

EY Türkiye
Risk ve Siber Güvenlik
Eđitim Katalođu
2024



Eğitim Anlayışımız	4	SG Siber Güvenlik Eğitimleri	31
KRY Risk Yönetimi Eğitimleri	5	KGS Kurumsal Güvenlik Eğitimleri	32
KRY1 Kurumsal Risk Yönetimi Eğitimi	6	KGS1 Yöneticiler İçin Siber Güvenlik Eğitimi	32
KRY2 ISO 31000 Tabanlı Risk Yönetim Sistemi Eğitimi	7	KGS2 Siber Güvenlik Analist Eğitimi	33
KRY3 Dinamik Risk Yönetimi Eğitimi	8	KGS3 Siber Tehdit İstihbaratı Eğitimi	34
KRY4 Operasyonel Risk Yönetimi Eğitimi	9	KGS4 SOME Eğitimi	35
KRY5 Üçüncü Parti Risk Yönetimi Eğitimi	10	KGS5 Cyber CPA Bilgilendirme Eğitimi	36
KRY6 ESG Risklerinin Yönetimi Eğitimi	11	KGS6 Teknoloji Sürekliliği Bilgilendirme Eğitimi	37
KRY7 İş Sürekliliği Yönetimi (ISO 22301 Yönetim Sistemi) Temel Eğitimi	12	BGS Bilgi Güvenliği Standardı Eğitimleri	38
KRY8 İş Sürekliliği Yönetimi (ISO 22301 Yönetim Sistemi) İleri Düzey Eğitimi	13	BGS1 PCI DSS İç Denetçi Eğitimi	38
KRY9 Kriz Yönetimi ve Kriz Yönetim Takımı Eğitimi	14	BGS2 PCI DSS Uyarlayıcı Eğitimi	39
İD İç Denetim ve İç Kontrol Eğitimleri	15	BGS3 PCI DSS Farkındalık Eğitimi	40
İD1 Süreç ve İç Kontrol Analizi Eğitimi	16	BGS4 ISO 27001 Bilgi Güvenliği Yönetim Sistemi Temel Bilgilendirme Eğitimi	41
İD2 Temel İç Denetim Eğitimi	17	BGS5 ISO 27001 Bilgi Güvenliği Yönetim Sistemi Farkındalık Eğitimi	42
İD3 Güncel Gelişmeler Işığında Risk Bazlı İç Denetim Eğitimi	18	BGS6 ISO 27701 Kişisel Veri/Gizlilik Bilgi Yönetim Sistemi Temel Bilgilendirme Eğitimi	43
İD4 İç Denetimde Veri Analitiği Uygulamaları Eğitimi	19	KVG Kişisel Veri Güvenliği Eğitimleri	44
İD5 Süreç Madenciliği ile İç Denetim	20	KVG1 Kişisel Verilerin Korunması Farkındalık Eğitimi	44
İD6 SAP Üzerinde Süreç ve Kontrollerin Denetimi	21	KVG2 Mahremiyet Temelli Tasarım (Privacy by Design) Eğitimi	45
İD7 GRC (Governance Risk & Compliance) Çözümleri Farkındalık Eğitimi	22	KVG3 KVKK ve GDPR Kapsamındaki Teknik ve İdari Tedbirlere Genel Bakış Eğitimi	46
İD8 Çevik (Agile) İç Denetim Eğitimi	23	KVG4 KVKK Teknik Sistem Yönetim Eğitimi	47
İD9 İç Kontrol Öz Değerlendirme Eğitimi	24	KVG5 Kişisel Verilerin Korunması Oyunlaştırma (Gamification) Çalışması	48
İD10 Kurumsal Yönetim Denetimi Eğitimi	25	TG Teknik Güvenlik Eğitimleri	49
BTD BT Denetimi Eğitimleri	26	TG1 Güvenli Yapılandırma Denetimi Eğitimi	49
BTD1 BT Uzmanı Olmayanlar İçin BT Denetimi Eğitimi	27	TG2 Blok Zinciri Güvenliği Eğitimi	50
BTD2 Temel BT Denetimi Teknikleri Eğitimi	28	TG3 Mobil Uygulama Güvenliği Eğitimi	51
BTD3 İleri BT Denetimi Eğitimi (Laboratuvar Çalışması Dahil)	29	TG4 Veri Tabanı Güvenliği Eğitimi	52
BTD4 SAP BT Genel Kontrollerinin Denetimi Eğitimi	30	TG5 Bulut Güvenliği Eğitimi	53
		TG6 Bulut Güvenliği Teknik İmplementasyon Eğitimi	54
		TG7 Log Yönetim Sistemleri Kurulum ve Teknik Uyarlama Eğitimi	55
		TG8 Veri Kaybı Önleme (DLP) Yönetimi ve Teknik Uyumlaştırma Eğitimi	56
		TG9 Kimlik Yönetimi (IDM) Temel Eğitimi	57

GA	Güvenlik Analizi Eğitimleri	58
GA1	Ağ Trafik Analizi Eğitimi	58
GA2	Adli Analiz ve Zararlı Yazılım Analizi	59
GA3	Blue Team Eğitimi	60
ST	Sızma Testi Eğitimleri	61
ST1	Offensive Security Certified Professional (OSCP) Hazırlık Eğitimi	61
ST2	Certified Ethical Hacker (CEH) Eğitimi	62
ST3	Web Uygulamalarına Yönelik Testler	63
ST4	Ethical Hacker Bootcamp	64
ST5	ICS/SCADA Güvenliği Eğitimi	65
ST6	SCADA Pentesting	66
<hr/>		
RM	Risk Modelleme Eğitimleri	67
RM1	R ile Gelişmiş Analitik Yöntemler Eğitimi	68
RM2	R'da Temerrüt Olasılığı Modellemesi ve Model Validasyonu Eğitimi	69
RM3	IRB (İçsel Derecelendirmeye Dayalı-İDD) Yaklaşımı Eğitimi	70
RM4	Üst Seviye Yöneticileri İçin Finansal Risk Yönetimi Regülasyonları	71
RM5	Denetçiler İçin IRB (İçsel Derecelendirmeye Dayalı-İDD) Yaklaşımı Eğitimi	72
RM6	Denetçiler İçin Kredi Riski Yönetimi Eğitimi	73
RM7	İSEDES (İçsel Sermaye Yeterliliği Değerlendirme Süreci) Eğitimi	74
RM8	Denetçiler İçin Validasyon Eğitimi	75
RM9	IFRS 9 Eğitimi	76
RM10	Risk İzleme ve Tahsilat Analitiği Eğitimi	77
RM11	Doğal Afetlerin Risk Yönetimine Etkileri Eğitimi	78
<hr/>		
YS	Yönetim Sistemleri Eğitimleri	79
YS1	ISO 9001 Kalite Yönetim Sistemi Temel Bilgilendirme	80
YS2	IATF 16949 Otomotiv Kalite Yönetim Sistemi Temel Bilgilendirme Eğitimi	81
YS3	ISO 14001 Çevre Yönetim Sistemi Temel Bilgilendirme Eğitimi	82
YS4	ISO 45001 İSG Yönetim Sistemi Temel Bilgilendirme Eğitimi	83
YS5	ISO 19011 Uyumlu Yönetim Sistemleri İç Tetkikçi Eğitimi	84
YS6	Sosyal Sorumluluk Standartları Temel Bilgilendirme (ISO 26000, SA 8000) Eğitimi	85
YS7	Entegre Yönetim Sistemleri Temel Bilgilendirme (ISO 9001, ISO 14001, ISO 45001) Eğitimi	86

Eđitim Yaklařımız

EY T¼rkiye olarak, Risk ve Siber G¼venlik Danıřmanlıđı alanında birok farklı sekt¼rde sahip olduđumuz bilgi birikimini ve tecr¼beyi, konu uzmanlarınca hazırlanan eđitim programımızla sizlerle paylařmaktan memnuniyet duyuyoruz.

G¼ncel riskleri ve řirketlerin deđiřen ihtiyalarını dikkate alarak eđitim katalođumuzu g¼ncelledik. Yeni eklenen eđitimlerin yanı sıra, mevcut eđitimlerin ieriđinde de iyileřtirmeler yaptık ve ¼zellikle ok ilgi g¼ren uygulama ve vaka alıřmalarının payını artırdık.

T¼m eđitim ieriđimizi řirketinize ¼zel olarak belirleyeceđiniz bir lokasyonda, EY ofisimizde ya da sanal ortamda gerekleřtirebiliriz.

Eđitim programımızla ilgili daha detaylı bilgi almak iin bizimle iletiřime geebilirsiniz.

EY T¼rkiye
Danıřmanlık Hizmetleri



Risk Yönetimi Eğitimleri



Eğitim
Anlayışımız

Risk Yönetimi
Eğitim Konuları

İç Denetim
Eğitim Konuları

BT Denetimi
Eğitim Konuları

Siber Güvenlik
Eğitim Konuları

Risk Modelleme
Eğitim Konuları

Yönetim Sistemleri
Eğitim Konuları





1 gün

- ▶ Risk yönetimi uzmanları
- ▶ İç kontrol uzmanları
- ▶ İç denetçiler

**AMAÇ**

Kurumların karşılaştıkları risklerin barındırdığı fırsat ve tehditleri etkin bir şekilde ölçmeleri ve yönetebilmeleri gittikçe daha fazla önem kazanmaktadır. Bu eğitimle, kurum içinde etkin bir kurumsal risk kültürünün oluşturulması ve risk yönetim süreçlerinin geliştirilmesine katkı sağlanması amaçlanmaktadır.

