağı bulunmalıdır.
Kontrol varlığını değerlendirme soruları	▪ Sistem kurulum projesi için yeterli mali ve insan kaynağı tahsis edilmiş mi?
Kontrol etkinliğini inceleme yöntemi	▪ Proje yönetimi ile görüşülerek ve proje belgeleri incelenerek yeterli zaman, insan ve mali kaynak tahsis edilip edilmediğinin incelenmesi
	İzleme
Kontrol	**SGK -4** Proje ilerleyişini izlemek için yeterli prosedürler bulunmalıdır.
Kontrol varlığını değerlendirme soruları	▪ Projenin düzenli olarak izleme ve değerlendirilmesini sağlayan prosedürler var mı?
Kontrol etkinliğini inceleme yöntemi	▪ Projenin düzenli olarak izlenmesini sağlayan prosedürlerin aşağıdaki hususları kapsayıp kapsamadığının incelenmesi: o İnsan, zaman ve maliyetlere göre iş programının hazırlanması o Tamamlanan faaliyete ilişkin iş durum belgesinin hazırlanması o Projenin bütçe ve zaman hedeflerinin takip ve kontrolünü sağlayan çizelgelerin hazırlanması o Proje yönetimi tarafından izleme ve değerlendirme faaliyetlerinin yapılması ve bunların yazılı hale getirilmesi

	Proje planı
Kontrol	**SGK -5** Proje için plan olmalıdır.
Kontrol varlığını değerlendirme soruları	▪ Proje planı hazırlanmış mı?
Kontrol etkinliğini inceleme yöntemi	▪ Proje yönetimi ile görüşülerek vebir proje planının incelenmesi suretiyle planın aşağıdaki hususları kapsayıp kapsamadığının incelenmesi: o Planın yeterince belgelendirilmesi o Proje aşamalarının (ihtiyaçların tespiti, kullanıcı testi ve eğitimi, uygulamaya geçiş gibi) takvime bağlanması ve bunların gerçekçi olması o Onay prosedürlerindeki gecikmeler ya da yapılması gerekecek ilave çalışmaların dikkate alınması o Hassas konuların tanımlanması o Olasılıkların dikkate alınması o Sistem geliştirme sürecinin tüm aşamalarını kapsaması o Projede olabilecek gecikme ve başarısızlıkların planda dikkate alınması
	Proje risk değerlendirmesi
Kontrol	**SGK -6** Proje süresince karşılaşılabilecek riskleri tanımlama, izleme ve çözmeye yönelik prosedürler bulunmalıdır.
Kontrol varlığını değerlendirme soruları	▪ Risklerin tanımlanması ve düzenli izlenmesine ilişkin prosedürler var mı?
Kontrol etkinliğini inceleme yöntemi	▪ Risklerin düzenli olarak izlenmesini sağlayan prosedürlerin aşağıdaki hususları kapsayıp kapsamadığının incelenmesi: o Riskleri anlama ve tanımlama o Önceliklendirme o Risklerin yönetimi o Risk kayıt sistemi
	Proje teklifi
Kontrol	**SGK -7** Her proje için kapsamlı proje teklif belgesi hazırlanmalıdır.
Kontrol varlığını değerlendirme soruları	▪ Kapsamlı bir teklif belgesi hazırlanmış mı?
Kontrol etkinliğini inceleme yöntemi	▪ Proje ekibiyle görüşülerek teklif belgesinin aşağıdaki hususları içerip içermediğinin incelenmesi: o Projenin gerekçesi o Girdi, süreç ve çıktılar

- Projenin finansmanı
- Yaklaşık maliyet hesaplamaları ve fayda tahminleri
- Seçeneklerin tanımlanması
- Projenin birimler üzerindeki etkileri
- Proje başlamadan önce gerekli eğitimler
- Tüm seçeneklerin yeterince dikkate alınıp alınmadığının araştırılması

Fizibilite Çalışması

Kontrol

SGK -8 Projeye ilişkin fizibilite raporu hazırlanmış olmalıdır.

Kontrol varlığını değerlendirme soruları

- Herhangi bir fizibilite çalışması yapılmış mı?

Kontrol etkinliğini inceleme yöntemi

- Yapılan fizibilite çalışmasının aşağıdaki hususları kapsayıp kapsamadığının incelenmesi:
  - Proje bilgi formu
    - Projenin amacı
    - Gerekçesi
    - Proje planı
    - Proje yönetim yapısı
    - Proje sorumluları
    - Projenin sahibi
  - İhtiyaç analizi
    - Risk değerlendirmesi
    - Projenin hedef kitlesi
    - Beklenen faydalar
  - Teknik analizler
  - Maliyet analizleri
  - Performans değerlendirme kriterleri
  - Ekonomik ve sosyal analizler
    - Fayda maliyet analizi
    - Risk analizi
    - Duyarlılık analizi
    - Sosyal analiz
  - Raporun onaylanması
  - Yapılacak işlerin belgelendirilmesi ve dönüm noktaları
- Proje takviminin incelenip bunun yerindeliğini sağlamaya yönelik olarak alınan önlemlerin değerlendirilmesi
- İlgili personelle görüşülerek yapılan risk değerlendirmelerin gözden geçirilip geçirilmediğinin incelenmesi

	İhale süreci
Kontrol	**SGK -9** Projenin ihale aşamasına ilişkin süreç tanımlanarak mevcut yasal düzenlemelere uygunluğu sağlanmalı ve uygun seçim kriterleri belirlenmelidir.
Kontrol varlığını değerlendirme soruları	▪ İhale aşamasına ilişkin süreçler yeterince tanımlanmış mı?
Kontrol etkinliğini inceleme yöntemi	▪ İhale süreciyle ilgili aşağıdaki belgelerin istenmesi ve incelenmesi: o İstekli listesi o Değerlendirme belgesi o Onay belgesi ▪ İhale sürecinin mevzuata uygunluğunun incelenmesi ▪ İhaleye teklif verenlerin yeterli olup olmadıklarının incelenmesi ▪ Uygun seçim kriterlerinin tesis edilip edilmediğinin araştırılması
	Etki değerlendirmesi
Kontrol	**SGK -10** Paket seçiminin mevcut altyapı ve destek kaynaklarına etkisi değerlendirilmiş olmalıdır.
Kontrol varlığını değerlendirme soruları	▪ Yeni paketin mevcut altyapı ve destek kaynakları üzerindeki etkisine ilişkin bir değerlendirme yapılmış mı?
Kontrol etkinliğini inceleme yöntemi	▪ Paketin mevcut yapının üzerine kurulup kurulmadığının veya ilave donanımı gerektirip gerektirmediğinin incelenmesi ▪ Yeni sistemin mevcut destek kaynakları üzerinde etkisinin aşağıdaki hususları kapsayacak şekilde yapılıp yapılmadığının incelenmesi: o Destek personelinin bilgi ve becerisi o Sistem ve veritabanı yazılımı lisanslarının sayı ve maliyeti
	Belgelendirme
Kontrol	**SGK -11** Sistem gerektiği gibi belgelendirilmelidir.
Kontrol varlığını değerlendirme soruları	▪ Sistem kullanılabilirlik, yönetim, destek ve bakım açısından yeterince belgelendirilmiş mi?
Kontrol etkinliğini inceleme yöntemi	▪ Belgelerin aşağıdaki unsurları içerip içermediğinin incelenmesi: o Kullanıcı talimatları o İşletim talimatları o Yönetim talimatları o Süreç tasarımına ilişkin akış şemaları ve tanımlamalar o Arayüz tanımlamaları o Kaynak kodu ve prosedürlerine ilişkin yorumlar

Sözleşme süreci

Kontrol

SGK -12 Sözleşme süreçleri tanımlanmış olmalıdır.

Kontrol varlığını değerlendirme soruları

- Sözleşme süreçleri yeterince tanımlanmış mı?

Kontrol etkinliğini inceleme yöntemi

- Sözleşme sürecinin incelenmesi ve yürürlükteki mevzuata uygunluğunun değerlendirilmesi
- İşin niteliğine bağlı olarak hazırlanan teknik ve idari şartnamelerin incelenmesi
- Söz konusu şartname ve sözleşmelerde aşağıdaki hususlara değinilip değinilmediğinin incelenmesi:
  - Telif hakları
  - Ismarlama işler
  - Eğitim
  - Sisteme ilişkin tüm belgeler
  - Talimatlara ilişkin tüm kılavuzlar
  - Üçüncü kişi lisansları
  - Garantiler
  - İsteklinin sağlamayı taahhüt ettiği donanım ve diğer araçlar
  - Kabul kriterleri
    - Performans standartları
    - Hata düzeltme
    - Teslimin kabul edilebileceği sürelerin başlangıç ve bitiş tarihleri
  - Cezai müeyyideler
  - Bakım ve destek
  - Modüllerin uyarlanması
  - Kaynak kodları

Proje onayı

Kontrol

SGK -13 Projenin sonraki aşamaya geçmeden tüm unsurlarını kapsayacak şekilde onaylandığına ilişkin açık bir imza prosedürü bulunmalıdır.

Kontrol varlığını değerlendirme soruları

- Sonraki aşamaya geçmeden önce projenin tüm belgelerinin onay prosedürleri tamamlanmış mı?

Kontrol etkinliğini inceleme yöntemi

- Prosedürlerde uygun onay sürecinin tamamlanıp tamamlanmadığının incelenmesi

2.1.6.2 DEĞİŞİM YÖNETİMİ (KURULUM VE KABUL) KONTROLLERİ

Kontrol Hedefi

Sistemde gerçekleştirilecek değişikliklerin istenilen sonucu sağlaması ve kullanıcı taleplerini karşılamasıdır.

Riskler

Yeni ve geliştirilen sistemlerin kurulumu ve kabulünde değişim sürecinin yönetilmesine ilişkin kontrollerin yeterli düzeyde kurulamaması durumunda karşılaşılabilecek riskler şunlardır:

- Sistem kurulum sürecinin yürütülebilmesini sağlayacak tasarım belgesinin yeterli ayrıntıyı içermemesi
- Kodlama işlemleri ve modül testlerinin yetersizliği
- Proje çalışmalarına nihai kullanıcıların yetersiz katılımı ya da kullanıcı kabul testinin tüm hata ve etkileri kapsayacak şekilde gerçekleştirilememesi
- Sistem uygulamaları sonucunda üretilen verinin kurumun ihtiyaçlarını karşılayamaması

Temel Kontroller

Geliştirilen sistemlerin kurulum ve kabul sürecinde oluşabilecek riskleri minimize edecek temel kontrol faaliyetleri şunlardır:

- Sistem kurulum sürecinin yürütülmesine ilişkin politika ve prosedürler bir tasarım belgesine dayandırılmalıdır.
- İhtiyaçların öngördüğü şekilde sistemin en az hatalarla bir bütün olarak çalışmasını sağlamak için yürütülmesi gereken kodlama işlemlerinin yanında birim testleri gibi bütünlük ve doğruluk testleri yeterli bir şekilde gerçekleştirilmiş olmalıdır.
- Sistemin gerçekte istendiği gibi çalıştığını öğrenmek için kullanıcılar üzerinde kullanıcı kabul testleri yapılmış olmalıdır.
- Uygulamaya geçişe ilişkin prosedürler belirlenmiş olmalıdır.
- Veri aktarma işlemlerinin sağlıklı bir şekilde gerçekleştirilmesini sağlayacak prosedürler oluşturulmalıdır.
- Paralel çalıştırmayı ve sonuçlarının değerlendirilmesini sağlayacak bir ortam oluşturulmalıdır.
- Sistemin başarı derecesini ölçebilmek amacıyla uygulama sonrasında sistem, iş amaçlarına uygunluk, kullanıcı beklentilerini ve diğer teknik koşulları karşılayıp karşılamadığı yönünden izlemeye alınmalıdır.

Kontrollerin Değerlendirilmesi

Sistem kurulum süreci

Kontrol

DYK-1 Sistem kurulum sürecine ilişkin prosedürler tanımlanmış olmalıdır.

Kontrol varlığını değerlendirme soruları

- Sistem kurulum süreci tanımlanmış mı?

Kontrol etkinliğini inceleme yöntemi

- Sistem kurulumuna ilişkin sürecin aşağıdaki hususları içerip içermediğinin incelenmesi:

	○ Sistem kurulum planlaması ve ana dönüm noktalarının belirlenerek uygulanması ○ Modül tasarımına ilişkin planlar ve modüller üzerinde birim testleri ○ Kodlama işlemleri ve kod hareketlerinin takibi ○ Sürecin izlenmesi ve eksikliklerin giderilmesi ○ Onaylama ▪ Kabul edilmiş değişikliklerin etkilerinin ve sonuçlarının değerlendirilmesi
	Belgeleme
Kontrol	**DYK-2** Kurulum tasarım belgesine dayandırılmalıdır.
Kontrol varlığını değerlendirme soruları	▪ Hazırlanmış herhangi bir tasarım belgesi var mı?
Kontrol etkinliğini inceleme yöntemi	▪ Tasarım belgesinin hazırlanmasında aşağıdaki hususların dikkate alınıp alınmadığının tespit edilmesi: ○ Donanım, ağ, işletim sistemi ve veri tabanı çevresi ○ Arayüz dosya tanımları ○ Veri akış diyagramlarıyla gösterilen iş prosedürleri ○ Mantıksal veri diyagramlarıyla belirlenen veri ○ Kurum kayıtları ○ İş kuralları ○ Muafiyet kuralları ○ Girdi ve soru ekranları ○ Alan vb onay kuralları ○ İş akış ve müştemilatı ○ Rapor ve diğer çıktı şartnameleri ○ Kodlama ○ Veri aktarma ve dönüştürme kural ve rutinleri ○ Yedekleme ve yeniden kurulum ○ Arşivleme ve yeniden kullanma ○ Sistem güvenliği ○ Denetim ve kontrol izleri ○ Performans kriteri ○ Miktarlar ○ Test stratejileri

Kodlama	
Kontrol	**DYK-3** Kodlama işlemleri ve kod hareketlerinin takibini sağlayacak prosedürler bulunmalıdır.
Kontrol varlığını değerlendirme soruları	▪ Kodlama işlemlerinin yürütülmesinde uygulanan bir prosedür var mı?
Kontrol etkinliğini inceleme yöntemi	▪ Kodlama işlemlerine ilişkin prosedürün aşağıdaki hususları kapsayıp kapsamadığının incelenmesi: o Programlara ilişkin yorumlar o Veri sözlüğü o Veri tabanı şablonu o Tablolar arasındaki ilişkiyi gösteren mantıksal veri yapısı o Ekranlar o CRUD analizi

Modüler testler	
Kontrol	**DYK-4** Oluşturulacak modüller için planlanmış testler uygulanmalıdır.
Kontrol varlığını değerlendirme soruları	▪ Modüller üzerinde testler planlanıyor ve uygulanıyor mu?
Kontrol etkinliğini inceleme yöntemi	▪ Modüller üzerinde test yapılmasını ve hataların düzeltilmesini, birimlerin yeniden test edilmesini ve hataların tekrar olmasını önleyecek kontrollerin var olup olmadığının incelenmesi ve özellikle aşağıdaki testlerin yapılıp yapılmadığının tespit edilmesi: o Regresyon testi o Birim testi o Bütünlük testi o Sistem testi

Kullanıcı kabul testleri	
Kontrol	**DYK-5** Kullanıcı kabul testine ilişkin prosedürler belirlenmiş olmalıdır.
Kontrol varlığını değerlendirme soruları	▪ Projenin bu aşamasında süreçler tanımlanmış mı?
Kontrol etkinliğini inceleme yöntemi	▪ Kullanıcı kabul testine ilişkin sürecin aşağıdaki hususları içerip içermediğinin incelenmesi: o Aşağıdaki hususları kapsayacak şekilde planlamanın yapılması: ♦ İşlevsellik (online veya yığın) ♦ Miktar ♦ Performans

- ♦ İstisnalar
- ♦ Güvenlik
- ♦ Yedekleme ve geri yükleme
- ♦ Arşiv ve geri alma
- ♦ Veri dönüştürme/mevcut sistemden veriyi çekme

o Planın onaylanması

o Kullanıcı kabul testi ekibinin oluşturulması

o Test sürecinin izlenmesi ve belgelendirilmesi

o Hataların kaydedilmesi, etkilerinin değerlendirilmesi ve giderilmesi

Uygulama

Kontrol

DYK-6 Uygulamaya geçişe ilişkin prosedürler belirlenmiş olmalıdır.

