Grant Thornton

Bilgi Teknolojileri Risk ve Yönetişim Hizmetleri

Bilgi Teknolojileri Uyum ve Denetim Hizmetleri

Bilgi Teknolojileri (BT) sistemlerinin regülasyonlara, sektörel gerekliliklere ve uluslararası çerçevelere uyumlu şekilde yönetilmesi, denetlenmesi ve raporlanması için bağımsız ve uzman kadromuzla denetim hizmetleri sunuyoruz. Hizmet kapsamında, hem düzenleyici otoritelerin beklentileri hem de küresel standartlarla uyumlu kontrol ortamları değerlendirilmekte, raporlanmakta ve kuruma özel geliştirme önerileri ile birlikte sunulmaktadır.

Yasal Uyum Denetimleri

BDDK, SPK, TCMB, BTK ve GİB gibi düzenleyici otoritelerin yayımladığı BT düzenlemelerine uygunluk açısından sistemsel ve yönetsel kontroller değerlendirilir. Kurumların iç kontrol ortamı, risk yönetim sistemleri ve veri güvenliği uygulamaları bu kapsamda analiz edilerek detaylı uyum raporları hazırlanır.

Uluslararası Standartlara Uyum

COBIT 2019, ISO/IEC 27001, SOX, ITIL ve DORA gibi uluslararası kabul görmüş çerçevelere göre sistem ve süreç denetimleri gerçekleştirilir. Kurumun mevcut uygulamaları ile standartlar arasındaki farklar belirlenir, olgunluk seviyesi ölçülür ve iyileştirme planları oluşturulur.

Sektörel Uyum ve Denetim

Finansal teknoloji (FinTech), sigorta teknolojileri (InsurTech) ve regülasyon teknolojileri (RegTech) alanlarında faaliyet gösteren kurumlara yönelik özel denetim yaklaşımları sunulmaktadır. Bu denetimlerde sektöre özgü BT kontrolleri, iş modeline uygunluk ve veri işleme süreçleri değerlendirilir.

Finansal Regülasyon Uyumları

IFRS, Basel II/III, Solvency II gibi finansal regülasyonlar doğrultusunda bilgi sistemlerinin bu çerçevelere ne ölçüde hizmet ettiği analiz edilir. Bu analiz sonucunda BT sistemlerinin finansal doğruluk, izlenebilirlik ve hesap verebilirlik gibi kriterlere uygunluğu raporlanır.

Uluslararası Güvence Raporları

SOC 1, SOC 2 ve ISAE 3402 gibi bağımsız güvence raporlarının hazırlanması süreçlerinde hem rapor yazımı hem de süreç hazırlığı danışmanlığı sunuyoruz. Bu raporlar, hizmet alan kurumlara BT sistemlerinin yeterliliği ve kontrol ortamının güvenilirliği hakkında uluslararası ölçekte geçerli güvence sağlar.

Risk ve Yönetişim

Kurumlar dijital dönüşüm yolculuklarında; teknolojik altyapılarının etkinliğini artırmak, siber tehditlere karşı dayanıklı hale gelmek ve regülasyonlara uyum sağlamak için Bilgi Teknolojileri yönetimini stratejik bir alan olarak ele almak zorundadır.

Bu kapsamda Bilgi Teknolojileri Risk ve Yönetişim Hizmetleri, kurumların BT operasyonlarının şeffaf, güvenli ve mevzuata uyumlu şekilde yönetilmesini sağlamaya yönelik uzmanlık hizmetlerini kapsamaktadır. Ulusal ve uluslararası standartları esas alan bu hizmetlerimiz, risk bazlı yaklaşımı benimseyerek BT yapılarının sürekliliği ve verimliliği için temel oluşturur.

Bilgi Teknolojileri Risk ve Yönetişim Hizmetleri

Bilgi Güvenliği Danışmanlığı

Bilgi güvenliği, sadece BT departmanlarının değil, tüm organizasyonun sorumluluğu altındaki kritik bir yönetim alanıdır. Bu hizmet grubumuz, kurumsal bilgi varlıklarının yetkisiz erişime, kayba ve bozulmaya karşı korunmasını hedeflerken aynı zamanda düzenleyici beklentilere uyumu da garanti altına almayı amaçlamaktadır.

Uluslararası standartlara (özellikle ISO/IEC 27001) uygun bilgi güvenliği yönetim sistemlerinin kurulması, kişisel veri koruma regülasyonlarına uyum, yönetişim ve farkındalık eğitimleri gibi çok boyutlu bir yaklaşım benimsenir. Hizmetlerimiz kurumun organizasyonel yapısına ve dijital risk profiline özel yapılandırılır.

ISO/IEC 27001 BGYS Danışmanlığı

Kuruma özel bilgi güvenliği politikalarının oluşturulması, risk değerlendirme süreçlerinin tanımlanması ve ISO/IEC 27001 sertifikasyonuna hazırlık çalışmaları yürütülür. Süreç boyunca teknik altyapı ve idari kontroller birlikte ele alınarak entegre bir sistem yaklaşımı benimsenir.