KAPSAM

- ▶ Kurumsal Risk Yönetiminin Temelleri:
 - ▶ KRY'nin kurum içindeki rolü ve önemi
 - ▶ KRY'de temel kavramlar
 - ▶ KRY'ye ilişkin temel yaklaşımlar ve metodlar
 - ▶ İlgili mevzuat
- ▶ Kurumsal Risk Yönetim (KRY) Süreci:
 - ▶ KRY süreci döngüsü ve temel bileşenleri
 - ▶ ISO 31000 standardının temel özellikleri
 - ▶ COSO ERM'in temel özellikleri
- ▶ Vaka çalışması: Tehdit ve fırsatlar, risk türleri, kontrollerin etkinliği, temel risk göstergeleri, risk ölçümlenme, aksiyon planı ve kalıntı risk
- ▶ GRC sistemlerinin özellikleri ve sürekli izleme yaklaşımı

KRY2 ISO 31000 Tabanlı Risk Yönetim Sistemi Eğitimi

KRY2/9



2 gün

- ▶ Risk yönetimi uzmanları
- ▶ Yönetim sistemi uzmanları

**AMAÇ**

ISO 31000 Risk Yönetimi Standardı, kuruluşlara kapsamlı ilke ve yönergeler sağlayarak uçtan uca risk yönetimi süreçlerinin kurulması ve işletilmesi için bir çerçeve oluşturmaktadır. ISO 31000 eğitimi ile risk yönetimi çerçevesinin planlanması, uygulanması, sürdürülmesi ve yönetilmesi konusunda farkındalığın ve temel pratiklerin sağlanması amaçlanmaktadır.

KAPSAM

- ▶ Yönetim sistemlerinin ve ISO standartlarının temel özellikleri
- ▶ Risk yönetiminin rolü, önemi ve faydaları
- ▶ Risk yönetiminin temel kavramları
- ▶ ISO 31000 temel gereklilikleri
- ▶ ISO 31000 prensipleri, çerçevesi ve süreci
- ▶ ISO 31000 uyarınca risk yönetim süreci ve uygulamaları
- ▶ ISO 31000'in kurumsal risk yönetiminde (KRY) uygulanması
- ▶ Entegre ISO yönetiminde ISO 31000'den yararlanma
- ▶ Vaka çalışması: ISO31000 döngüsünün örnek riskler üzerinde uygulanışı



KRY3 Dinamik Risk Yönetimi Eğitimi



1 gün

► Risk yönetimi uzmanları



AMAÇ

Bu eğitimle birlikte, değişen dünyada risklere daha hızlı adapte olabilmek, organizasyon için kritik risklere odaklanabilmek ve risk yönetimini sayısal temellere oturtarak performans üzerindeki etkisini ölçümlenebilmek adına risk profesyonellerine farkındalık yaratması amaçlanmaktadır. İleri seviye Risk Modelleme Eğitimleri öncesinde bu eğitimin alınması tavsiye edilir.

KAPSAM

- Dinamik risk yönetiminin özellikleri
- Geleneksel risk yönetimi ile dinamik risk yönetimi arasındaki temel farklar
- Risklerin sayısallaştırılması ve modellenmesine ilişkin temel yaklaşımlar ve gereklilikler
- Dinamik risk yönetiminin aşamaları:
 - Stratejik analiz ve hedef belirleme
 - Veri toplama
 - Model oluşturma ve validasyon
 - Sonuçların değerlendirilmesi ve kısıtlar
- Veri yönetimi ile ilgili önemli hususlar
- Vaka çalışması: Risk sayısallaştırma ve modelleme örneği ve değerlendirmeler



KRY4 Operasyonel Risk Yönetimi Eğitimi



KRY4/9



2 gün

- ▶ Risk yönetimi uzmanları
- ▶ Risk ve süreç sahipleri
- ▶ İç denetçiler



AMAÇ

Kurumlarda etkin bir risk yönetiminin sağlanabilmesi için operasyonel risklerin sağlıklı bir biçimde ele alınması önem arz etmektedir. Eğitimde konu yönetim ve uygulama boyutlarıyla ele alınacak olup, kurumlarda operasyonel risklere ilişkin yönetim, politika, prosedür, süreç, risk, kontrol, ölçüm ve raporlama perspektiflerinin oluşturulmasına katkı sağlamak amaçlanmaktadır.

KAPSAM

- ▶ Operasyonel Risk Yönetimi'nin (ORY) temel kavramları
- ▶ ORY'nin faaliyetleri, temel hedefleri ve Kurumsal Risk Yönetimi (KRY) çerçevesindeki rolü ve önemi
- ▶ ORY yönetim yapısı ve üst yönetimin rolü
- ▶ ORY ile ilgili uluslararası ve yerel düzenlemeler
- ▶ Operasyonel Risk Çerçevesi: ORY kaynakları, olay tipleri, maruz kalınabilecek kayıplar, risk iştahı ve diğer unsurlar
- ▶ Operasyonel risk envanteri örneği
- ▶ Temel ORY araç ve teknikleri
- ▶ ORY ölçümü ve analizi
- ▶ Örnek vaka incelemeleri
- ▶ ORY denetiminde dikkat edilmesi gereken hususlar



KRY5 Üçüncü Parti Risk Yönetimi Eğitimi



KRY5/9



1 gün

- ▶ Risk yönetimi uzmanları
- ▶ Risk ve süreç sahipleri
- ▶ Tedarik zinciri ve satınalma



AMAÇ

Kurumların iş birliği içinde oldukları kritik tedarikçileri dahil tüm üçüncü partiler, kurumları çeşitli risklere maruz bırakabilir. Eğitimde bu riskleri sistematik şekilde yönetmenin temellerinin oluşturulması hedeflenmektedir.

KAPSAM

- ▶ Üçüncü parti risk yönetimi yaşam döngüsü
- ▶ Üçüncü parti risk çerçevesinin temel unsurları
- ▶ Üçüncü partilerde risk ve kontrollerin belirlenmesi ve değerlendirilmesi
- ▶ Üçüncü partilerde iş sürekliliği ve kurumsal dayanıklılık kontrolleri
- ▶ Çıkış stratejisi ve önemi
- ▶ Üçüncü parti risklerinin izlenmesi ve raporlanması
- ▶ Üçüncü partiler için kullanılan bağımsız denetim rapor türleri
- ▶ Üçüncü partilerin denetiminde dikkat edilmesi gereken hususlar
- ▶ Vaka çalışması



KRY6 ESG Risklerinin Yönetimi Eğitimi



KRY6/9



1 gün

- ▶ Risk yönetimi uzmanları
- ▶ ESG paydaşları
- ▶ İç denetçiler



AMAÇ

Çevresel, Sosyal ve Kurumsal Yönetişim (ESG) risklerinin etkin yönetimi, risk yönetiminde güncel konulardan biri olarak karşımıza çıkmaktadır. Eğitimde ESG riskleri yönetim, kurumsal risk yönetimi, iç kontrol ve iç denetim başta olmak üzere çeşitli açılardan ele alınmakta ve tüm ilgili paydaşlara güçlü bir farkındalık sağlanması amaçlanmaktadır.

KAPSAM

- ▶ ESG ve sürdürülebilirlik kavramları
- ▶ ESG ile ilgili global gelişmeler, düzenleyici kuruluşlar, rehberler ve çerçeveler
- ▶ ESG risk ve fırsatlarının yönetimi
- ▶ ESG risklerinin tespiti ve değerlendirilmesi
- ▶ ESG risklerinin Kurumsal Risk Yönetimi (KRY) çerçevesine entegrasyonu
- ▶ ESG risklerinin yönetiminde GRC teknolojilerinin kullanımı ve entegrasyonu
- ▶ ESG risklerinin yönetiminde iç denetimin rolü
- ▶ Uygulama çalışması



KRY7 İş Sürekliliği Yönetimi (ISO 22301 Yönetim Sistemi) Temel Eğitimi



2 gün

- ▶ İş sürekliliği uzmanları
- ▶ Risk yönetimi uzmanları
- ▶ İç kontrol ve iç denetim uzmanları



AMAÇ

Günümüzde kurumlar salgın hastalık, deprem ve benzeri nedenlerden dolayı ciddi ve uzun süreli iş kesintileri yaşamaktadır. ISO 22301 standardını temel alan bu eğitim ile; İş Sürekliliği Yönetim Sistemi yapısının metodolojik bir şekilde nasıl kurulacağı ve kurum içerisinde yönetileceğine dair bilgilerin verilmesi amaçlanmaktadır.

KAPSAM

- ▶ İş sürekliliğine ilişkin temel kavramlar
- ▶ İş Sürekliliği Yönetim Sistemi'nin önemi ve faydaları
- ▶ ISO 22301 standardının kapsamı ve özellikleri
- ▶ İş sürekliliği yönetiminin planlanması
- ▶ İş sürekliliği yönetiminin uygulanması:
 - ▶ İşletimsel planlama ve kontrol
 - ▶ İş etki ve risk analizi
 - ▶ İş sürekliliği stratejisi
 - ▶ Prosedür ve iş kurtarma planları
 - ▶ Eğitim ve farkındalık
 - ▶ Tatbikatlar ve testler
 - ▶ Sürekli iyileştirme

KRY7/9



KRY8 İş Sürekliliği Yönetimi (ISO 22301 Yönetim Sistemi) İleri Düzey Eğitimi



4 gün

- ▶ İş sürekliliği uzmanları
- ▶ Risk yönetimi uzmanları
- ▶ İç kontrol ve iç denetim uzmanları

**AMAÇ**

Günümüzde kurumlar salgın hastalık, deprem ve benzeri nedenlerden dolayı ciddi ve uzun süreli iş kesintileri yaşamaktadır. ISO 22301 standardını temel alan ileri düzey iş sürekliliği eğitimi ile; İş Sürekliliği Yönetim Sistemi yapısının metodolojik bir şekilde nasıl kurulacağı ve kurum içerisinde yönetileceğine dair bilgilerin ilave çalıştaylar ile uygulamalı bir şekilde verilmesi amaçlanmaktadır.

KAPSAM

- ▶ İş sürekliliğine ilişkin temel kavramlar
- ▶ İş Sürekliliği Yönetim Sistemi'nin önemi ve faydaları
- ▶ ISO 22301 standardının kapsamı ve özellikleri
- ▶ İş sürekliliği ve kriz yönetimi
- ▶ İş sürekliliği yönetiminin planlanması
- ▶ İş sürekliliği yönetiminin uygulanması
- ▶ İş sürekliliği yönetimi çalıştayı (iki örnek süreç için uygulama):
 - ▶ İşletimsel planlama ve kontrol
 - ▶ İş etki ve risk analizi
 - ▶ İş sürekliliği stratejisi
 - ▶ Prosedür ve iş kurtarma planları
 - ▶ Eğitim ve farkındalık
 - ▶ Tatbikatlar ve testler
 - ▶ Sürekli iyileştirme

KRY8/9

KRY9 Kriz Yönetimi ve Kriz Yönetim Takımı Eğitimi



1 gün

- ▶ İş sürekliliği uzmanları
- ▶ Risk yönetimi uzmanları
- ▶ İç kontrol uzmanları



AMAÇ

Krizler, doğru bir şekilde yönetilemediklerinde felakete dönüşebilmektedir. Bu eğitim ile kurumların krizleri yönetmek için hangi metodolojik yaklaşımları benimsemesi gerektiği, krizi yönetecek ekibin özellikleri ve nasıl davranması gerektiğine ilişkin bilgilerin interaktif ve gerçek yaşanmış örneklere dayalı olarak verilmesi amaçlanmaktadır.

