T.C. SAYIŞTAY 1892

Cumhuriyetin
75' inci Yıldönümü Dizisi

Bilişim Teknolojisi Ortamında Denetim

Çeviri

75 TÜRKİYE CUMHURİYETİ'NİN YETMİŞBEŞ YILI

Bilişim Teknolojisi Ortamında Denetim

Çeviri

Cumhuriyetin 75'inci Yıldönümü Dizisi: 5

Özgün Adı: *Audit in an Information Technology Environment*

Cumhuriyetin 75' inci Yıldönümü Dizisi'nden Yayımlanan Kitaplar

*Cumhuriyetin 75' inci Yılında Kamu Harcamaları ve Denetimi Sempozyumu/**Tebliğler, Panel ve Tartışmalar***

*Avrupa Birliği Sayıştayı/**İsmail Hakkı Sayın***

*Bilişim Yönetiminin ve Teknolojisinin Denetimi/**Çeviri***

*Kamu Kurum ve Kuruluşlarına Yasayla Verilen Yetkilere Uygunluğun Denetimi/**Çeviri***

İngiltere Sayıştayının yabancı ülkeler yüksek denetim kurumları mensupları için düzenlemiş olduğu kurslarda dağıtılan kitapçıktan dilimize aktarılmıştır.

Sayıştay mensuplarının kullanımı için bastırılmıştır.

Kapak Tasarımı : *Alper Alpay*

Redaksiyon : *Gül Nogay, Gökhan Yazıcı*
Dizgi ve Mizanpaj : *Nezahat Önder, Havva Yılmaz, Gürkan Alpsoy*
Baskı ve Cilt : *Sayıştay Yayın İşleri Müdürlüğü*

Birinci Basım : *Aralık, 1998*

TC SAYIŞTAY BAŞKANLIĞI
06100 ULUS, ANKARA
Tlf: 310 23 00

SUNUŞ

Bilişim Teknolojisi, özel sektörce olduğu kadar kamu kurum ve kuruluşlarınca da, başta malî işlemler olmak üzere her alanda giderek daha yaygın bir şekilde kullanılmaktadır. 21'inci yüzyıl kamu kurum ve kuruluşlarının, içinde faaliyet gösterdiği Bilişim Teknolojisi ortamının çok daha yoğunlaştığı bir zaman dilimi olacaktır.

Bilişim Teknolojisinin malî işlemlerde kullanılması, pek çok yararının yanı sıra, işlemlerde anonimliğe yol açarak sorumluluğu azaltmak; veri giriş ve işlemede mükerrerliklere, yetkisiz değişim ve erişimlere açık olmak; denetim izini gizlemek gibi malî denetim açısından son derece önemli olan daha birçok zaafı da beraber getirmektedir. Bu itibarla, denetçi, denetimi planlayıp icra ederken Bilişim Teknolojisinin bu özelliklerini bilmek durumundadır. Hesapların denetimi sırasında bu özelliklerin etkilerini dikkate alan yaklaşım, metot ve tekniklerin benimsenmesi gerekmekte; dahası, malî verileri işlemede kullanılan yazılımları denetlemek için özel olarak geliştirilmiş denetim yazılımlarından yararlanılması zorunlu hale gelmektedir.

İngiltere Sayıştay'ı (NAO) tarafından yayımlanan ***Bilişim Teknolojisi Ortamında Denetim*** başlıklı bu malî denetim el kitabı, meselenin kurulu sistemlerin incelenmesi ve sistemlerin geliştirilmesi yönleri hakkında denetçilere rehberlik sağlama amacını taşımaktadır.

"Cumhuriyetin 75'inci Yıldönümü Dizisi" arasında yayımladığımız bu çevirinin, Bilişim Teknolojisi kullanımında ülkemizde son yıllarda kamu kurum ve kuruluşlarınca kaydedilen ivmeye paralel olarak, gerek Sayıştay'ın ve gerekse değişik kademelerdeki iç denetim organlarının denetimlerini Bilişim Teknolojisi ortamlarında etkili olarak yürütmelerinde ve zaten gündemlerine girmiş olan Bilişim Teknolojisi ortamlarının denetimi alanında yardımcı olacağına inanıyorum.

Bu vesileyle, çevirinin meslekî üslûp ve terminoloji yönünden redaksiyonunda emeği geçen Uzman denetçe Gül Nogay ile Programcı Gökhan Yazıcı'ya; kitabın dizgi, mizanpaj ve basımında görev alan mensuplarımıza teşekkür ederim.

Prof. Dr. M. Kâmil MUTLUER
Başkan

İçindekiler

Ekler

Bilişim Teknolojisi Ortamında Denetim

Başlangıç

1 Birçok kamu ve özel sektör kuruluşu, mali işlemlerini yürütmek ve mali tablolarını oluşturmak için bilişim teknolojisinden (BT) geniş ölçüde yararlanır. Bu modül, bilgisayarlı bir ortamda, hesapların denetimi için bir rehber niteliği taşır. Bu bölümde kullanılan bilgisayar terimlerine ve diğer sık rastlanan BT sözcüklerine ait bir sözlük, Ek 1' de verilmiştir.

2 Bilişim Teknolojisinin varlığının temel denetim hedeflerini değiştirmeyeceği başlangıçta vurgulanmalıdır. Ne var ki, BT sistemlerinin, denetçinin risk konusundaki görüşünü etkileyebilecek ya da farklı bir denetim yaklaşımını benimsemesini gerektirebilecek özel karakteristikleri vardır. Örneğin, Bilişim Teknolojisi sistemleri :

- gizliliğe sebep olabilir ve hesap verme sorumluluğunu azaltabilir;
- muhasebe verileri üzerinde yetkisiz ya da kaydedilmeden yapılan değişikliklere izin verebilir;
- girdi ya da işlemlerin tekrarına yol açabilir;
- uzaktan ve yetkisiz erişime hassas olabilir;
- bazı işlemleri gizli ya da görünmez kılabilir;
- denetim izini (audit trail) ortadan kaldırabilir ya da anlaşılmaz kılabilir;
- verileri dağıtılmış sistemler üzerine yayabilir; ya da
- dışarıdan müteahhitlerce kendi standart ve kontrollerini uygulayarak işletilebilir.

Bu nitelikler ve mali denetim üzerine etkileri Ek 2'de daha kapsamlı olarak tanımlanmıştır.

1.3 Bu ölçü öncelikle aşağıdakilerle birlikte göz önünde bulundurulmalıdır :

- verimli ve etkin bir denetim yaklaşımı için gereken BT'nin gözden geçirilmesi. Genel yaklaşım bölüm 2' de açıklanmış, BT'nin gözden geçirilmesine yardımcı olacak bir araç Ek 3'te ve tamamlamaya yardımcı olacak detaylı bir rehber Ek 4 ve 5' te sunulmuştur;
- denetçinin sistemlerin geliştirilmesine olan merak ve ilgisi. Özet rehber bölüm 3'te verilmiştir.

1.4 Bu modül içinde, bilgisayara dayalı sistemlerin her yönünü kapsayan detaylı bir rehber sağlamak mümkün değildir. Bu rehberde yer almayan ancak ilgi uyandıran konularla karşılaşan denetçiler, uzman BT denetçilerine danışmalıdırlar. Ek 6' da, BT denetimi konularıyla ilgili daha ayrıntılı bilgi sağlayan yayınların listeleri bulunmaktadır.

Bilişim Teknolojisi Sistemlerinin Gözden Geçirilmesi

Giriş

2.1 Denetim planlamasının amacı, denetlenen kuruluşu ve hesapları anlamak, hata ya da yanlış beyan riskini değerlendirmek ve denetim kanaatine ulaşmayı mümkün kılacak yeterli ve uygun kanıt toplanmasını ve bu denetimi yürütebilmek için gerekli denetim kaynaklarına karar verilmesini sağlayacak verimli bir denetim yaklaşımı geliştirmektir. Biz çalışmamızı, denetimi düşük maliyetle gerçekleştirecek şekilde planlarız.

2.2 Denetlenen kuruluşun mali sistemleri bilgisayara geçtiğinde, bu sistemlerin denetim planına yapacağı etkiyi göz önünde bulundurmalıyız. Özellikle, biz :

- mali tablolar ile bunları destekleyen ve bilgisayar ortamında yürütülen sistemler arasındaki ilişki hakkında bilgi sahibi olmalıyız;
- denetimde BT denetimi uzmanlarının yer almasının gerekliliğini değerlendirmeliyiz;
- hem kuruluş düzeyindeki hem de her hesap alanına ilişkin risk değerlendirmesinde BT'nin etkisini göz önünde bulundurmalıyız;
- denetimi desteklemek için bilgisayara dayalı denetim tekniklerinin kapsamını, işlem verilerinin girilmesinin ve analiz edilmesinin en uygun yollarının tanımını da kapsayacak şekilde değerlendirmeliyiz;
- denetim yaklaşımının, bilgisayar kontrolleri için bir güven sağlayıp sağlamadığını ya da sağlamasının gerekip gerekmediğini göz önünde bulundurmalıyız;
- denetime katılımı gerektirecek finansal sistemler geliştirilmesini sağlamalıyız;

Bu faaliyetler ve düşünceler, denetçilerin finansal denetim planlamalarının önemli bir parçası olarak tamamlamaları gereken bir BT incelemesinde bir araya getirilmiştir (Ek 3). Sistemler karmaşık olduğunda, bu incelemeyi tamamlamak ya da tamamı veya bir kısmı üzerinde öneride bulunmak üzere, bir BT denetim uzmanından yararlanılması uygun olacaktır.

2.3 Elimizde önceki yılın denetimine ait tamamlanmış bir BT incelemesi bulunduğunda, bunu, yeni sistemler ve mevcut sistemlerdeki önemli değişiklikler üzerinde yoğunlaşarak, güncelleştirmeliyiz. Bu tip güncelleştirmeler üzerinden birkaç yıl geçtikten sonra (genelde 3-4), yeni baştan tam bir gözden geçirme yapmalıyız.

2.4 BT'nin gözden geçirilmesi, aşağıda gösterildiği gibi, üç bölümden oluşur.

Bölüm A - Denetlenen kuruluşların Bilişim Teknolojisi sistemlerine ilişkin ön bilgi

Bölüm A denetçiden, müşterinin BT donanım ve yazılımına ilişkin ön bilgi toplamasını talep eder. Bilgisayar sistemlerinin boyutu, tipi ve teknik karmaşıklığı hakkındaki bilgi, denetçinin, bir BT

denetimi uzmanının desteğine gereksinim olup olmadığını değerlendirmesini sağlar. Bölüm A, gelecekte denetimin müdahil olmasını gerektirecek mali sistemler geliştirilmesini mümkün kılar. Bölüm A' nın, denetçinin, BT kontrol ortamının ya da uygulama kontrolü prosedürlerinin gözden geçirilmesini bitirmesinden önce tamamlanması gerekir.

Bölüm B – Bilişim Teknolojisi kontrol ortamının gözden geçirilmesi ve kurumsal riskin değerlendirmesi

Bölüm B, BT kontrol ortamında işleyen kontrol ve prosedürlerin değerlendirilmesi için kullanılır. BT kontrol ortamında belirlenen zayıflıklar, her bir mali uygulamadaki kontrol prosedürlerinin etkinliğini düşürebilir.

Bölüm C - Uygulama kontrollerinin gözden geçirilmesi ve hesap alanı risk değerlendirmesi

Denetçi, Bölüm C' yi her önemli finansal uygulamadaki kontrol prosedürlerini, iç kontrol sistemlerini ve denetim risklerini incelemek için kullanmalıdır.

2.5 Yukarıda gösterilen metod açık olmakla birlikte, BT' nin gözden geçirilmesi sırasında akılda tutmamız gereken bazı özel durumlar vardır:

- BT sistemlerinin ilk incelemesi, bir uygulama tarafından gerçekleştirilen işlemlerin, BT sistem aracılığıyla, her biri değişik denetim risklerine konu olabilecek, farklı yolları izleyebilecekleri gerçeğine bağlı olarak hesap alanlarının tekrar bölünmelerine yol açabilir;

- hem mali tabloların üretilmeleri hem de görev hedeflerine katkıda bulunulması ile ilgili olarak, bilgisayar sistemlerinin önemi;

- "bilgisayar aracılığıyla"denetimin uygulanabilirliği ve arzulanırlığı. Bu, uygulama kontrolü yöntemlerinin tanımlanmasını ve bunların yeterliliğinin bir ilk değerlendirmesinin yapılmasını gerektirir. Önemsiz bir sistemin, yüksek değerli ve önemli bir sistemle aynı denetim ilgisini çekmesi pek olası değildir; ve
- bilgisayar kontrollerinin tüm kontrol ortamı ile ilişkileri. Bu, BT sistemindeki kontrol zayıflıklarını hafifleten manuel kontrollerin mevcudiyetine önem verildiğini güvence altına almalıdır. Bundan sonra denetçi, kontrollere güvenen denetim yaklaşımını uyarlamanın olabilirliğini değerlendirmeye muktedir olacaktır.

2.6 BT' nin gözden geçirilmesi, orta ölçekli, ortalama karmaşıklıktaki bilgisayar sistemlerini incelerken denetçiye yardımcı olmak üzere geliştirilmiştir. Bir kuruluş, küçük, basit ya da önemli olmayan bir sistemi çalıştırırken, BT' nin gözden geçirilmesindeki bazı bölümler uygulanamaz. Bunun aksine, bir kuruluş, büyük, karmaşık ve iş önemine sahip bir sistemi çalıştırırken, denetçi BT' nin gözden geçirilmesi için belirtilenden daha derin bir inceleme yapma ihtiyacı duyabilir.

Denetlenen kuruluşların Bilişim Teknolojisi sistemlerine ilişkin ön bilgi

2.7 BT' nin gözden geçirilmesinin A kısmı, müşterilerin BT sistemleri konusunda ön bilgiler toplanmasını ve tanımlanmasını amaçlar. Bölüm A, BT kontrollerinin detaylı değerlendirilmesi tamamlanmadan bitirilmeli ve bitirildikten sonra BT kontrol ortamını ve uygulama kontrolü yöntemlerini gözden geçirecek herkes için kopya edilmelidir.

2.8 Bölüm A' nın bitirilmesi, sonradan BT incelemesinin B ve C bölümlerini tamamlamakla görevlendirilen herkesin, nelerle karşılaşabileceği konusunda bir ön bilgi edinmesini sağlamalıdır. Aynı zamanda, Bölüm A denetçiye, denetlenen kuruluşa gidilmeden önce hangi teknik kaynaklara başvurması gerektiği konusunda bilgi vermelidir (örneğin, sistemlerin çalıştırılması ve muhasebe paketleri konusundaki kaynaklar).

2.9 Bölüm A tamamlanınca, denetçi, BT denetimi uzmanlarından yararlanılıp yararlanılmayacağına karar verecektir. Bu kararı etkileyecek faktörler şunları içerir:

- denetçinin kendi BT becerileri ve deneyimi - denetçiler gereken becerilere ve deneyime sahip olmadıklarını hissediyorlarsa, BT incelemesini yürütmemelidirler;

- denetlenen kuruluşun BT işlemlerinin ölçeği - geniş bilgisayar işlemleri, hem sistemlerin kendisi hem de örgütsel yapılar cinsinden daha karmaşık olma eğilimindedir;

- BT donanım ve ağının teknik açıdan karmaşıklığı - yeni teknolojileri içeren daha karmaşık sistemler, denetim risklerinin tanımlanması ve değerlendirilmesi için, büyük bir olasılıkla BT uzmanlarının yardımını gerektirecektir;

- denetlenen kuruluşların ısmarlama uygulamalar geliştirip kullandıkları ya da standart rafa kaldırılmamış muhasebe paketlerini düzeltebildikleri durumlarda ve - genelde, kuruluşlar doğrudan muhasebe uygulamaları geliştirdiklerinde ya da düzenlediklerinde daha yüksek bir denetim riski söz konusudur;

- BT ile ilgili problemlerin geçmişi - denetçilerin, geçmişte bir müşterinin BT sistemleriyle ilgili problemler yaşadıkları durumlar (örneğin kullanıcı hatalarını, programlama yanlışlıklarını, bilgisayar sahtekârlıklarını, sisteme sızmaları ya da ciddi güvenlik gediklerini içeren bir geçmiş olduğunda);

- yürüttükleri işlemler ya da bilgisayar sistemleri Meclis, kamu ya da diğer ilgili grupların duyarlı olduğu işlem ve sistemler olduğu zaman; ve

- sistemler geliştirilmesi - denetçinin, mali sistemler için uygulama planları ve şartnameler konusunda yorum yapması istenebilir.

2.10 Bölüm A, aynı zamanda, müşterinin finans ve BT bölümlerindeki personel sözleşmeleri gibi idari detaylar için de bir alt bölümü içermektedir.

Bilişim Teknolojisi kontrol ortamının gözden geçirilmesi

2.11 BT incelemesinin B kısmı, genel BT kontrol ortamındaki kontrol güçünü, zayıflıklarını ya da risklerini tanımlamayı amaçlar. Genel BT kontrol ortamında belirlenen riskler temel uygulamalardaki kontrollerin etkinliğini zayıflatabilir ve bu nedenle kurumsal düzeydeki riskler olarak tarif edilebilirler. BT' nin incelemesi, denetçi tarafından, müşterinin bilgisayara dayalı finansal bilişim sistemleri kullanımına bağlı olan genel BT denetimi risklerinin kapsam ve niteliğini tanımlamak için kullanılmalıdır.

2.12 İnceleme denetlenen kuruluşun BT politikaları ile ilgili birkaç stratejik sorunun sorulmasıyla başlar. Bu inceleme, denetçinin, denetlenen kuruluşun BT stratejisinin, yönetiminin, iç denetiminin ve güvenlik politikalarının yeterliliğini incelemesini sağlar. Bu soruların erken bir aşamada sorulması, denetçiye, BT kontrol ortamının makul derecede güvenilir bir ön görünümünü verecektir. Deneyimler, BT politikaları az olan ya da uygun olmayan kuruluşların, sağlıklı bir iç kontrol ortamına sahip olmalarının olası olmadığını göstermiştir.

2.13 İnceleme işlemi, aynı zamanda, bilgisayar bölümündeki, sistem yazılımındaki ve BT donanımındaki genel kontrollerin bir değerlendirmesini de içerir. İncelenen alanlar:

- görevlerin ayırımını;
- fiziksel erişim kontrollerini;
- mantıksal erişim kontrollerini;
- çalıştırma kontrollerini;
- değişim yönetimi yöntemlerini;
- hasarı telafiye yönelik planlamayı;
- dış BT servis tedarikçilerinin kullanımı; ve
- kullanıcıların kendi kendilerine geliştirip yürüttükleri uygulamaların kontrollerini kapsar.

2.14 Genel BT kontrol ortamında belirlenen zayıflıklar, o yüklemede çalışan uygulamalardaki tüm kontrollerin etkinliğini azaltabilir. Örnek olarak, denetçi, eğer temeldeki veri tabanı yetki dışı değişiklikten korunmadıysa, bir uygulamanın işlem girdi kontrollerine az güven duyabilir.

2.15 Denetlenen kuruluş, birden fazla bilgisayar yüklemesi ile büyük ölçekli, çeşitli BT işlemlerine sahip olduğunda, BT incelemesinin bazı bölümlerinin tekrarlanması gerekebilir.

2.16 İnceleme işlemi bitirildiğinde, denetçinin, kuruluşun genel BT kontrol ortamı dahilindeki risklerin bir değerlendirmesini yapması mümkün olacaktır. Zayıf bir BT kontrol ortamına sahip olan bir kuruluş, normalde yüksek denetim riski taşıyan genel bir BT değerlendirmesine tabi tutulacak olsa da, bu her zaman gerçekleşen bir durum değildir. Eğer genel BT kontrol ortamı zayıf olarak değerlendirildiyse, telafi edici kontrollere ya da çok güçlü uygulama kontrollerine hâlâ biraz güven duyulması mümkün olabilir. Güçlü kontrollere sahip BT kontrol ortamına rağmen, mali bir uygulamanın çok zayıf kontrollere sahip olabilmesi de mümkündür.

2.17 Ek 4 BT kontrol ortamının incelenmesine ilişkin daha fazla bilgi içermektedir.

Uygulama incelemeleri ve hesap alanı risk değerlendirmesi

2.18 BT incelemesinin C kısmı her mali uygulamadaki kontrol yöntemlerinin değerlendirmesi için bir çerçeve oluşturur. Bu çerçeve, denetçinin aşağıdakileri gerçekleştirmesini sağlar :

- her uygulamaya bağlı denetim riskinin düzeyinin değerlendirilmesi;
- uygulamanın kontrol yöntemlerinin kavranması;
- kontrollere dayalı bir denetim yaklaşımının olası ya da arzulanır olup olmadığına karar verilmesi;
- uygunluk ve maddi test programlarının tasarımını etkileyebilecek özel risklerin tanımlanması.

2.19 Uygulama kontrol yöntemleri ayrı olarak incelenmemelidir. Denetçi BT' ne dayalı kontrolleri tamamlayan ya da destekleyen genel BT kontrol ortamı ve tüm manuel kontrol yöntemleri bağlamında, her uygulama kontrolünün etkinliğini değerlendirmelidir.

2.20 BT incelemesinin C kısmı, aşağıdaki kontrol şartlarının incelenmesi için bir çerçeve oluşturur :

- denetlenebilirlik;
- bilgisayar destekli denetim teknikleri;
- belgeleme;
- uygulama güvenliği;
- girdi kontrolleri;
- veri aktarımı kontrolleri;
- işletim kontrolleri;

- çıktı kontrolleri; ve
- ana/kalıcı veri kontrolleri.

2.21 Ek 5, uygulama kontrolü yöntemlerinin değerlendirilmesi konusunda daha fazla yönlendirici bilgi içermektedir.

Bulguların özeti

2.22 BT incelemesi tamamlandıktan sonra, denetçi bulgularını özetlemelidir. Özet aşağıdakileri kapsamalıdır :

- mali sistemlerin karmaşıklığının bir değerlendirmesi;
- BT ortamında kurumsal risklerin genel bir değerlendirmesi;
- her uygulama ve hesap alanındaki risklerin bir değerlendirmesi; ve
- denetçinin, her bir hesap alanı için, kontrollere dayalı denetim yaklaşımının fizibilitesi konusundaki görüşü.