Kontrol varlığını değerlendirme soruları

▪ Projenin bu aşamasında süreçler tanımlanmış mı?

Kontrol etkinliğini inceleme yöntemi

▪ Uygulama sürecinin aşağıdaki hususları içerip içermediğinin incelenmesi:

o Uygulama ekibi

o Uygulama planı

o Onaylama

o İzleme ve belgelendirme

o Eğitim

o Paralel çalıştırma

o Sistemin kullanıcılara, destek hizmetinin ise bilgi işlem birimine devredilmesi

Veri aktarılması

Kontrol

DYK-7 Verinin yeni veya değiştirilmiş ortama aktarılmasını sağlayan kontroller olmalıdır.

Kontrol varlığını değerlendirme soruları

▪ Verinin tam ve doğru olarak aktarılması için bir kontrol prosedürü var mı?

Kontrol etkinliğini inceleme yöntemi

▪ Verinin aktarımında aşağıdaki hususların dikkate alınıp alınmadığının incelenmesi:

o Aktarılacak verinin belirlenmesi

o Aktarım sonrası veri silinmesi

o Veri aktarımında kullanılacak metodun belirlenmesi

o Aktarma işlemlerinin sırasının planlanması

o Aktarım işlemlerinin izlenmesi, kaydedilmesi ve raporlanması

	o Aktarılması mümkün olmayacak verinin belirlenmesi ve raporlanması o Aktarmaya ilişkin görev ve sorumlulukların belirlenmesi
	Paralel çalıştırma
Kontrol	**DYK-8** Paralel çalıştırma mümkün olmalıdır.
Kontrol varlığını değerlendirme soruları	▪ Paralel çalıştırmayı ve sonuçlarının değerlendirilmesini sağlayacak bir ortam oluşturulmuş mu?
Kontrol etkinliğini inceleme yöntemi	▪ Kullanıcılarla mülakat yapılarak ve elde edilen çıktıların incelenmesi suretiyle paralel çalıştırma işlemlerinin yapılıp yapılmadığının ve elde edilen çıktılar arasında uyumluluğun sağlanıp sağlanmadığının tespit edilmesi ▪ Uyumsuzluk varsa nedenlerinin araştırılıp araştırılmadığının incelenmesi
	İzleme
Kontrol	**DYK-9** Uygulama sonrası yeni sistem izlenmelidir.
Kontrol varlığını değerlendirme soruları	▪ Yeni sistemin izlenmesini sağlayan kontroller oluşturulmuş mu?
Kontrol etkinliğini inceleme yöntemi	▪ İzleme prosedürlerinin aşağıdaki hususları karşılayıp karşılamadığının incelenmesi: o İş amaçlarına uygunluk o Kullanıcı beklentilerini karşılama o Teknik koşulları karşılama

2.1.7 ACİL DURUM VE İŞ SÜREKLİLİĞİ PLANLAMASI KONTROLLERİ

Acil durum ve iş sürekliliği planlaması ile ilgili kontrollerin amacı acil durum nedeniyle bilişim sistemlerinin geçici veya sürekli olarak aksaması durumunda kurumun işlevlerini sürdürebilmesini ve tutulan bilginin işlenmesi, erişilmesi ve korunması yeteneklerinin kaybedilmemesini sağlamaktır.

Acil durum, deprem, yangın, fırtına, sel, bombalama, sabotaj, donanım veya yazılım hatası, elektrik ve telekomünikasyon kesintisi gibi önceden tahmin edilebilen veya edilemeyen iç veya dış faktörler sonucu meydana gelen ve kurumun normal olarak işlerini sürdürmesi durumunu aksatan her şey olabilir.

Bu çerçevede, kurumlar detaylı bir acil durum ve iş sürekliliği planına sahip olmalıdır.

Riskler

Acil durum ve iş sürekliliği planının olmaması veya yetersiz olması kurumu aşağıdaki risklerle karşı karşıya getirecektir:

- Felaketlere maruz kalma olasılığının artması
- Felaketin verdiği zararlarla başa çıkma imkanının azalması
- Felaketten kaynaklanan kaybın veya zararın ağırlaşması
- Karşılaşılan felaket sonrasında makul bir sürede kurum faaliyetlerinin yeniden başlatılamaması
- Yasal veya üçüncü kişilere karşı olan sorumlulukların zamanında yerine getirilememesi
- Bir felaket durumunda iletişim imkanları, bilgi işleme kapasitesi, eğitimli insan kaynağı ve tüm varlıklar yitirilebileceğinden kurumun faaliyetlerini sürdürmesinde devamlılığın sağlanamaması

Temel Kontroller

Etkisi yıkıcı boyutlarda olabilecek acil ve beklenmedik durumların kuruma verebileceği kayıp veya zararları en aza indirmek için kurulması gereken temel kontrol faaliyetleri şunlardır:

- Önceden tahmin edilebilen veya edilemeyen iç veya dış faktörlerden kaynaklanan acil durumlara karşı hazırlıklı olunmalıdır. Bu nedenle kurumda acil durum ve iş sürekliliği için bir yönetim süreci oluşturulmalıdır.
- İş akışını kesintiye veya felakete uğratacak, kurumu ve binaları olumsuz etkileyebilecek olayları ve çevresel faktörleri belirlemek için risk değerlendirmesi yapılmalıdır.
- Yapılan risk değerlendirmesi sonucu belirlenen her bir risk için, olası bir acil durum esnasında kaybın veya aksaklıkların ana faaliyetler üzerindeki etkileri değerlendirilmeli ve potansiyel zararı önlemek veya kaybın etkilerini minimize etmek için uygun maliyetle gerekli tedbirler alınmalıdır.
- Olası felaketlere karşı hazırlıklı ve organize cevap verilebilmesi için yazılı bir acil durum ve iş sürekliliği planı bulunmalıdır.
- Hazırlanan bu plan düzenli olarak gözden geçirilmeli ve işleyip işlemediğini görmek için felaket senaryoları dikkate alınarak testleri yapılmalıdır.

- Acil durum ve iş sürekliliği planları belgelendirilmeli ve gerektiğinde güncellenmelidir.
- İşletim merkezlerinin mimarileri, tek nokta arızalara (single point of failure) esnek olmalıdır. Bu durum her ne kadar acil durum planının bir unsuru olarak görülmüyorsa da, alternatifi olmayan ve aksama olduğunda sisteme büyük zarar verebilecek arızaları önlemek için bu noktalar belirlenmeli ve dikkatle izlenmelidir. Bu noktaların bulunduğu yerlerde arızalanan unsurun yerine yedek veya yedekleme teçhizatı getirmeye ilişkin prosedür ve/veya süreçler olmalı, bu prosedür ve süreçler belgelenmeli ve düzenli olarak test edilmelidir. Ayrıca arızalı unsurların tamir edilmesi sonrasında tekrar yerine konmasına ilişkin prosedür ve süreçler olmalı ve bunlar da belgelenmelidir.
- Sistem yazılımlarının, mali uygulamaların ve bunları destekleyen dosyaların yedek kopyaları düzenli olarak alınmalıdır. Yedeklemeler günlük, haftalık veya aylık şeklinde belirli periyotlarla alınmalı ve acil durum planının bir kopyası ile birlikte kurum dışında özel olarak güvenlik önlemleri alınan bir yerde saklanmalıdır.

Kontrollerin Değerlendirilmesi

Plan

Kontrol

ADİS-1 Kurum, yazılı bir acil durum ve iş sürekliliği planına sahip olmalıdır.

Kontrol varlığını değerlendirme soruları

- Bilişim sistemlerini de içeren kurumun bütününü kapsayan acil durum ve iş sürekliliğine ilişkin yazılı bir plan var mı?
- Planın yürütülmesinden sorumlu bir üst düzey yönetici belirlenmiş mi?
- Kurum acil durum ve iş sürekliliğine yönelik çalışmalarını belgelendirmiş mi?

Kontrol etkinliğini inceleme yöntemi

- Kuruma ait acil durum ve iş sürekliliği planı elde edilerek bu planı uygulamaktan sorumlu üst yöneticiler ile görüşme yapılması ve mevcut planların aşağıdaki hususları içerip içermediğinin incelenmesi:
  - Planda aşağıdaki hususların acil durum olarak belirlenmesi:
    - Hard disk bozulması
    - Güç kaybı (bozuk veri oluşmasına yol açar)
    - Sistem yazılımı problemi
    - Kaza veya kasti olarak silme ve değiştirme
    - Kötü niyetli yazılımlar (virüs,…)
    - Doğal afetler (sel, yangın, deprem vb.)
    - Hırsızlık ve sabotaj
    - Veri tabanı

- Uygulama yazılımı
- Sunucular
- Ağ ürünleri
- Kablolama alt yapısı
- Enerji alt yapısı
- Güvenlik ürünleri
- İletişim hatları

o Planda aşağıdaki hususlara belgelendirilerek yer verilmesi:

- Mevcut durumu gösteren şemalar
- Plandan etkilenen grupların onayı (Üst yönetim, veri merkezi yönetimi ve program yöneticileri)
- Açık şekilde belirlenmiş sorumluluklar
- İş faaliyetlerinin yeniden oluşturulması için ayrıntılı talimatlar
- Alternatif işleme ve yedekleme depolama imkanı
- Veri/hizmet merkezinin veriyi alamaması veya iletememesi durumunda izlenecek prosedürler
- Hassas veri dosyaları
- Bütün birim yöneticileri tarafından planın okunup anlaşıldığını gösteren imzalar
- Bütün ilgili personele dağıtılmış olması

▪ Tüm uygulama personeline planın uygulanması konusunda hizmet içi eğitim verilip verilmediğinin eğitim belgelerinden incelenmesi ve örnekleme yoluyla seçilen eğitim almış personelle alınan eğitim ile ilgili görüşme yapılması

▪ Tüm çalışmaların, yazışmaların ve plan evraklarının belgelendirilerek dosyalarda saklanıp saklanmadığının ve mevcut planın birkaç kopyasının farklı bir yerde güvenli olarak tutulup tutulmadığının belirlenmesi için gözlem yapılması ve belgelerin incelenmesi

▪ Planın uygulanmasından sorumlu bir üst yöneticinin atanıp atanmadığının iç yazışmalardan ve plan belgelerinden belirlenmesi

Kontrol varlığını değerlendirme soruları

▪ Plan hazırlanırken risk değerlendirmesi yapılmış mı?

Kontrol etkinliğini inceleme yöntemi

▪ Risk değerlendirme ekibi ile görüşme yapılarak ve hazırladıkları raporlar incelenerek, risk değerlendirmesi yapılırken aşağıdaki hususların dikkate alınıp alınmadığının belirlenmesi:

o Sel

o Yangın

- Hizmet aksaması (elektrik, su vs.)
- Mekanik bozulma (donanım başarısızlıkları dahil)
- Donanım veya yazılımın gerektiği gibi çalışmaması
- Yazılım aksaklıkları (virüs saldırısı)
- Kazaen veya kasten verilen zarar (terörizm dahil)
- Personelden kaynaklanan problemler
- Özellikle çalışma alanını etkileyen başka riskler(yakındaki inşaat faaliyeti, tehlikeli zeminlerin belirlenmesi gibi)
- Belirlenen her bir riskin olma olasılıkları ve giderilme koşul ve maliyetlerinin belirlenmesi
- Sistemin yeniden kurulması ve çalıştırılması için gerekli zaman süresinin belirlenmesi
- Üçüncü kişilerden alınan hizmetler için bir değerlendirme yapılması ve acil durumda eşgüdüm halinde çalışılması konusunda mutabakata varılması
- Yapılan risk değerlendirmelerinin düzenli olarak gözden geçirilmesi

Kontrol varlığını değerlendirme soruları

- Plan hazırlanırken, belirlenen her bir risk için gerçekleşme durumunda işe olan etkilerine yönelik analizler yapılmış mı?