KAPSAM

- ▶ Temel kriz kavramları
- ▶ Yaşanmış kriz örnekleri
- ▶ Ortak çalışma: Siz ne yapardınız?
- ▶ Kriz yönetim metodolojisi
- ▶ Tehditlerin tanımlanması
- ▶ Kriz yönetim ekibinin oluşturulması
- ▶ Ekip liderinin önemi
- ▶ Kriz yönetim merkezi kurulumu
- ▶ Kriz yönetim planı ve kriz iletişimi
- ▶ Kriz simülasyonu

İç Denetim ve İç Kontrol Eğitimleri



Eğitim
Anlayışımız

Risk Yönetimi
Eğitim Konuları

İç Denetim
Eğitim Konuları

BT Denetimi
Eğitim Konuları

Siber Güvenlik
Eğitim Konuları

Risk Modelleme
Eğitim Konuları

Yönetim Sistemleri
Eğitim Konuları



İD1 Süreç ve İç Kontrol Analizi Eğitimi

İD1/10



2 gün

- ▶ İç denetçiler
- ▶ İç kontrol uzmanları
- ▶ Risk yönetimi uzmanları
- ▶ Süreç ve kontrol sahipleri
- ▶ Süreç yönetimi uzmanları

**AMAÇ**

Organizasyonun temelini iş süreçleri oluşturmaktadır. Doğru, verimli ve iç kontrollerle desteklenen iş süreçleri organizasyonun başarısına yardım ettiği gibi süreç içinde yer alan risklerin de önemli ölçüde azaltılmasını sağlar. İş süreçlerinin temellerini aktaran bu eğitimde çeşitli araç ve tekniklerle iş süreçlerinin kontrol etkinliklerinin artırılması hedeflenmektedir.

KAPSAM

- ▶ Süreç, alt süreç kavramları ve hiyerarşi seviyeleri
- ▶ Risk ve kontrol kavramları
- ▶ Süreçlere risk bazlı bakış
- ▶ Çeşitli yöntemlerle süreç haritalandırması yapılması
- ▶ Karar ağaçlarının kullanımı
- ▶ İç kontrollerin süreç üzerinde tanımlanması ve gösterimi
- ▶ Süreç değerlendirme ve gelişim önerilerinin saptanması
- ▶ RACI matrislerinin oluşturulması
- ▶ Vaka çalışması: Süreç haritalandırma örneği, risk ve kontrollerin tespiti ve gelişim önerilerinin belirlenmesi



İD2 Temel İç Denetim Eğitimi

İD2/10



2 gün

- ▶ İç denetçiler
- ▶ İç kontrol uzmanları
- ▶ Risk yönetimi uzmanları



AMAÇ

İç denetim metodolojisi ve ilgili kavramlarının uluslararası iç denetim standartları ile uyumlu bir şekilde, güncel sektör tecrübeleri çerçevesinde katılımcılara aktararak, iç denetim uygulamalarına yönelik yetkinlik seviyelerinin artırılması amaçlanmaktadır.

KAPSAM

- ▶ Denetimde temel kavramlar
- ▶ Riskler ve kontrollerin özellikleri, türleri ve uygulama alanları
- ▶ COSO İç Kontrol Çerçevesi ve önemi
- ▶ Risk odaklı iç denetim yaklaşımı
- ▶ İç denetim ve iç kontrol ilişkisi
- ▶ Bilgi teknolojileri genel kontrollerinin rolü ve önemi
- ▶ Mesleki uygulama çerçevesi ve uluslararası iç denetim standartlarına genel bakış
- ▶ İç denetim metodolojisi:
 - ▶ Risk değerlendirme
 - ▶ İç denetim planının hazırlanması
 - ▶ Saha çalışması/Denetimin gerçekleştirilmesi
 - ▶ Denetim sonuçlarının dokümante edilmesi ve raporlama
 - ▶ Takip denetimleri
- ▶ Vaka çalışması: Örnek senaryo üzerinden iç denetim metodolojisinin uygulaması



İD3 Güncel Gelişmeler Işığında Risk Bazlı İç Denetim Eğitimi

İD3/10

**1 gün**

- ▶ İç denetim yöneticileri
- ▶ Kıdemli denetçiler

**AMAÇ**

İç denetim, risklerin organizasyon içinde etkin bir şekilde yönetildiğine güvence vermekte önemli bir role sahiptir. Bu eğitimde son gelişmeler ışığında iç denetimin şirketin maruz kaldığı yeni riskleri daha etkin bir biçimde değerlendirmesi ve denetim planını buna göre oluşturması konusundaki yetkinliğinin artırılması amaçlanmaktadır.

KAPSAM

- ▶ Risk yönetimi ve iç denetimin etkileşimi
- ▶ Değişen risk evreni ve iç denetimden beklentiler
- ▶ Öne çıkan önemli riskler:
 - ▶ Stratejik riskler
 - ▶ Yönetişim riskleri
 - ▶ ESG riskleri
 - ▶ Operasyonel riskler: İş sürekliliği
 - ▶ Operasyonel riskler: Bilgi Teknolojileri
 - ▶ Operasyonel riskler: Siber güvenlik
 - ▶ Suistimal riskleri
- ▶ Risk bazlı denetim planı oluşturma



İD4 İç Denetimde Veri Analitiği Uygulamaları Eğitimi

İD4/10



2 gün

- ▶ İç denetçiler
- ▶ İç kontrol uzmanları
- ▶ Risk yönetimi uzmanları

**AMAÇ**

Veri analitiği uygulamaları, iç denetimin etkinliğini ve verimliliğini artırmada vazgeçilmez bir araç haline gelmiştir. Bu eğitimde iç denetimin çeşitli aşamalarında veri analitiğinin nasıl kullanılacağına açıklanması ve katılımcıların örnek senaryolar üzerinden uygulama yapması amaçlanmaktadır.

KAPSAM

- ▶ Veri analizine giriş:
 - ▶ Temel kavramların hatırlanması
 - ▶ Betimleyici istatistikten yararlanma
 - ▶ İç denetimde popülasyon ve örneklem seçimi
- ▶ Veri temini ve kontrolleri:
 - ▶ Verinin doğruluğu ve bütünlüğüne ilişkin beş temel kontrol alanı ve uygulanacak testler
 - ▶ Veri kalitesine ilişkin hususlar
- ▶ İç denetim süreçlerinde veri analitiği uygulama alanları:
 - ▶ Risk değerlendirmesi ve planlama
 - ▶ Saha çalışması ve testler
 - ▶ Raporlama ve izleme
- ▶ Senaryo çalışmaları (2.gün) - Senaryolar, katılımcıların aşına olduğu herhangi bir veri analizi aracı için uyarlanabilir



İD5 Süreç Madenciliği ile İç Denetim

**1 gün**

- ▶ İç denetçiler
- ▶ İç kontrol uzmanları
- ▶ Süreç ve kontrol sahipleri

**AMAÇ**

Süreç madenciliği, denetçilerin işlemleri ayrıntılı bir biçim incelemelerine olanak tanır. Bu eğitim ile denetçilerin süreç madenciliği teknikleri kullanarak manuel denetim prosedürlerini güncellemesine ve böylece denetim etkinliğini ve verimliliğini artırmasına yardımcı olmak hedeflenmektedir.

KAPSAM

- ▶ İş süreçleri yönetimi ve analizi araçları hakkında bilgilendirme
- ▶ Süreç madenciliği nedir?
- ▶ Süreç madenciliği ile gelen temel yetkinlikler
- ▶ İç denetimde dijital yaklaşımlar ve süreç madenciliğinin rolü
- ▶ Süreç madenciliğinde veri yönetimi, planlama, tasarım ve iç kontrollerin test edilmesi
- ▶ Süreç madenciliği tabanlı denetim uygulama örneği

İD5/10

İD6 SAP Üzerinde Süreç ve Kontrollerin Denetimi

**3 gün**

- ▶ İç denetçiler
- ▶ İç kontrol uzmanları
- ▶ Süreç ve kontrol sahipleri
- ▶ SAP/BT yönetimi

**AMAÇ**

SAP sistemleri birçok organizasyonun iş süreçlerinin temelini oluşturmaktadır. Tüm bilgi sistemleri için geçerli olduğu gibi, SAP sistemlerinin de gerekli iş/uygulama kontrollerini içermemesi durumunda önemli riskler ortaya çıkabilir. Bu eğitimde SAP sisteminde süreç risklerinin tespiti ile bu risklerin SAP üzerinde nasıl kapatılabileceğine yönelik bir farkındalık yaratılması hedeflenmektedir. Eğitimde, iş süreçleri ve uygulama kontrolleri çerçevesinde konfigürasyon, standart raporlar, veri analizleri, görevler ayrılığı ihlalleri, ana veriler gibi konular ele alınacaktır.

KAPSAM

- ▶ Kontrol türleri, kontrol hiyerarşisi ve uygulama kontrollerinin rolü ve önemi
- ▶ SAP sistemlerine genel bakış
- ▶ SAP mimarisi ve bileşenleri
- ▶ Örneklerle temel SAP süreçleri, riskler ve temel kontroller:
 - ▶ Bilgi teknolojileri genel kontrolleri
 - ▶ Satın alma ve ödemeler
 - ▶ Satış ve ticari alacaklar
 - ▶ Üretim, kalite ve bakım yönetimi
 - ▶ Envanter ve maliyetlendirme
 - ▶ Finans ve muhasebe
 - ▶ İnsan Kaynakları

İD6/10



İD7 GRC (Governance, Risk & Compliance) Çözümleri Farkındalık Eğitimi

**1 gün**

- ▶ İç denetçiler
- ▶ Risk yönetimi uzmanları
- ▶ İç kontrol uzmanları

**AMAÇ**

GRC çözümleri günümüzde oldukça talep görmekte birlikte, kritik başarı faktörleri göz önüne alınmadan ve doğru bir planlama yapılmadan gerçekleştirilen yatırımların hedeflenen başarıyı gösteremediği de bilinmektedir. Bu eğitimin amacı GRC çözümlerini tanıtmak ve seçimden kuruluma kadar göz önüne alınması gereken kritik konular ile ilgili farkındalık oluşturmaktır.