2.23 Denetçi, kontrol zaaflarının kapsamını ve niteliğini kısa bir raporda özetlemelidir. Denetçi, belirlenen kontrol zaaflarını bunların mali tablolar üzerindeki olası etkileriyle ilişkilendirmelidir. Bu zayıflıklara denetlenen kuruluşun dikkati idari bir mektupla çekilebilir. Denetçi, ciddi zaafları, denetlenen kuruluş ile birlikte ilk fırsatta görüşmelidir.

Sistemlerin geliştirilmesi

Giriş

3.1 Denetlenen kuruluşların mali sistemlerinin geliştirilmesinin, cari mali tabloların denetimi üzerinde bir etkisi olması pek olası değildir. Ne var ki, kötü tasarlanmış ya da uygulanmış bir mali sistem, gelecek yılların hesaplarının denetiminin pahalı ya da imkansız hale gelmesi sonucunu doğurabilir. Bu bölüm, dış denetçinin dışarıdan sağlanan ya da firma içinde geliştirilen mali sistemlere ilgisini kapsar.

3.2 Önerilen gelişme yaklaşımının, iş gereksinimlerini karşılayan bir sistem şeklinde sonuçlanıp sonuçlanmayacağına karar verilmesi, denetlenen kuruluşun ve özellikle iç denetimin işidir. Yaklaşımın kendisinin ya da özel yönlerinin onaylanması bizim görevimiz değildir. Ne var ki, biz, yaklaşımın, mali tablolar hakkında bir fikir oluşturulması konusunda güçlüğe sebep olabilecek yönleri üzerinde yorumda bulunmalıyız. Bu bölümün geri kalan kısmı, sistem tasarımına ya da tedarik sürecine dış denetimin dahil oluşunun zamanlaması kadar dış denetim zorluklarının engellenmesi konusunda da yardımcı olması gereken sistem tasarımı özelliklerini geniş şekilde tarif etmektedir.

3.3 Mali sistemlerin geliştirilmesinin denetimi, dikkat gerektiren birçok konusuyla, teknik olarak kompleks bir alandır. Bu bölümün aşağıdaki kısmı, denetlenen kuruluşun yeni bir mali sisteminin gelişiminden doğan bazı denetim konularının kısa bir özetini kapsamaktadır. Ek 6, gelişen sistemler ile ilgili yayınlar ve daha ileri düzeyde yardım içermektedir.

Dış denetim gereksinimleri

Mali denetim izi (Audit Trail)

3.4 Bir mali denetim izi (kayıt sistemlerinin kullandığı bir güvenlik denetim iziyle karıştırılmamalıdır) temel bir gereksinimdir. Bir denetim izi olmaksızın, bir mali tablolar kümesi üzerinde olumlu bir fikir oluşturulması mümkün olmayabilir. Bu sebeple, operasyon mali sistemleri :

- denetçinin, başlangıçtaki girdi ve sistemden doğan işlemler ile iç tahsis işlemleri ve mali tablo arasında her iki yönde ve birbirini izleyen düzeyler sürecinde, işlemleri izlemesine izin vermelidir.

- denetimin tamamlanması için yeterli bir zaman içinde, tüm ilgili verileri ve mali denetim izi bilgisini sağlamalıdır.

3.5 Kaynak belgeler de mali denetim izinin bir parçasını oluşturmalı ve, aynı zamanda, denetim tamamlanana kadar tutulmalıdır.

Verilerin soruşturulması ve düzeltilmesi

3.6 Bilgisayar destekli denetim teknikleri kullanmayı tasarlarsak, ihtiyaçların belirlenmesine, sistemden esnek bir şekilde veri elde etme gereksinimini de dahil etmek gerekli olacaktır. Bu esnek bir şekilde veri elde etme, belirlenen veri maddelerinin alınıp, bunların sonradan bilgisayar destekli denetim teknikleri işlemi için bir mikro bilgisayara transfer edilebilecek, manyetik bir dosyaya kaydedilmelerini mümkün kılmalıdır. (düz, sabit kayıt uzunluğunda bir ASCII dosyası tercih edilen biçimdir.)

3.7 Bilgisayar destekli denetim tekniklerinin kullanılabilmesi için ön şart, ilgili tüm verilerin işleme tabi tutulduğunun kanıtlanmasıdır. Denetçi tamlığı, kuruluşun mali tablosunu bilgisayar destekli denetim teknikleri kullanılarak üretilen kontrol toplamları ile mutabık kılmak suretiyle kanıtlar. Ne var ki, defter - i kebir bilgileri özet şeklinde saklandığında ve bu sebeple maddi test amaçları için uygun olmadığında, sistemdeki başka bir yerden, örneğin bir geçmiş işlemler dosyasından, detaylı işlem bilgilerinin seçilmesi gerekli olacaktır. Bu yaklaşımın mümkün olması halinde, denetçi, denetlenen kuruluşun ham işlem verilerinden mali tabloların türetilmesi için gerekli olan tüm paylara ayırma, tahsisat ve hesap özeti kurallarını tam olarak belgelediğinden emin olmalıdır.

3.8 Teknik belgeleme, gerekli verileri barındıran dosya ya da veri tabanlarının tanımlanmasında, hangi veri maddelerinin gerektiğinin belirlenmesinde ve bunların her birinin saklandığı belge hakkında bilgi edinilmesinde (örneğin çift, karakter, ondalık v b) kullanılmak üzere

de gerekli olabilir ve böylece genelleştirilen denetim sorgusu yazılımı ile birlikte kullanılmak üzere, doğru şekle dönüştürülebilir.

3.9 Verilerin indirilmesi (down loading), normalde büyük ölçekli seçme ve sorgu gereksinimleri için kullanılır. Bu yöntem, yalnız araştırmalar için, eğer sisteme on-line erişim ("salt okunabilir" kipinde) mümkünse ve bir bilgisayar terminali kullanılabiliyorsa, denetlenen kuruluşun mahallinde denetim yapılırken zaman kazandırabilir. Bu, belirli işlemlerin belirlenmesi ve detaylı şekilde incelenmesi için elverişli bir yol sağlamalıdır. (örneğin, genelde modern mali sistemde sunulan "sondaj" özelliklerinin kullanılması). Büyük bir kuruluşun mali sistemine, denetçinin kendi bürosuna yerleştirilen bir terminalden doğrudan erişim ("salt okunabilir" kipinde) için onay alınması yoluyla, denetimde bazı tasarruflar yapılması mümkün olabilir.

İç Kontrollar

3.10 Herhangi bir mali sistemde, yeterli iç kontrollerin bulunması, çok arzulanır bir özelliktir. Bizim bakış açımıza göre, bunların doğru şekilde işletilmesi, hataların ya da sistemin kasıtlı olarak yanlış kullanılmasının hesaplarda önemli bir yanlış belirleme ile sonuçlanabilmesini ve aynı zamanda, uzun süreli sistem arızaları ya da hasarların tam ve güvenli muhasebe kayıtlarının tutulmasını engellemesi riskini azaltır.

3.11 Sistemin geliştirilmesi esnasında önemli bir faaliyet, yeni sistemin gereksinimlerine dahil edilmesi gereken iç kontrollerin tanımlanmasıdır. Kuruluşun iç denetim ekibi bu görevle yakından ilgili olmalıdır. Bizim görevimiz, kuruluşun, mali verilerin girişinde, saklanmasında, işlenmesinde ve çıktısında ve sistemin yedeklenmesi ile düzeltilmesinde, temel iç kontrol hedeflerinin karşılanmasının öneminin farkında olduğunu doğrulamaktır. Kuruluşun bir iç denetim ekibi ya da bir güvenlik bölümü olmadığında, iç denetim hedeflerinin daha açık bir biçimde tanımlanmasına, gereksinim duyabiliriz. Bağımsızlığımızı koruyabilmek için, denetim hedeflerine nasıl ulaşılacağını belirtmektense, kendimizi neyin gerekli olduğunu belirlemekle sınırlamalıyız.

Müdahil olmanın zamanlaması

Planlama

3.12 Kullanıcı ihtiyaçlarını teknik olarak daha sonradan kolay olduğu düşünülerek eklemek yerine yeni bir sistemde tasarlamak değişmez bir şekilde daha ucuzdur. Bu sebepten dolayı, yönetime yeteri kadar çabuk bir şekilde tavsiyede bulunmak ve dolayısıyla tavsiyelerin Kullanıcı İhtiyaçları Şartnamesi'nde yer almasını sağlamak için denetlenen kurumun geleceğe ilişkin olarak yeni mali sistemler geliştirmek veya edinmek için oluşturacağı planlarından haberdar olunması önemlidir. Geleceğe ilişkin gelişmelere yönelik ipuçlarından bazen yıllık İş Planı'nda bahsedilir ve bunlar denetlenen kuruluşun Bilişim (Bilgi) Sistemleri Stratejisi'nde yer alan proje portfolyosunda yer almalıdır. Sonuç sağlayabilecek diğer yollar da varolan mali sistemlerin genel bir değerlendirilmesi (zayıf fonksiyonellik sunan ve yüksek bakım masrafları yaratan eski sistemler muhtemelen değiştirilecektir), ve BT Departmanı'nın ve Mali Departmanların yöneticileriyle tartışılmalıdır.

Kullanıcı Gereksinimleri Şartnamesi

3.13 Sistem gelişimi yaşam döngüsündeki belirleme aşaması, sistem kullanıcılarının özel gereksinimlerinin tanımlanması için yapılan bir araştırmadır. Eğer sistemin firma içinde geliştirilmesi gerekiyor ise, Kullanıcı Gereksinimleri Şartnamesi, sistem tasarım ve gelişimini yürütecek teknik şartnamenin temelini oluşturacaktır. Eğer sistemin tedarik edilmesi gerekiyorsa, Kullanıcı Gereksinimleri Şartnamesi, diğer iş bilgileri ile birlikte, değerlendirme için ilgili sistem satıcılarına gönderilecek bir İşletme Şartnamesi'nde birleştirilecektir. Proje Yöneticisinin gereksinimlerimizin farkında olduğundan emin olmalıyız ve bunların Kullanıcı Gereksinimleri Şartnamesi'nde yeteri kadar belirtilip belirtilmedikleri konusunda yorumda bulunmaya hazırlıklı olmalıyız.

Uygulama

3.14 Sistemin gelişme sürecini tamamlanmasına yakın, mevcut sistem ile yeni sistemler arasında veri transferi için yapılan planı gözden geçirmemiz gerekecektir. Bu plan, tüm verilerin doğru ve kesin olarak transfer edildiğinin ve özellikle hesapların iki grafiği farklılık gösterdiğinde, verilerin yeni sistemdeki doğru hesaba gönderildiğinin güvence altına alınmasını amaçlamalıdır. Bu, aynı zamanda, yeterli bir mali denetim izinin sağlandığını ve gerektiğinde, denetim izinin eski ve yeni sistemler arasında bir köprü kurduğunu doğrulamak için de gerekecektir.

Ek 1
Yaygın Olarak Kullanılan Bilişim Teknolojisi Terimleri Sözlükçesi

Assemblers / Compilers (Toplayıcılar / Derleyiciler)
Proglamlama dillerinde yazılan kaynak kodlarını bilgisayarın işlemcisinin anlayabileceği basit makina koduna çevirmek için tasarlanmış programlar.

ASCII (American Standard Code for Information Interchange- Bilgi Alışverişi İçin Amerikan Standart Kodu)
Bilgisayar sistemlerinde karakterleri (harfleri) sembolize etmek ve saklamak için genel bir standart (Örneğin işlem veriler).

Backup (Yedekleme)
Kuruluşların işlem hatalarından kurtulmasını sağlayan acil durum yöntemleri.

BACS (Bankacıların Otomatik Borç Temizleme Servisi)
Otomatik ödemeleri ve doğrudan borçları ya kaset ve disket ya da direkt iletişim bağlantısı ile kapatan Bankacıların Otomatik Borç Temizleme Servisi.

Bespoke (Ismarlama)
Kullanıcının şahsi ihtiyaçlarını karşılamak için tasarlanmış, kullanıcıya özel bir sistem.

Bridge (Köprü)
İki uyumlu ağı tek bir mantık ağında, fiziksel olarak bağlayan, bir iletişim aracı.

Business Continuity Planning (İş Sürekliliğinin Planlanması)
İşle ilgili kritik işlemlerin, büyük eksiklikler, ana sistem çökmelerinde ya da rutin işlemlerin kullanılamaması durumları sonrasında, devamını sağlamak için ileriye dönük planlama.

CAATS (Computer Assisted Audit Techniques-Bilgisayar Destekli Denetim Teknikleri)
Detaylı denetim için veri dosyalarının açılması, araştırılması ve analiz edilmesi ile işlem örneklerinin üretilmesi için kullanılan bilgi çekme yazılımı.

CASE (Computer Assisted Software Engineering-Bilgisayar Destekli Yazılım Mühendisliği)
Programcının düşük seviyeli tasarım ve programlama görevlerinden kurtarılarak yazılım sistemlerinin daha verimli tasarımı ve inşası için kullanılan bilgisayar araçları.

CCTA
BT sistemlerinin verimli bir şekilde işletilmesi için tavsiye, rehberlik ve destek sağlayan Devlet Bilişim Sistemleri Merkezi

Değişim Yönetimi
Bilişim sisteminin herhangi bir yönünü (donanım, yazılım, belgeleme, iletişim, sistem ayar dosyaları) değiştirmeye yönelik taleplerin kontrol ve yönetim süreci. Değişim yönetimi süreci, onaylanan değişiklikleri kontrol etme, yönetme ve uygulama ölçümlerini içine almalıdır.

CHAPS (Clearing Houses Automated Payment System-Borç Temizleme Odaları Otomatik Ödeme Sistemi)
Yüksek meblağlarla ve uluslararası nakit transferleri ile ilgilenen bir bankacılık sistemi.

CISA (Certified Information Systems Auditor-Onaylı Bilişim Sistemleri Denetçisi)
ISACA (Information Systems Audit and Control Association - Bilişim Sistemleri Denetimi ve Kontrolü Birliği) tarafından verilen bir mesleki yeterlik.

Client Server (Müşteri Sunucu)
Hem ağ dosyası sunucusunun hem de iş istasyonlarının (workstation) işlemleri sürdürdüğü bir ağ tipi.

Comms Switching (İletişim Anahtarlaması)
İhtiyaç duyulduğunda araçlar arasında, dinamik olarak iletişim kanalları kurma yeteneği.

Computer Applications (Bilgisayar Uygulamaları)
Belirli bir işlev için tasarlanmış ayrı sistemler. Örneğin, bordro, muhasebe, stok kontrolü.

Computer Controls (Bilgisayar Kontrolları)
Faaliyet ve yöntemlerin hedeflerine ulaşmasını sağlamak için uygulanan işlem, yöntem ve faaliyetler. Bilgisayar kontrolleri, önleyici, tespit edici, düzeltici ya da onarıcı olabilirler. Hataları ve yetkisiz faaliyet riskini en aza indirmeyi amaçlarlar.

Configuration Item (Ayarlama Aracı)
Diğer ünitelerden bağımsız olarak değiştirilebilen herhangi bir donanım, yazılım ya da altyapı parçası (genelde en küçük ünite). Ayarlama araçları karmaşıklık, boyut ya da tip olarak bütün bir sistemden tek bir modüle ya da donanım parçasına kadar geniş bir yelpazede olabilir.

Configuration management (Ayarlama Yönetimi)
Bir sistemdeki ayarlama araçlarının teşhisi ve tarifi, ayarlama araçlarının durumunun ve değişiklik isteklerinin rapor ve kayıt edilmesi ve ayar araçlarının doğruluğunun ve tamlığının kontrol edilmesi süreci.

CRAMM
CCTA Risk Analizi ve Yönetimi Metodu, BT sistemlerinde uygun bir güvenlik düzeyi sağlamayı amaçlayan koruyucu önlemleri tanımlamak ve düzenlemek için yapılandırılmış bir yöntem.

Database (Veri tabanı)
Birbirine bağlanabilen, birleştirilebilen, birbirleri ile ilişkilendirilebilen, paylaşılabilen ve hazır halde tutulabilen bilgisayara aktarılmış veri dosyaları seti.

Database Administrator (Veri tabanı Yöneticisi)
Veri tabanı sisteminden, özellikle de veriye ulaşılması, verinin değiştirilmesi ve saklanmasının kurallarını tanımlama açısından sorumlu olan kişi.

Data dictionary (Veri sözlüğü)
Veri tabanının yapısal açık bir tarifi. Bir veri sözlüğü, bütün veri tiplerinin isimlerini ve yapılarını içerir ve belirli veri tipleri için geçerli bir dağılımda bilgi saklayabilir.

Data preparation (Verilerin hazırlanması)
Ham veriyi bilgisayarın kabul edeceği girdi formuna dönüştürmektir.

DBMS (Database Management System - Veritabanı Yönetim Sistemi)
Verilerin yaratılmasına, güncelleştirilmesine, açılmasına ve silinmesine olanak tanıyan ve verilere erişimi yöneten yazılım.

Downloading (İndirme)
Bir uygulama sistemi dosyasından ya da veri tabanından, ikincil bir bilgisayara, daha ileri düzeyli bir analiz için veri aktarımı. Örnek olarak, bir denetçi, bir müşterinin bilgisayarından bir diz üstü bilgisayara, iki bilgisayarı birbirine bağlayarak ve dosya transferi olanağını kullanarak, veri "indirebilir".

EBCDIC (Extended Binary Coded Decimal Interchange Code - Genişletilmiş İkili Sistem Ondalık Alışveriş Kodu)
Bilgisayar sistemlerine veri kaydı için uluslararası bir standart. EBCDIC esas olarak büyük bilgisayarlarda kullanılır.

EDI (Electronic Data Interchange - Elektronik Veri Alışverişi)
İşlemlerin ya da bilginin bir sistemden bir başkasına sistemli bir biçimde aktarımı için kullanılan genel terim.

EFT (Electronic Funds Transfer - Elektronik Fon Transferi)
Elektronik fon transferi, fonları bir banka hesabından bir başkasına, kağıt kayıt araçları yerine elektronik araçlarla taşımak için kullanılır. Yaygın olarak kullanılan EFT sistemleri BACS (Bankacıların Otomatik Borç Temizleme Servisi) ve CHAPS (Borç Temizleme Odaları Otomatik Ödeme Sistemi)' tir.

Ethernet
Ya bir koaks kablo ya da kutupları çevrilmiş elektrik tertibatı üzerinden, CSMA/CD adında bir kayıt ortamı kontrol yöntemini kullanan, yaygın bir LAN teknolojisi. CSMA/CD bilgisayarların, ağ boş olduğu zaman, aktarım yapmasına izin verir.

Facilities Management (Olanakların Yönetimi)
Bir kuruluşun bilgisayar ya da iletişim ağının yönetiminin ya da bu konudaki desteğin, dışarıdan bir servis tedarikçisi tarafından, üzerinde anlaşılan hizmet düzeylerinde verilmesi.

Fourth Generation Language 4GL (Dördüncü Nesil Dil - 4 N D)
İngilizce terminolojisi kullanan ve yazılımların hızlı bir şekilde geliştirilmesine izin veren bir programlama dili. 4 N D ile kullanıcı neye ihtiyaç duyduğunu belirler ve programlama dili ihtiyaç duyulan görevlerin yerine getirilmesi için yapılması gerekenleri yapar. SQL (Structured Query Language - Yapılandırılmış Sorgulama Dili) yaygın olarak kullanılan bir 4 N D' dir.

Gateway (Geçit)
Birbirleriyle uyumsuz mimariye sahip ağları birbirine bağlamak için kullanılan yazılım ve donanım kombinasyonu.

GUI (Graphical User Interface - Görsel Kullanıcı Arabirimi)
Tamamı bir fare (mouse) ya da ok (pointer) ile kontrol edilen pencereleri, grafikleri ve menüleri birleştiren yazılım.

Help Desk (Danışma Masası)
Bilişim sistemi hizmetleri ile kullanıcılar arasındaki günlük temas noktası ya da ara birim. Danışma masaları, kullanıcıların sorunlarının kütüğe alındığı ve çözüldüğü noktalardır.

Host (Ev sahibi)
Ağa bağlı olan ve bir ya da daha fazla kullanıcıya hizmet sağlayan bilgisayar.

Hot/Cold Sites (Aktif/Pasif Siteler)
BT faaliyetinin düzeltilmesi için kullanılabilecek, alternatif bilgisayar işlem siteleri. Pasif sitelerin hazırlanmaları gerektiği halde, aktif siteler hazır olarak kullanılabilirler.

Hub
Birçok makinayı (terminaller, yazıcılar, v. b.) bir ağa bağlayan araç.

IDEA (Interactive Data Extraction and Analysis-Etkileşimli Veri Açma ve Analizi)
CAAT' in tescilli bir markası.

Incident (Tesadüfi Olay)
Sistemin standart işleyişinin bir parçası olmayan bir işlem. Bkz. Problem.

Internet
Bir haber servisini, dosyalara erişimi, elektronik postayı ve internet kaynaklarını taramayı ve görmeyi sağlayan dünya çapında bir bilgisayar ağı sistemi.

ISDN (Integrated Services Digital Network - Birleşik Servisler İçin Sayısal Ağ)
Uç uca sayısal bağlantı sağlayan haberleşme ağı.

LAN, MAN, WAN
Yerel, kentsel ya da geniş alan bilgisayar ağları. Yerel bilgisayar ağları sınırlı coğrafi bölgelerde, tipik olarak bir ofis binasında çalışır. Kentsel bilgisayar ağları şehir ölçeğinde çalışır. Geniş alan bilgisayar ağları ulusal ya da küresel çapta çalışır.

Log (Kütük)
Seri olaylar ya da aktivitelerin kaydı.

Logical access (Mantıksal Erişim)
Bilgisayar verilerine ya da dosyalarına izinsiz erişimi engellemek için bir yazılım kontrol formu.

Mainframe (Ana Bilgisayar)
Merkezi veri işleme avantajı sağlayan büyük ve güçlü bilgisayarlar. Çok çeşitli yan araçları kullanma, çok kullanıcıyı destekleme ve aynı anda birçok hizmeti verme yeteneğine sahiptir.

Mikrobilgisayar
Genellikle tek bir kişi tarafından kullanılan küçük, bütünleşik bilgisayarlar.

Mini Bilgisayarlar
Fiziksel olarak ana bilgisayarlardan daha küçük olan mini bilgisayarlar çok kullanıcılı ortam ve makul bir ölçüde özellik sunar.

MODEM
Sayısal bir sinyali telefon sistemi gibi bir sistemde aktarım için analog sinyallere dönüştüren bir alet. Alıcı tarafındaki modem de analog sinyalleri sayısala geri dönüştürür.