Kontrol etkinliğini inceleme yöntemi

- Üst yönetimle görüşme yapılarak ve ilgili belgeler incelenerek, olası bir felaketin gerçekleşmesi esnasında kayıp veya aksaklıkların ana faaliyetler üzerindeki etkileri aşağıdaki hususlar dikkate alınarak değerlendirilip değerlendirilmeğinin belirlenmesi:
  - Bütün iş süreçlerinin belirlenmesi
  - Bu süreçlerde birbiriyle bağımlı çalışanların tespitinin yapılması ve bir kurtarma önceliğinin tespit edilmesi
  - Her bir iş sürecinin kesilmesi veya aksaması sonucunda meydana gelecek etkinin değerlendirilmesi (olası iş etkileri belirlenen senaryolarla desteklenmiş olmalı, hangi senaryo yaşanırsa ne kadar sürede bunun giderilebileceği konusunda bir değerlendirme yapılmalıdır)
  - Olası iş etkilerinin değerlendirilmesinden sonra acil durum hedeflerinin belirlenmesi
  - Bu hedefleri karşılayacak personel, varlık ve hizmetlerin minimum gereksinimlerinin tespit edilmesi
  - Kritik faaliyetleri destekleyen kaynakların belirlenmesi
  - Yaşanabilecek aksaklıkların etkilerini belirleyecek bir analizin yapılması
  - Etki analizi yapılırken bütün iş birimlerinin yöneticilerine danışılması
  - Analizin sonuçlarının üst yönetimle paylaşılması ve mutabık kalınması

- Kurtarılacak sistemlerin bir listesinin istenildiğinde elde edilebilmesi
- Yazılım ve donanım dahil bilişim sistemlerinin unsurları için bakım sözleşmelerinin yapılması

Kontrol varlığını değerlendirme soruları

- Plan hazırlanırken olası kayıp ve aksaklıkların belirlenen makul süre içerisinde nasıl giderileceğine ilişkin bir strateji belirlenmiş mi?

Kontrol etkinliğini inceleme yöntemi

- Üst yönetimle görüşme yapılarak ve ilgili belgeler incelenerek olası felaket durumunda kayıp ve aksaklıkların belirlenen makul süre içerisinde nasıl giderileceğine ilişkin bir stratejinin seçilip seçilmediğinin belirlenmesi:
  - İş sürekliliğine ilişkin bir yaklaşım belirlemek için risk değerlendirme sonuçlarına dayanan bir strateji planının bulunması
  - Kurum gerekli zaman süreci içerisinde kritik sistemlerin kurtarılmasına imkan verecek uygun bir kurtarma stratejisinin var olması
  - Seçilen stratejinin iş içindeki iletişimin kullanımını öngörmesi
  - Stratejinin kurum içi teçhizatın çok amaçlı kullanımını öngörmesi
  - Stratejisi ve kurtarma düzenlemeleri gelecek iş genişlemeleri dikkate alınarak yeterince esnek olması
  - Veri işleme ve online hizmetlere erişime ilişkin yönetimce konan hedeflerin bulunması
  - Hizmet programlarının yerine getirilmesinde gerçek performans konusunda kayıtların tutulması
  - Karşılaşılan problemler ve ertelemelerin sebebinin ve karar için geçen zamanın kaydedilmesi
  - Üst yönetimin seçilen stratejiyi periyodik olarak gözden geçirmesi, hedeflerle elde edilen hizmet performansını değerlendirmesi ve ihtiyaçların giderilip giderilmediğini görmek için kullanıcı birimlerinde anket yapılması

Test etme ve güncelleme

Kontrol

ADİS-2 Kurum, acil durum ve iş sürekliliği planını gerçekçi senaryolarla işleyip işlemediğini test etmelidir.

Kontrol varlığını değerlendirme soruları

- Kurum hazırladığı acil durum ve iş sürekliliği planını düzenli olarak gözden geçiriyor mu?
- Planın işleyip işlemediğini görmek için testler yapılıyor mu?

Kontrol etkinliğini inceleme yöntemi

- Üst yönetimle görüşme yapılarak ve yapılan testlerin belgeleri incelenerek acil durum ve iş sürekliliği planının güncellenmesi ve test edilmesine yönelik çalışmaların aşağıdaki hususları içerip içermediğinin belirlenmesi:
  - Planın test edilmesi için kurum üst yönetiminden bir kişinin önderliğinde bir ekibin oluşturulması
  - Planı güncel tutmak için bir test programının belirlenmesi
  - Bütçede planın test edilmesi ve uygulanması için kaynak ayrılması
  - Programa uygun şekilde planın temel unsurlarının test edilmiş olması
  - Test ekibinin test edilmiş planı onaylaması
  - Planın periyodik olarak değerlendirilmesi ve gerekiyorsa donanım, yazılım ve personeldeki değişiklikleri yansıtacak şekilde düzeltmeler yapılması
  - Yapılan testlerin raporlanması
  - Planın acil durum esnasında görev alacak kilit personel için yazılı talimatlara dönüştürülmesi ve bunların düzenli olarak güncellenmesi
  - Plan içeriğinin anlaşılır olması için yeterli ancak aşırı olmayan ayrıntı düzeyinde bir belgeleme standartlarının belirlenmesi
  - Plan, geçici bilgilerin (temas telefon numaraları gibi) bütün planın yeniden yapılmasına imkan vermeden güncellenmesi
  - Yedekleme ve kurtarma prosedürlerinin test edilmesi
- Planın bütün unsurlarının test edildiğine ilişkin raporlar incelenerek, planda bir değişiklik yapılması öngörülüyorsa, bu değişikliklere uygun şekilde planın gözden geçirilip geçirilmediğinin belirlenmesi

Yedekleme

Kontrol

ADİS-3 Kurumun bir yedekleme politikası bulunmalı ve yedeklenen unsurların nasıl kullanılacağına ilişkin prosedürlere sahip olmalıdır.

Kontrol varlığını değerlendirme soruları

- Kurumun yedekleme yapılması ve yedeklenen unsurların kullanılmasına yönelik yazılı politika ve prosedürleri var mı?
- Yedekleme disketleri kullanıcı bölümler, tarih ve kullanıcılar dikkate alınarak etiketleniyor mu?
- Yedeklerin alındığı araçlar olası her türlü tehlikeden korunacak şekilde özel yerlerde saklanıyor mu?
- Yedekleme araçları kurum bilişim sisteminin bulunduğu coğrafi mekandan farklı güvenli bir ortamda saklanıyor mu?
- Yedekleme araçlarında muhafaza edilen veri dosyaları ve uygulamalarının sistemin yeniden kurulması için gerekli nitelikte bilgi içerip içermedikleri test ediliyor mu?

- Yedeklenen kayıtların tekrar istenmesi ve kullanılmasına yönelik prosedürler var mı?

Kontrol etkinliğini inceleme yöntemi

- Kurum yedekleme politika ve prosedürlerine ilişkin belgelerin incelenerek aşağıdaki hususları içerip içermediğinin belirlenmesi:
  - Veri dosyaları ve uygulamaların yedeklerinin düzenli olarak alınması
  - Yedeklenen veri dosyalarının listelenmesini, içerikleri ve konumlarının belirtilmesi
  - Tüm bilgi türleri ve söz konusu bilgilerin kaybedilmesinin yaratacağı olası etkiler dikkate alınarak yedekleme için önceliklerin belirlenmesi
  - Yazılım ve veri yedeklerinin ayrı bir alanda konumlandırılması
  - Yenilemenin sıklığı ve yedeklerin ne kadar süre ile saklanacağı (Dosyaların ne sıklıkla yedekleneceği uygulamaların ve dosyaların önem derecesine bağlıdır. Gün sonu yedekleme, anlık yedekleme, anlık sistem yedekleme gibi yöntemler kullanılabilir.)
  - Kullanılan yazılım ve donanımların, yedek sistemler ile uygunluğunun periyodik olarak gözden geçirilmesi
  - Yapılacak testler ile yedekleme hizmetinin etkinliğinin düzenli olarak kontrol edilmesi
  - Bilgi saklama araçları ile ilgili etiketleme, listeleme, iletim ve saklama faaliyetlerinin etkin ve verimli bir şekilde yürütülmesine yardımcı olacak rehberlerin hazırlanması
  - Yedeklenen araçların hangilerinin ne sıklıkla çalışma alanı dışına gönderileceğini ve bunların transferleri ile ilgili riskleri minimize edecek tedbirlerin alınması
- Yedekleme araçlarının saklandığı yerlerin yerinde inceleme yapılarak güvenlik açısından uygun olup olmadığının belirlenmesi
- Yedeklemenin belirlenen sıklıkta ve etiketleme standartlarına uygun şekilde yapılıp yapılmadığının örnekleme yoluyla seçilen yedekleme araçlarının incelenerek belirlenmesi
- Yedekleme araçlarında muhafaza edilen veri dosyaları ve uygulamalarının sistemin yeniden kurulması için gerekli nitelikte bilgi içerip içermediklerinin düzenli olarak test edilip edilmediğinin test kayıtlarından ve ilgililerle görüşme yapılarak tespit edilmesi
- Yedekleme araçlarının yeniden kullanılabilmesine ilişkin prosedürlerin aşağıdaki hususları içerip içermediğinin incelenmesi:
  - Kimin tarafından alındığı
  - Ne için kullanıldığı
  - Geri getirme süresi
  - Geri gelen araçların bozulup bozulmadığının ve yeniden kullanılabilir olduğunun testi sonrasında yeniden saklanması

- Örnekleme yoluyla seçilen yedekleme araçlarında bu prosedürlere uyulup uyulmadığının yeniden kullanma kayıtları incelenerek ve ilgili sorumlu ile görüşme yapılarak tespit edilmesi

2.2 UYGULAMA KONTROLLERİNİN DEĞERLENDİRİLMESİ

Uygulama programları, muhasebe, vergi, alacak takip işlemleri gibi bir iş fonksiyonuna destek veren yazılımlardır. Bu programlar, kurumun iş süreçlerinin bir kısmının veya tamamının bilgisayar ortamında yapılmasını sağlar.

Tüm mali uygulamalar, işlemlerin ve verilerin tamlığını, kullanılabilirliğini ve makul bir ölçüye kadar güvenilirliğini güvence altına alan kontrollere sahip olmalıdır.

Uygulama kontrolleri, bilgilerin sistemlere ya da programlara tam olarak, zamanında ve sadece bir kere girilmesini, bilgi-işlem ortamında tüm işlem ve süreçlerin istenilen sıra ve düzen içinde gerçekleşmesini, raporların tam ve güvenilir olarak üretilmesini, yetkili kişilere ulaştırılmasını ve uygun şekilde arşivlenmesini sağlayan kontrollerdir.

Uygulama kontrolleri değerlendirilmeden önce kurumun uygulama programları yeterince tanınmalıdır. Bunun için, verinin hazırlanması, veri giriş işlemlerinin yapılması, iletilmesi, işlenmesi ve çıktı alınması süreciyle ilgili iş akışları temin edilmeli ve bu süreçte kurum tarafından oluşturulmuş olan manuel ve otomatik kontroller belirlenmelidir. Ayrıca uygulamanın ilgili yasal düzenlemeler ve muhasebe sistemi ile ilişkilerinin iyi bilinmesi gerekir.

Uygulama kontrolleri değerlendirilirken, uygulamaların güvenilirliğine ilişkin makul bir güvence elde edebilmek için uygulamalarda olması gereken kontroller test edilerek kanıt toplanır. Bu aşamada bilgisayar destekli denetim tekniklerinden (BDDT) de yararlanılır.

BDDT, programlardaki süreçlerin doğruluğunun saptanması ve veri dosyalarının incelenmesinde kullanılır. Programlardaki süreçlerin doğruluğunun saptanmasında, anlık görüntü alma (snapshot), iz sürme (tracing), log analizi gibi teknikler kullanılabilir. Verilerin doğruluğu ve dosya güvenilirliği için paralel simülasyon, mükerrerlik kontrolü, sınıflandırma, örnekleme, karşılaştırma gibi analiz tekniklerinden yararlanılabilir.

Uygulama kontrolleri aşağıda belirtilen başlıklar altıda incelenebilir:

- Girdi Kontrolleri
- Veri Transfer Kontrolleri
- İşlem Kontrolleri
- Çıktı Kontrolleri

2.2.1 GİRDİ KONTROLLERİ

Kontrol Hedefi

Verilerin sisteme, tam, doğru ve yetki dahilinde girilmesini sağlamaktır.

Riskler

Veri girişine ilişkin olarak karşılaşılabilecek risklerden bazıları şunlardır:

- Yetkili olmayan kişilerce veri girişi yapılması
- Eksik veya hatalı veri girilmesi
- Mükerrer kayıtların sistem tarafından kabul edilmesi
- Hatalı veri girişlerinin tespit edilememesi
- Erişim Kontrollerinin ihlal edilmesi
- Görevlerin ayrılığı ilkesine uyulmaması

Temel Kontroller

Girdi kontrollerine ilişkin riskleri makul seviyeye düşürecek temel kontroller şunlardır:

- Uygulama programlarına ilişkin teknik dokümanlar ve kullanım rehberleri hazırlanmış olmalıdır.
- Kaynak belgelerin kullanılmasına ilişkin prosedür tanımlanmış olmalıdır.
- Tüm veri hazırlama, veri giriş işlemleri ve ana dosyalardaki değişiklikler yetki dahilinde yapılmalıdır.
- Hatalı veri girişlerini engelleyecek otomatik kontrol mekanizmaları kurulmalıdır.
- Hatalı ve kural dışı veri girişleri raporlanmalıdır.

Kontrollerin Değerlendirilmesi

Belgeleme

Kontrol

GK-1 Uygulama programlarına ilişkin teknik dokümanlar ve kullanım rehberleri hazırlanmış olmalıdır.

Kontrol varlığını değerlendirme soruları

- Uygulama programlarına ilişkin bir belgeleme standardı var mı?
- Kullanıcıların ihtiyaçlarını karşılayacak teknik dokümanlar hazırlanmış mı?

Kontrol etkinliğini inceleme yöntemi

- Teknik dokümanların aşağıdaki bilgileri içerecek şekilde hazırlanıp hazırlanmadığının tespit edilmesi:
  - Sistemi genel olarak gösteren bir şema
    - Uygulama programının ağ yapısı içerisindeki durumu
    - Kullanıcı sayısı
    - Kullanıcı yerleri
  - Kullanıma yönelik rehber
    - Program tanımlamaları

- Program içinde kullanılan ara yüzlerin tanıtımı ve şeması
- Programlar arasında ve program içinde kullanılan ara yüzlerin tanıtımı ve şeması
- Ana girdi, süreç ve çıktılar
- İşlem hacmi
- Sistem gereksinimleri

o İlişki içerisinde bulunduğu diğer yazılım ve donanıma ait detaylar

- Kullanılan programlara ilişkin belgelerin incelenerek;
  - o düzenli olarak gözden geçirilmesinin,
  - o güncellenmesinin ve
  - o güvenli bir şekilde muhafaza edilmesinin

  sağlanıp sağlamadığının belirlenmesi
- Kullanıcılarla görüşme yapılması suretiyle;
  - o kullanıcıların mevcut dokümanlara ulaşıp ulaşmadığının,
  - o söz konusu dokümanların kullanıcıların ihtiyacına cevap verip vermediğinin,

  tespit edilmesi

Kaynak belge

Kontrol

GK-2 Kaynak belgelerin kullanılmasına ilişkin prosedür tanımlanmış olmalıdır.