KAPSAM

- ▶ GRC teknolojilerinin kapsamı ve temel fonksiyonları
- ▶ GRC örnek mimarisi, veri akışları ve işleyişi
- ▶ GRC teknolojisi seçiminde dikkat edilmesi gereken hususlar
- ▶ Tipik bir GRC projesinin yönetimi ve kritik başarı faktörleri
- ▶ GRC olgunluk değerlendirme matrisi
- ▶ Türkiye'de sektörel olarak kullanımı yaygın GRC ürünleri
- ▶ Çeşitli sektörlerde GRC uygulama vaka analizleri

İD7/10

İD8 Çevik (Agile) İç Denetim Eğitimi

**1 gün**

► İç denetçiler

**AMAÇ**

Eğitimde çevik (agile) yaklaşım ile ilgili farkındalık kazandırılması ve çevik yaklaşım ile ilgili kavramlarının uluslararası iç denetim standartları ile uyumlu bir şekilde, güncel uygulama tecrübeleri çerçevesinde katılımcılara aktarılması amaçlanmaktadır.

KAPSAM

- Çevikliğin temel özellikleri, değerleri ve prensipleri
- Çevik kavramının yazılım geliştirme süreçlerinde ve proje yönetimde kullanımı
- Geleneksel yaklaşım ile çevik yaklaşım arasındaki farklar
- Scrum yönteminin özellikleri ve kavramları
- İç denetimin çevik hale getirilmesi:
 - Çevik iş modeline geçiş
 - Strateji ve operasyon modelinin belirlenmesi
 - Scrum'un çevik denetimde kullanımı
 - Zorluklar ve faydalar
- Vaka çalışması: Örnek bir iç denetim faaliyeti için sprint'ler ve product backlog hazırlama

İD8/10



İD9 İç Kontrol Öz Değerlendirme Eğitimi



2 gün

- ▶ İç kontrol uzmanları
- ▶ Süreç ve kontrol sahipleri
- ▶ İç denetçiler



AMAÇ

Bu eğitim içeriğiyle kurumların üçlü (savunma) hattını güçlendirmek, özellikle birinci seviyedeki kontrollerin etkin yönetimini sağlamak ve suistimal ve operasyonel riskleri azaltarak paydaşlara verilen güvencenin artırılmasını sağlamak hedeflenmektedir.

KAPSAM

- ▶ Kontrol öz değerlendirme nedir?
- ▶ Kontrol öz değerlendirme yönetim yapısı, rol ve sorumlulukları
- ▶ Kontrol öz değerlendirme yaşam döngüsü
- ▶ Kontrol arşivinin oluşturulması
- ▶ Kontrol öz değerlendirme modelinin oluşturulması
- ▶ Kontrol öz değerlendirme modelinin uygulanması
- ▶ Kontrol etkinliğinin belirlenmesi
- ▶ Kontrol öz değerlendirme sonuçlarının açıklanması ve raporlanması (örnek şablon)
- ▶ Vaka çalışması

İD9/10

İD10 Kurumsal Yönetim Denetimi Eğitimi



1 gün

- ▶ İç denetçiler
- ▶ İç kontrol uzmanları
- ▶ Yatırımcı ilişkileri



AMAÇ

Kurumsal yönetime ilişkin yapıların ve süreçlerin uyum durumunun denetlenmesi için gerekli temel bilgilerin ve örnek denetim uygulamalarının paylaşılması hedeflenmektedir.

KAPSAM

- ▶ Kurumsal Yönetimin (Corporate Governance) tanımı; yönetim kavramı ve unsurları
- ▶ Kurumsal yönetimin temel ilkeleri (SPK, OECD ve ISO37001)
- ▶ Üçlü (savunma) hat yapısının özellikleri; iç denetim, iç kontrol ve risk yönetimi entegrasyonu, çeşitli örnek uygulamalar
- ▶ Kurum seviyesi kontroller (entity level controls) ve örnek kapsam çalışması
- ▶ Kurumsal yönetimin denetimine ilişkin öne çıkan hususlar ve örnek denetim adımları

BTD1 BT Uzmanı Olmayanlar İçin BT Denetimi Eğitimi

BTD1/4



2 gün

- ▶ BT iç kontrol, risk ve uyum uzmanları
- ▶ BT iç denetçileri

**AMAÇ**

Bilgi Teknolojileri Denetimi ve Risk Yönetimi alanlarına ilgi duyan veya bu çerçevede yürütülen faaliyetlerin paydaşı olan kişilerin bu alanlara yönelik farkındalık düzeylerinin artırılması ve temel BT denetimi kavramları hakkında bilgilendirilmesi amaçlanmaktadır.

KAPSAM

- ▶ Temel BT kavramları
- ▶ Kurumlarda temel BT altyapısı ve mimarisi
- ▶ BT ve BT risk yönetimi organizasyon yapısı - roller ve sorumluluklar
- ▶ BT denetim ve risk yönetiminin kurumlar için önemi
- ▶ BT denetiminde kullanılan standartlar hakkında özet değerlendirme
- ▶ Bilgi sistemleri yönetimine ilişkin yürürlükteki mevzuat
- ▶ BT genel kontrolleri ve uygulama kontrollerinin temel özellikleri
- ▶ Vaka analiz çalışması (risklerin ve kontrol noktalarının tespiti)
- ▶ Bulgu raporlaması



BTD2 Temel BT Denetimi Eğitimi

BTD2/4



2 gün

- ▶ İç kontrol uzmanları
- ▶ İç denetçileri
- ▶ Risk yönetimi uzmanlar

**AMAÇ**

Bilgi Teknolojileri Denetimi ve Risk Yönetimi alanlarına yönelik kısa süreli deneyime sahip ve bu alanlarda mesleki gelişime ihtiyaç duyan kişilerin bu alanda sahip oldukları birikimleri geliştirmeleri ve temel BT denetim teknikleri ve BT risklerinin yönetimi hakkında bilgilendirilmeleri amaçlanmaktadır.

KAPSAM

- ▶ Kurumlarda temel BT altyapısı ve mimarisi
- ▶ BT ve BT risk yönetimi organizasyon yapısı, roller ve sorumluluklar
- ▶ BT denetim ve risk yönetiminin kurumlar için önemi
- ▶ BT denetiminde kullanılan standartlar hakkında özet değerlendirme
- ▶ BT risk yönetiminde kullanılan yaklaşımlar hakkında özet değerlendirme
- ▶ Bilgi sistemleri yönetimine ilişkin yürürlükteki mevzuat
- ▶ Uygulama kontrolleri ve denetim teknikleri
- ▶ Kritik BT süreçleri, bu süreçlerdeki önemli genel kontroller ve bunların denetim teknikleri
- ▶ Vaka analiz çalışması (risklerin ve kontrol noktalarının tespiti)
- ▶ Bulgu raporlaması



BTD3 İleri BT Denetimi Eğitimi (Laboratuvar Çalışması Dahil)

**2 gün**

- ▶ İç kontrol uzmanları
- ▶ İç denetim uzmanları
- ▶ Risk yönetimi uzmanları

**AMAÇ**

BT denetimleri hakkında temel bilgi birikiminin üzerine sürece yönelik sertifikasyon ve dijitalleşme içerisindeki BT anlayışı eklenmesi ve bilgi teknolojileri alanında uzmanlaşmak isteyen profesyonellerin kendilerine ileri bir vizyon katmaları amaçlanmaktadır.

KAPSAM

- ▶ Dünyada ve ülkemizde bilgi teknolojileri denetiminin gelişimi
- ▶ Bilgi teknolojileri denetimi ile ilgili global düzenlemeler ve standartlar (COBIT, PCAOB denetim standartları, IFAC / IAASB denetim standartları vb.)
- ▶ BT denetimi temel kavramlar ve denetim yöntemleri
- ▶ BT denetim stratejisi ve denetimin planlanması
- ▶ BT yönetim kontrol ve denetimi (laboratuvar ortamında katılımcılarla birlikte BT bileşenleri üzerinde uygulama):
 - ▶ Erişim yönetimi ve görevler ayrılığı
 - ▶ Bilgi sistemleri edinimi geliştirilmesi ve bakımı
 - ▶ Değişiklik yönetimi
 - ▶ Bilgi sistemleri risk yönetimi
 - ▶ Bilgi mimarisi ve veri yönetimi
 - ▶ Denetim izi yönetimi
 - ▶ Konfigürasyon yönetimi (özellikle siber güvenlik kontrolleri ve temel güvenlik konfigürasyonları)
 - ▶ BT sürekliliğinin sağlanması, iş sürekliliğine etkisi
 - ▶ Dış hizmet sağlayıcılarla ilişkilerin yönetimi
- ▶ BT denetim raporu ve görüş bildirme

BTD3/4

BTD4 SAP BT Genel Kontrollerinin Denetimi Eğitimi

**2 gün**

- ▶ İç kontrol uzmanları
- ▶ İç denetçileri
- ▶ Risk yönetimi uzmanları

**AMAÇ**

Özellikle SAP sistemini kullanan kurum ve kuruluşlarda, bu sisteme özgü ve BT kaynaklı riskleri tespit etmek ve bunları yönetmek için uygulanabilecek kontrollerin ve denetim tekniklerinin aktarılması amaçlanmaktadır.