Multiplexor
Bir ya da daha fazla veri kanalını alıp birleştirerek aktarım için tek bir genel kanala dönüştüren cihaz. Diğer uçta da, bir demultiplexer orijinal sinyalleri ayırır.

Bilgisayar Ağları
Bilgisayarların ya da diğer aletlerinin iletişim olanakları aracılığıyla birbirleriyle olan bağlantısı.

İşletim Sistemi
Bilgisayarın tüm kaynaklarını kontrol eden ve diğer yazılım programlarını denetleyen bir program.

Genel olarak kullanılan işletim sistemleri şunlardır :
MSDOS: (ya da PCDOS) masa üstü bilgisayarlarda ve diz üstü bilgisayarlarda çalışır.
MVS : (Multiple Virtual Storage) Çoklu Sanal Saklama IBM ana bilgisayarlarında çalışır.
VMS : (Virtual Memory Storage) Sanal Hafıza Saklama, DEC VAX bilgisayarlarında çalışır.
Unix : mini ve mikro bilgisayarlarda kullanılan genel amaçlı, çok kullanıcılı bir işletim sistemi.
Novell : standart bir bilgisayar ağı işletim sistemi.

Outsourcing (Dış Alım)
Hem Bilişim Teknolojisi sistemlerinin hem de bunları kullanmak için gerekli personelin sağlanmasında dış satıcılardan faydalanılması.

Packet (Paket)
Bir adresten, kontrol ve veri sinyallerinden oluşan, bir bilgisayar ağında bağımsız bir parça olarak taşınabilen bir mesajın bütünleşik bir parçası.

Performans Denetimi
Tutumluluk, verimlilik ve etkinliğin ne ölçüde gerçekleştirildiğini belirlemek için yapılan inceleme.

PRINCE (Projects in Controlled Environments-Kontrol Edilmiş Ortamlardaki Projeler)
Bilişim Teknolojisi ortamlarındaki projeleri yönetmek için özel olarak tasarlanmış gelişkin prosedürler dizisi. PRINCE, CCTA'nın tercih ettiği proje yönetim metodolojisidir.

Problem
Ortak bulguları ortaya koyan birçok olayla ya da belirli bir olayda sebebi bilinen tek bir hatanın göstergesi ile tanımlanan bir durum.

Production library (Üretim Kütüphanesi)
Programların güncel ve çalıştırılabilir sürümlerini bulunduran bir sistem parçası.

Protokol
Bilgisayar ağıyla birbirine bağlanmış bilgisayarlarda aktarılabilecek verilerin anlamını, formatını ve tipini belirleyen standartlar ve kurallar.

PSTN (Public Switched Telephone Network - Telefon Şebekesi Anahtarlama Ağı)
Farklı yerler arasında modem aracılığı ile veri aktarımı için kullanılan halka açık telefon sistemi.

RAD (Rapid Application Development - Çabuk Uygulama Geliştirilmesi)
CASE araçlarının kullanımı da dahil olmak üzere sistem geliştirmeye yönelik yaklaşım.

Release (Sürüm)
Birlikte test edilmiş ve güncel ortama bir arada sunulmuş yeni ve/veya değiştirilmiş ayar araçları topluluğu.

Repeaters (Tekrarlayıcılar)
Uzak mesafelerde veri aktarımına yardımcı olmak için kullanılan aletler.

Değişim İsteği
BT altyapısı ya da BT hizmetlerinin herhangi bir yönünün değiştirilmesi isteklerinin detaylarını kayıt etmede kullanılan bir form ya da bir ekran.

ROM (Read Only Memory - Salt Okunur Bellek)
Okunabilen ama değiştirilemeyen program ve/veya veri barındıran bilgisayar belleği.

Router (Yönlendirici)
Verinin bilgisayar ağında en verimli rotada iletildiğini garanti eden alet.

Güvenlik Görevlisi
Organizasyonun güvenlik politikalarının uygun ve yürürlükte olduğunu garanti etmekten sorumlu kişi.

Güvenlik Politikası
Organizasyonun hassas bilgilerinin yönetimini, korunmasını ve dağıtımını düzenleyen kurallar ve prensipler bütünü.

Server (Hizmet Sağlayıcısı)
Bilgisayar ağının bir bölümünde, ağ kullanıcılarına belirli hizmetleri sağlayan bilgisayar ünitesi. örnek : bir yazıcı hizmeti sağlayan ünite ağ kullanıcılarına yazıcı işleriyle ilgili hizmetler verir, bir dosya hizmeti sağlayan ünite ise kullanıcı dosyalarını saklar.

Service level agreements (Hizmet Düzeyi Anlaşmaları)
Üzerinde anlaşılan BT hizmetlerini belgeleyen ve kullanıcılarla servis tedarikçiler arasında bağıtlanan yazılı anlaşmalar ya da kontratlar. Genellikle servis saatlerini, servislerin erişilebilirliğini, destek düzeyini, bitirilmesi gereken iş miktarını, yanıt süresini, kısıtlamaları ve işlevselliği içerir.

SSADM (Structured System Analysis and Design Method-Yapılandırılmış Sistemlerin Analiz ve Tasarım Metodu)
Bilgisayar uygulamalarının analizi ve tasarımı için gelişkin bir yaklaşım. SSADM, bir dizi gelişkin prosedür, teknik ve belgeleme standartlarıdır.

Superuser (Süper kullanıcı)
Kullanıcı dosyalarına ve sistem yardımcı araçlarına sınırsız erişim ayrıcalıklarına sahip, sistem yöneticisi tipinde, yüksek düzeyli kullanıcı.

SDLC (Systems development lifecycle - Sistem geliştirme yaşam çevrimi)
Bir bilgisayar sisteminin geliştirme aşamasından uygulama ve kullanılmasına kadar çeşitli aşamalarını tanımlayan bir terim.

Sistem Yazılımı
Temel olarak donanımın ve iletişim kaynaklarının kontrol ve koordinasyonu, dosya ve kayıtlara erişim ve uygulamaların kontrolü ve zamanlaması ile ilgilenen yazılım.

Test ortamı
Gerçek ortama sunulmadan yazılımların kabul testine tabi tutulması için kullanılan yazılım ve donanım.

TCP/IP (Transmission Control Protocol/Internet Protocol-Aktarım Kontrol Protokolü/Internet Protokolü
Internet' e bağlı olanlar da dahil olmak üzere, bilgisayar ağı ile birbirine bağlanmış bilgisayarlar arasında veri aktarımı için kullanılan genel bir standart.

Üçüncü kuşak programlama dilleri (3GLs)
Bu programlama dilleri, programların İngilizce' ye benzer bir dilde yazılmasına olanak tanır. Program, bilgisayarın her adımda neler yapması gerektiğini belirler. Üçüncü kuşak programlama dillerine Fortran, C, C++ ve Pascal girmektedir.

Trojan Horse (Truva Atı)
Faydalı bir fonksiyonu yerine getiren, fakat aynı zamanda izinsiz, gizli fonksiyonları da yürüten bilgisayar programı. Başka bir deyişle, yetkili bir programın içine saklanmış ve bu programın erişim ayrıcalıklarını kullanan yetkisiz bir program.

UPS (Kesintisiz güç kaynağı)
(Uninterruptible power supply) : Ana kaynağın bozulmasını takiben kısa bir süre için güç sağlayan elektrik kaynağı. Ek olarak BT sistemlerini elektrik dalgalanmalarına karşı korur.

User profile (Kullanıcı profili)
Belirli sistem kullanıcılarının erişim haklarının listesi.

Virüs
Virüsler kendilerini programlara ekleyen kötü amaçlar için yazılmış, kendi kendine yayılabilen zararlı bilgisayar programlarıdır.

Worms (Solucanlar)
Yayılmak için bir programa ihtiyaç duymayan, kendi kendine çoğalabilen zararlı bilgisayar programlarıdır. Bilgisayar ağları solucan saldırılarına karşı korumasızdırlar, bir solucan, bilgisayar ağının bir yerinden sızar, burada yerel problemlere sebep olur ve kendi kopyalarını ağın komşu bölgelerine yollar.

WORM (Write Once Read Many)
Tek Kez Yazılır Çok Kez Okunur : Verilerin bir kez yazılabildiği fakat silinemediği ya da değiştirilemediği veri saklama araçları. örnek compact diskler ve CD ROM'lar.

X.25
Kamuya ait veri ağlarındaki paket modunda çalışan terminaller arasında bilgi aktarımı için genel iletişim standardı.

X.400
Mesaj sistemleri için iletişim standardı. örnek : elektronik posta.

X.500
Dağınık sistemlerde ev sahipleri ve kullanıcılar hakkında dizin bilgisinin saklanması ve alınması için bir standart.

EK 2
Bilişim Teknolojisi Sistemlerinin Kullanımıyla İlgili Denetim Konuları

1.1 Bilişim Teknolojisi sistemlerinin, denetim yaklaşımını ve denetçinin denetim riskine ilişkin değerlendirmesini etkileyebilecek birkaç doğal özelliği vardır. Bazı Bilişim Teknolojisi özellikleri riski arttırır ve denetçinin özel dikkat göstermesini gerektirir. Aşağıdaki alt bölümler, bu özelliklerin ve bunların üzerinde neden durulması gerektiğinin kısa birer özetini içermektedir.

- hesap verme sorumluluğu;
- değişikliğe hassaslık;
- tekrarların kolaylığı;
- uzaktan erişimin kolaylığı;
- görünmez işlemcilik;
- denetim izinin varlığı;
- dağıtılmış veriler;
- BT hizmet tedarikçilerine güven; ve
- kanıt olarak bilgisayar kayıtları.

Hesap Verme Sorumluluğu

2.1 Bilgisayar kullanıcılarının kimlikleri orijin olarak belirsizdir. Bireysel kullanıcıların işlemlerini teşhis edemeyen ve kaydedemeyen sistemler, onları işlemleri için sorumlu kılamazlar. Kullanıcılar teşhis edilmedikleri ya da sorumlu tutulmadıkları sürece, kendilerinin izinsiz bilgisayar işlemleri yapmaları daha muhtemeldir.

2.2 İzinsiz işlem riski, bireysel kullanıcıları ve kütük işlemlerini olumlu olarak teşhis eden kontrollerin varlığı ile azaltılabilir. Sistem sahipleri, kimliği belirsiz kullanıcılarla ilgili riskleri, önce kullanıcıları ayrı ayrı tanımlayıcı kodlarla maddeleyip sonra da sisteme girdiklerinde kimliklerini kontrol ederek, azaltabilir. Kullanıcının iddia ettiği kimliğin kontrolünün en yaygın şekilde kullanılan metodu, şifrelerdir.

2. 3 Elektronik imzalar şeklindeki ek kontroller, hesap verme sorumluluğunu arttırmak üzere işlemlere eklenebilir.

Değişikliğe Hassaslık

3.1 Bilgisayarlar, normal olarak, hem işlem verilerini hem de yazılımları, disket ve kasetler gibi manyetik kayıt ortamlarında, dokunulamayan bir formda saklarlar. Manyetik kayıt ortamının yapısı, değişikliklerin, ya verilere ya da uygulamalara hiçbir iz bırakılmaksızın, yapılabileceği şekildedir. Denetçiler, izinsiz değişikliklerin yapılmasını engelleyen kontrollerin varlıklarını ve etkinliklerini değerlendirmelidirler. Yetersiz kontroller, denetçinin, bireysel bilgisayar kayıtlarına ya da denetim izinin bütünlüğüne güvenememesine neden olabilir.

3.2 Uygulama yazılımları ve işlem verileri, uygun fiziksel ve mantıksal erişim kontrolleri ile, izinsiz değişiklikten korunmalıdır. Fiziksel erişim kontrolleri, kuruluşun mahalline, binalarına, bilgisayar odalarına ve BT donanımının her parçasına erişimi kısıtlamak üzere, fiziksel engellerin yerleştirilmesini içerir. Mantıksal erişim kontrolleri, bilgisayar yazılımı tarafından konulan kısıtlamalardır.

3.3 Elektronik fon transferleri gibi bilgisayar ödemeleri, kağıt üzerinde ödenebilen araçlardan daha kolay değiştirilir ve bu nedenle yeterli şekilde korunmaları gerekir. Elektronik işlemlerin bütünlüğü, veri şifrelemesi, elektronik imzalar ve karıştırma (şifreleme) algoritması gibi yollarla korunabilir.

Tekrarların Kolaylığı

4.1 Bilgisayar verilerinin kopyalarının, orijinallerinden ayırt edilmeleri mümkün olmayabilir. Elektronik fon transferi sistemlerindeki gibi, verilerin mali bir değeri olduğunda, tekrar işlemlerinin önlenmesi özellikle önemlidir. Bilgisayar sistemleri, tekrar işlemlerinin uygulanmasını teşhis etmek ve önlemek için, kontroller içermelidir.

4.2 Uygun kontroller, işlemlere sıra numaralarının verilmesini ve kontrol toplamlarının rutin incelemesini içerebilir. Fiziksel işaretleme ya da bilgisayar girdi belgelerinin iptali gibi manuel kontroller de, tekrar işlemleri riskini azaltabilir.

4.3 Denetçiler, konşimento ya da senetler gibi ciro edilebilir enstrümanlar (araçlar) saklandığında ve bilgisayarlar üzerinden değiştirildiğinde, olası problemlerin farkında olmalıdırlar. Bu tip durumlarda, güvenilen bir üçüncü kişinin arabuluculuğunun kullanılması uygun olabilir. Güvenilen üçüncü kişi, bir sicil memuru rolünü üstlenecek ve belirli ciro edilebilir araçların tescilli sahibinin bir kaydını tutacaktır. Kontratın tamamlanmasıyla, alıcı, ödemeye izin verilmeden önce, satıcının enstrüman üzerinde hakkı olduğunun doğrulanmasını bekleyecektir. Bu düzenleme, elektronik belgelerin iki kere alıverişe konu olmasını engelleyecektir.

Uzaktan Erişimin Kolaylığı

5.1 Kağıt dosyalar, kapı kilitleri, kasalar, video gözetimi, hırsız alarmları v.b. ile kolaylıkla, izinsiz erişimden korunabilir. Buna benzer koruma, manyetik kasetler ve disketler gibi taşınabilir veri saklama gereçleri için de kullanılabilir. Verilere erişim bir bilgisayar ağı üzerinden sağlandığında, yazılımlara ve veri dosyalarına kimin erişiminin bulunduğuna ilişkin bir belirsizlik oluşabilir.

5.2 Müşterilerin bilgisayar sistemlerini, küresel geniş alan ağına, yani Internet' e bağlamaları artarak yaygınlaşmaktadır. Bu tip bağlantılar, izinsiz uzaktan erişim ve bilgisayar virüs ve solucanlarının saldırıları riskini belirgin şekilde arttırmaktadır. Internet' e bağlı ağların korunmasının başarılması zordur ve yüksek dereceli uzmanlık bilgisi gerektirmektedir.

5.3 Bazı bilgisayar işletim sistemleri, uzaktaki kullanıcıların verileri görebilmelerini, değiştirebilmelerini , silebilmelerini ya da yaratabilmelerini sınırlayan erişim kontrolleri sağlarlar. İşletim sisteminin erişim kontrolleri, ek teşhisler ve her uygulama için doğruluk kontrolleri ile arttırılabilir. Her iki durumda da erişim kontrollerinin etkinliği, güçlü tanımlama ve aslına uygunluğun doğrulanması yöntemlerine ve güvenlik sistemlerinin iyi yönetilmesine bağlıdır.

Görünmez işlemcilik

6.1 Bir bilgisayarın içinde gerçekleşen işlem denetçi için fiilen görünmezdir. Denetçiler neyin girip neyin çıktığını görebilirler ancak ortada neyin olup bittiği hakkında az bir bilgi elde edebilirler. Bu zaaf, izinsiz programların izinli olanların içine yerleştirilmesi şeklinde istismar edilebilir. İzinsiz program değişiklikleri tehlikesi, etkin erişim kontrollerini, kütük işlemlerini, bu kütüklerin gözden geçirilmesini ve sistem geliştiricileri, bilgisayar işlem personeli ve son kullanıcılar arasındaki etkin bir görev dağılımını içeren uygun değişim kontrol yöntemlerinin benimsenmesiyle azaltılabilir.

Bir denetim izinin varlığı

7.1 Denetim izi, bir bilgisayarda saklanan kayıtlara dayandığında, denetçi, işlem verilerinin yeterli bir zaman tutulduğunu ve yetki dışı değişiklikten korunmuş olduğunu güvence altına almalıdır. Bazı bilgisayarların sınırlı saklama kapasiteleri, tutulabilecek olan eski işlem verilerinin miktarını kısıtlayabilir. Bu tip durumlarda, denetçi, ilgili muhasebe kayıtlarının düzenli olarak arşivlendiği ve güvenli bir ortamda tutulduğu konusunda ısrarcı olma ihtiyacını hissedebilir. Denetçi, aynı zamanda, denetim zamanlamasında, müşterinin veri arşivleme politikasının olası etkisini göz önünde bulundurmak ihtiyacını da hissedebilir.

Dağıtılmış veriler

8.1 Ağ'a dahil olan bilgisayarlar, mali uygulamaları ve veri dosyalarını tüm ağ veri saklama araçlarında saklayabilirler. Denetçi, bir mali uygulamayı bir bilgisayarda çalıştırırken, kullanılan işlem dosyalarını başka bir odada, binada, hatta başka bir ülkede saklayan bir sistemle karşılaşabilir.

8.2 Dağıtılmış veri işlemcilik, kuruluşun BT sistemlerinin gözden geçirilmesi için gereken kaynakları arttırabilir ve denetçinin, fiziksel ve mantıksal erişim kontrolleri değerlendirmesini güçleştirebilir. Kontrol ortamı bir yerde çok iyi, diğerinde çok zayıf olabilir.

Bilişim Teknolojisi servis tedarikçilerine güven

9.1 Bilişim Teknolojisi imkânları aşağıdaki üç yoldan biri ile sağlanır :

- firma-içi (yerleşik Bilişim Teknolojisi departmanı tarafından)-kuruluş bilgisayar sistemlerinin sahibidir ve sistem firma çalışanları tarafından işletilir;

- olanaklar yönetimi - müşteri sistemin sahibidir, ancak günlük işlemler ve bakım faaliyetleri için servis tedarikçisi bir üçüncü şahıs ile sözleşme yapılmıştır; ya da

- kaynakların dışarıdan sağlanması hem bilgisayar sistemleri hem de BT personeli üçüncü bir şahıs tarafından sağlanır.

9.2 Bir kuruluş üçüncü şahıs BT servislerini kullandığında, denetçi, inceleme haklarının varlığını ve eğer varsa, BT servis tedarikçilerinin kendi iç ya da dış denetçilerinden alınması gereken denetim güvencesini göz önünde bulundurma ihtiyacını hissedecektir.

9.3 İyi kontrol edilmiş bir BT uygulaması, uygulama sahibi, sistem kullanıcıları ve BT servis tedarikçileri arasında ayrılacaktır. Uygulama sahibi, genelde, uygulamanın kıdemli bir kullanıcısı olacaktır ve BT servis sağlayıcılarına karşı, kontrol gereksinimlerinin formüle edilmesi ve iletişimi konusunda sorumlu olacaktır. Denetçi, uygulama sahiplerinin, kontrol gereksinimlerinin yeterli bir tanımını verdiklerini ve BT sağlayıcılarının, gereksinimleri, BT sisteminin kontrolüne imkân verecek bir, tatminkârlık düzeyinde yansıttıklarını kontrol etme ihtiyacını duyacaktır.

Kanıt olarak bilgisayar kayıtları

10.1 Denetim kayıtlarına ilişkin prensipler değişmez, çünkü denetim, bir bilgisayar ortamında tamamlanmaktadır. Manyetik disketler ya da optik disketlerdeki veriler şeklindeki bilgisayar kayıtları, yine de denetçiye denetim güvencesi sağlar. Denetçi, aynı zamanda, bilgisayar destekli denetim teknikleri kullanarak da, denetim kanıtını oluşturabilir.

10.2 Bilgisayar kayıtlarının bir hukuk mahkemesinde kabul edilebilirliğini gösteren çok az örnek vardır. Hukuki davalarda bilgisayar kanıtları sunulduğunda, mahkemeler, bilgisayar verilerinin güvenilirliğini değerlendirmeden önce, BT kontrol ortamının etkinliği konusunda uzman kanıtlarını hesaba katarlar.

10.3 Denetçi, bilgisayara dayalı işlemlerin ya da belge kopyalarının, kontroller sistemde tutulan verilerin doğrulukları ve bütünlükleri hakkındaki haklı şüpheyi ortadan kaldırabilecek kadar güçlü olmadıkça, kabul edilemez olabileceklerini aklında bulundurmalıdır.

EK 3
Mali Denetim Planlaması-Bilişim Teknolojisinin Gözden Geçirilmesi

Sınıf	:	Değerlendirme :	
Kuruluş	:		
Hazırlayan	:	Tarih	:
Güncelleme	:	Tarih	:
Güncelleme	:	Tarih	:
Güncelleme	:	Tarih	:
Gözden Geçiren	:	Tarih	:
Güncelleme	:	Tarih	:
Güncelleme	:	Tarih	:
Güncelleme	:	Tarih	:

Bilişim Teknolojisi incelemesinin amaçları şunlardır :

- kuruluşun mali tablolarının hazırlanmasında kullanılan bilgisayar yükleme ve uygulamalarının teşhis edilmesi;
- denetçilerin, bilgisayar karmaşıklığının derecesini değerlendirmesinin sağlanması;
- Bilişim Teknolojisi ortamındaki risklerin teşhis edilmesi; ve
- denetçilerin, denetim planlaması yapmaları ve etkin bir denetim yaklaşımı geliştirmeleri için bilgisayara dayalı iç kontrol sistemleri konusunda yeterli bir fikir edinmelerinin sağlanması.

Bilişim Teknolojisinin incelenmesinin üç bölümü vardır :

Bölüm A- Kuruluşun Bilişim Teknolojisi sistemleri konusunda ön bilgi edinilmesi

Bölüm B- Bilişim Teknolojisi kontrol ortamının incelenmesi ve kurumsal riskin değerlendirilmesi

Bölüm C- Uygulama kontrollerinin incelenmesi ve hesap alanı risk değerlendirmesi

Önemli Not:

BT'nin incelenmesi kısmen kompleks olan BT sistemlerinde kullanılmak üzere geliştirilmiştir. Denetçiler, yargılarını, denetlenen kuruluşun mali BT sistemlerinin ölçeğini, karmaşıklığını ve önemini akılda tutarak, hangi kontrollerin makul olacağını değerlendirmek için kullanmalıdırlar. Bu incelemedeki bazı sorular, tüm kuruluşlara uygulanabilir olmayabilir.