KVKK ve GDPR Uyum Danışmanlığı

Kişisel veri işleme envanteri çıkarılır, açık rıza metinleri ve aydınlatma yükümlülükleri yeniden yapılandırılır. Ayrıca kurumun veri güvenliği önlemleri, idari ve teknik tedbirler açısından değerlendirilerek mevzuata uyum yol haritası oluşturulur.

ISO/IEC 20000 ve ITSM

BT hizmet yönetim süreçlerinin ISO/IEC 20000 standardına göre uyumlaştırılması sağlanır. Hizmet seviyesi yönetimi, değişiklik yönetimi ve problem yönetimi gibi temel süreçlerin etkinliği değerlendirilerek iyileştirme planları oluşturulur.

ISO/IEC 38500 BT Yönetişimi

Kurumsal BT yönetişimi için yönetim kurullarının ve üst düzey yöneticilerin rol ve sorumluluklarını tanımlayan ISO 38500 çerçevesinde danışmanlık sağlanır. BT yatırımları ile stratejik hedefler arasındaki uyumun güçlendirilmesi hedeflenir.

Farkındalık ve Eğitim Hizmetleri

Tüm çalışanlar için sosyal mühendislik, bilgi güvenliği farkındalığı ve veri koruma eğitimleri tasarlanır ve uygulanır. Eğitimler kurum kültürüne entegre olacak şekilde interaktif yöntemlerle gerçekleştirilir ve davranışsal riskleri azaltmayı hedefler.

Kurumsal Bilgi Güvenliği Yaklaşımı

Bilgi güvenliği, yalnızca BT birimlerinin değil, tüm kurumun sorumluluğundadır. Bu hizmet kapsamında, kurumsal bilgi varlıklarının korunması ve yasal gerekliliklere uyum hedeflenir. ISO/IEC 27001 gibi standartlara uygun sistemlerin kurulumu, veri koruma düzenlemeleri ve farkındalık eğitimleri temel başlıklardır.

Danışmanlıklar, kurumun yapısı ve risk düzeyi dikkate alınarak yürütülür. Bilgi güvenliği politikaları, kişisel veri envanteri, BT hizmet süreçlerinin uyumu ve yönetişim esasları ele alınır. Ayrıca çalışanlara yönelik farkındalık eğitimleri sunulur.

Bilgi Teknolojileri Risk ve Yönetişim Hizmetleri

Siber Güvenlik Hizmetleri

Siber güvenlik hizmetlerimiz, tehdit ortamının dinamik doğasına uyum sağlayan ve kurumsal varlıkları çok katmanlı savunma ilkesiyle koruyan bir yaklaşımı esas alır. Kurumların siber risklerini anlamasını, bu risklere karşı hazırlıklı olmasını ve olaylara etkili şekilde müdahale edebilmesini sağlayan yapılar oluşturulmasına odaklanırız.

Stratejik planlamadan operatif testlere, olay müdahale senaryolarından tedarikçi risk analizlerine kadar geniş kapsamlı hizmetlerimiz, hem mevzuatlara uyumu hem de operasyonel dayanıklılığı güvence altına alır. Her hizmet, kuruma özgü güvenlik mimarisi ve tehdit modellemesi doğrultusunda özelleştirilir.

Siber Güvenlik Strateji ve Yol Haritası

Kurumun mevcut siber güvenlik olgunluğu detaylı analiz edilir. Kritik zayıf alanlar, güçlü yönler ve sektörel tehditler doğrultusunda özelleştirilmiş bir stratejik yol haritası oluşturulur. Bu yol haritası teknik, yönetsel ve kültürel güvenlik adımlarını içeren bütünsel bir çerçevede sunulur.

Zafiyet Taraması ve Sızma Testleri

Kurumun BT altyapısı, ağları, uygulamaları ve bulut sistemleri üzerinde kapsamlı güvenlik testleri uygulanır. Hem otomatik zafiyet taramaları hem de manuel sızma testleri ile açıklıklar tespit edilerek detaylı raporlar ve iyileştirme planları sağlanır.

Kimlik ve Erişim Yönetimi (IAM)

Kritik sistemlere erişimlerin sadece yetkili kişilerce ve ihtiyaç duyulan düzeyde sağlanmasını garanti altına alan IAM sistemlerinin tasarımı ve uygulanması gerçekleştirilir. Rol tabanlı erişim kontrolleri ve çok faktörlü kimlik doğrulama süreçleri ile güvenlik seviyesi yükseltilir.

Olaylara Müdahale ve Kriz Simülasyonları

Siber olaylara karşı kurum içi ekiplerin hazırlıklı olması amacıyla olay müdahale planları oluşturulur, rollere özel senaryolar geliştirilir ve kriz simülasyonları (cyber wargames) düzenlenir. Bu çalışmalarla kurumun teknik refleksi ve yönetsel karar alma hızı ölçülür.