KAPSAM

- ▶ Kontrol türleri, kontrol hiyerarşisi ve BT genel kontrollerinin rolü ve önemi
- ▶ SAP sistemlerine genel bakış
- ▶ SAP mimarisi ve bileşenleri
- ▶ SAP yetkilendirme yapısı ve işleyiş mantığı
- ▶ SAP üzerinde değişiklik yönetimi
- ▶ SAP üzerinde güvenlik ve mantıksal erişim
- ▶ SAP üzerinde BT operasyonlarının yönetimi ve takibi
- ▶ Örnek denetim çalışması

BTD4/4

Siber Güvenlik Eđitimleri

Eđitim
Anlayışımız

Risk Yönetimi
Eđitim Konuları

İç Denetim
Eđitim Konuları

BT Denetimi
Eđitim Konuları

Siber Güvenlik
Eđitim Konuları

Risk Modelleme
Eđitim Konuları

Yönetim Sistemleri
Eđitim Konuları

Kurumsal Güvenlik
Eđitimleri

Bilgi Güvenliđi
Standartı
Eđitimleri

Kişisel Veri
Güvenliđi
Eđitimleri

Teknik Güvenlik
Eđitimleri

Güvenlik Analizi
Eđitimleri

Sızma Testi
Eđitimleri

KG1 Yöneticiler İçin Siber Güvenlik Eğitimi

KG1/6



1/2-1 gün

- ▶ Yönetim Kurulu üyeleri
- ▶ Üst yönetim
- ▶ İş birimi yöneticileri

**AMAÇ**

Bilgi güvenliğinin kapsamına giren ana alanlarla ilgili, uluslararası standartlar çerçevesinde, teknik dilden uzak ancak kapsamlı bir farkındalık programı sağlanması hedeflenmiştir.

KAPSAM

- ▶ Güvenlik ve risk yönetimi
- ▶ Varlık güvenliği
- ▶ Güvenlik mimarisi ve mühendisliği
- ▶ İletişim ve ağ güvenliği
- ▶ Kimlik ve erişim yönetimi
- ▶ Güvenlik değerlendirme ve testi
- ▶ Güvenlik operasyonları
- ▶ Yazılım geliştirme güvenliği
- ▶ Örnek vaka incelemeleri

Kurumsal Güvenlik Eğitimleri

Bilgi Güvenliği Standardı Eğitimleri

Kişisel Veri Güvenliği Eğitimleri

Teknik Güvenlik Eğitimleri

Güvenlik Analizi Eğitimleri

Sızma Testi Eğitimleri

Eğitim Anlayışımız

Risk Yönetimi Eğitim Konuları

İç Denetim Eğitim Konuları

BT Denetimi Eğitim Konuları

Siber Güvenlik Eğitim Konuları

Risk Modelleme Eğitim Konuları

Yönetim Sistemleri Eğitim Konuları



KG2 Siber Güvenlik Analist Eğitimi

KG2/6



2 gün

- ▶ SOC analistleri
- ▶ Siber güvenlik analistleri
- ▶ Giriş seviyesi siber güvenlik uzmanları



AMAÇ

Siber Güvenlik (SOC) Analist eğitimi, saldırıların nasıl belirlenip doğrulanacağına ilişkin temel bilgilerin sağlanmasına yönelik bütünsel yaklaşımı aktararak SIEM, tehdit istihbaratı vb. araçları kullanarak öngörü ve tespit yeteneklerini geliştirmeyi amaçlamaktadır.

KAPSAM

- ▶ Güvenlik operasyonları ve yönetimi
- ▶ Siber tehditleri, IoC'leri ve saldırı metodolojisini anlama
- ▶ Vaka, alarm ve loglama
- ▶ OSI ve TCP/IP modelleri
- ▶ Saldırı tespiti ve SIEM
- ▶ Tehdit istihbaratı ile olay tespiti
- ▶ Siber ataklar ve olay yönetimi

Kurumsal Güvenlik Eğitimleri

Bilgi Güvenliği Standardı Eğitimleri

Kişisel Veri Güvenliği Eğitimleri

Teknik Güvenlik Eğitimleri

Güvenlik Analizi Eğitimleri

Sızma Testi Eğitimleri

Eğitim Anlayışımız

Risk Yönetimi Eğitim Konuları

İç Denetim Eğitim Konuları

BT Denetimi Eğitim Konuları

Siber Güvenlik Eğitim Konuları

Risk Modelleme Eğitim Konuları

Yönetim Sistemleri Eğitim Konuları



KG3 Siber Tehdit İstihbaratı Eğitimi

**1 gün**

- ▶ Siber güvenlik ekipleri
- ▶ SOC analistleri

**AMAÇ**

Siber Tehdit İstihbaratı eğitimi, güvenlik ekiplerini daha etkin hale getirmek, tehdit avını daha doğru yapmak, olay müdahalesini daha etkili hale getirmek ve organizasyonları gelişen tehdit ortamında daha bilinçli hale getirmek için gereken taktik, operasyonel ve stratejik düzeydeki siber tehdit istihbarat becerilerini geliştirmeyi amaçlamaktadır.

KAPSAM

- ▶ İstihbarat nedir?
- ▶ İstihbarat analizi
- ▶ İstihbarata karşı koyma
- ▶ Siber terörizm, açık kaynak istihbaratı, siber savaş
- ▶ Siber güvenlik durum analizi
- ▶ Bireysel ve kurumsal siber güvenlik

Kurumsal Güvenlik Eğitimleri

Bilgi Güvenliği Standardı Eğitimleri

Kişisel Veri Güvenliği Eğitimleri

Teknik Güvenlik Eğitimleri

Güvenlik Analizi Eğitimleri

Sızma Testi Eğitimleri

Eğitim Anlayışımız

Risk Yönetimi Eğitim Konuları

İç Denetim Eğitim Konuları

BT Denetim Eğitim Konuları

Siber Güvenlik Eğitim Konuları

Risk Modelleme Eğitim Konuları

Yönetim Sistemleri Eğitim Konuları



KG3/6

KG4 SOME Eğitimi

KG4/6



3 gün

- ▶ Ağ yönetimi ekipleri
- ▶ Siber güvenlik ekipleri



AMAÇ

SOME personelinin sistemli bir şekilde kayıt analizi ve yönetimi yapabilmesi, kurumun bilişim sistemlerindeki önemli güvenlik zafiyetlerini tespit edebilmesi ve siber olay müdahale koordinasyonu yapabilmesi için gerekli olan temel yetkinlikleri vermeyi hedeflemektedir.

KAPSAM

- ▶ Bilgi teknolojileri temelleri
- ▶ Sistem ve veritabanı sızma testleri
- ▶ Uygulama güvenliği eğitimi
- ▶ Sosyal mühendislik ve DDoS
- ▶ Kayıt yönetimi ve SIEM
- ▶ Siber olaylarla mücadele ekibinin kurulumu ve yönetimi
- ▶ Adli analiz ve zararlı yazılım eğitimi

Kurumsal Güvenlik Eğitimleri

Bilgi Güvenliği Standardı Eğitimleri

Kişisel Veri Güvenliği Eğitimleri

Teknik Güvenlik Eğitimleri

Güvenlik Analizi Eğitimleri

Sızma Testi Eğitimleri

Eğitim Anlayışımız

Risk Yönetimini Eğitim Konuları

İç Denetim Eğitim Konuları

BT Denetimini Eğitim Konuları

Siber Güvenlik Eğitim Konuları

Risk Modelleme Eğitim Konuları

Yönetim Sistemleri Eğitim Konuları



KG5 Cyber CPA Bilgilendirme Eğitimi

**1 gün**

- ▶ İç denetçiler
- ▶ Siber güvenlik ekipleri
- ▶ Ağ yönetim ekipleri

**AMAÇ**

Kurum ve kuruluşların, siber güvenlik olgunluklarının değerlendirilmesi amacıyla başvuru EY Cyber Program Assessment (CPA) çerçevesi, metodolojisi, kaynakları ve çıktıları hakkında bilgi verilmesi hedeflenmektedir.

KAPSAM

- ▶ Mimari
- ▶ Varlık yönetimi
- ▶ Farkındalık
- ▶ İş sürekliliği planlaması (BCP) / Felaketten kurtarma (DR)
- ▶ Veri koruma
- ▶ Yönetişim ve organizasyon
- ▶ Ana sistem (Host) güvenliği
- ▶ Kimlik ve erişim yönetimi (IAM)
- ▶ Olay müdahale
- ▶ Metrikler ve raporlama
- ▶ Ağ güvenliği
- ▶ Operasyonlar
- ▶ Politika ve Standartlar çerçevesi
- ▶ Gizlilik
- ▶ Güvenlik izleme
- ▶ Yazılım güvenliği
- ▶ Strateji
- ▶ Üçüncü taraf yönetimi
- ▶ Tehdit istihbaratı
- ▶ Güvenlik açığı tanımlama ve düzeltme

Kurumsal Güvenlik Eğitimleri

Bilgi Güvenliği Standardı Eğitimleri

Kişisel Veri Güvenliği Eğitimleri

Teknik Güvenlik Eğitimleri

Güvenlik Analizi Eğitimleri

Sızma Testi Eğitimleri

Eğitim Anlayışımız

Risk Yönetimi Eğitim Konuları

İç Denetim Eğitim Konuları

BT Denetimi Eğitim Konuları

Siber Güvenlik Eğitim Konuları

Risk Modelleme Eğitim Konuları

Yönetim Sistemleri Eğitim Konuları



KG6 Teknoloji Sürekliliği Bilgilendirme Eğitimi

**1 gün**

- ▶ Teknoloji sürekliliği ekipleri
- ▶ İş sürekliliği ekipleri
- ▶ Bilgi teknolojileri uzmanları

**AMAÇ**

Günümüzde kurumlar salgın hastalık, deprem ve benzeri nedenlerden dolayı ciddi ve uzun süreli iş kesintileri yaşamaktadır. Bu kesintilere istinaden alınan önlemlerin başında da teknoloji sürekliliği önlemleri gelmektedir. ISO 22301 standardını temel alan teknoloji sürekliliği bilgilendirme eğitimi ile; İş Sürekliliği Yönetim Sistemi yapısının teknoloji sürekliliği ayağının metodolojik bir şekilde nasıl kurulacağı ve kurum içerisinde yönetileceğine dair bilgilerin detaylı bir şekilde verilmesi amaçlanmaktadır.