Bilişim Teknolojisinin Gözden Geçirilmesinin İçeriği

	Bölüm
A: Kuruluşun Bilişim Teknolojisi sistemi hakkında ön bilgi edinilmesi	
Kuruluşun genel incelenmesi	A1
Önceki denetimlerden doğan ana sorunlar	A2
Planlanan bilgisayar gelişmeleri	A3
Donanım ve yazılım	A4
Bilgisayar denetim uzmanlarına duyulan ihtiyaç	A5
İhtiyaç duyulan sistem inceleme işi	A6
Ana temaslar	A7
B: Bilişim Teknolojisi kontrol ortamının incelenmesi ve kuruluş riski değerlendirmesi	
Genel politika, yönetim ve kontrol	B1
Görevlerin Ayrımı	B2
Fiziksel erişim kontrolleri	B3
Mantıksal erişim kontrolleri	B4
Değişim yönetimi kontrolleri	B5
İşin sürekliliğinin planlanması	B6
Dış BT servis tedarikçilerinden yararlanma	B7
Operasyonel kontroller	B8
Son kullanıcı bilgisayar işlemleri	B9
C: Uygulama kontrolünün gözden geçirilmesi ve hesap alanı risk değerlendirmesi	
Bilgisayara dayalı mali uygulamanın tanımlanması	C1
Denetlenebilirlik	C2
Bilgisayar destekli denetim tekniklerinin kullanımı	C3
Uygulamanın belgelenmesi	C4
Uygulamanın güvenliği : fiziksel ve mantıksal erişim	C5
Girdi kontrolleri	C6
Veri iletim kontrolleri	C7
İşletim kontrolleri	C8
Çıktı kontrolleri	C9
Ana dosya ve kalıcı veri kontrolleri	C10

Bölüm A: Kuruluşun Bilişim Teknolojisi sistemi hakkında ön bilgi edinilmesi

Amaç : BT incelemesinin bu kısmının amacı, kuruluş tarafından kullanılan bilgisayarlı mali sistemlerin boyutu, tipi ve karmaşıklığı hakkında ön bilgi edinmektir. Denetçi daha sonra sistemlerin karmaşıklığını sınıflandırabilir ve BT incelemesinin B ve C kısımlarının bir BT denetimi uzmanı tarafından tamamlanıp tamamlanmaması konusunda karara varabilir.

A1. Kuruluşun Genel İncelenmesi (daha önceki bilgiler ve kalıcı denetim dosyalarına göre)

Denetlenen kurumun faaliyetlerinin niteliği :
Ana faaliyetler:

Yıllık ödemeler/harcamalar (sterlin)
Yıllık alındılar/gelirler (sterlin)
Toplam varlıklar (sterlin)
BT varlıklarının değeri (sterlin)
Yıllık BT bütçesi (sterlin)
Yıllık BT bütçesi (sterlin)
BT personelinin sayısı

A2. Önceki denetimlerden doğan ana sorunlar

(daha önce yönetimin dikkatinin çekildiği hususlara, hesap sistemlerinin gözden geçirilmesine, risk denetim değerlendirmelerine, vs'ye dayanır.)

A.3 Planlanan bilgisayar gelişmeleri

Ana BT sistemi geliştirme projeleri nelerdir? Bunlar ne zaman hayata geçecek? Herhangi bir problem tanımlandı mı? Yeni sistemler şimdiki ve gelecekteki denetimlerde ne gibi etkiler yapabilir? Kuruluşun yeni bir BT sistemi yerleştirmeyi düşündüğü yerde denetçi, bir BT sistemi uzmanı ile ilişki kurmayı düşünmelidir. (Normal olarak sistem özelliklerinin belirlenmesi aşamasında ya da sistemin çalışmasından hemen önce.)

A4. Donanım ve Yazılım

4.1 Donanım/işlemci detayları

İsim üretici/model/özellikler	Yer(ler)	Terminaller	Ağa bağlı olma durumu

4.2 Ağ Donanım ve Yazılımı

(nirengi, kablolama, iletişim protokolü, modemler, köprüler, yönlendiriciler)

4.3 Sistem yazılımı

İşletim Sistemi

Güvenlik Yazılımı

Veri Tabanı Yönetimi Yazılımı

Denetim Yazılımı

Rapor Hazırlayıcılar

Programlama Yazılımı

Diğerleri

4.4 Muhasebe/Uygulama Yazılımı

(isim, sağlayıcı, sürüm, platform, programlama, dil, kullanıcı sayısı, tesis tarihi, paket ya da ısmarlama, modüller, gurup/on-line, EDI kullanımı)

Uygulamanın Adı Sürüm	**Donanım Platformu**	**Ismarlama ya da Paket**	**Yorumlar** Örneğin tesis tarihi

A5. Bilgisayar Denetim Uzmanlarına Duyulan İhtiyaç

Bilgisayar denetim uzmanlarının hizmetlerine ihtiyaç duyulacak mı? Denetçiler, kendilerinin izlemeyi kabul edilebilir bir seviyede sürdürmek için gerekli BT ve denetim becerisine sahip olup olmadıklarını değerlendirmelidir. Göz önünde tutulması gereken faktörler: BT departmanının boyutu; ağa bağlanmış iletişimin kullanılması; dağıtılan veri işleme; yeni teknolojilerin kullanımı; geliştirilen sistemler; müşterinin geçmişteki BT problemleri ile ilgili bilgi ve kontrollere dayalı bir denetim yaklaşımının nerede arzulanacağı.

A.6 İhtiyaç duyulan sistem inceleme işi

(Hangi kurumlar/uygulamalar incelenmelidir)

A7 **Ana Temaslar** (maliye ve Bilişim Teknolojisi içinde):

İsim	Pozisyon/Derece	Yer	Telefon No

Bölüm B: Bilişim Teknolojisi kontrol ortamının incelenmesi ve kuruluş riski değerlendirmesi

Amaç: Kuruluşun bilişim teknolojisini kullanmasının, organizasyonunun mali durumuna yönelttiği risklerin niteliğini, büyüklüğünü ve bizim bunları denetleme gücümüzü tanımlamak. BT kontrollerinin kurum düzeyinde değerlendirilmesi, mali faaliyetlerin yürütüldüğü genel hesaplama ortamını sürekli gözden geçirerek başarılabilir. Genel bilgisayar ortamındaki zayıflıklar, temeldeki bilgisayar faaliyetlerinin ve işledikleri muhasebe verilerinin güvenilirliğini ve uygulanabilirliğini ters etkileyebilir.

B1. Genel politika, Yönetim ve Kontrol

Bu yüksek seviyeli kontroller, muhasebe uygulamalarıyla çalışan daha düşük seviyedeki kontrolün etkinliğini etkilediği için önemlidir. Yönetim, uygun BT politikaları ve standartları sağlamazsa, diğer kontrollerin kontrole dayalı bir denetim yaklaşımını desteklemesi zor olacaktır.

B1 . Genel Politika, Yönetim ve Kontrol	Yorumlar	Çalışma Kağıdı
1.1 Bilişim Teknolojisi Stratejisi Denetlenen kurumun Bilişim Teknolojisi stratejisi ne kadar uygun? • Onaylandı mı? • Güncel tutuluyor mu? • Mali bilgi sistemlerini kapsıyor mu? • Personel konuları biliyor mu? • Uygulamalarını izlemek için prosedürler mevcut mu? *Zayıf ya da eksik bir Bilişim Teknolojisi stratejisi, iş ihtiyaçlarına uygun olmayan sistemlerin geliştirilmesine sebep olabilir. Bir BT stratejisi, denetçinin yeni sistemleri başlangıçta tanımasına yardımcı olabilir.*		
1.2 Üst Düzey Yönetimin Rolü Üst düzey yönetim, denetlenen kurumun BT fonksiyonlarına ne derecede ilgi duyuyor? (Örn: BT yönlendirme komiteleri) *Yönetimin ilgisizliği, kontrolsüz sistemlerin geliştirilmesine ve denetlenemeyen sistemlere sebep olabilir. Üst düzey yönetim ayrıca diğer bilgisayar Kontrollerinin geliştirilmesi için bir itici güç oluşturabilir.*		

B1 . Genel Politika, Yönetim ve Kontrol

	Yorumlar	Çalışma Kağıdı
1.3 Belgeleme Politikaları Kuruluş uygun BT belgeleme sistemlerine sahip midir? Politikalar, dokümanların güncel, kapsamlı ve uygun personel tarafından ulaşılabilir olduğunu garanti etmelidir. *Yetersiz belgeleme politikaları yetkisiz çalışma uygulamalarının benimsenme riskini artırır ve sistemin çalışmasını güçleştirir.*		
1.4 Kayıt/Doküman Muhafazası Elektronik dokümanların ve yazıcı çıktılarının saklanması için uygun kontroller var mıdır? Örn: • Elektronik kayıtlar • Eski mizanlar • Kapasite planlaması *Bu tip politikaların eksikliği denetim kanıtlarının elde edilmesinde zorluk yaratabilir. Ör: Kayıtlar silinmiş ya da arşivlenmişse.*		
1.5 İç Denetimin Rolü Kurumun iç denetim fonksiyonu bilgisayarlı mali sistemlerin BT incelemelerini yapıyor mu? • Görev alanı nedir? • BT becerileri/eğitimi/deneyimi *İç denetimin sonuçlarına güvenmek mümkün olabilir. Bazı denetim risklerini tanımlayabilirler. Denetçi, İç Denetimin yıllık denetim sonuçlarına başvurma ihtiyacı duyabilir.*		
1.6 Personel Politikaları Politikalar, BT ortamına uygun mudur? • Yüksek devir • Yeni işe alınanların izlenmesi • Disiplin politikaları *Uygun olmayan personel politikaları, zayıf yetiştirilmiş personelin hata yapmasına, dikkat edilmeden işe alınanlar tarafından suç işlenmesine ve bazı canı sıkılmış çalışanlar tarafından sabotaj yapılmasına sebep olabilir.*		

B1 . Genel Politika, Yönetim ve Kontrol		
	Yorumlar	**Çalışma Kağıdı**
1.7 Bilgisayar Güvenlik Politikaları Güvenlik politikası yeterli mi? • Risk değerlendirmesi üzerine mi kurulmuş? • Çalışanlara duyurulmuş mu? • Güncel tutuluyor mu? • Olayların ve güvenlik zayıflığının rapor edilmesini kapsıyor mu? • BT güvenlik eğitimi var mı? • Güvenlikten kim sorumlu? • Hangi uygunluk kontrolü yapılmış? *Yetersiz güvenlik politikaları personeli ve yönetimi güvenlik risklerinden ve sorumluluklarından habersiz olmaya sürükleyebilir.*		
1.8 Yasal ve Düzenleyici Konular Kuruluşun BT olanaklarının yasal ve düzenleyici gerekliliklere uymasını sağlayacak uygun politikaları ve yöntemleri var mı? *Uygun politikaların noksanlığı düzensiz işlem riskini artırır. (açıklama: örneğin : yasalara ya da düzenlemelere uymakta başarısızlık. Veri koruma yasası. Sağlık ve güvenlik düzenlemeleri)*		
1.9 Pazar Kontrolü/Dış alım/Olanaklar Yönetimi Denetlenen kurum, BT servislerini dış kaynaklardan mı sağlıyor? Tanımlanan riskleri (örneğin giriş hakları) karşılamak için uygun prosedürler geliştirilmiş mi? Üçüncü şahıs BT servis tedarikçilerinden yararlanmak üzere herhangi bir plan var mı? *Bağımsız servis tedarikçilerinden yararlanmak, içten ya da dıştan, veri ulaşımı ve güvenilirliği riskini arttırabilir. Uygun denetleme olmadığında dışarıdan servis sağlayanların verilerine güvenmek olanaklı olmayabilir.*		

B2. Görevlerin Ayrımı

BT bölümleri arasında görev bölüşümü hata ve sahtekarlık riskini düşürür. Zayıf bir görev bölüşümü, bilgisayarın bir fonksiyonu üzerinde kontrolü olan herhangi bir insanı fark edilmeden hataya ya da sahtekarlık yapmaya sürükleyebilir. Görev ayrımı ayrıca hataların daha kısa sürede fark edilmesini de sağlayabilir. Görev bölüşümü ile ilgili bilgi, BT personeli ile konuşarak ve rapor verme hatları ile iş açıklamalarını gösteren grafiği elde ederek sağlanabilir. Yetetli görev ayrımı olanaklı olmadığında, örneğin küçük bir BT departmanında, denetçi, telafi edici kontrollerin varlığını aramalıdır/

B2 . Görevlerin ayrımı		
	Yorumlar	**Çalışma Kağıdı**
2.1 Kuruluşun BT departmanının formel bir organizasyon yapısı var mı? BT personelinin sorumlulukları ve bölümlerin işlem alanları açıkça ortaya konmuş mu? *Formel bir organizasyon yapısının/rapor verme hatlarının varlığı çalışanların kendilerinin ve diğerlerinin sorumluluk sınırlarının farkında olmalarının sağlanmasına yardım eder. Bu durum yetkisiz davranışların fark edilmeksizin yapılmasını zorlaştıracaktır.*		
2.2 BT çalışanlarına uygun iş açıklamaları verilmiş mi? Her görevin kendi açıklaması var mı? Açıklamalar BT güvenlik şartlarını içeriyor mu? *İş açıklamaları çalışanların kendi yetki sınırlarını aşan eylemleri gerçekleştirme riskini azaltır*		
2.3 Bilgisayar bölümü fiziksel ve yönetsel olarak kullanıcılardan özellikle mali işlevlerden ayrı mı? *Fiziksel ve yönetsel ayrım, sahtekarlık riskini düşürür. BT işlevlerini kullanıcılardan ayrı tutmak, ayrıca kullanıcıların yazılımlarda veya verilerde yetkileri olmadan değişiklik yapma riskini de düşürür. Hem mali görevleri hem de BT görevleri olan personelin izinsiz faaliyetleri yakalanmadan sürdürmek için daha büyük fırsatları vardır.*		
2.4 Görevlerin ayrılmasında ulaşılan düzey, BT departmanının ölçeğine uygun mudur? Görev ayrımına nasıl ulaşılmaktadır.		

B2 . Görevlerin ayrımı		
• Sistem tasarımı ve programlama • Sistem desteği • Rutin BT işlemleri • Veri girişi • Sistem güvenliği • Veri tabanı idaresi • Değişim yönetimi *Görevlerin ayrılmasının yetersiz olması, sistem hakkında önemli bilgilere sahip bilgisayar personelinin uygunsuz işlemler yapmalarını ve işlemlerinin izlerini yok etmeleri riskini arttırır. Görevlerin ayrılması, aynı zamanda, bir gözden geçirme, hata tespiti ve kalite kontrolü formu yerine geçer*	**Yorumlar**	**Çalışma Kağıdı**

B3. Fiziksel Erişim kontrolleri

Fiziksel erişim kontrolleri, tüm BT ortamı içinde işleyen ve tüm temel bilgisayar uygulamalarını etkileyen çevresel kontrolleri içerir. Bu kontroller, bilgisayar donanım ve yazılımını, zarar görmekten, hırsızlıktan ve yetki dışı erişimden korumak üzere tasarlanmıştır. Erişim kontrolleri, çeşitli düzeylerde işleyebilir (örneğin, müşterinin sistemine kısıtlı erişimden bireysel PC'lere klavye kilitleri takılmasına kadar). Fiziksel erişim kontrollerinin hızlı bir değerlendirmesi, genelde, görsel bir inceleme ile sağlanabilir. BT sistemlerine fiziksel erişimin kısıtlanması, yetkisiz kişilerin mali bilgileri değiştirmesi riskini azaltır.

B3 . Fiziksel Erişim kontrolleri		
3.1 BT olanaklarının hasardan korunması için ne tip fiziksel kontroller uygulanmıştır? Kontroller, kuruluş için yeterli midir? • Ateşten koruma • Sudan koruma • Havadan koruma • Veri girişi • Güç kaynakları *Yetersiz çevresel kontroller, sistem hasarına ve hesap olanaklarının sonradan kaybına yol açabilir.*	**Yorumlar**	**Çalışma Kağıdı**

B3 . Fiziksel Erişim kontrolleri		
	Yorumlar	**Çalışma Kağıdı**
3.2 Sisteme ve bilgisayar olanaklarına erişim nasıl kısıtlanmıştır? Kimin neye erişim izni vardır ve bu izni nasıl almaktadır? • Bilgisayar işletmenleri • Mali personel • Temizlikçiler • Bakım personeli *Kısıtlanmamış erişim, hırsızlık ve bilgisayar olanaklarının hasar görmesi riskini arttırır. Değiştirilmiş, silinmiş veriler ve hile riski de artar.*		
3.3 Donanım ve yazılım kayıtlarının doğru şekilde tutulduğunun güvence altına alınması için, müşteri tarafından ne tip önlemler alınmıştır? Müşteri tüm bilgisayar parçalarının ayar kayıtlarını tutmakta mıdır? Parçalar, teşhislerinin kolaylaştırılması için işaretleniyor ya da etiketleniyor mu? *Bilgisayar parçalarının kaydedilmesindeki ya da kontrol edilmesindeki bir başarısızlık, donanımda ve içindeki verilerde istenmeyen kayıplara yol açabilir.*		

B 4. Mantıksal Erişim Kontrolleri

Mantıksal erişim kontrolleri, hem sistem hem de uygulama düzeyinde ortaya çıkabilir. Sistem düzeyindeki kontroller, kullanıcıların özel uygulama ve verilere ulaşımını kısıtlamak üzere kullanılabilir. Mantıksal erişim kontrolleri, dosya editörleri gibi güçlü sistemlerin yardımcı programlarına erişimi de kısıtlamak için kullanılabilir. Mantıksal erişim kontrolleri, genelde, programların ve veri dosyalarının yetkisiz olarak değiştirilmesi riskinin azaltılması için, fiziksel erişim kontrolleri ile birlikte kullanılır. Yönetim raporlarının ve bilgisayar kütüklerinin etkinlikleri, bunlar yönetim tarafından, düzenli olarak gözden geçirilip incelenmediği takdirde belirgin şekilde azaltır.

B4 . Mantıksal Erişim Kontrolleri		
	Yorumlar	**Çalışma Kağıdı**
4.1 Kuruluşun, bir erişim kontrol politikası var mıdır? Bu belgelenmiş ve güncelleştirilmiş midir? *Bir politika olmaksızın, kuruluşun mantıksal erişim kontrollerinin uygun olup olmadığını ölçmek zordur. Bu politika özel kontrollerin benimsenmesini sağlayacaktır.*		

B4 . Mantıksal Erişim Kontrolleri

	Yorumlar	Çalışma Kağıdı
4.2 İşletim sistemine, veri dosyalarına ve uygulamalara erişimin kısıtlanması için ne tip mantıksal erişim önlemleri mevcuttur? Bu önlemler uygun mudur? • Kullanıcılar için kısıtlı menüler • Kullanıcı isimleri ve şifreler • Kullanıcı erişim haklarının gözden geçirilmesi • Kullanıcı ve grup profilleri Not : Denetçi-kuruluşun işletim sisteminde, örneğin Unix, Novell, ne tip erişim kontrollerinin mümkün olduğunu bulmalıdır. *Yetersiz mantıksal erişim kontrolleri, sistemi hem içeriden hem de dışarıdan yetkisiz kullanıcılardan korumayacaktır. Dosya editörlerine yetki dışı erişim, uygulama dosyalarının değiştirilmesine sebep olabilir.*		
4.3 Tüm kullanıcılara ayrı birer kullanıcı tanımlama kodu tahsis edilmiş midir? *Kullanıcı kodunun sistem ve uyguiama kullanımı için kütüğe kaydedilmesi koşuluyla ayrı ayrı kullanıcı kodları denetim izi sağlayabilir. Kullanıcı kodları, aynı zamanda, yetki dışı işlemler yapma girişiminde bulunan personelin teşhis edilmesinde de kullanılabilir.*		
4.4 Kuruluşun şifre uygulamaları ne kadar uygundur? Örneğin, • Şifre uzunluğu (minimum/ maximum) • Süreler/son kullanım tarihleri • Değişim yöntemleri • Şifre oluşumu • Ayrılanların kullanıcı kodlarının kaldırılması • Şifre kriptolaması (şifreleme) • Yeni kullanıcılar için şifrelerin kaydı ve tahsis edilmesi • Şifre uygulamalarının yürütülmesi *Yetersiz şifre uygulamaları, varolmayan ya da tahmini kolay şifrelere ve bu nedenle de yetersiz kullanıcılar tarafından daha kolay erişilebilen sistemlere sebep olabilir.*		

B4 . Mantıksal Erişim Kontrolleri

	Yorumlar	Çalışma Kağıdı
4.5 Başka ne tip mantıksal erişim kontrolleri kullanılmaktadır? • Kısıtlanmış işe girişim denemeleri • İşe giriş yöntemleri ve tarihçe kütükleri • Terminal özel erişimi • Yetkisiz girişim kütükleri • Birden çok işe giriş üzerinde kısıtlama • Terminalin otomatik olarak kapanması • Sistemin yardımcı programları ve denetim araçlarına kısıtlı erişim ve kısıtlı kullanım • İhmal edilmiş terminallerin kontrolü *Ek mantıksal erişim kontrollerinin kullanımı, yetki dışı erişim ve veri sahtekârlığı riskini azaltır ve bunların ortaya çıkarılması ihtimalini arttırır.*		
4.6 Sistem geliştirme personelinin güncel verilere ve üretim ortamına erişiminin kısıtlanması için ne tip mantıksal erişim önlemleri vardır? *Güncel veriler ve programlara erişimi mümkün olan geliştirme personelinin rastlantısal veya kasıtlı olarak ya da hileli değişiklikler yapma ihtimali vardır.*		
4.7 Kuruluş, sistem ve veri tabanı yöneticileri ve programları gibi ayrıcalıklı kullanıcıları, nasıl yerleştirir, yetkilendirir, kontrol eder ve gözlemler? *Güçlü kullanıcılar üzerinde yetersiz kontrol, programlar ve mali verilerde yetki dışı değişiklik riskini arttırır.*		
4.8 Sisteme hangi dış kuruluşların erişimi söz konusudur? (örneğin, internet yoluyla, modemler üzerinde on - line sistemler yardımıyla) Kuruluş güvenlik uygulamaları üzerinde düşünmüş müdür? Sistem nasıl korunmaktadır? • Firewalls (ağ kontrolü) kullanımı • Bilgisayar ağlarında ayrım • Ağ yönlendirme kontrolleri *Zayıf erişim kontrolleri mali kayıtların bütünlüğünü ve kullanılabilirliğini etkileyen kaçakların, solucanların ve virüslerin ortaya çıkması riskini arttırır.*		