Kontrol varlığını değerlendirme soruları

- Veri giriş işlemlerinin yapılmasına ilişkin tanımlanmış bir prosedür var mı?
- Veri girişlerinde kullanılacak kaynak belgeler belirlenmiş mi?
- Kaynak belge olarak veri giriş formları kullanılıyor mu?

Kontrol etkinliğini inceleme yöntemi

- Veri giriş işlemlerinin yapılmasına ilişkin prosedürlerde aşağıdaki hususların bulunup bulunmadığının incelenmesi:
  - o Veri giriş şeklinin tespiti (manuel, online vs)
  - o Kaynak belgelerin belirlenmesi, düzenlenmesi ve onaylanması ve bunlara ilişkin görev, yetki ve sorumluluklar
  - o Kaynak belgeyi hazırlayan, sisteme girişini yapan, sisteme girişi yapılan veriyi işleyen ve çıktıların dağıtımını yapan personelin birbirinden farklı kişiler olup olmadığının tespiti
  - o Belge veya iş akışı ve zamanlaması
  - o Belge düzenleme sürecinde hataların ve düzensizliklerin tespit edilmesi, raporlanması ve düzeltilmesi
  - o Kaynak belgelerin yeterli bir süre boyunca saklanması
  - o Kaynak belge olarak veri giriş formu kullanılıyorsa
    - Standart formların tespit edilmesi

- Standart veri giriş formlarının bütün temel işlemlerde kullanılıp kullanılmadığının belirlenmesi
- Formlarda sıra numaraları ve tarihlerin kullanılması
- Veri giriş formunun sistem içerisinde referans olarak ilişkilendirilmesi ve tekrar kullanılmasının önlenmesi
- Form düzeninin ve formda girilmesi istenen verilerin ekran formatıyla uyumlu olup olmadığının tespit edilmesi

- Veri kütüphanesinin incelenmesi ve verilerin tasnif edilmesinde kullanılan ana başlıklarla girdi formlarının karşılaştırılması, farklılık varsa bunun nedenlerinin tespit edilmesi

Yetkilendirme

Kontrol

GK-3 Tüm veri hazırlama, veri giriş işlemleri ve ana dosyalardaki değişiklikler yetki dahilinde yapılmalıdır.

Kontrol varlığını değerlendirme soruları

- Erişim ve yetkilendirme işlemlerini tanımlayan ve düzenleyen bir politika veya prosedür var mı?
- Kaynak belgeler dahil bütün veri hazırlama işlemleri yetkili kişiler tarafından yapılıyor mu?
- Manuel veya bilgisayar ortamında yetkisiz işlemlerin yapılmasını önleyen tedbirle alınmış mı?

Kontrol etkinliğini inceleme yöntemi

- İşlemlerin yetki dahilinde yapılıp yapılmadığının tespiti amacıyla;
  - Uygulama programlarına özgü olarak erişim tablolarının incelenmesi
  - Yetkili kullanıcı listelerinin bir çıktısının alınması
  - Yetki değişikliğine ilişkin kayıtların yer aldığı denetim kütüklerinin gözden geçirilmesi;
  - Bilgilerin doğru ve eksiksiz kaydedilmesinin sağlanması amacıyla çift imza, kontrol edildi parafı gibi kontrol mekanizmasının oluşturulup oluşturulmadığının belirlenmesi
  - Farklı dönemlere ait kaynak belgelerin üzerindeki imzalarla yetkilendirme listelerinin karşılaştırılması ve işlemlerin yetki dahilinde gerçekleştirildiğinin test edilmesi
  - Ana dosyalarda yer alan parametrelere ilişkin tüm veri girişlerinin ve değişikliklerinin yetki dahilinde, zamanında ve doğru yapıldığının ve yıl içinde bu parametrelerin yetkisiz kişilerce veya suiistimale yönelik olarak değiştirilmediğinin tespit edilmesi
- Örnek seçilen kullanıcı işlemlerinin incelenerek fiziksel ve mantıksal erişim kontrollerinin etkin olarak işleyip işlemediğinin test edilmesi (bkz. Fiziksel ve Mantıksal Erişim Kontrolleri)

Hatalı veri girişinin engellenmesi

Kontrol

GK-4 Hatalı veri girişlerini engelleyecek otomatik kontrol mekanizmaları kurulmalıdır.

Kontrol varlığını değerlendirme soruları

- Kullanılan programda eksik, yanlış, mantıksız veya mevcut verilerle çelişen veri girişlerini engelleyen otomatik kontroller var mı?
- Yanlış tarih veya belirli sınırların dışındaki veri girişlerinde uyarı mekanizmaları kurulmuş mu?
- Yanlış formatta veri girişlerinin sistem tarafından kabul edilmesi önlenmiş mi?
- Aynı verinin sisteme mükerrer kaydedilmesini önleyecek mekanizmalar var mı?

Kontrol etkinliğini inceleme yöntemi

- Kullanıcılarla görüşme yapılması, ilgili dokümanların incelenmesi ve program uygulamalarının gözlemlenmesi suretiyle sistem tarafından verilerin doğruluğu ve geçerliliğini test edecek aşağıda yazılı otomatik kontrollerin olup olmadığının belirlenmesi:
  - Üst limit kontrolü
  - Aralık kontrolü
  - Karşılaştırılabilirlik kontrolü
  - Zorunlu alan kontrolü
  - Rakam kontrolü
  - Açıklamalı tablolar
  - Seri veya sıra kontrolü
  - Mükerrerlik kontrolü
  - Geçerlilik Kontrolü
  - Makullük kontrolü
  - Mevcutluk kontrolü
  - Tamlık kontrolü
  - Boşluk Kontrolü
- Mükerrer kayıtların önlenmesi amacıyla aşağıdaki kontrollerden yararlanılıp yaralanılmadığının belirlenmesi:
  - Kaynak dokümanların silinmez yazıyla işaretlenmesi
  - Ayrı referans numaralarının kullanılması
  - Kaynak belgelerin fiziksel olarak imhası veya işaretlenmesi
  - Kullanıcı, sicil numarası, vatandaşlık numarası, hesap kodları, adres veya miktarlar gibi alanların birbirleriyle karşılaştırılarak eşleştirme yapılması
  - Genel toplamların kontrol edilmesi
  - Girdilerde seri numaralarının kullanılması
  - Bilgisayar destekli denetim teknikleri kullanılarak yevmiye kayıtlarında, yapılan ödemelerde mükerrerlik olup olmadığının tespit edilmesi

- Bilgisayar destekli denetim teknikleri kullanılarak veriler üzerinde aşağıdaki testlerin yapılması:
  - Sistem saat ve tarihi ile resmi kayıtlarda yer alan tarihlerin karşılaştırılarak uyumsuzluk olup olmadığının tespiti, bunun yasal düzenlemelere uygunluğunun belirlenmesi
  - Veri girişlerinin tamamlanıp onaylanmasından sonra kilitlenip kilitlenmediğinin ve geriye dönük işlem yapılıp yapılmadığının tespit edilmesi
  - Verilerin silinip silinemediğinin tespit edilmesi
  - Düzeltmelerin, üzerine yazma yöntemiyle yapılıp yapılamadığının belirlenmesi
  - Sistem sıra numarası ile yevmiye numaralarının karşılaştırılması, yevmiye numaralarında boşluk olması halinde bunun nedeninin belirlenmesi
  - Verilerin doğru hesaplara kaydedildiğinin, hesapların birbirleri ile uygun şekilde çalıştırıldığının tespit edilmesi
  - Bir önceki yıldan devreden hesap bakiyeleri ve vergi borçları gibi işlemlerin bir sonraki döneme otomatik olarak aktarılıp aktarılmadığının incelenmesi

Hata ve kural dışı durum raporu

Kontrol

GK-5 Hatalı ve kural dışı veri girişleri raporlanmalıdır.

Kontrol varlığını değerlendirme soruları

- Hatalı veya kural dışı durumlara ait rapor üretiliyor ve saklanıyor mu?
- Yönetim düzenli olarak hata veya kural dışı durum raporlarını gözden geçiriyor mu?

Kontrol etkinliğini inceleme yöntemi

- Yetkililerle görüşme yapmak suretiyle hata veya kural dışı raporlarının ne kadar sıklıkla üretildiğinin ve dağıtıldığının belirlenmesi
- Uygulamalar tarafından üretilen örnek hata ve kural dışı rapor incelenerek;
  - detayları, kayıtların durumunu ve hataların nedenlerini gösterip göstermediğinin,
  - söz konusu raporlarının yönetim tarafından incelenerek sorunun çözülüp çözülmediğinin,
  - bu hataların mali tablolara etkide bulunup bulunmadığının,
  - bu hataların zamanında düzeltildiğinin ve tekrar giriş için yetkili personel tarafından gözden geçirilerek onaylandığının tespitinin

  belirlenmesi

2.2.2 VERİ TRANSFER KONTROLLERİ

Kontrol Hedefi

Verilerin tam, doğru, zamanında ve güvenli bir şekilde transferini sağlamaktır.

Riskler

Veri transferi ile ilgili olarak karşılaşılabilecek risklerden bazıları şunlardır:

- Transfer edilen verinin bozulması, kaybolması, çalınması, değiştirilmesi
- Verinin iletilememesi veya iletilip iletilemediğinin bilinememesi
- Mükerrer veri iletilmesi
- Veri transferinin reddedilmesi

Temel Kontroller

Veri transfer kontrollerine ilişkin riskleri makul seviyeye düşürecek temel kontroller şunlardır;

- Veri transferinden sorumlu personele rehberlik yapacak prosedürler tanımlanmış olmalıdır.
- Veri transferi ile ilgili detaylı teknik bilgiler yazılı hale getirilmeli ve personel ihtiyaç duyduğunda bu bilgilere erişebilmelidir.
- Sistemler arasında yapılan veri transferlerinin tam ve doğru olarak yapılmasını sağlayan manuel veya otomatik kontroller olmalıdır.

Kontrollerin Değerlendirilmesi

Politika ve prosedürler

Kontrol

VTK- 1 Veri transferinden sorumlu personele rehberlik yapacak prosedürler tanımlanmış olmalıdır.

Kontrol varlığını değerlendirme soruları

- Veri transferine ilişkin tanımlanmış bir prosedür var mı?

Kontrol etkinliğini inceleme yöntemi

- Veri transferine ilişkin sürecin incelenerek aşağıdaki hususları kapsayıp kapsamadığının belirlenmesi:
  - Görevliler, yetki ve sorumlulukları
  - Transfer edilecek dosya ve mesajlar
  - Transfer sürecinin altyapısına ait bilgiler örneğin ilgili programlar
  - Güvenlik ve veri işlemeye ilişkin konular
  - Transfer şeması ve sıklığı
  - İletinin başlatılması, alınması ve saklanması
  - Disket, kaset gibi bilgi ortamı araçlarıyla yapılan aktarımlara ilişkin prosedürler
  - Transfer yönetimi yönergesi

- Transferlerin izlenmesini sağlayan arayüzlerin oluşturulması
- Transferin başarı ile tamamlandığına dair kontroller
- Hatalarla baş etme prosedürleri
- Yeniden başlatma mekanizması
- Acil durum ve felaket sonrası durumla baş etme işlemleri
- Günlük tutulması ve saklaması

- Sürecin yeterliliğinin ve güncellenip güncellenmediğinin belirlenmesi için gözden geçirilmesi
- Uygulanan mantıksal ve fiziksel erişimlerinin yeterliliğinin test edilmesi amacıyla veri transferi yapılan örnek işlemlerin seçilmesi ve yetkili kişiler tarafından yapılıp yapılmadığının belirlenmesi

Belgeleme

Kontrol

VTK-2 Veri transferi ile ilgili detaylı teknik bilgiler yazılı hale getirilmeli ve personel ihtiyaç duyduğunda bu bilgilere erişebilmelidir.

Kontrol varlığını değerlendirme soruları

- Veri transferine ilişkin teknik detayları içeren yazılı dokümanlar var mı?
- Personel ihtiyaç duyduğunda bunlara ulaşabiliyor ve yararlanabiliyor mu?

Kontrol etkinliğini inceleme yöntemi

- Veri transfer sürecinin kontrolünde kullanılan donanım ve yazılımlara ait dokümanların elde edilmesi ve bunların yeterli olup olmadıklarının değerlendirilmesi
- Uygulama programlarına veri gönderilmesi veya alınmasına ilişkin detay bilgilerin temin edilmesi:
  - Veri akış yönü
  - Transfer edilen bilgilerin türü
  - Transfer edilen işlemlerin yaklaşık hacmi veya değeri
- Yönetimle görüşme yapılarak veri transfer alt yapısının beklendiği şekilde çalışmasına ilişkin riskleri öngörüp öngörmediğinin tespit edilmesi
- Tüm belgelerin güncellendiğinin ve muhafaza edildiğinin belirlenmesi

Kontroller

Kontrol

VTK-3 Sistemler arasında yapılan veri transferlerinin tam ve doğru olarak yapılmasını sağlayan manuel veya otomatik kontroller olmalıdır.

Kontrol varlığını değerlendirme soruları

- Veri transferinin tam ve doğru olarak yapılmasını güvence altına alan otomatik veya manuel kontroller var mı?

Kontrol etkinliğini inceleme yöntemi

- Bilişim sitemleri personeli ile görüşme yaparak ve dokümanları gözden geçirerek veri transferinin tam ve doğru olarak

gerçekleşmesini sağlayacak otomatik ve manuel kontrollerin aşağıdaki hususları kapsayıp kapsamadığının belirlenmesi:

- Transfer edilen dosyaların üstünde büyüklüğü ve parasal değerine ilişkin bilgilerin yer alması
- Elektronik olarak hedef veya kaynak dosya büyüklüğünün karşılaştırılması
- Transferde doğru prosedürün uygulandığının kontrol edilmesi
- Mesaj veya raporlara ilişkin transferin başarıyla gerçekleşip gerçekleşmediğine ilişkin aşağıda yazılı otomatik kontrollerin bulunması:
  - Döngü\ yankı kontrolü
  - Fazlalık kontrolü
  - Eşlik kontrolü
  - Mükerrerlik kontrolü
  - Eşitlik kontrolü.
  - Hata kodu
  - Ardışık işlem (dizi) kontrolü
- Hata raporlarının üretilmesi
- Verinin kriptolanması (bkz ağ yönetimi)

2.2.3 İŞLEM KONTROLLERİ

Kontrol Hedefi

Verinin uygulama programı içerisinde tam ve doğru olarak işleme tabi tutulmasını ve denetlenebilir olmasını sağlamaktır.