KAPSAM

- ▶ İş sürekliliği temel kavramları
- ▶ İş sürekliliği yönetiminin planlanması ve uygulanması
- ▶ Teknoloji sürekliliği kavramı
- ▶ Teknoloji sürekliliği yönetimi:
 - ▶ Süreklilik gereksinimleri
 - ▶ Teknoloji envanteri
 - ▶ Mevcut durum incelemesi
 - ▶ GAP analizi
 - ▶ Siber güvenlik incelemesi
 - ▶ Senaryolar ve kümeler
 - ▶ Değişkenler ve varsayımlar
 - ▶ Hedef durum belirlenmesi
 - ▶ Maliyet hesaplamaları

Kurumsal Güvenlik Eğitimleri

Bilgi Güvenliği Standardı Eğitimleri

Kişisel Veri Güvenliği Eğitimleri

Teknik Güvenlik Eğitimleri

Güvenlik Analizi Eğitimleri

Sızma Testi Eğitimleri

Eğitim Anlayışımız

Risk Yönetimi Eğitim Konuları

İç Denetim Eğitim Konuları

BT Denetim Eğitim Konuları

Siber Güvenlik Eğitim Konuları

Risk Modelleme Eğitim Konuları

Yönetim Sistemleri Eğitim Konuları



BGS1 PCI DSS İç Denetçi Eğitimi

BGS1/6



2 gün

- ▶ İç kontrol uzmanları
- ▶ İç denetçiler

**AMAÇ**

Bankalar tarafından üye iş yerleri ve ödeme servis sağlayıcıları için standart bir güvenlik yaklaşımı olan PCI DSS kredi kartı güvenliğinin sağlanması için tek sertifikasyondur. Standarda hakim olmak şirketlerin kredi kartı güvenliğini sağlamasında fayda sağlayacaktır.

Eğitim iç denetçi ve kontrolörlerin PCI DSS standartları denetimine önden hazırlanma ve eksikleri PCI QSA bakışıyla bulmalarını sağlayacaktır.

KAPSAM

- ▶ Kredi kartı güvenlik olaylarının tanıtımı
- ▶ Kredi kartı süreç akışlarının anlatımı
- ▶ PCI DSS denetim süreçleri
- ▶ PCI DSS 3.2.1 standardı genel anlatımı
- ▶ PCI DSS 3.2.1 detay kontrol anlatımı
- ▶ Teknik gereksinim analizleri
- ▶ PCI DSS genel durum analiz adımları
- ▶ PCI DSS kontrollerinde beklenen çıktılar
- ▶ PCI DSS controller arasındaki bağıntı ve bulgular
- ▶ Denetim kapsam belirleme, eksiklik tespiti, değerlendirme ve giderme planları
- ▶ PCI donanım ve iletişim altyapısı
- ▶ Kompanse kontrol tasarımı ve riskler
- ▶ Denetim kontrolünde dikkat edilecek konular

Kurumsal Güvenlik Eğitimleri

Bilgi Güvenliği Standardı Eğitimleri

Kişisel Veri Güvenliği Eğitimleri

Teknik Güvenlik Eğitimleri

Güvenlik Analizi Eğitimleri

Sızma Testi Eğitimleri

Eğitim Anlayışımız

Risk Yönetimi Eğitim Konuları

İç Denetim Eğitim Konuları

BT Denetim Eğitim Konuları

Siber Güvenlik Eğitim Konuları

Risk Modelleme Eğitim Konuları

Yönetim Sistemleri Eğitim Konuları



BGS2 PCI DSS Uyarlayıcı Eđitimi

**2 gün**

- ▶ BT teknik personeli
- ▶ PCI DSS program uyarlayıcıları
- ▶ Güvenlik yönetim ekipleri

**AMAÇ**

Bankalar tarafından üye işyerleri ve ödeme servis sağlayıcıları için standart bir güvenlik yaklaşımı olan PCI DSS kredi kartı güvenliğinin sağlanması için tek sertifikasyondur. Standarda hakim olmak şirketlerin kredi kartı güvenliğini sağlamasında fayda sağlayacaktır.

Bu eğitimle PCI DSS standartlarını şirketlerinde uyarlayan ekiplerin etkin, doğru maliyetli ve kapsamı doğru belirlenmiş şekilde değerlendirme ve uyarlama yapmalarını sağlamak amaçlanmıştır.

KAPSAM

- ▶ Kredi kartı güvenlik olaylarının tanıtımı
- ▶ Kredi kartı süreç akışlarının anlatımı
- ▶ PCI DSS denetim süreçleri
- ▶ PCI DSS 3.2.1 ve 4.0 standardı genel anlatımı
- ▶ PCI DSS 3.2.1 ve 4.0 detay kontrol anlatımı
- ▶ Teknik gereksinim analizleri
- ▶ PCI DSS genel durum analiz adımları
- ▶ PCI DSS kontrollerinin pratik uyarlamaları
- ▶ PCI DSS uyumluluđu için yapılmaması gerekenler
- ▶ Şirket iç uyumluluk analiz anlatımı
- ▶ Gereksinimlere ilişkin soru cevaplar

Kurumsal Güvenlik Eđitimi

Bilgi Güvenliđi Standardı Eđitimi

Kişisel Veri Güvenliđi Eđitimi

Teknik Güvenlik Eđitimi

Güvenlik Analizi Eđitimi

Sızma Testi Eđitimi

Eđitim Anlayışımız

Risk Yönetimi Eđitim Konuları

İç Denetim Eđitim Konuları

BT Denetimi Eđitim Konuları

Siber Güvenlik Eđitim Konuları

Risk Modelleme Eđitim Konuları

Yönetim Sistemleri Eđitim Konuları



BGS3 PCI DSS Farkındalık Eğitimi

**2 saat**

► PCI DSS kapsamında hizmet veren tüm çalışanlar

**AMAÇ**

Kredi kartı ve siber güvenlik ilkelerinin kurum çalışanlarına aktarılması ve çalışanların günlük faaliyetlerinde PCI DSS kültürünü koruması amaçlanmaktadır.

KAPSAM

- PCI DSS genel anlatımı ve test adımları
- PCI DSS ile ilintili PA-DSS PTS DSS ve P2PE standartlarına genel bakış
- Kart endüstrisi ve çeşitli organizasyonların ilişkileri
- Kart şirketleri gereksinimleri
- PCI donanım ve iletişim altyapısı
- PCI raporlama standartları
- PCI güvenlik farkındalığı

BGS3/6

Kurumsal Güvenlik Eğitimleri

Bilgi Güvenliği Standardı Eğitimleri

Kişisel Veri Güvenliği Eğitimleri

Teknik Güvenlik Eğitimleri

Güvenlik Analizi Eğitimleri

Sızma Testi Eğitimleri

Eğitim Anlayışımız

Risk Yönetimi Eğitim Konuları

İç Denetim Eğitim Konuları

BT Denetimi Eğitim Konuları

Siber Güvenlik Eğitim Konuları

Risk Modelleme Eğitim Konuları

Yönetim Sistemleri Eğitim Konuları



BGS4 ISO 27001 Bilgi Güvenliği Yönetim Sistemi Temel Bilgilendirme Eğitimi

**2 gün**

- ▶ Bilgi güvenliği uzmanları
- ▶ Yönetim sistemi uzmanları

**AMAÇ**

ISO 27001 bilgi güvenliği yönetiminin uluslararası standardıdır. ISO 27001 BGYS Temel Bilgilendirme Eğitimi ile faaliyetlerinizde yer alan bütün paydaşlarınızın sistemdeki rollerinden bağımsız olarak temel bilgi güvenliği farkındalıklarının artırılması amaçlanmaktadır.

KAPSAM

- ▶ Bilgi güvenliği kavramı
- ▶ Bilgi güvenliği yönetim sistemleri
- ▶ ISO 27001 standardı
- ▶ Bilgi güvenliği tehditleri
- ▶ Bilgi güvenliği riskleri
- ▶ Bilgi güvenliği farkındalığı
- ▶ Bilgi güvenliği politikaları ve kabul edilebilir kullanım
- ▶ Bilgi güvenliği farkındalık yönetimi
- ▶ Zararlı yazılımlar
- ▶ Sosyal mühendislik
- ▶ ISO 27002 bilgi güvenliği kontrolleri (örnek kontroller ve uygulamaları)

Kurumsal Güvenlik Eğitimleri

Bilgi Güvenliği Standardı Eğitimleri

Kişisel Veri Güvenliği Eğitimleri

Teknik Güvenlik Eğitimleri

Güvenlik Analizi Eğitimleri

Sızma Testi Eğitimleri

Eğitim Anlayışımız

Risk Yönetimi Eğitim Konuları

İç Denetim Eğitim Konuları

BT Denetim Eğitim Konuları

Siber Güvenlik Eğitim Konuları

Risk Modelleme Eğitim Konuları

Yönetim Sistemleri Eğitim Konuları

BGS4/6



BGS5 ISO 27001 Bilgi Güvenliği Yönetim Sistemi Farkındalık Eğitimi

**1 gün**

- ▶ Üst yönetim
- ▶ Kurum çalışanları
- ▶ Tedarikçiler

**AMAÇ**

ISO 27001 bilgi güvenliği yönetiminin uluslararası standardıdır. ISO 27001 BGYS Farkındalık Eğitimi ile faaliyetlerinizde yer alan paydaşlarınızın sistemdeki rolleri (Üst yönetim, tedarikçi, mavi yaka çalışan vb.) ile ilişkili olarak temel bilgi güvenliği farkındalıklarının artırılması amaçlanmaktadır.