B5. Değişim Yönetimi Kontrolleri

	Yorumlar	Çalışma Kağıdı
5.4 Ne tip değişiklik kayıtları tutulmaktadır? Ayar kayıtları güncel, açıklayıcı ve tam mıdır? Kullanıcı/prosedür el kitapları güncelleştirilmiş midir? Personel hangilerinin en güncel el kitapları olduğunu nasıl bilir? *Yetersiz belgeleme, sistemin korunmasını daha zorlaştırır. Uygun standartlar olmaksızın belgeleme takibi zor hale gelebilir ya da güncelliğini yitirebilir. Yeterli değişim belgelemesi, sistem hatalarının teşhisinde yardımcı olabilir.*		
5.5 Firma içi gelişmeler için benimsenmiş standart geliştirme metodolojileri ve araçları var ise bunlar nelerdir? Bu tip metodolojilerin kullanımı belgeli yöntemlere çevrilmiş midir? Örneğin, • PRINCE • SSADM • CASE araçları *Standart metodolojilerin kullanımı, yeni bir sistemin kullanıcı gereksinimlerini (denetçinin ihtiyaçlarını da kapsamak üzere) karşılama konusunda başarısızlığa uğrama riskini azaltır.*		
5.6 Kuruluşun, acil değişiklikler yapmak için ne tip düzenlemeleri vardır? • Belgeleme • Önceki olayları kapsayan yaklaşım • Test etme *Onaylanmamış acil değişiklikler bilgisayar sisteminin diğer parçalarında önceden tahmin edilmeyen problemlere neden olabilir.*		
5.7 Testten aktif ortama sadece izinli değişikliklerin transfer edildiğinin garanti edilmesi için ne tip kontroller mevcuttur? *Yetersiz kontroller, izinsiz değişikliklerin aktif ortamda kullanıldığı programlara sebep olabilir. İzinsiz sistem değişiklikleri müşterinin aldatılması için kullanılabilir. Bunlar, aynı zamanda, sistemin kullanılabilirliğini de etkileyebilir ve mali verileri bozabilir.*		

B5. Değişim Yönetimi Kontrolleri	Yorumlar	Çalışma Kağıdı
5.8 Kurum, geliştirme araçlarından ya da program değişikliği olanaklarından nasıl bir fayda sağlamaktadır. (örneğin, ZAP, derleyiciler taplayıcılar) Bunlara kimlerin erişimi vardır ve kontrol edilen bu tip araçların kullanımı nasıldır? *Bu olanakların yetki dışı kullanımı, düzenlenmiş değişim yönetimi yöntemlerinin atlanması amacıyla kullanılabilir ve böylece izinsiz uygulamaların gelişmesine neden olabilir.*		
5.9 Kuruluş yazılım arızalarına ve kullanıcı problemlerine karşı ne yapar? Kuruluş danışma masası fonksiyonuna sahip midir? Ne tip danışma istatistikleri mevcuttur ve müşteri bunlardan nasıl bir fayda sağlar? *İyi işleyen bir danışma masası çözülmemiş problemlerin bulunması riskini azaltır. Mali sistemlerle ilgili problemler analiz edilmeli ve bir an önce üzerlerine eğilinmelidir.*		
5.10 Kuruluş, yetkisiz kişilerin program kaynak kütüphanesindeki programlara erişerek değişiklik yapmalarını nasıl engeller? *Yetersiz kontroller, mali programlar üzerinde rastlantısal, kasıtlı ya da hileli olarak izinsiz değişiklikler yapılması riskini arttırır.*		

B6. İşin Sürekliliğinin Planlanması

Denetlenen kurum, bilgisayarın işleyişinin bozulması durumunda, işlemlerin devam etmesi için uygun planlara sahip olduğunu güvence altına almalıdır. Sürekliliğin planlanmasının derecesi, BT bölümünün ölçeğine ve bilgisayar işleyişinin bağımsızlığına dayanır. BT kapasitesinin belirgin ve uzun süreli bir kaybı, mali tabloların kullanılmaz hale gelmeleri ya da yanlış ifade edilmeleri riskini artırabilir.

B6. İşin Sürekliliğinin Planlanması		
	Yorumlar	Çalışma Kağıdı
6.1 Yönetim bir iş süreklilik planı hazırlamış mıdır? Bu plan mali sistemleri kapsıyor mu? • Bu planın varsayımları ne kadar makul dur? • Belgeleme yeterli midir?		

B6. İşin Sürekliliğinin Planlanması

	Yorumlar	Çalışma Kağıdı
• Bu plan hangi sıklıkla gözden geçirilmektedir? • Bu plan, son olarak ne zaman test edilmiştir? • Yeterince kapsamlı mıdır? • Yönetim işlemlere devam edilmeye başlanmasının ne kadar zaman alacağını düşünmektedir? • İşlem kaybının sonuçları neler olacaktır? *Yetersiz süreklilik planlaması, bir hasar durumunda, işlemlerin yeniden kurulması için gereken zamanı arttıracaktır. Bu, hesapların eksik kalmasına sebep olabilir ve kuruluşun çalışmasını etkileyebilir.*		
6.2 Kurumun yedekleme yöntemleri nelerdir? • Veri dosyalarının ve programların kopyaları düzenli olarak (günlük / haftalık) alınıyor mu? • Bunlar ne kadar sürede bir sistemden çıkarılır? • Yöntem ve işletime ilişkin el kitapları ile hasar düzeltme planının kopyaları da sistem dışında mı saklanmaktadır? Bunlar yeteri kadar korunmakta mıdır? *Yetersiz yedekleme politika ve yöntemleri, kurumun yeterli bir demetim izi bulunduramayacak olması riskini arttırır.*		
6.3 Yedekleme disket ve kasetleri, yeteri kadar korunmakta mıdır? *Yedeklerin emniyetsiz şekilde saklanması , veri kaybına ya da izinsiz değişikliklere yol açabilir. Yeterli güvenlik ölçümleri benimsenmelidir.*		
6.4 Hasar telafi planı, mikro bilgisayar olanaklarının yedekleme ve yenilenmelerini ne kadar kapsamaktadır? *Mikro bilgisayarlar, işin sürekliliğinin planlanmasında, sık sık unutulur. Bunlar, denetim için vazgeçilmez olan veriler ya da mali modelleri barındırıyor olabilir.*		
6.5 Plan, BT altyapı sistemini ne kadar kapsamaktadır? Bu kaysam yeterli midir? Örneğin, • İletişim / ağ • İşlemler • Güç, aydınlatma, v.b. • Güvenlik		

B6. İşin Sürekliliğinin Planlanması		
	Yorumlar	**Çalışma Kağıdı**
• Personel / büro yerleşme düzeni • Sistemin belgelenmesi *Süreklilik planları BT altyapı sisteminin yeterli derecede kapsanması konusunda, sık sık başarısız olur. Eğer, uygun iletişim araçları, terminaller, yazıcılar, v.b. bulunmuyorsa, yenileme işlemciliği yapabilen uzaktaki bir sistemin faydası kısıtlı olur.* 6.6 Önemli personele ne derece güvenilmektedir? *Önemli personelin bulunmaması, mali BT sistemlerinin kullanılabilirliğini azaltabilir. Bunların varlığına denetim sırasında da ihtiyaç duyulabilir.*		

B7. Dış Bilişim Teknolojisi Servis Tedarikçilerinden Yararlanma

Denetlenen kuruluşlar, üçüncü şahıs BT servis tedarikçilerinden, pazar araştırması, kaynakların dışarıdan sağlanması ve olanakların yönetimi gibi şekillerde, giderek daha fazla yararlanmaktadırlar. Kuruluş, dış denetçinin ihtiyaçlarını, göz önünde bulundurmuş olmalıdır. Üçüncü şahıslarca sağlananların, önemli derecede yanlış ifade edilmiş olmadığına dair güvencemiz olmalıdır. Bu güvence normalde, üçüncü şahsın direkt olarak denetlenmesiyle ya da başka bir denetçi tarafından doğruluğunun belgelenmesine dayanılarak sağlanır.

B7. Dış Bilişim Teknolojisi Servis Tedarikçilerinden Yararlanma		
	Yorumlar	**Çalışma Kağıdı**
7.1 Kuruluş, dış servis tedarikçilerinin performansını nasıl gözlemler? • Emniyet • Kalite *Yetersiz gözetim yanlış ya da eksik işlemlerin tespit edilmemesi riskini arttırır* 7.2 Bir sözleşme ve /veya hizmet düzeyi anlaşması var mıdır ve eğer varsa, bunlar tüm önemli konuları kapsamakta mıdır? Örneğin, • Performans (SLA'lar) • Emniyet • Verilerin mülkiyeti		

B7. Dış Bilişim Teknolojisi Servis Tedarikçilerinden Yararlanma		
	Yorumlar	**Çalışma Kağıdı**
• Müşteri veri erişimi • **Denetim Erişimi** • Servisin elde edilebilirliği • Olasılık planlaması *Denetlenen kurum, sözleşmeyi gereksinim duyulan kontrollerin (hangi denetim izinin bulunması gerektiği) resmi olarak belirlenmesi için kullanmalıdır.*		
7.3 Üçüncü şahıs işlemlerinin doğru ve tam olduğunun güvence altına alınması için ne tip önlemler alınmıştır? *Üçüncü şahıs servis tedarikçilerinin işlemleri tam ve doğru olarak tamamladığı güvence altına alınmalıdır. Denetçi, inceleme haklarını kullanarak ya da bağımsız üçüncü şahıs teminatı sağlayarak, ilk elden güvence sağlama ihtiyacını hissedebilir.*		

B.8. Operasyonel Kontroller

İşlemsel kontroller, bir bilgisayar departmanında, uygun olmayan bilgisayar kullanımı pratiklerinin benimsenmesi riskini azaltır. Uygun olmayan çalışma pratikleri denetimi,mali tabloların hazırlanması için sorgulamak şeklinde etkileyebilir. İşlem ortamındaki zayıflıklar, izinsiz programların çalıştırılması ve mali veriler üzerinde değişiklikler yapılması şeklinde suistimal edilebilir.

B.8. Operasyonel Kontroller		
	Yorumlar	**Çalışma Kağıdı**
8.1 Bilgisayar departmanının, kuruluşun geri kalanıyla, hizmet düzeyindeki bir anlaşması var mıdır, örneğin, sistem kullanıcıları? SLA kullanılabilirliğini, hizmet standartlarını v.b. kapsamakta mıdır? *Bilgisayar işlemleri mali verilerin sürekli ve tutarlı olarak işlenmesini sağlamalıdır. SLA'lar gözetimi kolaylaştırır.*		
8.2 Bilgisayar işlemleri ve sistemleri, personelin yeteri kadar gözlemlenmesini ne derece sağlamaktadır? Ne tip gözetim yöntemleri mevcuttur?		

B.8. Operasyonel Kontroller

	Yorumlar	Çalışma Kağıdı
Bilgisayar operatörleri üzerindeki yetersiz kontroller, izinsiz faaliyetler riskini arttırır. Gözlemlenmeyen operatörler, sistemin sağladığı kolaylıklardan yararlanarak verilerde izinsiz değişiklikler yapabilirler.		
8.3 İşlem personeli ne tip eğitime ve deneyimlere sahiptir?		
Yetersiz deneyim ve eğitim, bilgisayar departmanında hataların yapılması riskini artırır. Hatalar sistemin çökmesinden bir dönemin verilerinin silinmesine kadar değişik şekillerde sonuçlanabilir.		
8.4 Kuruluşun bilgisayar bakımı ne derece uygundur? Örneğin, firma içinden yada dışarıdan bakım		
Donanımın yetersiz bakımı elde hazır bulundurma yönünden problemlere yol açabilir. Sistem arızaları, hatalı verilere sebep olabilir.		
8.5 Bilgisayar ne tip işlem kütükleri üretir? Bunlar, nasıl kullanılır? Örneğin, • Alışılmadık ya da yetki dışı faaliyetlerin tespiti • Güçlü imkânların kullanımının gözetimi		
İşlem tarihçe kütükleri yetki dışı faaliyetler riskini azaltabilir. Bunlar, aynı zamanda, işlem hatalarının kapsamının belirlenmesinde de kullanılabilir.		
8.6 Prosedürler ne derce uygun belgelenmiştir? Örneğin, • Gözetmen prosedürleri • Görev işlem prosedürleri • İşletim prosedürleri • Olayların yönetimi • Disket ve kasetlerin idaresi		
Zayıf ya da eksik belgeleme, sistemin elverişsizliği, veri bütünlüğünün kaybı ya da sistem bozulmalarının düzeltilmesinde gecikmeler gibi problemlere yol açabilir.		
8.7 Kuruluşun bir BT ağı yöneticisi var mıdır? Ağın gözetimi için ne tip faaliyetler yürütülmektedir? Örneğin, • Güvenlik • Performans		

B.8. Operasyonel Kontroller		
	Yorumlar	**Çalışma Kağıdı**
Yetersiz ağ yönetimi, kuruluşu, veri bütünlüğü açısından iç ve dış tehlikelere karşı korunmasız bırakır. Güvenliği zayıf olan bir ağ, örneğin, bilgisayar virüslerinin yayılmasına karşı duyarlı olabilir.		

B9. Son Kullanıcı Bilgisayar İşlemleri

Kuruluşlar, mali verileri, örneğin, hesap tablolarını kelime-işlem raporlarını ve masa üstü yayınlarını, yönetmek ve sunmak için son kullanıcı hesaplama paketlerinden giderek artan ölçüde yararlanmaktadırlar. Bu tip paketlere daha düşük düzeyli bir dikkat gösterilmesi ve kontrol uygulanması eğilimi vardır ve sonuç olarak sık sık hatalar ortaya çıkar. Denetçi bu paketler aracılığıyla yapılan özetlemenin ve yönetim sonrası elde edilen tüm mali verilerin orijinal çıktı ile uyumlu olabilmesini güvence altına almalıdır.

B9. Son Kullanıcı Bilgisayar İşlemleri		
	Yorumlar	**Çalışma Kağıdı**
9.1 Kuruluşun uygun son kullanıcı hesaplaması politikaları var mıdır? Bunlar, aşağıdakileri kapsamakta mıdır? • Yetkili donanımın kullanımı • Yetkili yazılımın kullanımı • Güvenlik gereksinimleri • Belgeleme • Verilerin ve programların yedeklenmesi • Test • Virüs koruması • Yazılım hırsızlığı ve kopyacılık • Sağlanan kolaylıklar ve PC araçları *Yetersiz politikalar verilerin kaybını ve bozulması riskini arttırır. İzinsiz yazılımların kullanımı bir kurumun BT'sini bir süre için kapatabilme yetkisi bulunan Yazılım Hırsızlığını Önleme Federasyonunun dikkatini çekebilir.*		
9.2 Tüm raporlar, programlar ve hesap tablosu modelleri aktif bir ortamda kullanılmadan önce yeteri kadar test edilmiş midir? *Yeterli belgeleme, denetim izinin belirlenmesine yardımcı olabilir. Bu aynı zamanda paketin planlandığı şekilde işlediğine dair güvence sağlar.*		

Bölüm C : Uygulama kontrolünün gözden geçirilmesi ve hesap alanı risk değerlendirmesi

Amaç : BT'nin gözden geçirilmesi faaliyetinin bu bölümünün amaçları şunlardır:

a) Yüklemenin gözden geçirilmesiyle edinilen müşterinin bilgisayar sistemi hakkındaki bilgiye dayanmak; (Bölüm C)

b) Mali denetçinin, her bir mali uygulamada işleyen tüm prosedürleri ve kontrolleri tanımlamasını, belgelemesini ve değerlendirmesini sağlamak;

c) Denetçinin, her bir uygulamaya bağlı denetim riskinin genel düzeyini belirlemesini sağlamak; ve

c) Hem uygunluk hem de maddi test programlarının tasarımını etkileyebilecek özel riskleri tanımlamak;

C1. Bilgisayara Dayalı Mali Uygulamanın Tanımlanması

	Yorumlar	Çalışma Kağıdı
1.1 Uygulamanın adı		
1.2 Uygulama hangi mali fonksiyonları yerine getiriyor? Örneğin satışlar / satış defterleri, kasa defteri, bordro		
1.3 Uygulama hangi donanım temelinde çalışıyor? (bölüm A bölüm 4.4 Bak)		
1.4 Uygulama hazır mı yoksa ısmarlama mı?		
1.5 Uygulama ne zaman satın alınmış ve ömrünün ne kadar olacağı tahmin ediliyor?		
1.6 Uygulamanın sahibi / sorumlusu / yöneticisi kimdir?		
1.7 Kullanıcılar kimlerdir? • Gruplar • Konumlar • Sayılar		
1.8 Uygulama bir yılda hangi hacimde ve hangi değerde işlem yapar?		
1.9 Uygulamanın bilinen zaafları ya da problemleri var mıdır? Örneğin; • Geçmiş denetim deneyimi • Aynı uygulamaya sahip kuruluşları olan başka denetçiler		

C1. Bilgisayara Dayalı Mali Uygulamanın Tanımlanması		
• Kuruluşun geçmişe ait bilgileri • Bilinen muhasebe paketleri için rehberler • İç denetim raporları	**Yorumlar**	**Çalışma Kağıdı**

C2 Denetlenebilirlik		
2.1 Uygulamanın detaylı şekilde gözden geçirilmesinde önce, denetçi sistemin denetlenebilir olup olmadığını değerlendirmelidir. Denetçi aşağıdakilerin bulunup bulunmadığını kontrol etmelidir: • Tüm muhasebe dönemi için tam işlem kayıtları • Bir denetim izinin varlığı *Eğer kayıtlar tam ya da denetim izi yeterli değil ise, denetçinin yeterli sayıda ilgili ve güvenilir denetim kanıtı toplaması mümkün olmayacaktır. Bu gibi durumlarda, denetçi bilgisayar işleminde denetim yapmak zorunda kalabilir.*	**Yorumlar**	**Çalışma Kağıdı**

C3. Bilgisayar Destekli Denetim Tekniklerinin Kullanımı		
3.1 Uygulama bilgisayar destekli denetim teknikleri kullanılarak incelenebilecek mali veriler üretiyor mu? Uygulama tüm mali dönem için işlem raporları üretebilir mi? 3.2 Gereken veri dosyaları, dış denetim yazılımı tarafından yapılacak sonraki bir sorgulama için kullanılabilir bir formatta indirilebilir mi (örneğin ; IDEA, Excel) ? Denetçilerin daha geniş yardım için kendi bölümlerinin bilgisayar destekli denetim teknikleri ekibine başvurmaları gerekebilir. 3.3 Örnek kaynaklar defter- i kebirlere, mizan ve mali tablolara mutabık kılınabilir mi? 3.4 Uygulama doğal denetim modüllerine sahip mi? Eğer sahip ise, bunlar dış denetçi tarafından denetim güvencesi sağlanması amacıyla kullanılabilir mi?	**Yorumlar**	**Çalışma Kağıdı**

C4. Uygulamanın Belgelenmesi

Amaç : Yeterli sistem belgesinin sağlandığından emin olunması. Yeterli belgelemenin aşağıdaki faydaları vardır:

- personelin hata yapma riskini azaltır;
- personel için eğitimi kolaylaştırır;
- yazılımın daha kolay şekilde muhafazasına ve geliştirilmesine imkân sağlar;
- denetçinin sistemi kavramasına destek olur.

C4. Uygulamanın Belgelenmesi	Yorumlar	Çalışma Kağıdı
4.1 Uygulamanın belgelenmesi yeterli midir? Kapsamlı ve güncel midir? Belgeleme aşağıdakileri kapsar mı? • Bir sistem incelemesi • Program tarifleri • Girdi / çıktı tarifleri • Veri tabanı / veri sözlüğü tarifleri • Kontrol yöntemleri *Yetersiz belgeleme personelin hata yapma riskini arttırır. Ayrıca uygulamanın işlemi planlandığı gibi yürütmesi riski de artar.*		
4.2 Yeterli sayıda personel ilgili belgelerin kopyalarına sahip midir? *Belgeleme, düzenli sistem kullanıcılarınca elde edilebilir olmalıdır. Kullanıcı kılavuzunun tek kopyası finans bölümü müdürünün kitaplığında kilitli ise, belgelemenin pek yararı olmaz.*		
4.3 Günlük sistem kullanıcıları problemlerle karşılaştıklarında hangi rehbere başvurmaktadırlar? *Standart kılavuzlar genelde kullanıcılara pek yardımcı olamaz. Bunlar kullanıcı talimatları ile birleştirilmelidir.*		
4.4 Hasar telafi amacıyla uygulama belgelerinin yedek kopyaları bulunduruluyor mu? *Yedek kopyalar bulundurulması, sürekli sistem gelişimine ve işlemlerin daha çabuk geri alınmasına imkan sağlar.*		

C 5. Uygulama Güvenliği : Fiziksel ve Mantıksal Erişim

Amaç : Girdi verilerinin, kalıcı verilerin ve çıktı raporlarının, kesinliğini tamlığını ve elde edilebilirliğini garantilemek. BT'nin gözden geçirilmesinin C Kısmının bu bölümü her uygulamada işleyen kontrolleri göz önünde bulundurarak denetçinin genel BT ortamındaki erişim kontrolleri üzerindeki değerlendirmesini ekler. İyi uygulama kontrolleri aşağıdakileri gerçekleştirmek için kullanılabilir:

- işlem verilerinin ve kalıcı verilerin bütünlüğünün, özel uygulama fonksiyonlarına ve verilerin sadece yetkili kullanıcıların erişimine olanak sağlanarak, güvence altına alınması;
- görevlerin ayrımının, bireysel kullanıcılara farklı ayrıcalık düzeyleri ve menüler tahsis edilerek sağlanması; ve
- işlemlerde şifreleri kaydedilerek, kullanıcıların işlemleri için sorumlu kılınması.