Riskler

İşlem kontrollerinin yetersizliği aşağıda yazılı risklerin gerçekleşmesine neden olabilir:

- Sürecin yanlış işletilmesi
- Sistematik hataların oluşması
- Yanlış dosyaların işleme tabi tutulması
- Hataların tespit edilip düzeltilememesi
- Denetim izinin kaybolması ve işlem sahibine başvurulamamasına
- Mantıksız işlemlerin meydana gelmesi
- İşlemlerin doğrulanamaması

Temel Kontroller

İşlem kontrollerine ilişkin riskleri makul seviyeye düşürecek temel kontroller şunlardır;

- İş ve zaman çizelgesi hazırlanmalı ve bu çizelge kullanıcı ve işletim personeli tarafından anlaşılır olmalıdır.
- Yönetim tarafından bilgisayar işlemlerinin doğru zamanda ve doğru bir silsile ile işletildiğinin teyidini sağlayan yeterli bir kontrol mekanizması kurulmalıdır.
- Süreçte başarısızlık veya problemle karşılaşıldığında, personel, işlemleri onaylandıkları en son noktadan yeniden başlatabilmelidir.
- Bütün işlemler ve bilgisayar kaynaklı hatalar hata ve beklenmedik durum raporlarında yer almalı ve bunlar yönetim tarafından gözden geçirilmelidir.

Kontrollerin Değerlendirilmesi

İş ve zaman çizelgesi

Kontrol

İK-1 İş ve zaman çizelgesi hazırlanmalı ve bu çizelge kullanıcı ve işletim personeli tarafından anlaşılır olmalıdır.

Kontrol varlığını değerlendirme soruları

- İş sürecini tanımlayan bir iş ve zaman çizelgesi var mı?

Kontrol etkinliğini inceleme yöntemi

- İş ve zaman çizelgesinin temin edilmesi, incelenmesi ve iş çizelgesinin aşağıda yazılı bilgileri içerip içermediğinin belirlenmesi:
  - Yapılması gereken işler ve iş öncelikleri
  - İş uygulamalarındaki sıra akışı
  - Ulaşılması gereken bilgi ortamı ve dosyalar

- o İşlem sonrası süreç, örneğin yeniden uzlaştırma ve beklenin üstündeki çıktıların gözden geçirilmesi
- Örnek seçilen iş akışlarının incelenmesi suretiyle iş ve zaman çizelgelerinin doğru bir sırayı takip edecek, doğru bir zamanda doğru bilgi dosyalarına erişecek şekilde tasarlanıp tasarlanmadığının tespit edilmesi

Kontroller

Kontrol

İK-2 Yönetim tarafından bilgisayar işlemlerinin doğru zamanda ve doğru bir silsile ile işletildiğinin teyidini sağlayan yeterli bir kontrol mekanizması kurulmalıdır.

Kontrol varlığını değerlendirme soruları

- Sistemde işlemlerin tam ve doğru yapılmasını sağlamaya yönelik otomatik kontroller var mı?
- İş akışını izlemek amacıyla özel yazılımlar kullanılıyor mu?
- İşlem uygulama süreci gözden geçiriliyor mu?

Kontrol etkinliğini inceleme yöntemi

- Bilişim sitemleri personeliyle görüşme yapılarak veya dokümanlar incelenerek yazılıma entegre edilmiş aşağıda yazılı işlem kontrollerinden hangilerinin kullanıldığının belirlenmesi:
  - o Düzen ve biçim kontrolü
  - o Programlanmış kontroller
  - o Birebir toplam kontrolü
  - o Hesaplanmış miktarlarda makullük kontrolü
  - o Hesaplanmış miktarlarda limit kontrolü
  - o Dosya toplamlarını uyumlaştırma kontrolü
- İş akışını izleyen özel yazılımların aşağıdaki bilgileri sağlayıp sağlamadığının belirlenmesi:
  - o İş akışına göre işlemlerin çalışma şekli
  - o İşlemlerin yetki dahilinde yapılması
  - o Doğru dosyalara ulaşıldığının teyidi
  - o Sadece onaylanmış programların hassas verilere ulaşabilmesi
- Otomatik kontrollerin olmaması durumunda amaca uygun telafi edici kontrollerin olup olmadığının belirlenmesi
- Uygulama işlem prosedürlerinin hangi aralıklarla ve nasıl gözden geçirildiğinin öğrenilmesi ve kontrol süreci için yeterli olup olmadığının değerlendirilmesi
- Verilere ilişkin akışın istenildiği gibi doğru bir şekilde gerçekleştiğini test etmek amacıyla aşağıdaki testlerin uygulanması:
  - o Anlık görüntü alma (snapshot)
  - o İz sürme (Tracing)
  - o Haritalandırma (mapping)
- Örnekleme yoluyla seçilen işlemlerin doğru hesaplanıp hesaplanmadığının tespiti amacıyla manuel olarak hesaplamalarının yapılması ve sonuçların bilgisayar çıktılarıyla karşılaştırılması

	İşlemleri yeniden başlatma
Kontrol	**İK-3** Süreçte başarısızlık veya problemle karşılaşıldığında, personel, işlemleri onaylandıkları en son noktadan yeniden başlatabilmelidir.
Kontrol varlığını değerlendirme soruları	▪ Problemlerle karşılaşılması durumunda işlemleri yeniden başlatma prosedürleri tanımlanmış mı?
Kontrol etkinliğini inceleme yöntemi	▪ Yönetim ile görüşme yapılarak ve ilgili dokümanlar gözden geçirilerek gerektiğinde verilerin yedeklenmesi, dosya kurtarma işlemlerinin başlatılması ile ilgili belirlenmiş bir prosedürün olup olmadığının belirlenmesi ▪ İncelenen dönemde, kontroller onaylandıktan sonra sürecin yeniden başlatılmak zorunda olduğu kayıtlı vakaların tespit edilmesi ve onaylanma sürecinin doğru bir şekilde işletilip işletilmediğinin belirlenmesi
	Hata kontrolü ve gözden geçirme
Kontrol	**İK-4** Bütün işlemler ve bilgisayar kaynaklı hatalar, hata ve beklenmedik durum raporlarında yer almalı ve bunlar yönetim tarafından gözden geçirilmelidir.
Kontrol varlığını değerlendirme soruları	▪ Hata ve kural dışı durumlara dair raporlar üretiliyor mu? ▪ Hata ve beklenmedik durum raporları yönetim tarafından günlük olarak gözden geçiriliyor mu?
Kontrol etkinliğini inceleme yöntemi	▪ Hata ve kural dışı rapor temin edilmesi ve bütün sorunların makul bir süre içinde açıklığa kavuşturulup kavuşturulmadığının ve düzeltme işlemlerinin yönetim tarafından onaylanıp onaylanmadığının belirlenmesi

2.2.4 ÇIKTI KONTROLLERİ

Kontrol Hedefi

Çıktıların tam, doğru ve zamanında üretilmesini, doğru yere/kişilere dağıtılmasını, gizliliklerinin korunmasını, tespit edilen hataların detaylı olarak incelenmesini ve gereğinin yapılmasını sağlamaktır.

Riskler

Çıktı kontrollerinin yetersizliği nedeniyle karşılaşılabilecek risklerin bir kısmı aşağıda belirtilmiştir:

- Çıktıların tam ve doğru olmaması
- Uygun bir şekilde sınıflandırılıp dağıtılamaması
- Yetkisiz kişilerin eline geçmesi
- Hataların tespit edilememesi ve düzetilememesi
- Çıktıların muhafaza edilememesi

Temel Kontroller

Çıktı kontrollerine ilişkin riskleri makul seviyeye düşürecek temel kontroller şunlardır;

- Çıktıların elde edilmesine ve korunmasına ilişkin bir prosedür olmalıdır.
- Çıktıların dağıtımı ile ilgili prosedürler tanımlanmalı ve uygulanmalıdır.
- İlgili personel tarafından çıktı raporlarının doğruluğu gözden geçirilmeli ve hataları düzeltilmelidir.
- Çıktılara ilişkin hata veya beklenmedik durum raporu üretilmeli ve yönetim tarafından gözden geçirilmelidir.
- Çıktılar önceden tanımlanmış arşiv yönetmeliğine göre muhafaza edilmelidir.
- Kullanıcılar tarafından kullanılan özel rapor yazım araçları kontrol edilmelidir.

Kontrollerin Değerlendirilmesi

Prosedür

Kontrol

ÇK-1 Çıktıların elde edilmesine ve korunmasına ilişkin bir prosedür olmalıdır.

Kontrol varlığını değerlendirme soruları

- Çıktıların elde edilmesine ve korunmasına ilişkin bir prosedür var mı?

Kontrol etkinliğini inceleme yöntemi

- Çıktıların üretilmesine yönelik prosedürlerin incelenmesi ve aşağıda yazılı hususları kapsayıp kapsamadığının belirlenmesi:
  - Üretilmesi istenen veya beklenen çıktıların bir listesi
    - Ödeme emri, çek gibi mali nitelikli evraklar
    - Elektronik dosya ve veriler
    - Elektronik dosya veya verinin saklandığı araçlar (disket, kaset, kartuş vb.)
    - Yazılı raporlar

	o Çıktıların yasal zorunluluk gereği veya kurumun inisiyatifi ile belirlenmiş formatı o Çıktıların kim tarafından ne zaman üretileceği ve kimlere dağıtılacağı o Tanımlanmış iş ve zaman çizelgesi o Sürecin yürütülmesine ilişkin sorumluluklar o Elde edilen çıktıların saklanması ve güvenliğinin sağlanması
	Çıktıların dağıtımı
Kontrol	**ÇK-2** Çıktıların dağıtımı ile ilgili prosedürler tanımlanmalı ve uygulanmalıdır.
Kontrol varlığını değerlendirme soruları	▪ Bütün çıktıların doğru yere/kullanıcıya ulaşmasını ve gerekiyorsa bunun gizlilik içinde sürdürülmesini sağlayan bir dağıtım prosedürü var mı?
Kontrol etkinliğini inceleme yöntemi	▪ Uygulayıcılarla görüşme yapılması ve çıktıların dağıtımına ilişkin prosedürün incelenmesi suretiyle; o Doğru alıcıların nasıl tespit edildiğinin ve gönderilecek çıktıların gereken yere zamanında ulaştırılıp ulaştırılmadığının araştırılması o Çıktıların ulaştırılması beklenen alıcılarına beklenen zamanda ulaşmadığında neler yapıldığının belirlenmesi o Raporların uygun gizlilik işaretlerini içerip içermediğinin belirlenmesi o Üretilen ve dağıtılan raporların gizlilik esasına göre dağıtıldığının teyit edilmesi
	Uyumluluk
Kontrol	**ÇK-3** Çıktıların doğruluğu gözden geçirilmeli ve hatalar düzeltilmelidir
Kontrol varlığını değerlendirme soruları	▪ Çıktı üzerinde uygunluk, tamlık ve doğruluk kontrolleri yapılıyor mu?
Kontrol etkinliğini inceleme yöntemi	▪ Personel tarafından çıktılar üzerinde yürütülen kontrollerin aşağıdaki hususları kapsayıp kapsamadığının belirlenmesi: o Kontrol raporlarının uygun bir başlık, tarih, birbirini takip eden sayfa numaraları ve raporun bitimini gösteren işaretlere sahip olması o Bir işlem süreci için üretilen bütün fiziksel çıktıların beklenen çıktı listesiyle karşılaştırılması o Fiziksel çıktı ile elektronik ortamdaki çıktının aynı olması o Her bir işletim sürecinin sonucunda, üretilen rapor toplamları ile fiziksel belge toplamlarının karşılaştırılması, bütün tutarsızlıkların incelenmesi ve düzeltilmesi ▪ Eğer muhasebe programı üzerinde çalışılıyorsa bilgisayar destekli denetim yazılımları vasıtasıyla alınmış tüm yevmiye kayıtlarından hareketle mali tabloların yeniden üretilmesi ve

belgelerde yer alan mali tablolarla karşılaştırılarak bir farklılığın olup olmadığının tespit edilmesi

Hata raporları

Kontrol

ÇK-4 Çıktılara ilişkin hata veya beklenmedik durum raporu üretilmeli ve yönetim tarafından gözden geçirilmelidir.

Kontrol varlığını değerlendirme soruları

- Hata ve beklenmedik durum raporları üretiliyor ve düzenli olarak gözden geçiriliyor mu?

Kontrol etkinliğini inceleme yöntemi

- Yönetimle görüşme yapılarak sistem/uygulama programlarının hatalı çıktılarının nasıl raporlandığının ve değerlendirildiğinin belirlenmesi
- Örnekleme yoluyla seçilen hata raporların incelenerek, hataların nedenleri, bu hataların neticesinde yapılan işlemlerin ve bunların tekrarlanmaması için alınan önlemlerin tespit edilmesi

Muhafaza

Kontrol

ÇK-5 Çıktılar önceden tanımlanmış arşiv yönetmeliğine göre muhafaza edilmelidir.

Kontrol varlığını değerlendirme soruları

- Çıktılarının saklanmasına yönelik belirlenmiş kontroller var mı?
- Manyetik çıktılar uygun fiziksel ortamlarda saklanıyor mu?

Kontrol etkinliğini inceleme yöntemi

- Bütün kağıt ve elektronik çıktıların arşivleme, muhafaza ve depolama işlemlerinin yerinde olup olmadığının belirlenmesi
- Güvenlik, etiketleme ve saklama dönemlerinin birimin, işin, denetimin ve yasal gereksinimlerin ihtiyacını karşılayıp karşılamadığının incelenmesi
- Bütün manyetik çıktıların uygun iklim şartlarında muhafaza edilip edilmediğini belirlenmesi
- Kaset, disket veya kartuş çıktılarının bilgi ortam kütüphanesinde saklanıp saklanmadığının tespiti

(Bkz. Yönetim kontrolleri, fiziksel ve çevresel kontroller, acil durum ve iş sürekliliği planlaması)

Özel raporlama araçları

Kontrol

ÇK-6 Kullanıcılar tarafından kullanılan özel rapor yazım araçları kontrol edilmelidir.