KAPSAM

- ▶ Bilgi güvenliği temel kavramları
- ▶ Bilgi güvenliği yönetim sistemi
- ▶ ISO 27001 standardı
- ▶ Bilgi güvenliği tehditleri
- ▶ Bilgi güvenliği riskleri
- ▶ Bilgi güvenliği farkındalığı
- ▶ Kabul edilebilir kullanım
- ▶ Zararlı yazılımlar
- ▶ Sosyal mühendislik

Kurumsal Güvenlik Eğitimleri

Bilgi Güvenliği Standardı Eğitimleri

Kişisel Veri Güvenliği Eğitimleri

Teknik Güvenlik Eğitimleri

Güvenlik Analizi Eğitimleri

Sızma Testi Eğitimleri

Eğitim Anlayışımız

Risk Yönetimi Eğitim Konuları

İç Denetim Eğitim Konuları

BT Denetim Eğitim Konuları

Siber Güvenlik Eğitim Konuları

Risk Modelleme Eğitim Konuları

Yönetim Sistemleri Eğitim Konuları

BGS5/6



BGS6 ISO 27701 Kişisel Veri/Gizlilik Bilgi Yönetim Sistemi Temel Bilgilendirme Eğitimi

**1 gün**

- ▶ Kişisel veri uzmanları
- ▶ Bilgi güvenliği uzmanları
- ▶ Yönetim sistemi uzmanları

**AMAÇ**

ISO 27701 standardı, ISO 27001 Bilgi Güvenliği Yönetim Sistemi standardına kişisel bilgilerin korunması ile ilişkili kontrollerin eklenerek, kişisel veri yönetiminin bir yönetim sistemi disiplini ile yürütülmesine olanak sağlama amacıyla 2019 yılında yayımlanmıştır.

ISO 27701 Kişisel Veri/Gizlilik Bilgi Yönetim Sistemi Temel Bilgilendirme Eğitimi ile faaliyetlerinizde yer alan bütün paydaşlarınızın sistemdeki rollerinden bağımsız olarak kişisel veri ve kişisel veri güvenliği ile ilgili farkındalıklarının artırılması amaçlanmaktadır.

KAPSAM

- ▶ Kişisel veri koruma ve ilgili mevzuatlar (KVKK, GDPR, vb.)
- ▶ ISO 27701 standardı amacı ve faydaları
- ▶ Kişisel veri tehditleri
- ▶ Kişisel veri riskleri
- ▶ Kişisel veri farkındalığı

Kurumsal Güvenlik Eğitimleri

Bilgi Güvenliği Standardı Eğitimleri

Kişisel Veri Güvenliği Eğitimleri

Teknik Güvenlik Eğitimleri

Güvenlik Analizi Eğitimleri

Sızma Testi Eğitimleri

Eğitim Anlayışımız

Risk Yönetimi Eğitim Konuları

İç Denetim Eğitim Konuları

BT Denetim Eğitim Konuları

Siber Güvenlik Eğitim Konuları

Risk Modelleme Eğitim Konuları

Yönetim Sistemleri Eğitim Konuları



KVG1 Kişisel Verilerin Korunması Farkındalık Eğitimi

KVG1/5



1/2-1 gün

- ▶ Üst yönetim
- ▶ Kişisel veri koruma sorumluları
- ▶ Kurum çalışanları



AMAÇ

6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) ile Avrupa Birliği Genel Veri Koruma Yönetmeliği (General Data Protection Regulation - GDPR) kapsamında kurum yönetimlerinin, kişisel veri koruma program paydaşlarının (hukuk, regülasyon, uyum, bilgi güvenliği, veri yönetimi vb.) ve kurum çalışanlarının kanun ve alt düzenlemeleriyle ilgili son gelişmeler, teknik ve idari tedbirler ile teknoloji gereksinimleriyle ilgili bilgilendirilmesi hedeflenmektedir.

KAPSAM

- ▶ KVKK ve GDPR kapsamında genel görünüm ve temel kavramlar
- ▶ Kişisel verilerin işlenmesinde temel ilkeler
- ▶ Kişisel verilerin işlenme şartları
- ▶ Veri sorumlusu, veri işleyen kavramları
- ▶ Özel nitelikli kişisel veriler
- ▶ İlgili kişinin hakları
- ▶ Yönetmelik ve rehberler
- ▶ Kişisel veri ihlalleri kapsamında Türkiye ve dünyadan örnekler
- ▶ Sektörler özelinde çeşitli uygulamaları

Kurumsal Güvenlik Eğitimleri

Bilgi Güvenliği Standardı Eğitimleri

Kişisel Veri Güvenliği Eğitimleri

Teknik Güvenlik Eğitimleri

Güvenlik Analizi Eğitimleri

Sızma Testi Eğitimleri

Eğitim Anlayışımız

Risk Yönetimi Eğitim Konuları

İç Denetim Eğitim Konuları

BT Denetim Eğitim Konuları

Siber Güvenlik Eğitim Konuları

Risk Modelleme Eğitim Konuları

Yönetim Sistemleri Eğitim Konuları



KVG2 Mahremiyet Temelli Tasarım (Privacy by Design) Eğitimi



2 gün

- ▶ Kişisel veri koruma sorumluları
- ▶ Siber güvenlik ekipleri
- ▶ BT geliştirme ekipleri



AMAÇ

Mahremiyet temelli tasarım eğitimi, ürünlerin, hizmetlerin, iş uygulamalarının ve fiziksel altyapıların geliştirilmesinin en başından itibaren gizlilik konularını bütünleştirerek kurumsal gizliliğinin korunmasını sağlamaya çalışan sistem mühendisliği yaklaşımı konusunda katılımcıları bilgilendirmeyi amaçlamaktadır.

KAPSAM

- ▶ "Tasarımla Gizlilik" felsefesi
- ▶ Mahremiyet temelli tasarım ilkeleri ve adımları
- ▶ Gizlilik ve veri koruması tasarımı
- ▶ Yeni ürünler veya hizmetlerle ortaya çıkabilecek gizlilik sorunlarının yönetilmesi
- ▶ Uygulamalı vaka çalışması

Kurumsal Güvenlik Eğitimleri

Bilgi Güvenliği Standardı Eğitimleri

Kişisel Veri Güvenliği Eğitimleri

Teknik Güvenlik Eğitimleri

Güvenlik Analizi Eğitimleri

Sızma Testi Eğitimleri

Eğitim Anlayışımız

Risk Yönetimi Eğitim Konuları

İç Denetim Eğitim Konuları

BT Denetimi Eğitim Konuları

Siber Güvenlik Eğitim Konuları

Risk Modelleme Eğitim Konuları

Yönetim Sistemleri Eğitim Konuları



KVG2/5

KVG3 KVKK ve GDPR Kapsamındaki Teknik ve İdari Tedbirlere Genel Bakış Eğitimi



1/2-1 gün

- ▶ Üst yönetim
- ▶ Kişisel veri koruma sorumluları
- ▶ Kurum çalışanları

**AMAÇ**

6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) ile Avrupa Birliği Genel Veri Koruma Yönetmeliği (General Data Protection Regulation - GDPR) kapsamında tanımlı olan teknik ve idari tedbirler hakkında bilinç oluşturulması ve KVKK ile GDPR arasındaki temel farklılıkların tarificationı hedeflenmektedir.

KAPSAM

- ▶ KVKK ve GDPR kapsamında tanımlı teknik ve idari tedbir gereksinimlerine genel bakış:
 - ▶ Kişisel veri koruma politikaları
 - ▶ Kişisel veri eğitim ve farkındalık programları
 - ▶ Kişisel veri risk yönetim yaklaşımı
 - ▶ Kişisel veri denetimleri
 - ▶ Kişisel veri taleplerinin yönetimi
 - ▶ Kişisel veri ihlallerinin yönetilmesi
 - ▶ Erişim, yetki ve kullanıcı hesap yönetimi
 - ▶ Ağ güvenliği ve saldırı yönetimi
 - ▶ Uygulama güvenliği
 - ▶ Şifreleme ve maskeleyme kontrolleri
 - ▶ Log yönetimi
 - ▶ Veri kaybı önleme kontrolleri
 - ▶ Yedekleme yönetimi
 - ▶ Antivirüs yönetimi
 - ▶ Bilgi güvenliği testleri ve uygunluk değerlendirme
 - ▶ Kişisel veri saklama ve imha kontrolleri
- ▶ Kişisel verilerin korunması kapsamında yol haritası oluşturma ve uyumlaştırma çalışmaları yürütme yaklaşımı
- ▶ Sektörler özelinde örnek uygulamaları

Kurumsal Güvenlik Eğitimleri

Bilgi Güvenliği Standardı Eğitimleri

Kişisel Veri Güvenliği Eğitimleri

Teknik Güvenlik Eğitimleri

Güvenlik Analizi Eğitimleri

Sızma Testi Eğitimleri

Eğitim Anlayışımız

Risk Yönetimi Eğitim Konuları

İç Denetim Eğitim Konuları

BT Denetimi Eğitim Konuları

Siber Güvenlik Eğitim Konuları

Risk Modelleme Eğitim Konuları

Yönetim Sistemleri Eğitim Konuları



KVG4 KVKK Teknik Sistem Yönetim Eğitimi



1-2 gün

- ▶ İç kontrol uzmanları
- ▶ İç denetçiler



AMAÇ

6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) ile Avrupa Birliği Genel Veri Koruma Yönetmeliği (General Data Protection Regulation - GDPR) kapsamında tanımlı olan teknik tedbirlerin uygulanma yöntemlerinin, iyi uygulamalar, sektörel örnekler ve güvenlik kriterleri çerçevesinde tariflenmesi hedeflenmektedir.

Buna ilaveten, kişisel verilerin korunması kapsamında Türkiye'de ve dünyadaki teknoloji ihtiyaçlarına ilişkin trendler örneklenecek, öne çıkan teknik uyum faaliyetleri açıklanacak ve kişisel veri teknoloji ihtiyaçları kapsamındaki temel güvenlik gereksinimleri detaylandırılacaktır.

KAPSAM

- ▶ Kişisel veri teknik tedbirlerine genel bakış
- ▶ Kişisel verilerin korunmasında teknoloji gereksinimleri
- ▶ Kişisel verilerin korunması kapsamındaki teknoloji trendleri
- ▶ Öne çıkan teknik uyum faaliyetleri
- ▶ Kişisel veri teknoloji ihtiyaçları kapsamındaki temel güvenlik gereksinimleri
- ▶ İyi uygulama örnekleri

Kurumsal Güvenlik Eğitimleri

Bilgi Güvenliği Standardı Eğitimleri

Kişisel Veri Güvenliği Eğitimleri

Teknik Güvenlik Eğitimleri

Güvenlik Analizi Eğitimleri

Sızma Testi Eğitimleri

Eğitim Anlayışımız

Risk Yönetimi Eğitim Konuları

İç Denetim Eğitim Konuları

BT Denetim Eğitim Konuları

Siber Güvenlik Eğitim Konuları

Risk Modelleme Eğitim Konuları

Yönetim Sistemleri Eğitim Konuları



KVG5 Kişisel Verilerin Korunması Oyunlaştırma (Gamification) Çalışması



1-2 gün

- ▶ İç kontrol uzmanları
- ▶ İç denetçiler



AMAÇ

Kişisel verilerin korunması kapsamında oyunlaştırma (gamification) teknikleri kullanılarak, önden tanımlı bir senaryo çerçevesinde katılımcılar tarafından kişisel veri uyum gereksinimlerinin değerlendirilerek uygulanması amacıyla interaktif bir çalıştay (workshop) gerçekleştirilmesi hedeflenmektedir.