C5. Uygulama Güvenliği; Fiziksel ve Mantıksal Erişim	Yorumlar	Çalışma Kağıdı
5.1 Bilgisayar terminallerine yetki dışı erişimin engellenmesi için ne tip fiziksel önlemler vardır? Örneğin: • Finans bölümüne, • Personel bölümüne, • Stoklara ve kalıcı bölümlere sınırlı erişim *Yetersiz fiziksel kontroller, donanım hasarları, hırsızlık ve mali veriler yetki dışı erişim riskini arttırır.*		
5.2 Bu özel uygulamaya erişimin kısıtlanması için ne tip mantıksal erişim kontrolleri kullanılır? • Uygulamaya özel kayıt ve şifreler • Kısıtlı uygulama menüleri • Her uygulama için kullanıcı profilleri (erişim düzeyleri) • Bilinen / yetkili kullanıcılar *İyi tasarlanmış mantıksal erişim kontrolleri, yetki dışı erişim verilerin değiştirilmesi ve silinmesi riskini arttırır. Mantıksal erişim kontrolleri görevlerin ayrımının gerçekleşmesinin sağlanması için kullanılabilir.*		
5.3 Kuruluşun yetkili uygulama kullanıcılarına ait güncel listeleri ya da çizelgeleri var mıdır? Bu listeler ayrıcalıkları da içermekte mi? (kopyaların edinilmesi) *Modası geçmiş kullanıcı listeleri personelin görev gereklerini aşan ayrıcalık düzeylerine erişim sağlaması riskini arttırır.*		

C5. Uygulama Güvenliği; Fiziksel ve Mantıksal Erişim		
	Yorumlar	**Çalışma Kağıdı**
5.4 Bir uygulamaya erişildiğinde, kullanıcıların faaliyetlerinin kısıtlanması için ne tip mantıksal kontroller vardır? Örneğin, kısıtlı menüler. *Bir uygulamadaki kontrol edilmemiş erişim, ayrılmış görevlerin atlanması için istismar edilebilir. Kısıtlanmamış erişim aynı zamanda, kullanıcıların hata yapmaları ya da kendilerine verilen yetkiyi aşmaları riskini arttırır.*		
5.5 Uygulama kullanıcılarının eklenip /kaldırılmaları için ne tip yöntemler vardır? Kullanıcılar kim tarafından yönetilirler ve nasıl kontrol edilirler? *Yetersiz prosedürler, yetkisiz kullanıcıların uygulamaya erişmeleri riskini arttırır. Örneğin, personel ve uygulama yöneticisi arasındaki zayıf iletişim uygunsuz erişim sağlayan personelin işten çıkarılması sonucunu doğurabilir.*		
5.6 Uygulamada, bireysel kullanıcıların işlemlerinin tanınması için ne tip kontroller vardır? • Tek kullanıcı adlarının kullanımı • Denetim tarihçe kütüklerinin üretilmesi • Elektronik imzaların kullanımı *Bireysel olarak tanınabilen ve işlemleri için sorumlu tutulabilen kullanıcıların hata yapmaları ya da yetki dışı işlemlerde bulunmaları olasılığı daha azdır.*		
5.7 Bireysel kullanıcıların işlemlerinin gözden geçirilmesi için nasıl bir uygulama yapılmaktadır? Örneğin, denetim kütüklerinin yönetimce incelenmesi. *Kullanıcı kütükleri eğer sadece yönetim tarafından düzenli olarak gözden geçiriliyorsa, faydalıdır. Eğer ortaya çıkardıkları uyumsuzlukların farkına varılmazsa ya da bunlara karşı bir şey yapılmazsa denetim kütüklerinden elde edilebilecekler çok kısıtlıdır.*		
5.8 Denetim kütükleri, yetki dışı değişiklikten yeteri kadar korunuyor mu? Örneğin, • Kütüklerin şifrelenmesi • Yazma korumalı kütükler • Kütüklerin korunan dizinlerde saklanması		

C5. Uygulama Güvenliği; Fiziksel ve Mantıksal Erişim		
	Yorumlar	**Çalışma Kağıdı**
Yönetim sadece değişiklikten uygun şekilde korunmuşlarsa denetim raporlarına güvenebilir. Koruma, şifreleme ya da denetim kütüklerinin korunmuş bir dizine yazılması şeklinde sağlanabilir.		

C6. Girdi Kontrolleri

Amaç : Tüm girdi işlem verilerinin kesin tam ve yetki dahilinde olduğundan emin olunmasıdır. Veri girişleri üzerindeki kontrol, manuel ve bilgisayara dayalı uygulama kontrollerinin bir kombinasyonu ile sağlanabilir. Ortak manuel kontroller şunları içerebilir : Girdi belgelerinin fiziksel olarak iptali, imzaların yetkili imza listesine göre kontrol edilmesi, hatalı girdiler için uygulanan yöntemler ve girdi belgelerinin yönetim tarafından gözden geçirilmesi. Bilgisayara dayalı kontroller şunları içerebilir : Sıra kontrolleri, düzenleme kontrolleri, otomatik denkleştirmeler ve istisnaların rapor edilmesi.

C6. Girdi Kontrolleri		
	Yorumlar	**Çalışma Kağıdı**
6.1 Veri girişinin yetki dahilinde ve doğru olduğundan emin olunması için ne tip yöntemler /kontroller vardır? Örneğin, • Yetkili kullanıcı listeleri • Standart giriş biçimleri • Biçim kontrolleri • Sıra kontrolleri • Makullük kontrolleri • Bağımlılık kontrolleri • Kontrol rakamlarının kullanımı *Yetersiz giriş kontrolleri, hatalı ya da hileli veriler işlem için girdi olarak kullanılması riskini arttırır.*		
6.2 İşlemlerin çift girilmesini engellemek için ne tip önlemler alınmıştır? • Ayrı referans numaralarının kullanılması • Kaynak belgelerin fiziksel olarak imhası • Çift girdinin mantıksal olarak reddi Çift işlem denetimi riskinin azaltılması için manuel ve/veya bilgisayar kontrolleri bulunmalıdır.		
6.3 Personel, tüm geçerli işlemlerin girildiğinden nasıl emin olur? Tüm girdi belgelerinin alındığından emin olunması için ne tip kontroller bulunmaktadır? Örneğin tamlık ve kesinlik kontrolleri.		

C6. Girdi Kontrolleri		
	Yorumlar	**Çalışma Kağıdı**
• Grup toplamları • Karışık toplamlar • Sıra kontrolleri *Tamlık ve kesinlik kontrolleri eksik ya da mevcut olmayan girdi verilerinin bulunması riskini azaltır.*		
6.4 Reddedilen işlemler için ne tip yöntemler uygulanır? *Yetersiz yöntemler eksik mali tabloların bulunması riskini arttırır.*		
6.5 Veri girdilerinin izlenmesi için yönetim tarafından hangi işlemler yapılmaktadır? *Yönetimin girdileri izlemesi ve gözden geçirmesi, yetki dışı veri girişi riskini azaltır. Yönetimin incelemesi, aynı zamanda, kullanılmasına karar verilen girdi yöntemlerinin izlendiğinden emin olunmasını sağlar.*		
6.6 Verilerin girilmeden önce dönüştürülmeleri gerekiyor mu? Eğer gerekiyor ise, dönüştürülen girdilerin kesin ve tam olduğundan emin olunması için ne tip önlemler alınır? *Bir bilgisayar sisteminden transfer edilen verilerin, bir diğerine girilmeden önce dönüştürülmeleri gerekebilir. Yetersiz dönüşüm kontrolleri yanlış ya da eksik işlem verilerinin bulunması riskini arttırır.*		

C 7. Verilerin İletim Kontrolleri

Amaç : Dar ya da geniş alan ağları üzerinden iletilen verilerin geçerli, kesin ve tam olduğundan emin olunması. Ağ kullanan kuruluşlar, veri kaybı yetki dışı işlemler ve verilerin bozulması riskini, kabul edilebilir bir düzeye indirmek için yeterli kontrollerin bulunduğunu güvence altına almalıdırlar

C 7. Verilerin İletim Kontrolleri		
	Yorumlar	**Çalışma Kağıdı**
7.1 Verilerin transferi için ağlar, disketler ya da kasetler kullanıldığında, müşteri verilerinin transferinin0hem tam hem de kesin olduğundan nasıl emin olur? Örneğin;		

C 7. Verilerin İletim Kontrolleri		
	Yorumlar	**Çalışma Kağıdı**
• Dijital imzaların kullanımı • Verilerin şifrelenmesi • İşlemlerin sıralanması *Yetersiz kontroller eksik, yanlış, bozuk ya da hileli işlem riskini arttırır.*		
7.2 Kuruluş elektronik veri değişimi (EDI) teknolojisinden faydalanmakta mıdır? Eğer faydalanıyor ise, ilişkili riskler teşhis edilmiş ve üzerlerinde düşünülmüş müdür? Not : EDI elektronik fonların BACS, CHAPS v.b. aracılığıyla transfer edilmesini kapsayabilir. *EDI'nin kullanımı denetçiyi, daha fazla denetim riskiyle karşı karşıya bırakır. EDI'nin çok fazla kontrol problemi bulunmaktadır ve kullanımı belirgin olduğunda, denetçinin, bir Sayıştay BT denetimi uzmanına danışması gerekir.*		

C 8. İşletim Kontrolleri

Amaç: geçerli girdi verilerinin kesin ve tam olarak işlendiğinden emin olunması. İşlem kontrolleri, orijinal girdi verilerine ve ek olarak oluşturulan verilere uygulanmalıdır. İşlem kontrolleri, aynı zamanda işlem sırasında, veriler üzerinde, kazara, kasıtlı ya da hileli olarak yapılan değişikliklerin teşhis edilmesi ve önlenmesi için de tasarlanmalıdır.

C 8. İşletim Kontrolleri		
	Yorumlar	**Çalışma Kağıdı**
8.1 Tüm işlemlerin yürütüldüğünden emin olunması için ne tip kontroller bulunmaktadır? Örneğin. • Girdi/çıktı mutabakatı • Sıra kontrolü • Kontrol toplamları *İşlem verileri üzerinde yetersiz kontroller, eksik, hatalı ya da hileli işlemlerin yürütülmesi riskini artırır*		
8.2 Doğru dosyaların işlendiğinden emin olunması için ne tip kontroller vardır, örneğin, bordro akışları haftalık BACS akışları, v b ? Kontroller, yapı gereği, fiziksel ya da mantıksal olabilir. Örneğin,		

C 9. Çıktı Kontrolleri	Yorumlar	Çalışma kağıdı
9.1 Bilgisayar çıktılarının (yazıcı çıktıları, çekler, faturalar, alım emirleri. vb.) doğru şekilde saklandıklarının ve gönderildiklerinde uygun yerlere ulaştıklarının güvence altına alınması için kontroller var mıdır? *Yetersiz kontroller, işletimdeki hataların yönetimin dikkatine sunulmama riskini artırır.*		
9.2 Bilgisayar kırtasiyesinin saklanmasına ilişkin uygun kontroller var mıdır? Örneğin, • ödeme emirleri • yazılım lisansları *Yetersiz kontroller, hileli faaliyetlerin ve eksik muhasebe kayıtlarının bulunması riskini arttırır.*		
9.3 Çıktı üzerinde hangi uygunluk, kesinlik ve tamlık kontrolleri yapılmaktadır? Örneğin, ardışık sayfa0numaraları, çalışmadan çalışmaya kontroller *Bu kontroller , işlem hatalarını ve/veya yetkisiz olarak yapılan işlemleri tespit etmek için kullanılır.*		
9.4 BACS kasetlerinin ve diğer elektronik fon transferi (EFT) kayıt ortamlarının üretiminde , saklanmasında ve taşınmasında uygun kontroller uygulanmakta mıdır? Kontroller yürürlükte rehber ile uyum halinde midir? Yetersiz kontroller yetki dışı ödemelerin yapılması riskini artırır.		

C 10. Ana dosya ve kalıcı veri kontrolleri

Amaç : Ana dosyaların ve kalıcı verilerin bütünlüğünün ve kesinliğinin güvence altına alınması. Ana ve kalıcı veri dosyalarında saklanan bilgiler, genelde, mali verilerin işlenmesi de ve rapor edilmesinde önemli bir rol oynar. Ana dosyalardaki bilgiler, pek çok ilgili mali işlemi etkileyebilir ve bu sebeple yeterli şekilde korunmalıdır. Örneğin, bir bordro sisteminde, bir verginin ya da ulusal sigorta oranının değiştirilmesi tüm çalışanların ödemelerini etkileyebilir. Kalıcı verilerin yaygın tipleri, hesap çizelgelerini, bordro detaylarını, satıcı ve müşteri detaylarını, genel masraflarla ilgili bölüm oranlarını ve ürün fiyat listelerini içerir.

C 10. Ana dosya ve kalıcı veri kontrolleri	Yorumlar	Çalışma Kağıdı
10.1 Kalıcı veriler üzerindeki değişikliklerin izine bağlı olmaları gerekir mi? Bu izin nasıl alınır? *Yetersiz kontroller, kalıcı veri üzerinde izinsiz değişiklikler yapılması riskini artırır. İzinsiz değişiklikler birden çok hatalı ya da hileli işlemler şeklinde sonuçlanabilir.* **10.2** Kalıcı verilere izinsiz erişimin ve bunların izinsiz olarak değiştirilmesinin engellenmesi için ne tip kontroller bulunmaktadır? *Kuruluş içi mantıksal erişim kontrolleri, erişimin sadece yetkili personel için mümkün olacak şekilde sınırlanması için kullanılabilir. Bunlar, izinsiz değişiklik riskini azaltır.* **10.3** Uygulama ne tip iç düzenleme araçlarına sahiptir? Kontrol edilen bu araçların kullanımı nasıldır? *Düzenleme araçlarına kontrol edilmemiş erişim, izinsiz değişiklik riskini arttırır.* **10.4** Kalıcı veriler üzerindeki izinsiz değişliklerin tespiti için kontroller mevcut mudur? Örneğin, • Kontrol toplamları • Diğer kalıcı veri kaynakları ile mutabakat • Yönetim tarafından düzenli kontrol *İzinsiz değişiklikleri belirleyen iç kontroller, tespit edilmemiş değişiklerin bulunması riskini azaltır.*		

Ek 4
Bilişim Teknolojisi Kontrol Ortamının Gözden Geçirilmesi ve Kurumun Risk Değerlendirmesi

Ek 4'ün İçindekiler

Giriş

1.1 Bir BT kontrol ortamı incelemesinin amacı, bir kurumun BT olanaklarında bulunan kontrollerin, prosedürlerin ve risklerin incelenmesi ve değerlendirilmesidir. Bir uygulamanın incelenmesi (EK 5) her uygulamanın işlemlerin bütünlüğü ve elde edilebilirliği üzerinde yoğunlaşırken, BT kontrol ortamının bir incelemesi, mali programların ve uygulamaların bütünlüğünü ve elde edilebilirliğini sağlayan kontrolleri değerlendirir.

1.2 BT kontrol ortamı terimi, bilgisayar donanımı, sistem yazılımı ve çalışma ortamını kapsar. Bir BT donanımının boyutu, çok sayıda bilgisayar personelinin bulunduğu özel amaçla yapılmış bir binadaki büyük bir ana bilgisayardan, bir maliye bürosunun bir köşesindeki bir tek ayrı kişisel bilgisayara (PC) kadar değişebilir.

1.3 BT kontrol ortamı, aşağıdakiler için yeterli kontrollere sahip olmalıdır :

- güvenli ve düzenli bir veri işleme ortamı;
- programların ve bunların temeli olan veri dosyalarının izinsiz erişimden, değişiklikten yada silinmeden korunması; ve
- bilgisayar işlemlerindeki bir aksaklığın, şirketin denetlenmeye hazır mali tablolar hazırlama yeteneğini kaybetmesine sebep olmadığını garanti altına alma

1.4 Bu ekte bulunan donanım kontrolleri üzerine detaylı rehber, BT incelemesinin B kısmının formatındadır. Bölümler aşağıdaki şekilde ele alınmıştır:

- genel politika, yönetim ve kontrol;
- görevlerin ayrımı;
- fiziksel erişim kontrolleri;
- mantıksal erişim kontrolleri;
- değişiklik yöntemi kontrolleri;
- iş sürekliliğinin planlanması;
- dış BT hizmeti sağlayıcılarının kullanımı;
- işletme ile ilgili kontroller; ve
- son kullanıcı bilgisayar işlemleri.

1.5 Denetçi, her bilgisayar donanımı için hangi kontrollerin uygun olacağına karar vermelidir. Bir BT kontrol ortamını denetlerken denetçi, kuruluşun faaliyetinin niteliği, BT departmanının boyutu, yaşanmış sorunlar ve bilgisayar sistemlerine ne kadar güvenildiği de dahil olmak üzere çeşitli faktörleri hesaba katmalıdır.

1.6 Denetçi genel BT ortamı hakkında bilgi almak için gerekli personel ile görüşmeler ya da tartışmalar yapabilir, sistem dökümlerini yeniden inceleyebilir, iç denetim ile birlikte çalışabilir ve direkt gözlem yapabilir.

Genel politika, yönetim ve kontrol

2.1 Kontrol hedefi: yönetimin taahhüdü ve uygun üst düzey BT politikaları ile desteklenmiş güvenli bir bilgisayar ortamı sağlamak.

2.2 BT incelemesinin B kısmının ilk bölümündeki sorular denetçinin tüm bilgisayar ortamını etkileyecek üst düzey politikalar hakkında fikir sahibi olmasını sağlamalıdır. Üst düzey BT politikalarının, stratejilerinin ve prosedürlerinin bir değerlendirilmesi denetçiye daha alt düzeydeki ayrıntılı kontrol sistemlerinin varlığı ve etkinliği konusunda makul bir gösterge sağlar. Deneyim göstermiştir ki, yetersiz BT politikaları olan, iç denetimi bulunmayan ya da konuyla ilgisiz üst yöntemi olan kuruluşlar büyük bir ihtimalle kontrolsüz, yüksek riskli bilgisayar sistemlerine sahiptirler.

Görevlerin ayrımı

3.1 Kontrol hedefi: Bilgisayar departmanı bünyesinde etkin bir görev ayrımı sağlamak.

3.2 Görevlerin yetersiz ayrımı, hataların ortaya çıkması ve fark edilmemesi, sahtekârlıkların ve işlerin uygunsuz bir şekilde yürütülmesinin kanıksanması riskini artırır.

3.3 Hata ve sahtekârlık riskini azalttığı için, görevlerin ayrımı temel bir kontrol gereksinimidir. BT personelinin görevleri bir kişinin işinin diğer bir kişinin işinin kontrolünü içerecek şeklinde düzenlenmelidir. Bu iş tanımlarının oluşturulması ve bu iş tanımlarına uyulması ile sağlanabilir. Bilgisayar sistemleri önceden programlanmış bireysel ve grup güvenlik profilleri aracılığı ile görev ayrımını zorunlu hale getirebilir.

3.4 Görev ayrımının kanıtı iş tanımlarının organizasyon şemalarının kopyasının alınması ile ve BT personelinin faaliyetlerinin gözlenmesi ile sağlanabilir. Bilgisayar sistemlerinin görev ayrımını zorunlu hale getirmek için güvenlik profilleri kullandığı yerlerde denetçi personelin işlevsel sorumluluklarıyla ilişkili güvenlik profillerini ekrandan ya da yazıcı çıktısından takip etmelidir.

3.5 Uygun görev dağılımının sağlanması ve uygulanması imkânı esas olarak BT departmanının boyutuna ve ilgili bilgisayar personelinin sayısına dayanır. Küçük bir bilgisayar departmanında görev ayrımının eksikliği kontrollerin telâfi edilmesiyle giderilebilir, örneğin; düzenli yönetim kontrolleri ve gözetim, denetim izi ve manuel kontrollerin kullanımı. Ne var ki, büyük bir bilgisayar departmanında aşağıdaki BT görevleri uygun bir şekilde ayrılmalıdır:

- sistem tasarımı ve programlaması;
- sistem desteği;
- rutin BT işlemleri ve yönetimi;
- sistem güvenliği; ve
- veri tabanı yönetimi.

3.6 BT departmanında görev ayrımına ek olarak, hem BT hem de mali departmqn görevleri yüklenmiş bir personel bulunmamaktadır. Bilgisayar departmanı hem fiziksel hem de yönetsel olarak finans ve personel gibi son kullanıcılardan ayrı olmalıdır.

Fiziksel erişim kontrolleri

4.1 Kontrol hedefi: bilgisayar donanımını kasten ya da kazaen oluşan hasarlardan, doğal tehlikelerden, izinsiz erişimden ve hırsızlıktan fiziki olarak korumak.

4.2 Bilgisayar donanımı, yangın, su baskını, elektrik kesilmesi, fiziksel hasar ve hırsızlık gibi tehlikelere karşı korunmalıdır. Yetersiz koruma, sistemin kullanabilirliğini ve en sonunda da kuruluşun tam bir mali işlemler kaydı oluşturmasını riske atabilir. Müşteri, hasara açıklığı değerlendirmelidir ve riski kabul edilebilir bir seviyeye indirmek için uygun kontroller oluşturmalıdır.

4.3 Yangın hasarı riski, yangın alarmı ve yangın söndürme donanımı sağlanarak azaltılabilir. Bilgisayar odasının düzenli olarak temizlenmesi ve artıklardan temizlenmesi gibi diğer önlemler yangın hasarı riskini azaltacaktır.

4.4 Su baskını riski büyük ölçüde bilgisayar donanımının bulunduğu yer ile ilgilidir. Borulara ve su depolarına yakın mesafedeki donanım, daha büyük risk altındadır. Mümkün olduğu durumlarda, kuruluşlar bilgisayar donanımının bodrum katında ya da su depolarının hemen altında ya da civarında olmasından kaçınmalıdır. Potansiyel su sızıntılarına karşı BT personelini uyarmak amacıyla otomatik nem dedektörleri kullanılabilir.

4.5 Bilgisayar donanımı, elektrik kaynağındaki dalgalanmalar yüzünden zarar görebilir ya da bozulabilir. Güç dalgalanmaları, bilgisayar sistemlerinin verileri silmesine ya da bozmasına sebep olabilir. Kesintisiz güç kaynakları, sistemin hasar görmesi ve bozulması riskini azaltır ve elektrik kesilmesi sonrasında işlerin aksamadan yapılmasını sağlar.

4.6 Bazı büyük ve eski bilgisayar donanımları, civarındaki sıcaklığı ve nemi düzenlemek için özel çevre kontrolleri gerektirir. Bu kontroller genellikle havalandırma tertibatı şeklinde olur. Son kuşak mikro ya da mini bilgisayarların bir çoğu ofis ortamında çalışmak üzere tasarlanmıştır ve bu sebeple özel ortam kontrollerine ihtiyaç göstermez.

