Kontrol	ISA6.0.3 (Eski)	ISA2027 (Yeni)	Değişikliğin Etkisi	Kuruluşlar Ne Yapmalı?
1.1.1 Information Security Policy	Bilgi güvenliği politikasının oluşturulması ve yönetim tarafından onaylanması **zorunluydu (Must)**. Politikanın çalışanlara uygun bir ortamda yayımlanması ve değişikliklerin çalışanlar ile ilgili iş ortaklarına duyurulması ise **öneri (Should)** seviyesindeydi.	Politikanın çalışanlara uygun bir ortamda (örn. intranet) erişilebilir olması ve çalışanlar ile ilgili dış iş ortaklarının politika değişikliklerinden haberdar edilmesi artık **Must** kapsamına alındı. Ayrıca "approved by management" ve "adapted to organization's goals" ifadeleri daha net ve denetlenebilir şekilde yeniden yazıldı.	Artık denetimlerde sadece politikanın varlığı yeterli olmayacak. **Politikanın yayımlandığı**, **çalışanların erişebildiği** ve **ilgili taraflara değişikliklerin duyurulduğu** da zorunlu olarak doğrulanacak. Bu, bilgi güvenliği politikasının yaşayan bir yönetim dokümanı olmasını hedefliyor.	- Politikanın intranet, doküman yönetim sistemi vb. erişilebilir bir platformda yayımlandığını doğrulayın. - Politika revizyonlarında çalışanlara ve gerekiyorsa tedarikçilere/iş ortaklarına yapılan bildirimleri kayıt altına alın. - Denetimde sunulmak üzere yayın kayıtları, duyuru e-postaları veya eğitim kayıtlarını kanıt olarak hazırlayın.
6.1.3 IT Service Responsibilities *(Eski 1.2.4)*	Kontrol "1.2.4" altında yer alıyordu. "Concerned services and IT services" ifadesi kullanılıyor, ISA kontrollerinin uygulanabilirliği **verified** (doğrulandı) olarak ifade ediliyordu.	Kontrol numarası **6.1.3** olarak yeniden konumlandırıldı. "Concerned services" ifadesi kaldırılarak doğrudan **IT services** kavramı kullanıldı. Ayrıca ISA kontrollerinin uygulanabilirliği **verified** yerine **evaluated** olarak değiştirildi. Excelde karşılığı yok ama change history deki ifadeden yüksek koruma seviyesinde her ilgili IT hizmet sağlayıcısı için ISA kontrollerine ilişkin Statement of Applicability (Supplier SoA) tutulması zorunlu hale getirildiği anlaşılıyor.	Kontrol artık tamamen **IT servislerinin güvenlik yönetişimine** odaklanıyor. Denetimde, IT hizmetlerinin sorumluluklarının tanımlanması, paylaşımlı sorumluluk modelinin belirlenmesi ve güvenlik gereksinimlerinin sistematik olarak değerlendirilmesi ön plana çıkıyor.	- Tüm kullanılan IT servislerinin (özellikle bulut hizmetleri) envanterini oluşturun. - Her servis için müşteri–sağlayıcı sorumluluk matrisini (Shared Responsibility Matrix) dokümante edin. - Servis sağlayıcıların güvenlik kontrollerinin hangi ISA maddelerini karşıladığını değerlendirin ve kayıt altına alın. - Düzenli güvenlik değerlendirmelerine IT servis konfigürasyonlarını dahil edin.
2.1.4 Mobile Work	Kontrol "Teleworking" (uzaktan çalışma) kavramı üzerine kuruluydu. Evden çalışma, güvenli bilgi erişimi, VPN ve güçlü kimlik doğrulama temel gereksinimler arasındaydı.	Kontrol "Mobile Work" olarak yeniden tanımlandı. Artık evden çalışma yanında ortak çalışma alanları (coworking), seyahat sırasında çalışma ve hareket halindeki çalışma senaryoları açıkça kapsanıyor. VPN ve güçlü kimlik doğrulama ifadesi kaldırılarak bunun yerine kuruluşun IT hizmetlerine güvenli erişim sağlayacak önlemler alınması bekleniyor.	Kontrolün kapsamı genişletildi. Artık yalnızca home office değil, hibrit çalışma modeli ve mobil çalışma senaryoları değerlendirilecek. Ayrıca belirli bir teknik çözüm (VPN) yerine **teknoloji bağımsız** güvenli erişim yaklaşımı benimsendi.	- Uzaktan çalışma politikasını "Mobile Work Policy" yaklaşımıyla güncelleyin. - Coworking alanları, seyahat, otel, havaalanı gibi ortamlara yönelik güvenlik kurallarını ekleyin. - Güvenli erişim yöntemlerini (VPN, ZTNA, Secure Access Service Edge, cloud access vb.) risk bazlı olarak tanımlayın. - Mobil çalışma farkındalık eğitimlerini güncelleyin.