Kontrol varlığını değerlendirme soruları

- Özel yazılım araçları kullanılıyor mu?

Kontrol etkinliğini inceleme yöntemi

- Satın alınan herhangi bir rapor yazım yazılımının olup olmadığının belirlenmesi
- SQL gibi raporlamada kullanılan yazılımların kimler tarafından kullanıldığının, raporların nasıl tasarlandığının belirlenmesi ve denetim için sunulan raporların yetkililer tarafından onaylanıp onaylanmadığının tespit edilmesi

ÜÇÜNCÜ BÖLÜM
DENETİM SONUÇLARININ RAPORLANMASI VE İZLENMESİ

Kesinleştirilen denetim bulguları temelinde denetim sonuçları denetim amacına uygun olarak denetçi görüşünü de içerecek şekilde raporlanır. Denetim sonuçlarının raporlanması, taslak raporun hazırlanması, kurumla görüşülmesi, nihai raporun yazılması ve ilgililere sunulması süreçlerinden oluşur.

Denetim raporu tam, güvenilir, objektif, yeterli kanıta dayalı, açık, öz ve anlaşılır olmalıdır.

Raporun tam olması; denetimden beklenen amaçların tamamının raporda yer alması, raporda yer verilmeyen hususlara ilişkin olarak objektif kriterlere dayalı açıklamaların yapılmasıdır.

Raporun güvenilir olması; raporda yer alan bulguların yeterli ve ispat edilebilir kanıtlara dayalı olmasını ve raporun tam olmasını gerektirir.

Raporun objektif olması; denetim sonucu elde edilen bulguların tarafsız bir şekilde rapora yansıtılmasıdır. Raporda denetimin tarafsızlığını zedeleyebilecek savunucu ve/veya suçlayıcı ifadelerden kaçınılmalıdır.

Raporun yeterli kanıta dayalı olması; denetim sonunda elde edilen bulgu ve sonuçların yeterli sayıda ve ikna edici nitelikte olmasıdır.

Raporunun açık, öz ve anlaşılır olması; yazılacak ifadelerin sade ve kısa olmasını, gereksiz detay ve tekrarlardan, teknik terim ve kısaltmalardan kaçınılmasını gerektirir. Teknik terimlerin veya kısaltmaların kullanılması gerekli olduğu durumlarda bu terimler ayrıca açıklanır ve kullanılan kısaltmalara ilişkin bilgilere raporda ayrı bir bölümde yer verilir.

3.1 TASLAK RAPORUN HAZIRLANMASI

Taslak denetim raporu, aşağıda belirtilen bölümlerden oluşacak şekilde hazırlanır:

- Giriş
- Genel kontrollerin değerlendirilmesi bölümü
- Uygulama kontrollerinin değerlendirilmesi bölümü

- Sonuç
- Ekler ve tablolar

Taslak raporun kapağında Sayıştay Başkanlığı ibaresi, denetlenen kurum ve/veya sistemin adı ve rapor tarihi yer alır.

Taslak raporun giriş bölümünde raporun amacı, denetlenen kuruma ve kurumun bilişim sistemine ilişkin genel bilgiler verildikten sonra denetim metodolojisine ilişkin olarak denetim kapsamı ve denetim yaklaşımı ifade edilir.

> *Raporun amacı* başlığı altında denetlenen kurum bilişim sistemlerinin niçin denetlendiği, denetimden beklenen çıktının ne olduğu açık ve net bir şekilde ifade edilir.
>
> *Denetlenen kuruma ve kurumun bilişim sistemleri hakkında genel bilgi* verilirken, kurumun ana faaliyetleri, idari yapılanmadaki yeri, organizasyon yapısı ve birimlerine ilişkin açıklamalardan sonra, bilişim sistemleri ile ilgili birimin çalışan profili, organizasyon yapısı, kurumun ana faaliyetlerinin yerine getirilmesi için kullanılan sistemler ve uygulamalar, bilişim sistemleri topolojisi, kurumun ağ altyapısı, kurum bütçesinin bilişim sistemlerine harcanan miktarı gibi hususlara da ver verilir. Bu amaçla denetim planlama aşamasında kullanılan "Bilişim Sistemleri Bilgi Edinme Form"undan (EK-1) faydalanılır.
>
> *Denetim kapsamı* bölümünde denetim faaliyetlerinin hangi süreç, sistem ve faaliyet alanları üzerinde yürütüldüğü belirtilir. Denetçi, denetlenmesi öngörülen alanların belirlenmesinde nasıl hareket edildiğini, hangi faktörlerin dikkate alındığını bu bölümde belirtmelidir.
>
> *Denetim yaklaşımı* bölümünde denetçi, risk değerlendirmesinin ne şekilde yapıldığını, denetim sırasında göz önünde tutulan varsayımları, kanıt toplama ve analiz tekniklerini, bu tekniklerin niçin tercih edildiğini, örnekleme yöntemi kullanılmışsa kullanılan örnekleme yöntemi, neden bu yöntemin kullanıldığı ve kullanılan bu örnekleme yöntemi sonucunda elde edilen bulguların popülasyonun bütününe genellenip genellenemeyeceği bilgilerine yer verir.

Taslak raporun giriş bölümünden sonra **genel kontrollerin ve uygulama kontrollerinin değerlendirilmesi** bölümlerine yer verilir. BS kontrollerin değerlendirilmesinde rehberin sistematiği izlenerek önce genel kontrollerin daha sonra uygulama kontrollerinin değerlendirilmesi yapılır. Bu değerlendirmelerde her bir kontrol alanı bir başlık oluşturacak şekilde kontrol açıklıklarına göre elde edilen bulgulara ve bu bulgulara ilişkin risk değerlendirmesine göre risk düzeyleri, olası etkileri ve -eğer varsa- söz konusu açıklığın giderilmesine yönelik kurumun çözüm çalışmalarına da yer verilir. Son olarak denetçi bulgu, risk düzeyi, olası etkiler ve kurum çözüm çalışmalarını bir arada değerlendirerek önerilerde bulunur.

Taslak raporun **sonuç** kısmında ise, elde edilen bulgular çerçevesinde bilişim sistemleri kontrollerinin genel bir değerlendirmesi yapılır ve bilişim sistemlerinin güvenilirliğine ilişkin denetim ekibinin görüşü yazılır.

Taslak raporun **ekleri** bölümünde ise, kontrol alanları bazında bulguların nasıl elde edildiğine ilişkin detay bilgiler ve gerekli görülen tablolar yer alır.

3.2 TASLAK RAPORUN KURUMLA GÖRÜŞÜLMESİ

Hazırlanan taslak rapor kurum yönetimine gönderilir ve çalışma programına uygun şekilde kurum üst yönetiminin görüşlerinin alınması için toplantı düzenlenir. Bu toplantıda raporda belirtilen konular ve yapılan öneriler ile kurum tarafından başlatılmış olan çalışmalar ve geleceğe ilişkin yapmayı düşündükleri düzeltme çalışmaları konusunda bilgi alınır. Raporda

ifade edilen hususlar konusundaki itirazları veya düzeltme istekleri varsa not edilir. Toplantı sonrasında belirli bir süre verilerek görüşlerini ve yapılan çalışmaları yazılı bir şekilde sunmaları istenir.

Denetlenen kurumun herhangi bir nedenle görüş bildiremediği veya görüş bildirmeyi reddettiği durumlarda, bu durum nedenleriyle birlikte açıkça raporda yer alır.

3.3 NİHAİ RAPORUN YAZILMASI

Denetlenen kurum yönetimi ile yapılan görüşmeler ve yazılı cevapları dikkate alınarak rapora son şekli verilir. Denetçi, denetlenen kurumun görüşlerini haklı bulması halinde, raporda gerekli düzeltmeleri yapar. Kurum tarafından düzeltilmesi kabul edilen ve rapor hazırlandığı ana kadar yapılan düzeltme çalışmalarına da "çözüm çalışmaları" başlığı altında raporda yer verir.

TBMM'ye ve denetlenen kuruma gönderilecek nihai raporda, taslak raporun giriş bölümünün önüne, dilerse Sayıştay Başkanı'nın **sunuş**u ve **özet** bölümleri eklenir.

R**aporun özet bölümü**nde; denetimin amaçları tanımlanarak bu denetim amaçlarının gerçekleştirilmesi için uygulanan denetim metodolojisi özet olarak ifade edilir. Yine bu bölümde başlıklar halinde temel bulgulara ve bu bulgulara göre iç kontrollerin genel değerlendirmesini içeren denetim sonucuna yer verilir.

Ayrıca raporun sonuç bölümünden sonra gelmek üzere kurum, sistem, mevzuat vs. isimleri için kısaltma kullanılması durumunda bu kısaltmaların açılımları **kısaltmalar** ve raporda kullanılan teknik ve bilinmeyen ifadelere ilişkin tanımlamaların yer aldığı **sözlük** bölümleri de eklenebilir.

3.4 RAPORUN İLGİLİLERE SUNULMASI

Bilişim sistemleri denetimi sonucunda hazırlanan nihai rapor, öncelikle denetlenen kuruma verilir.

Bilişim sistemleri denetimi mali denetim ile birlikte yürütüldüğü durumlarda, mali denetim ekibi ile görüşme yapılarak, bilişim sistemleri denetimi sonunda bulunan kontrol zayıflıklarının mali denetim sürecine ve raporlamaya etkileri tartışılmalıdır. Bilişim sistemleri denetim sonuçları, mali denetim sürecinde özellikle risk değerlendirmesinde kullanılacağından, bilişim sistemleri denetim sonuçlarının mali denetimin risk değerlendirmesinin yapılacağı zamana kadar yetiştirilmesi için BS denetimi yapılmasının da zaman alacağı göz önünde bulundurularak denetime başlanacak zamanın iyi planlanması gerekir.

Bilişim sistemleri denetimi mali denetim sürecinden bağımsız yapıldığı durumlarda ise rapor, görevlendirmenin amacına göre, ilgili denetim grubuna, denetimin yapıldığı sistemle ilgili olan kuruma ve Parlamentoya gönderilmek üzere Başkanlığa sunulur. Raporun Parlamentoya sunulup sunulmayacağı kararını Başkanlık verir.

3.5 SONUÇLARIN İZLENMESİ VE KALİTE KONTROLÜ

Bilişim sistemleri denetim raporunda tespit edilen hususlar ve öneriler konusunda kurum tarafından yapılan çalışmaların düzenli aralıklarla izlenmesi ve bu izleme faaliyeti sonuçlarının, bir sonraki denetimin planlama aşamasında kullanılması gerekir. Bu amaçla, elde edilen denetim bulgularının çözümü için kurum tarafından verilmiş bir yarih varsa bunu da

gösterecek şekilde bir izleme tablosu hazırlanır ve bu tablo bilişim sistemleri denetim ekibi tarafından düzenlenen, kuruma ait kalıcı dosyada muhafaza edilir.Bu amaçla "Bilişim Sistemleri Denetimi İzleme Tablosu Formu" (EK-10) kullanılır.

İzleme çalışmalarının hangi sıklıkla ve ne zaman yapılacağı denetim ekibince ayrıca planlanmalıdır.

Taslak denetim raporunda acil olarak giderilmesi gerektiği ifade edilen kritik konuların takibi denetim sürecinde yapılır ve söz konusu konuların nihai rapor tamamlanmadan önce düzeltilmesi hedeflenir. Bunun mümkün olmadığı durumlarda konunun takibinin yapılması için mali denetim ekibine de bilgi verilir.

Eğer düzenli bir izleme faaliyeti söz konusu değil ise denetçi önceki dönemlerde yapılan bilişim sistemleri denetimlerine ilişkin raporları inceleyerek bu raporlarda yer alan bütün bulguları kendi denetimi sırasında değerlendirir. Bu bulguların son durumlarına,konuya ilişkin kurum açıklamalarına ve açıklığın devam edip etmediklerine ilişkin değerlendirmelerine raporunda yer verir.

Yapılan Bilişim sistemleri denetiminin kalite kontrolünün sağlanması için, denetimin uluslararası standartlara ve Sayıştay Bilişim Sistemleri Denetim Rehberine uygun şekilde yapılıp yapılmadığı bilişim sistemleri denetimi konusunda uzmanlaşmış başka bir ekip veya denetçi tarafından incelenerek raporlanmalıdır. Bu amaçla "Bilişim Sistemleri Denetimi Kalite Kontrol Formu" (EK-9) kullanılır.

Denetimin kalite kontrolü, denetim raporu ilgililerine sunulmadan önce tamamlanmalıdır.

Ekler

EK - 1: BİLİŞİM SİSTEMLERİ BİLGİ EDİNME FORMU

(Bu form kurumun bilişim sistemi yetkilileri tarafından doldurulmalı ve imzalanmalıdır.)

Formda doldurulması gereken her alan bir bilişim sistemi yetkilisi tarafından gözden geçirilmelidir. Eğer bilişim sisteminize uygun olmayan sorular varsa lütfen "U" (Uygulanamaz) harfi ile işaretleyin.

A. KURUM HAKKINDA GENEL BİLGİLER

1. Kurumunuz hakkında genel bilgileri içeren aşağıdaki tabloyu doldurunuz.

Denetlenen Kurumun Adı	
Ana faaliyetler	
Yıllık ödemeler/harcamalar (YTL)	
Toplam varlıklar (YTL)	
Bilişim sistemleri varlıklarının toplam değeri (YTL)	
Yıllık bilişim sistemleri bütçesi (YTL)	

2. Bilişim sistemiyle ilişkili olarak son bütçe dönemi içinde yapılan harcamaların listesini aşağıdaki şablona uygun şekilde hazırlayarak forma ekleyiniz.

No	Harcamanın Niteliği	Tutar (YTL)	Tarih
1			
2			

3. Son iki yılın bütçe tahminleri ile harcama miktarlarını ekleyiniz.

B. KURUMSAL YAPI VE ÇALIŞANLAR

1. Bilişim sisteminin güncel yapısını gösteren sistem topolojisini ve organizasyon şemasını bu belgeye ekleyiniz.
2. Bilişim sistemi yöneticisinin kime karşı sorumlu olduğunu belirtiniz.