4.7 Fiziksel erişim kontrolleri, yetkisiz kişilerin bilgisayar donanımına erişim riskini azaltır. Denetçi, kuruluşun bulunduğu yere, bilgisayar odalarına, terminallerine, yazıcılarına ve veri saklama ortamlarına erişimi kısıtlayan kontrolleri belirlemelidir. Kuruluş, aynı zamanda temizlikçiler, güvenlik ve bakım personeli yüzünden ortaya çıkabilecek riskleri de göz önünde bulundurmalıdır. Yaygın fiziksel erişim kontrolleri arasında kilitli kapılar, güvenlik kameraları, alarmlar, şifreli kapılar ve koruma görevlileri bulunur.

Mantıksal erişim kontrolleri

5.1 Kontrol hedefi: Mali uygulamaları ve bunların veri dosyalarını izinsiz erişime, değiştirmeye ve silmeye karşı korumak.

5.2 Mantıksal erişim kontrolleri hem donanım hem de uygulama düzeyinde olabilir. Genel BT ortamındaki kontroller, işletim sistemine, sistem kaynaklarına ve uygulamalarına erişimi sınırlandırırken, Ek 5'deki uygulama düzeyindeki kontroller, tek tek uygulamalar bünyesindeki kullanıcı faaliyetlerini kısıtlar.

5.3 Mantıksal erişim kontrollerinin önemi, fiziksel erişim kontrollerinin daha az etkin olduğu yerlerde, örneğin bilgisayar sistemlerinin haberleşme ağlarını kullandığı (LAN'lar Local Area Networks -- Yerel Alan Bilgisayar Ağları ve WAN'lar Wide Area Networks - Geniş Alan Bilgisayar Ağları) durumlarda artar. Yeterli mantıksal erişim güvenliğinin var olması, kuruluşun geniş alan bilgisayar ağlarını (WAN) ve Internet gibi küresel imkânları kullandığı durumlarda özel bir önem taşır.

5.4 Mantıksal veri erişim kontrolleri genellikle, işletim sistemi (örnek: NOVELL Network) ya da kullanılan donanımda bulunan hazır güvenlik imkânlarına dayanır. Ek erişim kontrolleri, tescilli güvenlik programlarının (örnek: IBM ana makinalarında kullanılan RACF, PC'lerde kullanılan Stoplock) uygun bir şekilde kullanımı ile sağlanabilir.

5.5 En genel mantıksal erişim kontrol tipi giriş tanımlayıcısını (kullanıcı adı) takip eden şifre kontrolüdür. Şifrelerin etkin olabilmesi için bütün personelin bildiği ve kullanılmak zorunda olduğu uygun şifreleme politikaları ve yöntemleri bulunmalıdır. Kuruluşlar örnek olarak minimum şifre uzunluğu belirleyerek, şifrelerin düzenli aralıklarla değiştirilmesini zorunlu tutarak ve salt rakamsal şifreleri, kişi isimlerini veya İngilizce sözcüklerde bulunabilecek kelimeleri otomatik olarak reddederek şifre sistemini kendine göre düzenleyebilirler.

5.6 Menü kısıtlamaları uygulamalara ve sistemin yardımcı programlarına erişimi kontrol etmekte etkin olabilir. Sistemler, her bir kullanıcıyı, o kullanıcıya ait ayrı kullanıcı adı ile tanımlayarak ve onlar için önceden belirlenmiş yetki menüleri oluşturarak erişimi kontrol edebilir. Denetçi, menü sistemini atlatarak işletim sistemine ya da diğer uygulamalara sızmanın kullanıcılar için ne kadar kolay olacağını düşünmelidir.

5.7 Bazı bilgisayar sistemleri, dosya izinleri kullanarak uygulamalara ve veri dosyalarına erişimi kontrol edebilir. Bu sadece gerekli erişim iznine sahip kullanıcıların bu dosyaları okuyabileceğini, değiştirebileceğini, silebileceğini ya da çalıştırabileceğini güvence altına alır.

5.8 Önemli riskler, genellikle güçlü sistem ayrıcalıklarına sahip sistem yönetimi personeli tarafından yaratılabilir. Bu "ayrıcalıklı kullanıcılar", varolan sistem kontrollerini aşabilen güçlü yardımcı araçlara erişime sahip olabilir. Yönetim, bu güçlü kullanıcıların faaliyetlerini kontrol etmek için bir takım önlemler ortaya koymalıdır ve eğer mümkünse, sistem yöneticilerinin ayrıcalıklarını, görevlerinin gerektirdiği kadarıyla sınırlandırmalıdır.

5.9 Organizasyonlar, CRAMM (CCTA Risk Analizi ve Yönetimi Metodu) gibi yapılandırılmış güvenlik değerlendirme metodolojileri kullanarak kendi BT güvenliklerini gözden geçirebilirler. Bu metodlar, güvenlik risklerini meydana çıkartmak ve tanımlanmış riskleri kabul edilebilir bir düzeye indirecek güvenlik önlemlerini ortaya koymak için tasarlanmışlardır.

Değişim yönetimi kontrolü

6.1 Kontrol hedefi : mali sistemde yapılacak değişikliklerin uygun olarak yetkilendirdiğinden, test edildiğinden, belgelendiğinden ve bunların istenildiği gibi işlendiğinden emin olmak.

6.2 Yeni ya da değişikliğe uğramış bir bilgisayar sisteminin bütününün, aktif kullanımdan önce son kullanıcılar tarafından test edilmesi halinde hem kuruluşun yönetimi, hem de denetçi, sistemin arzu edildiği gibi çalıştığından emin olabilir. Ne var ki, sistemler nadiren sabit kalır ve sıklıkla değiştirilir ya da güncellenir. Bu düzenli değişiklikler, verimliliği ve işlerliği arttırmak ya da programlama hatalarını ortadan kaldırmak için gerekli olabilir. Muhasebe paket programı üreticilerinin, devam eden bakım kontratlarının bir parçası olarak güncellemeler için ısrar etmesi genelde görülen bir durumdur.

6.3 Bilgisayar sistemlerini güncelleyen organizasyonlar, uygun değişim yönetimi ve ayar yönetimi kontrollerine sahip olmalıdır. Ayar yönetimi prosedürleri BT varlıklarının kontrolü (yeni: donanım, yazılım, belgeleme ve iletişim) ve kayıtların sonradan güncellenmesi anlamına gelirken, değişim yönetimi, yetkilendirme, etki değerlendirmesi, varlık güncellemesi, değişikliklerin test edilmesi ve değişikliklerin uygulanması anlamına gelir. Daha küçük organizasyonlarda, tek bir işlevin hem değişim hem de ayar yönetiminden sorumlu tutulması muhtemeldir.

6.4 Erişim kontrolleri, program ve dosya değişikliklerinin yetkilendirilmesini, kütüğe alınmasını ve izlenmesini sağlamalıdır. Yeni programları kullanıma sunma imkânı, bilgisayar programcılarından ve işlemleri giren ya da kalıcı olan veriyi saklayan personelden bağımsız olan yetkili değişiklik yönetimi personeli ile sınırlandırılmalıdır.

6.5 Denetçi, hızla çoğalan hazır mali uygulamaların, kuruluşun yazılım değişikliklerini kontrol etme, belirleme ve kendi yazılım değişikliklerini yapma imkânını önemli ölçüde ortada kaldırdığından haberdar olmalıdır. Hazır paket programlar, program değişikliklerini sınırlasa da, genellikle kullanıcılara sistemin çalışma şeklini değiştirme imkânı sunar. (örnek: hesap tablolarını, güvenlik ayarlarını değiştirerek ve özel mali raporları oluşturarak ya da değiştirerek)

6.6 Uygun değişim yönetimi kontrolleriyle riskler azaltılabilir. Bu kontroller tüm sistem ve program değişikliklerinin tatmin edici bir şekilde gerekçelendirildiğini, yetkilendirildiğini, belgelendiğini ve test edildiğini ve değişikliklerin yeterli denetim izinin elde edildiğini garanti etmelidir. Bütün değişiklik prosedürleri belgelenmelidir.

6.7 Bilgisayar donanımına, sistem yazılımına ve mali uygulamalara yönelik değişiklikler test edilmeli ve test sonuçları, değiştirilen sistem güncel verileri işlemeye başlamadan kullanıcılar tarafından kabul edilmelidir.

6.8 Kuruluşlar, sistem geliştirmeyi ve uygulama programlamayı kuruluş içinde sürdürebilirler ya da danışmalardan faydalanabilirler. Sistem kullanıcı ihtiyaçlarını karşılayamama durumuna karşı metodolojiler, standartlar ve araçlar geliştirilmiştir. Bunlar:

- PRINCE: Projects IN Controlled Environments-Kontrol Edilmiş Ortamlardaki Projeler: Hükümet tarafından hazırlanan bu metodoloji yönetim bileşenleri (örgüt, planlar ve kontroller) ve proje yönetiminin teknik bileşenleri hakkında rehberlik sağlar. PRINCE özel olarak bilişim sistemi projelerinin yönetimi ile ilgilidir.

- SSADM: The Structured Systems Analysis and Design Methodology-(Yapılandırılmış Sistemlerin Analiz ve Tasarım Metedolojisi) iş ihtiyaçlarının analizi ve yazılım geliştirme için özel olarak tasarlanmış yöntemsel ve teknik standartlardan ve belgeleme standartlarından oluşur.

- CASE araçları: Computer Aided Software Engineering- Bilgisayar Destekli Yazılım Mühendisliği araçları, tasarım özelliklerinin, çalışan bilgisayar uygulamalarına dönüştürülmesine yardımcı olmak için tasarlanmış geliştirme programlarıdır.

6.9 Normal değişim işlemi prosedürleri, acil durum değişikliklerinin gerekli olduğu yerlerde uygun olmayabilir. Bu gibi durumlarda, acil durum değişikliği prosedürleri kullanılmalıdır. Prosedürler, yeterli belgeleme şartlarını, sistem testini ve geçmişle ilgili onaylamaları kapsamalıdır.

6.10 Bilgisayar sistemleri, mali uygulamaların yetkisiz değiştirilmesini önlemek için yeterli kontrolleri içermelidir. Mantıksal erişim kontrolleri, kaynak kodunu program değişikliği araçlarında korumak üzere mevcut olmalıdır.

İş sürekliliğinin planlanması

7.1 Kontrol hedefi: kuruluşun, bilgisayar imkanlarının geçici ya da kalıcı bir kaybı durumunda hala denetlenebilir mali tablolar oluşturabilmesini güvence altına almak.

7.2 BT olanakları için kötü durumların düzeltilmesi planlaması, organizasyonunun genel iş sürekliliği planının bir parçası olarak görülmelidir. Mali denetçi, kuruluşun işi makul bir süre içinde tamamlayabilmesi ve mali tabloların her muhasebe dönemi sonunda tamamlanması ile ilgilenir.

7.3 Bilgisayarlı mali sisteme sahip olan her müşteri, sisteme yönelik tehlikeleri, sistemin zayıflıklarını, işlemlerin kaybının organizasyonun işlerliğine ve denetlenebilir mali tablolar

oluşturma imkânına olan etkilerini değerlendirmelidir. Bundan sonra, riskleri üst düzey yönetim için kabul edilebilir bir seviyeye çekmek amacıyla yeterli önlemler alınmalıdır.

7.4 Kötü durumları düzeltme planlamasının boyutu ve ihtiyaç duyulacak detaylı önlemler önemli ölçüde değişiklik gösterebilir. Ana bilgisayarlar ve karmaşık iletişim ağlarına sahip büyük BT departmanı olan organizasyonlar alternatif mevkilerde yedekleme imkânları sunan çok yönlü ve güncel düzeltme planlarına ihtiyaç duyabilirler. Diğer taraftan basit bir hazır paket kullanan bir masa üstü bir PC'li küçük bir daire ya da bakanlık şeklinde olmayan bir kamu kurumu, daha basit bir plana sahip olacaktır.

7.5 Kötü durumları düzeltme planları belgelenmeli, periyodik olarak test edilmeli ve gerekli görüldükçe güncelleştirilmelidir. Test edilmemiş planlar kağıt üzerinde tatmin edici olabilir, fakat pratikte işe yaramayabilir. Test etmek, yetersizliği açığa çıkartacak ve değişikliklerin yapılmasına imkân sağlayacaktır.

7.6 Yeterli belgelemenin önemi, sorumluluğun büyük bir kısmının BT departmanındaki birkaç önemli çalışanın üzerinde olması durumunda artacaktır. Önemli personelin işten ayrılması, ki bu da muhtemelen bilgisayarların bozulmasıyla aynı sebepten ötürü olacaktır, bir organizasyonun işlemlerini kabul edilebilir bir süre içerisinde tamamlama yeteneğini etkileyecektir.

7.7 Sistem yazılımlarının, mali uygulamaların ve bunların veri dosyalarının düzenli olarak yedek kopyaları alınmalıdır. Yedek kopyalar kuşaktan kuşağa geçirilmelidir. Örneğin: günlük, haftalık, aylık ve üç aylık kasetler kullanarak. Yedek kopyalar kötü durumları düzeltme planının ve sistem belgelerinin bir kopyasıyla bulunulan yer dışında, yangından korunaklı bir yerde saklanmalıdır.

7.8 Mini bilgisayarlara ya da ana bilgisayarlara ek olarak mikro bilgisayarların da kullanıldığı yerlerde denetçi, sabit disklerde saklanan mali verilerin yedeklenmesi için bir takım prosedürlerin bulunduğundan emin olmalıdır.

Şirket dışı Bilişim Teknolojisi servis tedarikçilerinden yararlanma

8.1 Kontrol hedefi: Şirket dışı BT servis tedarikçilerinin güvenli bir işlem ortamı sağladıklarından ve servisin belirli servis sözleşmelerine uygun olduğundan emin olmak. Denetim hedefleri aynı kalır ve BT servislerinin şirket içinden ya da dış servis tedarikçileri tarafından sağlanması durumlarından bağımsızdır.

8.2 Hem kamu hem de özel sektör kuruluşları üçüncü kişiler tarafından sağlanan BT servislerinden artan oranlarda yararlanmaktadırlar. Üçüncü kişiler tarafından yürütülen hizmetler dışardan sağlanan olanaklar ya da bir hizmetin ihale yoluyla üçüncü bir şahsa gördürülmesi şeklinde algılanabilir.

8.3 Denetçi bilgisayar işlemlerinin kesinliği ve tamlığı konusunda teminat verecek yeterli kontrollerin bulunduğundan emin olmalıdır. Bu tip bir güvence, mutabakatlar sağlamak, diğer servis sağlayıcıların çıktı raporlarını gözden geçirmek ve diğer denetçilerin çalışmalarına dayanmak sureti ile elde edilebilir.

8.4 Denetçi denetim yetkileri konusunu gözden geçirme ihtiyacı duyabilir ve bu durumda uygun bir denetim rehberine başvurmalıdır. Denetim yetkileri üçüncü kişi servis tedarikçilerinin mali kayıtların (yani güvenlik ve süreklilik planları) bütünlüğü ve kullanabilirliğini sağlamak amacıyla başvurdukları kontrol ve yöntemleri değerlendirmek amacıyla gerekli olabilir.

8.5. BT servislerinin sağlanması konusunda kabul görmüş standartların bulunması gerekir Nicel ve nitel performans standartları yazılı sözleşmelere ya da servis düzeyi anlaşmalarına dahil edilmelidir. Performans sözleşmedeki standartlar göz önünde bulundurularak düzenli olarak incelenmelidir.

Operasyonel kontroller

9.1 Kontrol hedefi: BT personelinin yeterli olduğundan ve yalnızca izin verilen uygulamaların kullanıldığından emin olmak.

9.2 Yönetim, personelin yetki dahilinde olmayan faaliyetlerde bulunmasını önlemek için yeterli derecede gözetim yapmalıdır. Gerçekte daha küçük bilgisayar sistemlerine sahip bazı kuruluşlar ayrı ayrı tanımlanabilen bilgisayar operatörlerine sahip olamayabilir ve sistem yöneticisi ile sistem operatörünün rolü tek bir kişiye verilebilir.

9.3 Standart işlem prosedürleri belgelenmeli, ilgili personele gönderilmeli ve bu personelce bilinmelidir. İyi hazırlanmış bir operatör talimatnamesi hata riskini azaltacaktır.

9.4 Bilgisayar işlerinin takvime bağlanması gerektiğinde işlemlerin doğru sırada yapıldığından emin olmak için kontroller bulunmalıdır. Örnek olarak ay sonu bordro hesabına başlamadan önce bir "başlat ve git" alt programı çalıştırmak gerekli olabilir. Otomatik iş programlamasının ve iş kontrol prosedürlerinin kullanılması operatör hata riskini azaltır.

9.5 Büyük bilgisayar sistemlerinin çoğu, yürütülen işler, kullanıcı faaliyetleri, çevre birimleri kullanımı ve sistem destek personelinin faaliyetleri için denetim kütükleri tutar. Bu kütükler yetkisiz faaliyetleri saptamak için kullanılabilir. İstisnai raporlar bu kütüklerden oluşturulmalı ve yönetim tarafından gözden geçirilmelidir.

Son kullanıcı bilgisayar işlemleri

10.1 Kontrol hedefi: kullanıcıların kendi masaüstü bilgisayarlarında işledikleri verinin yeterli derecede kontrol edildiğinden emin olmak.

10.2 Son kullanıcıların bilgisayar işlemleri, masaüstü kişisel bilgisayarlarda yapılan merkezileştirilmemiş bir şekilde (yani BT departmanı olmadan) veri işlemidir. Son kullanıcı bilgisayar işlemlerinin en bilinen biçimleri, merkezi işlem sistemlerinden indirilen bilgilerin organize edilmesi için tabloların kullanılması ve özel mali raporların üretimidir.

10.3 Maliye, personel ya da diğer BT dışı departmanlardaki çalışanlar verilerin tamlığı ve kullanabilirliği ile ilgili riskler konusunda daha az hassastırlar. Buna bağlı olarak mali verileri korumak ve yedeklemek için bu bölümlerde kontrol genelde daha azdır.

10.4 Kullanıcıların verileri masaüstü bilgisayarlarında kullanmaları imkân dahilinde olduğunda, bununla ilişkili riskleri ortadan kaldırmak için uygun politikalar bulunmalıdır. Kullanıcılar en azından güvenlik virüslerden korunma ve uygun yedeklemelerin sağlanması hakkında bilgilendirilmelidirler. Son kullanıcılar tarafından hazırlanan tüm mali raporlar, program ve tablolar, mali tabloların hazırlanmasında değerlendirilip kullanılmadan önce uygun şekilde belgelenmeli ve test edilmelidir.

Ek 5
Uygulama Kontrol Prosedürleri Ve Hesap Alanı Risk Değerlendirmesi

Ek 5'in İçindekiler

Giriş

1.1 Uygulamalar, bir iş fonksiyonuna destek veren bir ya da daha fazla bilgisayar programıdır. Uygulamalar bir kuruluş için özel olarak hazırlanabilir, (yani ısmarlama olarak müşteriye hazırlanan sistemler) ya da dışardan hazır olarak satın alınabilir.

1.2 Denetçilerin en çok karşılaştığı hazır satılan paketler arasında:

- entegre muhasebe paketleri
- bordro/ personel/ emekli maaşı sistemleri
- sabit varlıklar için kayıt defteri
- bağış yönetim programları

1.3 Ismarlama sistemler, normal olarak piyasada ihtiyacı karşılayacak uygun bir program olmadığında ya da yeteri kadar alternatif bulunmadığında geliştirilir. Ismarlama sistemler, Ülke İçi Vergi Geliri Ajansı ve İşsizlik ve Sağlık Ödeneği Ajansı gibi büyük kamu organizasyonlarının bazılarında kullanılır.

1.4 Tüm mali uygulamalar, hem işlemlerin hem de kalıcı verilerin tamlığını, kullanabilirliğini ve sınırlı bir ölçüye kadar güvenirliğini güvence altına alan kontrollere sahip olmalıdır. Ne var ki, her sistemin her düzeyde mantıken olması gereken tüm kontrollere sahip olması beklenmemelidir. Kuruluş her uygulamadaki riski değerlendirmeli ve bu riskleri kabul edilebilir bir seviyeye indirmek için uygun maliyetli kontrolleri hazırlamalıdır. Bu prensip, kuruluşa gelişme için tavsiyelerde bulunurken akılda bulundurulmalıdır.

1.5 Bu ek, bilgisayarlı mali uygulamaların incelenmesinde kuruluş için detaylı bir rehberlik sağlar. Bu ekin yapısı incelemenin C bölümünün formatı benzeridir.

Kuruluşun Bilişim Teknolojisi sistemlerinin anlaşılması ve hesap alanlarının tanımlanması

2.1 Denetçi işlemlerin dış dünya ile mali tablolar arasında izleyebileceği tüm yolları anlama ihtiyacı duyar. BT sistemleri çoğunlukla bir işlem akışının tek bir yönünü oluşturacaktır. Denetim işlemlerinin başlangıçtan itibaren belli bir BT sistemi aracılığıyla mali tablolarda özetlenene kadar izlenmesine izin verilmelidir.

2.2 Uygulamanın izlenmesinin bir parçası olarak denetçi, tüm bilgisayar donanımını ve buna bağlı mali işlemlerin girişi, işlenmesi saklanması ya da çıkışı ile ilişkili tüm BT ortamlarını belirlemeli ve belgelemelidir. Belgeleme, mali tablolara veri gönderen tüm BT uygulamalarını da tanımlamalıdır. Her önemli (material) mali uygulama için denetçi aşağıdakileri akış şeması formunda ya da açıklamalı olarak belgelemelidir:

- yazışma işleri ile BT işlemleri arasındaki etkileşimler;
- denetlenmiş mali tablolara katkıda bulunan BT donanımları ve uygulamaları;
- her uygulama tarafından işlenen işlemlerin değeri ve hacmi;
- konu ile ilgili sistemlerin giriş, işleme, çıkış ve saklama öğeleri; ve
- işlemlerin başlamasından denetlenmiş mali tablolara kadar veri akışı.

2.3 BT denetim uzmanın hizmetlerine başvurulduğunda, kuruluşun uygulama kontrol prosedürlerinin gözden geçirilmesi işi için kuruluşun muhasebe sistemlerini en iyi tanıyan ve söz konusu işte sorumluluğu bulunan denetçiden (line auditor) yardımı istenmelidir. Bu durum gözden geçirme işinin manuel ve telafi edici kontrollerin varlığını ve etkinliğini hesaba kattığı konusunda teminat verecektir. Yapılan işte sorumluluğu bulunan denetçinin varlığı aynı zamanda, bilgisayar denetçisinin sistemler hakkında daha hızlı şekilde genel bir fikre sahip olmasını sağlayacak ve BT denetçisinin çabalarının belirli bazı risklere ya da ilgi alanlarına odaklanmasına imkân verecektir.