4.1.1 Identification Means Lifecycle	Kimlik tanımlama araçlarının (kart, rozet, anahtar, erişim kartı vb.) yaşam döngüsünün yönetimi zorunluydu. Yüksek koruma seviyesinde ayrıca kimlik araçlarının geçerlilik süresinin belirli bir süre ile sınırlandırılması isteniyordu.	Temel gereksinimler değişmedi. Ancak yüksek koruma seviyesindeki **"kimlik araçlarının geçerlilik süresi sınırlandırılmalıdır"** şartı kaldırıldı. Kayıp durumunda engelleme/geçersiz kılma stratejisi ise korunmaya devam ediyor.	TISAX artık belirli bir süre tanımlanmasını zorunlu tutmak yerine, kimlik araçlarının yaşam döngüsünün etkin yönetilmesine odaklanıyor. Önemli olan kartın ne kadar süre geçerli olduğu değil; gerektiğinde hızla iptal edilebilmesi ve izlenebilir olması.	- Kimlik araçlarının oluşturulması, teslimi, iadesi ve imhasına ilişkin süreçleri gözden geçirin. - Kayıp veya çalıntı durumlarında hızlı iptal mekanizmalarının çalıştığını doğrulayın. - Süre bazlı yenileme uygulanıyorsa devam ettirilebilir; ancak artık TISAX açısından zorunlu bir beklenti değildir.
4.1.2 User Authentication	Kullanıcıların en az "state of the art" güçlü parolalar ile doğrulanması bekleniyordu.	"State of the art" ifadesi yerine **"proven and widely accepted practices"** ifadesi kullanıldı. Diğer gereksinimlerde önemli bir değişiklik bulunmuyor.	Parola gereksinimi belirli bir teknoloji veya döneme bağlı olmaktan çıkarılarak, sektör tarafından kabul görmüş iyi uygulamalara dayandırıldı. Böylece denetimlerde daha uygulanabilir ve zamana karşı daha dayanıklı bir değerlendirme yaklaşımı benimsendi.	- Parola politikanızın NIST SP 800-63B, ENISA veya kurumunuzun kabul ettiği iyi uygulamalarla uyumlu olduğunu doğrulayın. - Ayrıcalıklı hesaplarda PAM ve MFA kullanımını sürdürün. - Risk değerlendirmesine göre ek doğrulama mekanizmalarını (MFA, brute force koruması, oturum zaman aşımı vb.) uygulamaya devam edin.
5.2.3 Protection Against Malware	Zararlı yazılımlara karşı teknik ve organizasyonel önlemler tanımlanıyordu. Gateway'lerde taşınan verilerin zararlı yazılım açısından incelenmesi bekleniyor, ayrıca olay bazlı çalışan farkındalık faaliyetleri öneriliyordu.	Çalışan farkındalığı maddesi kaldırılarak bu konu 2.1.3 kontrolüne taşındı. Ayrıca merkezi ağ geçitlerinde yapılan malware kontrollerinde yalnızca **şifreli bağlantılar (encrypted connections)** değil, **şifrelenmiş içeriklerin (encrypted content)** de dikkate alınması gerektiği açıkça eklendi.	Kontrol tekrar eden gereksinimlerden arındırıldı ve teknik odak güçlendirildi. Özellikle TLS/HTTPS trafiği ile taşınan dosyalar ve şifreli içeriklerin güvenlik kontrolleri daha görünür hale geldi.	- Malware farkındalık eğitimlerini 2.1.3 kapsamında yönetin. - E-posta ve web güvenlik geçitlerinin TLS Inspection/SSL Inspection ve şifreli içerik analiz yeteneklerini değerlendirin. - Şifrelenmiş dosya ve bağlantılar için uygulanan güvenlik kontrollerini dokümante edin.