Adı		Görevi	

3. Bilişim sistemi personeli ile ilgili olarak aşağıdaki tabloyu doldurunuz.

Genel Yönetim: Bilgi işlem biriminin yönetiminden sorumlu kişi.

"Yetkili kişi" bilgi işlem biriminde yürütülen işlerden birim yönetimine karşı sorumlu olan kişi.

"İrtibat kurulacak kişi", söz konusu alanla ilgili olarak denetim çalışmalarında muhatap olunacak kişi.

	Pozisyon		İrtibat Kurulacak Personel	
Faaliyet Alanı	Yetkili Personel Sayısı	İşi Yürüten Personel Sayısı	Adı - Soyadı	Telefon Numarası
Genel Yönetim				
BS Güvenliği				
Fiziksel Güvenlik				
Sistem Yönetimi				
İletişim/ Ağ Yönetimi				
Veri Yönetimi				
Veritabanı Yönetimi				
Yazılım Geliştirme				
Web Tasarım				
Teknik Destek				
Diğer				
Toplam Personel				

4. Yukarıdaki listede yer alan personelden kilit nitelikte olanları lütfen belirtin.

5 Son bir yıl içinde bilişim sistemi kilit pozisyonlarında meydana gelen personel değişikliklerini ve/veya yeniden yapılanma sonucu oluşan değişiklikleri ve gelecekte yapılması öngörülen değişiklikleri beli rtiniz.

Adı Soyadı	Eski Pozisyonu ve Çalışma Tarihleri	Yeni Pozisyonu ve Görevlendirme Tarihi

6. Bilgi işlem dairesinde görevli personelin son iki yıl içinde kullandığı izinleri gösteren bir tabloyu forma ekleyiniz.

C. BİLİŞİM SİSTEMLERİ HAKKINDA TEKNİK BİLGİLER

Bilişim sisteminin teknik yapısı ile ilgili olarak aşağıdaki kısımlarda istenen bilgileri doldurunuz:

1- Donanım

Donanımın Türü	Model	Adet	Yeri	Ağa bağlı olma durumu

Ayrıntılı donanım envanterini ekleyiniz.

2- Yazılım (Tablo eklenecek)

2.1 Uygulama Yazılımları

Kelime işlemci ve tablolama programları

- ☐ Ofis yazılımları
- ☐ Uygulama programı yazılımları (file maker vs.)
- ☐ Diğer

Veri Tabanı yönetim Sistemleri

- ☐ Oracle
- ☐ Microsoft Access
- ☐ SQL
- ☐ Dbase
- ☐ Diğer

2.2 İşletim Sistemleri

- ☐ Windows NT
- ☐ Windows (9x, 2000, XP, Vista)
- ☐ Novell Netware
- ☐ Unix
- ☐ Linux
- ☐ Diğer

2.3 Güvenlik Yazılımı

Güvenlik duvarı:

Antivirus:

Diğer:

2.4 Mali Sistem Yazılımları

2.4.1 Mevcut Yazılımlar

(CPU tarafından işlenen veya PC tabanlı olan bütün sistemler aşağıdaki tabloda tanımlanmalıdır.)

Mali Sistemin Adı	Program Sorumlusu	Paket/Kuruma Özgü	Kurulum Tarihi Sürüm	Programlama Dili	Kullanıcı Sayısı	Veri Giriş Yöntemi (Yığın/on-line)	Modüller

- Uygulama programlarına ait satın alma sözleşmelerini ve muayene kabul komisyon raporlarını ve uygulama sonrası gözden geçirme raporlarını;
- Uygulama programlarının fonksiyonlarını, program içinde veya sistemler arasında kullanılan ara yüzleri ve programın genel işleyişini tanımlayan bir bilgi notunu;
- Uygulama programlarına ait kullanıcı rehberlerini ve talimatlarını;

Ekleyiniz

2.4.2 Geliştirilmekte olan yazılımlar

Mali uygulamalara ilişkin bilişim sistemi bileşenlerinden şu anda önemli revizyonlara tabi tutulanlar ile ilerde revize edilmesi planlananları ayrıca belirtiniz

Programın adı	Amacı	Planlanan Bitiş Tarihi	Mevcut Durumu (Bulunduğu Aşama)

D- İŞ AKIŞ ŞEMALARI

Kurumun mali tablolarını üreten veya üretilmesine yardımcı olan bilişim sisteminin fiziksel özelliklerini gösteren bir çizelge hazırlayınız. Çizelgede şu hususlar çizimle gösterilmelidir:

1. Temel girdiler ve giriş noktaları,
2. Temel çıktılar ve çıkış noktaları,
3. Veri akışları,
4. Verilerin işlendiği yerler
5. Veri iletimini sağlayan ağlar

E- AĞ YAPISI

Açıklamaları içeren detaylı ağ haritasını forma ekleyiniz. (ağ altyapısında kullanılan teknolojiler, anahtarlama ve yönlendiricilerin konumları, internet bağlantısı (varsa) ne şekilde sağlandığı, ağların türü, mimari yapıları, topolojileri gibi bilgiler detaylı olarak açıklanmalıdır)

☐

F- HİZMETİN DEVAMLILIĞI

1. Bilişim sistemi ile ilgili beklenmedik ve acil durumlar karşısında kullanılmak üzere hazırlanan bir plan (acil durum planı) var mı? [ ] Evet [ ] Hayır

   Cevabınız evetse lütfen planın bir kopyasını ekleyin.

2. Bilişim sistemi için kullanılan ana merkez dışı depolama ünitesi/birimi var mı? [ ] Evet [ ] Hayır

   Cevabınız evetse, lütfen kurum dışı yedekleme stratejisini/politikasını açıklayan belgelerin özetini ekleyin.

3. Acil durum planının en son test edilme tarihi ve testin sonuçları nelerdir? (Test değerlendirme raporunu ekleyiniz.)

4. Ana merkez dışında depolama ünitesien son hangi tarihte teftiş edilmiş/gözden geçirilmiştir?

G. DENETİM RAPORLARI

Varsa önceki yıllara ait sistemle ilgili yapılmış olan tüm denetim raporlarını ekleyiniz

H. DİĞER HUSUSLAR

Bilişim sistemi ortamını daha iyi anlamak için önemli olduğunu düşündüğünüz diğer bilgileri belirtiniz

I. İMZALAR

Aşağıdaki tabloyu doldurunuz.

Hazırlayan:
Görevi:
Tarih:
Telefon no:
Fax no:
E-mail:
İmza

Gözden geçiren:
Görevi:
Tarih:
Telefon no:
Fax no:
E-mail:
İmza

EK - 2: BİLİŞİM SİSTEMLERİNDEN ETKİLENEN HESAP ALANLARININ BELİRLENMESİ FORMU

Kurum/Sistem Adı:			
No	**Yapılan İş**	**İşi Destekleyen Bilişim Sistemi (Program)**	**Etkilediği Hesap Alanları**

EK - 3: SİSTEM RİSK DEĞERLENDİRME FORMU

Kurum Adı:				
Sistem Adı:				
Risk Faktörleri	**Parametreler**	**Puan**	**Ağırlık**	**Risk**
Önemlilik (36%)				
Sistemin kurumun mali talolarına olan etkisi	Çok yüksek	4	20	
	Yüksek	3		
	Orta	2		
	Düşük	1		
Sistemin kurum mali işlemlerinin yürütülmesi ve kaynakların yönetilmesindeki rolü	Çok yüksek	4	20	
	Yüksek	3		
	Orta	2		
	Düşük	1		
Sistemin Kurumun misyonu ve ana faaliyetleriyle ilişkisi(bunlar açısından taşıdığı önem, rol)	Çok yüksek	4	15	
	Yüksek	3		
	Orta	2		
	Düşük	1		
Sistemin ilgili olduğu faaliyetin etkisi	Tüm ülkeyi ilgilendiriyor	4	15	
	Birden çok kurumu ilgilendiriyor	3		
	Kurumun tamamını ilgilendiriyor	2		
	Sadece birkaç birimi etkiliyor	1		
Sistemdeki hataların yol açabileceği muhtemel mali kayıplar	Çok yüksek	4	20	
	Yüksek	3		
	Orta	2		
	Düşük	1		
		Toplam:	90	
			Maksimum Risk Puanı:	360
Kritiklik Düzeyi (20%)				
Sistemin kritiklik derecesi (hizmet kesintisi olduğunda tolere edilebilecek zaman)	4 saatten az	4	9	
	4-24 saat arası	3		
	1-3 gün	2		
	4 günden fazla	1		
Sistemin bilgi varlıklarının gizliliği yönünden değeri	Çok yüksek	4	9	
	Yüksek	3		
	Orta	2		
	Düşük	1		
Sistemin bilgi varlıklarının bütünlüğü yönünden değeri	Çok yüksek	4	9	
	Yüksek	3		
	Orta	2		
	Düşük	1		

Sistemin bilgi varlıklarının kullanılabilirliği yönünden değeri	Çok yüksek	4	9	
	Yüksek	3		
	Orta	2		
	Düşük	1		
Sistemin mali değeri	Çok yüksek	4	5	
	Yüksek	3		
	Orta	2		
	Düşük	1		
Sistemdeki muhtemel bir hatanın ülke komuoyuna etkisi ve kurumun prestij kaybı	Çok yüksek	4	5	
	Yüksek	3		
	Orta	2		
	Düşük	1		
Sistemin üçüncü kişiler üzerindeki etkisi	Çok yüksek	4	4	
	Yüksek	3		
	Orta	2		
	Düşük	1		
		Toplam:	50	
			Maksimum Risk Puanı:	200
Karmaşıklık (16%)				
Kullanıcı sayısı	5.000 den çok	4	5	
	1.000-5.000 arası	3		
	100-1.000 arası	2		
	100 den az	1		
Destek personelinin sayısı	Hiç yok	4	6	
	1	3		
	2-3 arası	2		
	3 ten çok	1		
Sistemin işlem noktası sayısı	15.000 işlem noktasından çok	4	7	
	10..000-15.000 arası işlem noktası	3		
	5.000-10.000 arası işlem noktası	2		
	5.000 işlem noktasından az	1		
İşlem hacmi (yıllık)	10 milyondan çok	4	6	
	5-10 milyon arası	3		
	1-5 milyon arası	2		
	1 milyondan az	1		
Diğer sistemlerle yapılan günlük bağlantı sayısı	10 dan çok	4	6	
	5-10 arası	3		
	3-5 arası	2		
	3 ten az	1		
Ana dosyalardaki değişim (borçlular, alacaklılar vs)	İşlem sayısı yüksek, işlem miktarı yüksek	4	4	
	İşlem sayısı yüksek, işlem miktarı düşük	3		
	İşlem sayısı düşük, işlem miktarı yüksek	2		
	İşlem sayısı düşük, işlem miktarı düşük	1		

Sisteme internet üzerinden ve uzaktan erişen kitlenin büyüklüğü (günlük)	1000'den fazla	4	6	
	100-1000	3		
	10-100	2		
	10'dan az	1		
		Toplam:	40	
			Maksimum Risk Puanı:	160
Teknolojik Altyapı (16%)				
Yazılımın türü	3. taraflarca kurum için geliştirilmiş	4	8	
	Dışarıdan destek alınarak kurumda geliştirilmiş	3		
	Kurum içinde geliştirilmiş	2		
	Paket program	1		
Programlama dili	Eski ve destek alınması güç	4	6	
	Güncel ve kolay destek alınabiliyor	1		
Veritabanı	CC sertifikalı olmayan veritabanı	4	4	
	CC sertifikalı bilinen veritabanı	1		
İşletim sistemi	PC/Windows	4	7	
	Mid-range (Unix, Linux)	3		
	Mainframe	1		
Sisteme erişim durumu	İnternet	4	9	
	Diğer uzaktan erişim (İnternet hariç)	3		
	Intranet	2		
	Ağ erişimi yok	1		
Sisteme bağlı olarak çalışan donanım sayısının kurumdaki (aynı kategorideki) toplam donanım sayısına oranı	% 40 ve üzeri	4	6	
	%25 - % 40 arası	3		
	%10 - %25	2		
	%10'un altında	1		
		Toplam:	40	
			Maksimum Risk Puanı:	160
Kontrol Çevresi			**12%**	
Sistem yöneticilerinin ve personelinin bilgi-beceri düzeyi ve iş tecrübesi, bunların görev tanımlarına uygunluğu	Çok yüksek	4	5	
	Yüksek	3		
	Orta	2		
	Düşük	1		
Sistemin çalışması için extra eğitim gerekip gerekmediği ve eğitimli personel sayısı	Tam bağımlılk söz konusu	4	5	
	Sınırlı sayıda ve bağımlılık var	3		
	Sınırlı sayıda	2		
	Yeterli	1		
Sisteme erişim, yedekleme ve kurtarma prosedürlerinin bulunup bulunmadığı ve bunlara uyulup uyulmadığı	Yok	4	5	
	Var fakat uygulanmıyor	3		
	Var fakat iyi uygulanmıyor	2		
	Var ve uygulanıyor	1		
Sisteme ilişkin prosedürlerin belgelenmesi	%50'den az	4	4	
	%75-50	3		
	%90-75	2		
	%90'dan fazla	1		

Sistemde yapılan veya yapılması planlanan yıllık değişikliklerin sayısı	60 tan çok	4	3	
	30-60 arası	3		
	10-30 arası	2		
	10 dan az	1		
Yıllık karşılaşılan problem sayısı	100 den çok	4	5	
	70-100 arası	3		
	30-70 arası	2		
	30 dan az	1		
Önceden yapılan denetim sayısı	Daha önce hiç denetim yapılmamış	4	3	
	Son üç yıl içinde bazı incelemeler yapılmış	3		
	Önceki yıl incelenmiş	1		
		Toplam:	30	
			Maksimum Risk Puanı:	120
			Genel risk puanı:	

EK - 4: RİSK DEĞERLENDİRME MATRİSİ

RİSK DEĞERLENDİRME MATRİSİ	
Kurum Adı:	
Sistem Adı:	

	Risk alanı	maksimum risk puanı	Toplam risk puanı	Uygulama sisteminin risk puanlarına göre risk derecesi		
				yüksek	orta	düşük
1	**Önemlilik**	360		360-270	270-180	180-90
2	**Kritiklik**	200		200-150	150-100	100-50
3	**teknik altyapı**	160		160-120	120-80	80-40
4	**karmaşıklık**	160		160-120	120-80	80-40
5	**kontrol çevresi**	120		120-90	90-60	60-30
	Genel	1000		1000-750	750-500	500-250

EK - 5: RİSK DERECELENDİRME FORMU

Kurum Adı:		
Sistemin Adı	**Toplam risk puanı**	**Risk Derecesi**

EK - 6: BULGU/RİSK DEĞERLENDİRME MATRİSİ

BULGU/ RİSK DEĞERLENDİRME MATRİSİ		GERÇEKLEŞME OLASILIĞI			
		SIKLIKLA	ARASIRA	SEYREK	ÇOK ZOR
ETKİ DÜZEYİ	ÇOK YÜKSEK				
	YÜKSEK				
	ORTA				
	DÜŞÜK				

ÇOK YÜKSEK RİSK:	Derhal önlem alınmazsa kurum varlıklarında telafisi güç kayıplara sebebiyet verebilecek belirgin kontrol zayıflıkları veya eksiklikleri var. Kesinlikle kabul edilemiyecek bir risk düzeyidir ve ivedili olarak gerekli tedbirler alınmalıdır.
YÜKSEK RİSK:	Önemli bir kontrol zayıflığı ya da eksikliği görülmekte ve makul bir süre içerisinde önlem alınmasını gerektirmektedir. İstenmeyen bir risk düzeyi ve kurum tarafından mevcut riskler değerlendirilerek gerekli tedbirler alınmalıdır.
ORTA RİSK:	Kurum tarafından tekrar değerlendirmesi gereken bir risk düzeyi. Kurum risk değerlendirmesi çerçevesinde kabul edilebilecek bir risk düzeyi. Sistemde belirli kontrol zayıflıkları olmakla birlikte etkisi derhal önlem almayı gerektirmeyebilir, ancak uzun dönemde bu zayıflıkların giderilmesi gerekir.
DÜŞÜK RİSK:	Kabul edilebilir risk seviyesi.