2.4 Mali yazılım endüstrisindeki gelişmeler birden fazla tip işlemi yapabilen bütünleşik muhasebe paketlerinin çoğalmasına yol açmıştır. Kuruluşlar gelir işlemlerini, harcama işlemlerini, aylık bordro hesaplarını, iş maliyetlerini ve sabit varlıkları işleyen mali uygulamalar geliştirmiş olabilir. Bu nedenle de bir uygulamanın farklı hesap alanlarından işlemleri yürütmesi olasıdır.

2.5 Müşterinin alışılagelmiş bir muhasebe paketi kullanması durumunda denetçi paketin denetimi için bir rehberin bulunup bulunmadığını öğrenmelidir.

2.6 Hesap alanları tanımlanırken denetçi her uygulamadaki ana işlem akışlarını belirleme ihtiyacı duyacaktır. İşlem akışının tek bir hesap alanı olarak değerlendirilmesi için her işlemin benzer şekilde yapılması ve yakın bir risk derecesine sahip olması gerekir.

2.7 Denetçi, her süreçteki denetim riskinin derecesini aşağıdaki üç faktöründen yararlanarak değerlendirilmelidir.

(a) mali bilgilerin bütünlüğüne ve elde edilebilirliğine karşı **tehditler**;

(b) mali bilgilerin tanımlanan tehditlere karşı **hassaslığı**; ve

(c) denetim hedefleri biçimindeki muhtemel **etkiler**.

2.8 Tek bir hesap alanında tehdidin, hassaslığın ve etkinin düzeyi benzer olmalıdır. Bir uygulamanın giriş, aktarım, işleme, saklama ve çıkış işlemlerinin herhangi birindeki denetim riski farklılığı, işlem akışlarının ayrı hesap alanları şeklinde alt gruplara ayrılmasına yol açabilir.

Denetlenebilirlik

3.1 Herhangi bir mali sitemin denetlenebilirliği yeterli ve uygun denetim kanıtlarının varlığına bağlıdır. Denetlenen mali tablolar bir bilgisayar sistemi tarafından hazırlandığında bundan şu sonuçlar çıkarılabilir:

- işlem kayıtları tüm hesap dönemi için tutulmuştur ve tamdır.
- işlem kayıtları bir denetim izi oluşturmak için yeterli bilgiyi saklamaktadır.
- işlem toplamları, mali tablolarla denkleştirilebilir.

3.2 Eğer bu kriterlerden herhangi biri eksikse o zaman denetçi bilgisayar sistemlerinin mali tablo oluşturmak için temel teşkil etme konusunda yeterli olup olmadığına karar vermelidir. Bu koşullar altında, denetçi sorunu düzeltmek için ne yapılması gerektiğine karar vermelidir. Denetçi, bilgisayar ortamı dışında tutulan alternatif hesap kayıtlarının bulunup bulunmadığını bilgisayar sisteminin "etrafında" denetim yapmanın mümkün olup olmadığını belirlemek isteyebilir.

CAAT kullanımı

4.1 Denetçi denetim kanıtı elde etmek için bilgisayar destekli denetim tekniklerinin özellikle IDEA yazılımının kullanılması ihtimalini araştırmayı isteyebilir.

Hesap verme sorumluluğu

5.1 Bilgisayar sistemleri hangi kullanıcının ne zaman ne yaptığını belirleyebilmelidirler. Tanınan ve yaptıkları izlenen kullanıcıların yetkisiz işler yürütmesi daha düşük bir ihtimaldir. Hesap verme sorumluluğu, kullanıcıları, yaptıkları işlemlerle ilişkilendiren ve bilgileri bir denetim kütüğüne kaydeden kontrollerle sağlanabilir.

5.2 Kullanıcıların faaliyetlerinin denetim kütüklerine kaydedilmesi yürütülen faaliyetleri büyük bir oranda azaltmak için tek başına yeterli değildir. Yönetim, kütüklerden çıkarılan istisna raporlarını düzenli olarak gözden geçirmeli ve uyumsuzluklar gördüğünde takip etmelidir.

5.3 Denetim kütükleri, ancak üzerinde düzeltme yapılması mümkün olmadığı takdirde güvenli olabilir. İşlemleri giren ya da işleyen personelin kendi faaliyetleri ile ilgili kütükleri değiştirmemeleri için yeterli kontroller bulunmalıdır. Denetim kütüklerinin bütünlüğü, veri şifreleme ya da kütükleri korunan bir dizine ya da dosyaya kopyalama ile sağlanabilir.

Uygulamanın belgelenmesi

6.1 Uygulamanın yeterli biçimde belgelenmesi kullanıcıların hata yapmaları ya da yetkilerini aşmaları riskini azaltır. Kapsamlı, güncel bir belgelemenin gözden geçirilmesi, denetçinin

her uygulamanın nasıl işlediği hakkında bir fikir edinmesine yardımcı olmalıdır. Bu yöntem ayrıca denetçinin belirli denetim risklerini belirlemesine de yardımcı olabilir. Bu belgeleme şunları içermelidir:

- sistemin genel bir değerlendirilmesi;
- kullanıcı ihtiyaçlarının belirlenmesi;
- program tanımları ve listeleri;
- girdi/çıktı tanımları;
- dosyaların içindekilerin belirlenmesi;
- kullanıcı rehberleri; ve
- ana talimatlar.

Uygulama güvenliği

7.1 Genel Bilişim Teknolojisi kontrolü ortamının gözden geçirilmesi tamamlandığında denetçi, kullanıcıların belirli bir uygulamayı seçmesi noktasına kadar, bilgisayarlara erişimin kontrolü hakkında genel bir fikir edinmiş olacaktır. Uygulama güvenliğinin gözden geçirilmesi erişim kontrollerini bir adım ileri götürür ve bir uygulamaya erişimi olan kullanıcıların nasıl kontrol edileceği ile ilgilenir. Örnek olarak, bir maliye departmanındaki tüm personel, kurulu kontroller aracılığı ile on-line mali uygulamalarına erişime sahip olacaktır. Maliye uygulamasındaki ek erişim kontrolleri bu durumda kimin satış defterine, alım defterine, rapor hazırlayıcılara, bordro modülü vs.'ye erişimi olduğunu kontrol edecektir.

Giriş Kontrolleri

8.1 Veri birkaç farklı formatta işlenmek için girilebilir. Bilgisayar uygulamaları elektronik veri değişimi (electronic data interchange-EDI) ve optik ya da manyetik karakter tanıma araçları da dahil olmak üzere son bilgisayar teknolojilerini gittikçe daha çok kullanıyor. Hangi formda veri girişi kullanılırsa kullanılsın tam girdi kontrolü hedefleri aynı olup, şunların bulunduğunu güvence altına alırlar:

- tüm işlemlerin **eksiksiz** ve **doğru** bir şekilde girildiği;
- tüm işlemlerin **geçerli** olduğu;
- tüm işlemlerin **yetkilendirilmiş** olduğu; ve
- tüm işlemlerin doğru mali dönemde **kaydedildiği**

8.2 Fiziksel ve mantıksal erişim kontrolleri, sadece geçerli işlemlerin girdi için kabul edildiği konusunda teminat verilmesine katkıda bulunur. Fiziksel erişim kontrolleri mali bölüm odalarının kapılarındaki kilitleri ve kilitlenebilir bilgisayar terminallerini kapsar.

8.3 Mantıksal erişim kontrolleri bilgisayar sistemlerinin bireysel kullanıcıları ayrı ayrı tanımlayabilmesine ve bu tanımların kullanıcıların yetkileri dahilinde olan faaliyetlerin önceden belirlenmiş listeleri ile ilişkilendirilmesine dayanır. Giriş ve yetkilendirme kontrollerini geçtikten sonra uygulama, her kullanıcının hakkını kontrol edebilir. Bu her kullanıcı ya da kullanıcı grubu için istenen erişim ayrıcalıkları ve hakların profilini çıkartmayı kapsayacaktır. Örnek olarak bir kullanıcı, satış defteri memuru profiline kaydedilmiş olabilir ve böylece satın alma defterini ya da uygulamadaki diğer modülleri kullanması engellenmiş olur.

8.4 Ekstra teminat görev ayrımına zorlanmış bilgisayar aracılığıyla sağlanabilir. Kullanıcılar ancak başka bir yetkili memurun izni ile girilen verinin işlenebilmesi kısıtlamasına göre profile kaydedilmiş olabilir. Kullanıcıları profile kaydetme bir tek personelin mali işlemleri baştan sona sürdürememesini güvence altına almak için yeteri kadar detaylı olmalıdır.

8.5 Girişin bitmiş olmasının güvencesi işlemleri gruplandırarak ve girilen işlemlerin sayısını ve değerini bağımsız olarak hesaplanmış toplamlarla karşılaştırarak elde edilebilir.

8.6 Uygulamaların girdi işlemlerine grup kontrolleri uygulanmadığı yerlerde denetçi bütünlük için alternatif kanıtlar aramalıdır. Bu kanıtlar kaynak dokümanların gözden geçirilmesini ve bunların veri girişini sağladığının doğrulanmasını kapsayabilir.

8.7 Uygulamalar girişi girdiyi sistemde bulunan bilgiyle karşılaştırarak onaylayabilir. Örnek olarak, satış ya da satın alma defterlerindeki adreslerin doğruluğunu kontrol etmenin yaygın bir yolu, ev numarasını ve posta kodunu girmektir. Bilgisayar, adresleri dosyalarından geri çağıracak ve operatör de bunu girdi dokümanlarındaki adresle karşılaştıracaktır.

8.8 Hesap numaraları diğer önemli alanlarını ve kontrol rakamlarını içerebilir. Kontrol rakamları, bölümdeki verilere bir algoritma uygulanarak kaydedilir ve bölümün doğru girildiğini kontrol etmek için kullanılabilir.

8.9 Mali alanlar yetkisiz girişleri ya da yanlış miktarların girilmesini önlemek için dağılım kontrollerine tabi tutulabilir. Önceden belirlenmiş bir dağılımı ihlâl eden veri girişi kabul edilmeyecek ve denetim kütüğüne kaydedilecektir.

8.10 İşlem sıralama rakamlarının kullanımı: eksik işlemleri açığa çıkarabilir; çift ya da yetkisiz işlemlerin engellenmesine yardımcı olabilir; ve bir denetim izi sağlayabilir.

8.11 Yukarıda taslağı çizilen kontroller, uygulamanın dışından veri girilmesi ya da değiştirilmesi ile geçersiz kılınabilir. Denetçi veriye dışarıdan yapılacak değişiklikleri, örneğin bilgisayar işlemleri personeli tarafından temel işlemler veri tabanında yapılan izinsiz değişiklikleri, fark eden ve rapor eden bütünlük testlerinin mevcudiyetini aramalıdır. Denetçi ayrıca sistem değişikliği imkanlarının (örneğin editörler) düzgün bir şekilde kontrol edildiğinden emin olmak için kurumun incelemesini tekrar gözden geçirmelidir.

Veri iletim kontrolleri

9.1 Bazı bilgisayar sistemleri ayrı yerlere veri göndermelerine ya da ayrı yerlerden veri almalarına izin veren yerel ya da geniş alan bilgisayar ağlarına (LAN'lar ya da WAN'lar) bağlı olabilir. Daha yaygın veri aktarım ortamlarına telefon kabloları, koax kablolar, fiber optik kablolar ve radyo dalgaları dahildir. Hangi aktarım yolu kullanılmış olursa olsun aktarılan verinin bütünlüğünden emin olmak için yeterli kontroller bulunmalıdır.

9.2 Bilgisayar ağları üzerinden veri aktaran uygulamalar, aşağıdaki risklere tabidir.

- veri, aktarım sırasında ya da aracı sitelerde depolandığında durdurulabilir ve değiştirilebilir;
- haberleşme bağlantısı kullanılarak işlem akışına izinsiz veri eklenebilir; ve
- aktarım sırasında veri bozulabilir.

9.3 Denetçi, yetkisiz işlemlerin önlenmesini ve ortaya çıkarılmasını sağlamak için kontrollerin bulunduğundan emin olmalıdır. Örneğin, haberleşme hatalarının tasarımı ya da tesisi kontrol edilerek ya da her aktarıma sayısal imzalar eklenerek sağlanabilir.

9.4 Aktarılan verilerin bütünlüğü iletişim hataları nedeniyle bozulabilir. Denetçi gerekli yerlerde ya bilgisayar ağı sisteminde ya da mali uygulamalarda bozulmuş verileri tespit etmek için uygun kontrollerin olduğundan emin olmalıdır. Bu bilgisayar ağının iletişim protokolünün, yani aktarılan verinin formatı ve anlamını belirleyen önceden oluşturulmuş kuralların, otomatik hata tespiti ve düzeltme imkânları olabilir.

9.5 Çoğu yerel ve geniş alan bilgisayar ağında aktarılan veriyi durdurmak oldukça kolaydır. Yetersiz ağ koruması, izinsiz veri değiştirilmesi, silinmesi ve kopyalanması riskini arttırır. Bu problemler için bir takım kontroller vardır.

- işlem içeriğinin bozulmamış olduğunu ve işlemlerin yetkili bir kullanıcı tarafından gönderildiğini doğrulamak için sayısal imzalar kullanılabilir;
- işlemlerin durdurulmasını ve değiştirilmesini önlemek için veri şifreleme teknikleri kullanılabilir;
- verilerin sıralanması, mükerrer ya da silinmiş işlemlerin tespitine ve engellenmesine yardımcı olabilir ve izinsiz işlemlerin tanınmasını sağlayabilir.

İşletim kontrolleri

10.1 İşlem kontrollerinin hedefi şunlardan emin olmaktır:

- işlemlerin yürütüldüğü **kesindir;**
- işlemlerin yürütülmesi **tamamlanmıştır;**
- işlemler **tektir** (yani kopyalama yoktur);
- tüm işlemler **geçerlidir;** ve
- tüm bilgisayar işlemleri **denetlenebilirdir**.

10.2 Bir bilgisayar uygulamasındaki işlem kontrolleri, sadece geçerli verilerin ve program dosyalarının kullanıldığını, işlemlerin tamamlanmış ve kesin olduğunu ve işlenmiş verilerin doğru dosyalara yazıldığını garanti etmelidir.

10.3 İşlemin kesin ve tamamlanmış olduğundan girdi işlemlerinden elde edilen toplamların işlem tarafından yapılan değişikliklerle elde edilen veri dosyaları ile denkleştirilmesi suretiyle emin olunabilir. Denetçi, veri girişinin eksik ya da kesin olmayan bir biçimde işleme tabi tutulduğunu tespit etmek için kontroller bulunduğundan emin olmalıdır.

10.4 Uygulama işlemleri, verinin kopyalanıp kopyalanmadığını ve sistemin diğer kısımlarında tutulan bilgi ile tutarlılığını kontrol ederek işlemlerin daha ileri bir sağlamasını yapabilir. İşlem, sahip olduğu verinin bütünlüğünü kontrol etmelidir, örnek olarak veriden elde edilen kontrol toplamlarının kullanılması verilebilir. Bu tip kontrollerin amacı, sistem çökmesine ya da sistemin değişiklik imkânlarının kullanılmasına (editörler gibi) bağlı olan dış değişikliklerin tespitidir.

10.5 Bilgisayarlı mali sistemler, yürütülen işlemlerin bir kütüğünü tutmalıdır. İşlem kütüğü, ki denetim izi dosyası da denebilir, her işlemin kaynağını belirlemek için yeterli bilgiyi içermelidir.

10.6 Grup işleme ortamlarında, işlem sırasında tespit edilen hatalar kullanıcının dikkatine sunulmalıdır. Geri dönmüş (kabul edilmemiş) gruplar kütüğe kaydedilmeli ve gönderene geri itilmelidir. On-line sistemler, yapılmamış ya da netleştirilmemiş işlemleri izlemek ve rapor etmek için kullanılan kontrolleri kapsamalıdır (bir kısım ödenmiş faturalar gibi). Yönetimin belli bir süreye kadar olan ve henüz netleşmemiş bulunan işlemleri tespit etmesine ve yeniden gözden geçirmesine İmkân veren prosedürler bulunmalıdır.

10.7 Uygulamalar, elektrik kesintisi ya da donanımın bozulması gibi tersliklerle başa çıkacak şekilde tasarlanmalıdır. Sistem tüm tamamlanmamış işlemleri belirlemeye yetkin olmalı ve işlemlere kesinti noktasından itibaren hiç kesinti olmamış gibi devam edebilmelidir.

Çıktı kontrolleri

11.1 Çıktı üzerindeki kontroller şunlardan emin olmak içindir:

- **tamam** olmaları;
- **kesin** olmaları; ve
- doğru bir şekilde **dağıtılmış** olmaları.

11.2 İşlemlerin girişinden ve yetkilendirilmesinden sorumlu olanların, tamamlanmış ve kesin işlemlerin yapıldığından emin olmasına olanak tanıyan bir mekanizma bulunmalıdır. Bu, işlem sırasında tespit edilen hata mesajlarını rapor etmek için bir görev kütüğü şeklinde ya da girdi sırasında yaratılan kontrol toplamlarının denkleştirilmesi/karşılaştırılması şeklinde olabilir (açıklama: girdilerin çıktılarla denkleştirilmesi).

11.3 Çıktı raporlarının tamlığı ve bütünlüğü, kontrol toplamları ve sayfa numaraları gibi tamlık kontrollerine ve çıktılarının değiştirilebilmesi imkânının kısıtlanmasına dayanır.

11.4 Bilgisayar çıktıları düzenli ve programlı olmalıdır. Kullanıcılar eğer düzenli olarak almaya alışmışlarsa eksik çıktıları daha iyi tespit edebilir. Bilgisayar çıktılarının düzenliliği istisnai raporlama gibi bilgisayar raporlarının düzensiz olduğu durumlarda bile boş raporların hazırlanması ile sağlanabilir.

11.5 Çıktıların önemli bir kontrolün bir parçasını oluşturduğu durumlarda denetçi alıcılardan çıktıların alındığına ve kabul edilebilir olduğuna dair bir onay almalıdır.

11.6 Çıktı dosyaları, yetkisiz değişiklik riskini azaltmak için korunmalıdır. Bilgisayar çıktısının değiştirilmesine sebep olabilecek durumlara izinsiz işlemlerin gizlenmesi ya da istenmeyen mali sonuçları değiştirme dahildir. Bir fatura ödeme sistemindeki korunmayan çıktı dosyaları, çek ya da ödeme emri miktarlarını ve ödenecek tarafa ait detayları değiştirerek istismar edilebilir. Bilgisayar çıktısının bütünlüğünü korumak için fiziksel ve mantıksal kontrollerin bir kombinasyonu kullanılabilir.

11.7 Bir BT sisteminin çıktısı, mali tablolara yansıtılmadan önce başka bir sistemin girdisini oluşturabilir örneğin, bordro gibi besleyici bir sistemin çıktısı, defteri kebire girdi olarak aktarılabilir. Böyle bir durumda denetçi, çıktıların bir işlem aşamasından diğerine kesin olarak iletildiğini garanti eden kontroller aramalıdır. Daha ileri bir örnek, mizandan alınan çıktıların bir kelime işlem ya da tablolama paketine girdi olarak aktarılması ve burada verinin tekrar mali tabloları oluşturan bir formata dönüştürülmesidir.

Ana/kalıcı veri kontrolleri

12.1 Ana ve kalıcı verilerin kontrolünün hedefleri şunları sağlamaktır:

- verilere yapılan değişikliklerin **yetki dahilinde** olması;
- kullanıcıların değişikliklerden **sorumlu** olması; ve
- **bütünlüğün** sağlanması.

12.2 Güçlü tanımlama ve yetkilendirme kontrolleriyle beraber kullanılan erişim kontrolleri, kalıcı verilerin sadece yetkili personel tarafından yaratıldığı, değiştirildiği, kullanıldığı ya da silindiği konusundaki teminatın temelini oluşturabilir. Bu tip kontroller işletim sistemi tarafından uygulandığında, sistem değişiklik imkanlarının verileri uygulama kontrol ortamı dışında değiştirmek amacıyla yetkisiz kullanımını imkânsız kılacağı için en etkin durumdadır.

12.3 Satıcı detayları gibi kalıcı veri dosyaları, geçerli işlemlerin yanlış yürütülmesini engellemek için korunmalıdır. Örneğin, satıcı detaylarının değiştirilmesi, geçerli bir ödemenin yetkisiz bir alıcıya ödenmesine sebep olabilir. Erişim kontrolleri, kalıcı verileri tutanlar ile işlemleri girenler arasında bir görev ayrımı olduğunu güvence altına almalıdır. Denetim kütükleri, değişikliğin tarihi, zamanı ve kimin tarafından girildiği sorumlu kişinin tanımını ve etkilenen veri alanları gibi bilgileri kaydetmelidir. Önemli kalıcı veri dosyaları, her önemli değişiklik yapıldığında yedeklenmelidir.

12.4 Kullanıcı erişim iznini kontrol eden uygulamalar bu izinlerle ilgili detayları kalıcı veri dosyalarında saklar. Bu tip dosyalar izinsiz değişikliklerden korunmalıdır. Yönetim, uygulamanın erişim kontrol sistemini yöneten kişinin ayrıcalıklarını kötüye kullanmadığından emin olmak için bağımsız kontrollerin yapıldığından emin olmalıdır. Kurumlar kalıcı veri dosyalarının içindekileri test kontrolü amacıyla periyodik olarak listeleyebilirler (örnek: kullanıcı güvenlik profilleri).

Ek 6
İleri düzeyde rehberler ve referanslar

CIPFA bilgisayar denetimine ilişkin rehberler

Denetim ve mali bilgi sistemlerinin kontrolünün şartları
CCTA/NAO/Hazine ortak yayın

Devlet bilişim sistemleri denetim rehberi

Hazine

Aşağıdakiler dahil olmak üzere CCTA rehberleri:
- program ve proje yönetim kütüphanesi
- değerlendirme kütüphanesi
- bilişim sistemi mühendisliği kütüphanesi
- BT altyapı kütüphanesi
- iktisap süreci rehberleri
- BT sistemleri için temel güvenlik
- bilişim teknolojisi güvenliğini yönlendirmek için direktifler
- bilişim sistemleri stratejisini yönlendirmek için direktifler

Denetim direktifi 407: Bilgisayar ortamında denetim

BS7799 Bilişim güvenliği yönetimi için bir uygulama kodu

EDPAA CISA inceleme rehberi