5.2.8 Continuity Planning	Kritik IT hizmetleri için süreklilik planlaması, senaryolar, RTO, yedekleme ve test gereksinimleri tanımlanıyordu.	Temel gereksinimler korunurken ifadeler yeniden yapılandırıldı. İş sürekliliği senaryoları daha okunabilir hale getirildi, yedekleme gereksinimleri ayrıştırıldı ve test sonuçlarının kayıt altına alınmasına daha fazla vurgu yapıldı.	Kontrolün amacı değişmedi ancak denetimlerde **kanıt üretilebilirlik** ve **operasyonel uygulanabilirlik** ön plana çıktı. İş sürekliliği planlarının yalnızca hazırlanması değil, düzenli olarak gözden geçirilmesi, test edilmesi ve sonuçlarının kayıt altına alınması daha belirgin hale geldi.	- İş Sürekliliği ve Felaket Kurtarma planlarını gözden geçirin. - Test sonuçlarını ve çıkarılan dersleri kayıt altına alın. - Yedekleme stratejilerinin bütünlük (Integrity) ve gizlilik (Confidentiality) açısından yeterli koruma sağladığını doğrulayın. - Kritik hizmetler için RTO, SLA ve iletişim planlarını güncel tutun.
5.3.1 Secure Design, Development and Acquisition	Gereksinimler ağırlıklı olarak **IT System** kavramı üzerinden tanımlanıyordu. Test ortamlarında üretim verisi kullanımı ve sistem kabul testleri güvenlik gereksinimleri kapsamında ele alınıyordu.	Kontrol kapsamı **IT Service** olarak güncellendi. Test verisi yönetimi, test ortamlarının korunması ve gereksinim spesifikasyonları yeniden yapılandırılarak daha açık hale getirildi. Güvenlik testlerine ilişkin gereksinim değişmedi.	Güvenlik yalnızca sistem bazında değil, sunulan hizmet bazında ele alınıyor. Bu yaklaşım bulut servisleri, SaaS ve yönetilen hizmetleri de doğal olarak kapsıyor. Test verilerinin yaşam döngüsü ve test ortamlarının korunmasına ilişkin beklentiler daha görünür hale getirildi.	- SDLC ve Secure Development süreçlerinde "IT System" yerine "IT Service" yaklaşımını benimseyin. - Test verisi yönetimi prosedürlerini gözden geçirin. - Üretim verisi kullanılıyorsa anonimleştirme/pseudonimleştirme ve test ortamı kontrollerini doğrulayın. - Güvenlik testlerinin (ör. penetrasyon testleri) devreye alma, önemli değişiklikler ve periyodik aralıklarla gerçekleştirildiğini belgeleyin.
6.1.1 Supplier Information Security	Tedarikçiler için risk değerlendirmesi yapılması, sözleşmelerle güvenlik gereksinimlerinin tanımlanması ve sözleşmelere uyumun doğrulanması bekleniyordu. Yüksek koruma seviyesinde tedarikçinin güvenlik seviyesini gösteren kanıtlar (sertifika, attestation, internal audit vb.) yeterli kabul ediliyordu.	Kontrol kapsamı önemli ölçüde genişletildi. Artık tedarikçi güvenlik seviyesinin **düzenli olarak izlenmesi**, **değişikliklerde yeniden değerlendirilmesi**, **sözleşmesel yükümlülüklerin periyodik olarak doğrulanması**, yüksek koruma seviyesinde güvenlik kanıtlarının daha geniş yöntemlerle (self-assessment, questionnaire, supplier audit vb.) desteklenmesi ve çok yüksek koruma seviyesinde mümkünse **TISAX veya eşdeğer üçüncü taraf denetimi** ile doğrulanması bekleniyor.	Tedarikçi değerlendirmesi tek seferlik bir faaliyet olmaktan çıkarılarak **yaşam döngüsü boyunca sürdürülen bir yönetişim sürecine** dönüştürülüyor. Ayrıca kritik tedarikçiler için bağımsız güvence beklentisi önemli ölçüde artırılıyor.	- Tedarikçi risk değerlendirmelerini periyodik hale getirin. - Güvenlik kanıtlarının (TISAX, ISO 27001, SOC 2 vb.) güncelliğini takip edin. - Tedarikçi değişikliklerini (kapsam, sahiplik, alt yüklenici vb.) yeniden değerlendirme tetikleyicisi olarak tanımlayın. - Kritik tedarikçiler için periyodik güvenlik gözden geçirme süreci oluşturun. - Tedarik zinciri şeffaflığına ilişkin müşteri yükümlülüklerini sözleşmelere yansıtın.