SIEM ve Tehdit İstihbaratı

Gelişmiş SIEM sistemleri ile kurum içi tehdit izleme kabiliyeti artırılır. Log toplama, anomali tespiti ve otomasyon destekli güvenlik olaylarına müdahale altyapısı kurularak gerçek zamanlı savunma mekanizmaları etkinleştirilir.

Tedarikçi ve Üçüncü Taraf Riskleri

Kurumun birlikte çalıştığı dış hizmet sağlayıcıların güvenlik seviyeleri değerlendirilir. Sözleşme ve SLA uyumluluğu denetlenerek tedarik zinciri güvenliği sağlanır. Bu süreçte risk profili yüksek olan üçüncü taraflar için özel takip ve kontrol önerileri sunulur.

Siber Güvenlik Yönetimi ve Uygulama Alanları

Siber güvenlik hizmetleri, kurumların dijital varlıklarını çok katmanlı savunma prensibiyle korumayı ve tehdit ortamına uyum sağlayan yapıların oluşturulmasını hedefler. Mevcut güvenlik olgunluğunun değerlendirilmesi, zafiyet taramaları, sızma testleri, kimlik ve erişim yönetimi gibi başlıklar doğrultusunda kurumlara özel stratejiler geliştirilir.

Olay müdahale planları, kriz senaryoları, tehdit istihbaratı sistemleri ve tedarikçi risk analizleri ile kurumun operasyonel ve yönetsel dayanıklılığı desteklenir.

İş Sürekliliği ve Kriz Yönetimi Hizmetleri

İş sürekliliği yönetimi, kurumsal operasyonların sürdürülebilirliğini sağlarken aynı zamanda kriz zamanlarında dayanıklılığı test eder. Kurumların hizmet kesintilerine, doğal afetlere, siber saldırılara ve operasyonel aksaklıklara karşı hazırlıklı olmalarını sağlayacak stratejik çözümler geliştiriyoruz.

Sunulan hizmetler, sadece dokümantasyon değil; aynı zamanda kurumun tüm organizasyon yapısına entegre edilen, test edilen ve sürekli geliştirilen kapsamlı bir sistem yaklaşımını temel alır. BT sistemleri ile organizasyonel planlamayı entegre ederek bütünsel iş sürekliliği çözümleri sunulur.

ISO 22301 Danışmanlığı

Kurum için kritik süreçler ve kaynaklar analiz edilerek iş etki analizi (BIA) gerçekleştirilir. Bu veriler ışığında felaket senaryolarına yönelik olarak iş sürekliliği stratejileri geliştirilir ve ISO 22301 standardına uygun yönetim sistemi kurulumu sağlanır.

Tatbikatlar ve Fark Analizi

Hazırlanan iş sürekliliği planları, masa başı ve saha bazlı tatbikatlarla test edilir. Bu tatbikatlar aracılığıyla planların uygulanabilirliği, personel farkındalığı ve organizasyonun kriz refleksi ölçülür; sonuçlara göre fark analizi yapılır.

BT Sürekliliği ve Kurtarma Planları

Veri merkezleri, ağ altyapıları ve uygulama sistemleri için felaket kurtarma (disaster recovery) planları hazırlanır. Yedekleme stratejileri, alternatif çalışma yöntemleri ve olağanüstü durum geçiş senaryoları oluşturularak BT altyapısının kesintisizliği güvence altına alınır.

Bilgi Teknolojileri Felaket Senaryolarına Hazırlık

Kurumsal faaliyetlerin kesintisiz sürdürülebilmesi için kritik süreçler belirlenerek iş etki analizi (BIA) yapılır. Elde edilen verilerle iş sürekliliği stratejileri geliştirilir ve ISO 22301 standardına uygun bir yönetim sistemi kurulması sağlanır. Planların uygulanabilirliği, masa başı ve saha tatbikatları ile test edilir; sonuçlara göre fark analizi gerçekleştirilir.

BT sürekliliği kapsamında, veri merkezleri ve ağ altyapısı gibi sistemler için felaket kurtarma planları hazırlanır. Yedekleme senaryoları, geçiş prosedürleri ve olağanüstü durum planları ile teknolojik altyapının dayanıklılığı artırılır.

Can Taylan
Kıdemli Müdür
T +90 212 373 00 00
E can.taylan@tr.gt.com

Enis Seven
Müdür
T +90 212 373 00 00
E enis.seven@tr.gt.com

Hakkımızda

Grant Thornton, bağımsız denetim, vergi ve danışmanlık hizmetleri sunan dünyanın önde gelen organizasyonlarından biridir. Bünyesindeki firmalar, dinamik kurumların büyüme potansiyelini açığa çıkarmalarına anlamlı ve geleceğe yönelik rehberlik sağlayarak destek olur. 150'den fazla ülkede 76.000 çalışanıyla, müşterilerimize, ekip arkadaşlarımıza ve yaşayıp çalıştığımız topluluklara değer katmak için çalışmaktadır.

Grant Thornton