EK -7: BULGU DEĞERLENDİRME FORMU

BULGU DEĞERLENDİRME FORMU				
Kurum/Sistem Adı	**:**			
Kontrol Alanı	**:**			
Bulgu No	**:**		**Ref:**	
Bulgu	**:**			
Kontrol Hedefi	**:**			
Etki	**:**			
Risk Düzeyi	**:**			
Öneri	**:**			
Kurum Cevabı	**:**			

EK - 8: BULGU ÖZET TABLOSU FORMU

BULGU ÖZET TABLOSU						
Kurum/Sistem Adı:						
Kontrol Alanı **Bulgu**	**Bulgu sayısı**	**Risk düzeyine göre bulgu sayısı**				**Mali tabloları doğrudan etkileyebilecek veya mali kayba yol açabilecek bulgu sayısı**
		çok yüksek	**yüksek**	**orta**	**düşük**	
I. GENEL KONTROLLER						
1 Yönetim Kontrolleri						
1.1 Stratejik planlama						
1.2 Güvenlik Politikaları						
1.3 Organizasyon						
1.4 Varlık Yönetimi						
1.5 Personel ve Eğitim Politikaları						
1.6 Uygunluk						
2 Fiziksel ve Çevresel Kontroller						
2.1 Fiziksel Kontroller						
2.2 Çevresel Kontroller						
3 Ağ Yönetimi ve Güvenliği Kontrolleri						
4 Mantıksal Erişim Kontrolleri						
4.1 Mantıksal Erişim Politikaları						
4.2 İşletim Sistemi Erişim Kontrolleri						
4.3 Uygulama Programlarına Erişim Kontrolleri						
5 İşletim Kontrolleri						
5.1 İşletim Sistemi ve Bilgisayar İşlemleri Kontrolleri						
5.2 Veri Tabanı Güvenlik Kontrolleri						

6 Sistem Geliştirme ve Değişim Yönetimi Kontrolleri						
6.1 Sistem Geliştirme Kontrolleri						
6.2 Değişim Yönetimi (Kurulum ve Kabul) Kontrolleri						

7 Acil Durum ve İş Sürekliliği Planlaması Kontrolleri						

II. UYGULAMA KONTROLLERİ						
1 Girdi Kontrolleri						
2 Veri Transfer Kontrolleri						
3 İşlem Kontrolleri						
4 Çıktı Kontrolleri						

EK - 9: BİLİŞİM SİSTEMLERİ DENETİMİ KALİTE KONTROL FORMU

Denetlenen Kurum veya Sistem	**:**
Denetimin Yapıldığı Tarih	**:**
Denetim Ekip Yöneticisi	**:**
Denetim Ekibinde Görevli Denetçiler	**:**
Denetim Kalite Kontrolünü Yapan Denetçi	**:**
Denetim Kalite Kontrolü Başlangıç ve Bitiş Tarihi	**:**

A	**Denetimin Planlanması**	**Değerlendirme**

A1 Kurum Bilişim Sistemlerinin Tanınması

- Kurum hakkında genel bilgiler edinilmiş mi? (Ana faaliyetler, Toplam varlıklar, BS varlıklarının toplam değeri, Yıllık BS bütçesi vb.)
- Bilişim sistemlerine ilişkin yeterli bilgi toplanmış mı? (Bilişim Sistemleri Bilgi Edinme Formu doldurulmuş mu?)
- Kurum yetkilileriyle görüşülmüş mü?
- Kurumsal yapı ve bilişim sistemi personeli hakkında bilgi edinilmiş mi? (Organizasyon şeması, sistem omurga şeması, bilişim sistemleri yöneticisi ve kime karşı sorumlu olduğu ve diğer bilişim sistemi personeli)
- İşletim sistemi hakkında teknik bilgiler elde edilmiş mi? (donanım, yazılım, uygulama programları)
- Hazırlanmış iş akış şemaları elde edilmiş mi?
- Ağ yapısı ve ağ hizmetlerine ilişkin teknik bilgiler toplanmış mı?
- Kurum bilişim sistemlerini etkileyebilecek her türlü düzenlemeye ilişkin dokümanlar toplanmış mı?

A2 Önceki Dönem Denetim Raporları

- Önceki dönem denetim raporlarından bilgi edinilmiş mi? (Bilişim Sistemleri denetim raporları, Mali denetim raporları, Performans denetimi raporları, iç denetim raporları vb.)

A3 Kurum iş süreçlerinin belirlenmesi

- Kurumun gerçekleştirdiği işler dikkate alınarak iş süreçleri belirlenmiş mi?
  - İş akış şemaları çıkartılmış mı?

- İş akış şemaları yapılan işlerin her bir aşamasını gösterecek ayrıntıda düzenlenmiş mi?
- İş akış şemaları yapılan işin kurumun hangi birimi tarafından ve hangi sistem kullanılarak yapıldığını gösterecek şekilde düzenlenmiş mi?

A4 Bilişim ortamında yapılan işlerin belirlenmesi

- Kurumun yaptığı işlerin hangilerinin bilişim ortamında gerçekleştirildiği belirlenmiş mi?
- Bilişim ortamında gerçekleştirilen işler için kullanılan programlar hakkında genel bilgi elde edilmiş mi? (kullanılan donanım, donanımın bulunduğu yer, kullanıcı sayısı, sistem sorumlusu,…)

A5 Mali Tabloları Etkileyen Sistemlerin Belirlenmesi

- Bilişim ortamında gerçekleştirilen işlerden hangilerinin çıktılarının muhasebe sistemine aktarıldığı ve hangi hesap alanlarını etkilediği belirlenmiş mi? (Bilişim Sisteminden Etkilenen Hesap Alanlarının Belirlenmesi Formu doldurulmuş mu?)

A6 Sistem risk değerlendirmesinin yapılması

- Bilişim ortamında gerçekleştirilen işlerden hesap alanlarını etkileyen sistemlerin riskleri değerlendirilmiş mi? (Her bir sistem için Sistem Risk Değerlendirme Formu doldurulmuş mu?)

A7 Risk Derecelendirmesinin Yapılması

- Sistemlerin risk değerlendirmesine göre önceliklendirme sıralaması yapılmış mı? (Risk Derecelendirme Formu doldurulmuş mu?)

A8 Diğer Denetim Ekipleriyle İşbirliği

- Bilişim Sistemleri denetiminin planlanması mali denetim ekibiyle birlikte çalışılarak koordineli şekilde yapılmış mı?

A9 Denetim Stratejisinin oluşturulması

- Yazılı bir Denetim Strateji Belgesi oluşturulmuş mu? (denetimin amacı, kapsamı, denetim yaklaşımını belirlemeye yönelik yapılan çalışmalar, izlenecek denetim süreci ve buna ilişkin çalışma programı)
- Denetim Stratejisi kurum yönetimiyle paylaşılmış mı?

A10 Denetin Programının Hazırlanması

- Denetim stratejisinde belirlenmiş inceleme alanları dikkate alınarak denetim programları düzenlenmiş mi?

B Sistem Kontrollerinin Değerlendirilmesi

B1 Sistem Kontrollerinin Değerlendirilmesi

- Her bir kontrol alanlarına ilişkin belirlenmiş kontroller o alana ilişkin denetim programına uygun şekilde değerlendirilmiş mi?
- Kontrol değerlendirmelerine ilişkin kullanılan yöntemler ve kontrollerin varlığına ve etkinliğine ilişkin bulgular çalışma kağıtlarına not edilmiş mi?

B2 Yapılan İncelemelerin Yönetimi ve Belgelenmesi

- Tamamlanan denetim programına ilişkin formlar ve çalışma kağıtları uygun şekilde numaralandırılarak dosyalanmış mı?
- Yapılan çalışmalar ekip yöneticisi tarafından kontrol edilmiş mi?

B3 Bulguların Gözden Geçirilmesi

- Elde edilen bulguları destekleyecek yeterli ve uygun kanıtlar toplanmış mı?
- Bulgular, olası etkileri, denetçi önerileri ve risk düzeyini de içerecek şekilde değerlendirilmiş mi? (Bulgu Değerlendirme Formları doldurulmuş mu?)
- Elde edilen bulgular kurum personeliyle kapanış toplantıları yapılarak dayanakları açısından hata yapılıp yapılmadığı, yazım üslubu ve önemliliği açısından değerlendirilmiş mi?

C Denetim Sonuçlarının Raporlanması

C1 Taslak Raporun Hazırlanması

- Yapılan inceleme sonuçlarına göre taslak rapor hazırlanmış mı?
- Taslak rapor, Bilişim Sistemleri Denetim Rehberinde belirtilen formata uygun şekilde hazırlanmış mı?
- Denetim bulguları, meydana getireceği etkileri ve bunları karşılamaya yönelik denetçi önerilerini de içerecek şekilde taslak raporda yer almış mı?
- Taslak raporun sonuç bölümü, elde edilen bulgular ışığında kurum bilişim sistemlerinin güvelik ve güvenilirliğine ilişkin denetçi görüşlerini içeriyor mu?

C2 Taslak Raporun Kurumla Görüşülmesi

- Son şekli verilmeden önce hazırlanan taslak rapor kurumla paylaşılmış mı?
- Rapora ilişkin kurum görüşleri alınmış mı?

C3 Nihai Raporun Yazılması

- Kurum tarafından düzeltilmesi kabul edilen ve rapor hazırlandığı ana kadar yapılan düzeltme çalışmalarına da yer verecek şekilde nihai rapor yazılmış mı?

Genel Değerlendirme
Denetim çalışması ile ilgili olarak eksik bulunan veya geliştirilmesi gerekli görülen hususlar
Tespit edilen iyi uygulama örnekleri

Sonuç

Denetimin kalite kontrolüne ilişkin değerlendirme, denetimin planlanması, yürütülmesi ve sonuçlarının raporlanmasına ilişkin süreçlere uygun olarak yapılmalıdır ve sonuçları aşağıdaki şekilde sınıflandırılmalıdır.

- 'A' Denetim, tüm yönleri ile Sayıştay Bilişim Sistemleri Denetim Rehberi ve uluslararası standartlara uygun olarak yürütülmüştür.
- 'B' Denetim, önemli ölçüde Sayıştay Bilişim Sistemleri Denetim Rehberi ve uluslararası standartlara uygun olmakla beraber kalitesinin artırılması gerekli alanlar bulunmaktadır.
- 'C' Denetim, Sayıştay Bilişim Sistemleri Denetim Rehberi ve uluslar arası standartlara uygun olarak yürütülmemiş ve denetim görüşünü etkileyecek derecede eksik yerine getirilmiştir.

Nihai Değerlendirme **A** **B** **C**

Değerlendirmenin gerekçeleri:

Kalite Kontrolünü yapan denetçinin İmzası ……

Tarih……

Not:

Denetimin kalite kontrolünü yapan denetçi, kurumun bilişim sistemlerinin güvenlik ve güvenilirliği ile ilgili olarak verilen denetim görüşünün doğruluğundan, verilen denetim görüşünü destekleyen yeterli ve uygun denetim kanıtı toplandığından ve gerçekleştirilen denetimin uluslararası denetim standartlarına ve Sayıştay uygulamalarına uygun olduğundan emin olmalıdır.

Kalite kontrolü yapan denetçi değerlendirmelerinin dayanaklarını özetlemeli ve imzalamalıdır.

Değerlendirme sonucunda elde edilen iyi uygulama örnekleri ve eksik bulunan alanların geliştirilmesi için yapılan öneriler, ileride yapılacak denetimlerin kalitesini artırmak için detaylı bir şekilde kayıt edilmelidir

EK – 10: BİLİŞİM SİSTEMLERİ DENETİMİ İZLEME TABLOSU FORMU

Denetlenen Kurum veya Sistemin Adı	
Denetim Tarihi	
Denetim Ekip Yöneticisi ve Görevli Denetçiler	

Kontrol Alanı	Bulgu	Risk Düzeyi	Çözüm Taahhüt Edilen Tarih	I. İzleme	II. İzleme

EK - 11: DENETİM PROGRAMI FORMU

Kurum/Sistem Adı:

İncelenen Kontrol Alanı:

Olması Gereken Kontroller	Kontrol Değerlendirme Soruları	Bulgular (E/H)	Ref.	Kontrol Etkinliğini Belgeleme ve İnceleme Yöntemi	Bulgular	Ref.

EK - 12: KONTROL SETİ FORMU

Kurum/Sistem Adı:

İncelenen Kontrol Alanı:

Olması Gereken Kontroller	Kontrol Değerlendirme Soruları	Cevaplar	İstenen Kanıtlayıcı Belgeler

T.C. Sayıştay Başkanlığı

06100 Balgat/ANKARA
www.sayistay.gov.tr