Oyunlaştırma mekaniklerinin ve bileşenlerinin gerçek hayattaki kişisel veri uyum ihtiyaçlarını baz alacak şekilde simüle edilmesi ile, katılımcıların birer oyuncuya dönüşerek, yüksek motivasyonla, oyun dinamiği içinde yapmaları gereken aktivitelere odaklanmalarının sağlanması amaçlanmaktadır.

KAPSAM

- ▶ İnteraktif ve dijital EY Kişisel Verilerin Korunması Oyunlaştırma (Gamification) Çalışması, aşağıdaki 3 temel ve kritik bileşenin oyunlaştırma deneyimi kapsamında bir araya getirilmesiyle sürekli değişen kişisel veri koruma ekosisteminde benzersiz bir öğrenme deneyimi oluşturur:
 - ▶ İnsan
 - ▶ Teknoloji
 - ▶ Kişisel Verilerin Korunması ve Mahremiyeti
- ▶ Katılımcılar, önceden tanımlanmış ve hedeflenen çalışma sonucuna ulaşmak için motive edilmektedir.
- ▶ Eğitim üç aşamadan oluşmaktadır:
 - ▶ Katılımcılara yeni işlerini tanıtma
 - ▶ Gizlilik sorunlarını çözme oyunu
 - ▶ Değerlendirme

Kurumsal Güvenlik Eğitimleri

Bilgi Güvenliği Standardı Eğitimleri

Kişisel Veri Güvenliği Eğitimleri

Teknik Güvenlik Eğitimleri

Güvenlik Analizi Eğitimleri

Sızma Testi Eğitimleri



TG1 Güvenli Yapılandırma Denetimi Eğitimi

TG1/9



2 gün

- ▶ İç denetçiler
- ▶ Siber güvenlik ekipleri

**AMAÇ**

Katılımcılara bilgi güvenliği ürünlerinin ve yapılarının güvenli yapılandırma ayarları ile ilgili denetleme becerisi kazandırmak amaçlanmaktadır.

KAPSAM

- ▶ Tehdit ve zafiyet tanımı
- ▶ Zafiyet tarama araçları
- ▶ Ağ cihazlarının güvenli yapılandırılması
- ▶ Veritabanı ve uygulamaların güvenli yapılandırması
- ▶ Yapılandırma denetim araçları
- ▶ Web uygulama güvenliği
- ▶ İşletim sistemi denetimi
- ▶ Ağ topolojisi oluşturma
- ▶ Sınır sistemleri denetimi

Kurumsal Güvenlik Eğitimleri

Bilgi Güvenliği Standardı Eğitimleri

Kişisel Veri Güvenliği Eğitimleri

Teknik Güvenlik Eğitimleri

Güvenlik Analizi Eğitimleri

Sızma Testi Eğitimleri

Eğitim Anlayışımız

Risk Yönetimi Eğitim Konuları

İç Denetim Eğitim Konuları

BT Denetimi Eğitim Konuları

Siber Güvenlik Eğitim Konuları

Risk Modelleme Eğitim Konuları

Yönetim Sistemleri Eğitim Konuları



TG2 Blok Zinciri Güvenliği Eğitimi



2 gün

- ▶ Akıllı sözleşme geliştiricileri
- ▶ Blok zinciri geliştiricileri
- ▶ Bilgi güvenliği uzmanları
- ▶ Sızma testi uzmanları



AMAÇ

Katılımcılara blok zinciri (blockchain) ve akıllı sözleşme teknolojisinin anlama, yapılandırma, denetleme becerisi kazandırmak amaçlanmaktadır.

KAPSAM

- ▶ Temel blok zinciri güvenliği
- ▶ Gelişmiş blok zinciri güvenlik mekanizmaları
- ▶ Akıllı sözleşme güvenliği
- ▶ Blok zinciri risk değerlendirmesi
- ▶ İşletmeler için blok zincirlerinin kullanımı
- ▶ Ağ düzeyinde güvenlik açıkları ve istismar yöntemleri
- ▶ Sistem düzeyinde güvenlik açıkları ve istismar yöntemleri
- ▶ Akıllı sözleşme zafiyetleri ve istismar yöntemleri
- ▶ Alternatif DLT mimarilerinin güvenliği

Kurumsal Güvenlik Eğitimleri

Bilgi Güvenliği Standardı Eğitimleri

Kişisel Veri Güvenliği Eğitimleri

Teknik Güvenlik Eğitimleri

Güvenlik Analizi Eğitimleri

Sızma Testi Eğitimleri

Eğitim Anlayışımız

Risk Yönetimi Eğitim Konuları

İç Denetim Eğitim Konuları

BT Denetim Eğitim Konuları

Siber Güvenlik Eğitim Konuları

Risk Modelleme Eğitim Konuları

Yönetim Sistemleri Eğitim Konuları



TG3 Mobil Uygulama Güvenliği Eğitimi

TG3/9



3 gün

- ▶ İç denetçiler
- ▶ İç kontrol uzmanları
- ▶ Uygulama geliştiriciler



AMAÇ

Kurum ve kuruluşların sistemlerinde kullanılmaya başlanılan veya alım yaptığı mobil uygulamaların güvenliğinin sağlanması amacıyla gerçekleştirdiği sızma testlerinin ve analizlerin gerçekleştirilme metodolojisi, ihtiyaç duyulan bilgi birikimi düzeyi, kullanılan araçlar ve gerçekleştirilen faaliyetler hakkında bilgi sağlanması hedeflenmektedir.

KAPSAM

- ▶ iOS temelleri
- ▶ Android temelleri
- ▶ Bilgi toplama
- ▶ Statik analiz
- ▶ Dinamik analiz
- ▶ Güvenlik denetimleri
- ▶ Sık kullanılan araçların incelenmesi
- ▶ OWASP TOP 10 ile sık karşılaşılan zafiyetlerin incelenmesi
- ▶ Mobil uygulama iletişim yöntemleri
- ▶ Wi-Fi, NFC, GSM, 3G, Bluetooth
- ▶ İstemci-sunucu arasında iletişim amaçlı kullanılan protokollerin güvenlik analizi
- ▶ Uygulamaların iletişim kurduğu açık sistemlerin belirlenmesi

Kurumsal Güvenlik Eğitimleri

Bilgi Güvenliği Standardı Eğitimleri

Kişisel Veri Güvenliği Eğitimleri

Teknik Güvenlik Eğitimleri

Güvenlik Analizi Eğitimleri

Sızma Testi Eğitimleri

Eğitim Anlayışımız

Risk Yönetimi Eğitim Konuları

İç Denetim Eğitim Konuları

BT Denetim Eğitim Konuları

Siber Güvenlik Eğitim Konuları

Risk Modelleme Eğitim Konuları

Yönetim Sistemleri Eğitim Konuları



TG4 Veri Tabanı Güvenliği Eğitimi



2 gün

- ▶ İç denetçiler
- ▶ Sistem ekipleri
- ▶ Siber güvenlik ekipleri



AMAÇ

Katılımcıların MS-SQL, MySQL, Oracle, MongoDB gibi veritabanlarında güvenlik açıklarının en aza indirilmesi ve veri tabanı güvenliğinin nasıl yönetileceği konusunda bilgilendirilmesi amaçlanmaktadır.

KAPSAM

- ▶ Veritabanı yapıları
- ▶ Güvenli veritabanı kurulumu
- ▶ Güvenlik yapılandırmaları
- ▶ Veritabanı iletişim protokolleri
- ▶ Veritabanı kullanıcılarının kimlik yönetimi
- ▶ Kullanıcı faaliyetleri ve faaliyetlerin denetlenmesi
- ▶ Parola yönetimi, şifre güvenliği, dikkat edilmesi gereken noktalar
- ▶ Veritabanlarını hedefleyen saldırılar
- ▶ Veritabanları için güvenlik çözümleri
- ▶ Veri sızıntılarına karşı önlemler
- ▶ Veritabanlarında kötüye kullanım faaliyetlerini tespit etme
- ▶ Veritabanı uygulamalarının güvenli geliştirilmesi, kritik verilerin şifrelenmesi/maskelenmesi

Kurumsal Güvenlik Eğitimleri

Bilgi Güvenliği Standardı Eğitimleri

Kişisel Veri Güvenliği Eğitimleri

Teknik Güvenlik Eğitimleri

Güvenlik Analizi Eğitimleri

Sızma Testi Eğitimleri

Eğitim Anlayışımız

Risk Yönetimi Eğitim Konuları

İç Denetim Eğitim Konuları

BT Denetimi Eğitim Konuları

Siber Güvenlik Eğitim Konuları

Risk Modelleme Eğitim Konuları

Yönetim Sistemleri Eğitim Konuları



TG5 Bulut Güvenliği Eğitimi



3 gün

- ▶ İç denetçiler
- ▶ Siber güvenlik ekipleri



AMAÇ

Popüler bulut platformlarının sahip olabileceği açıklıkların tespiti yöntemleri, bu açıklıkların istismar edilmesi, sızma testlerinin gerçekleştirilme metodolojisi, kullanılan araçlar ve gerçekleştirilen faaliyetler hakkında bilgi sağlanması hedeflenmektedir.

KAPSAM

- ▶ Geniş ölçekte mimari ve keşif
- ▶ Kimlik oturumlarına saldırı
- ▶ Bulut hizmetlerine saldırı ve istismar
- ▶ Bulut uygulamalarındaki güvenlik açıkları
- ▶ Altyapı saldırıları ve kırmızı takım çalışması

Kurumsal Güvenlik Eğitimleri

Bilgi Güvenliği Standardı Eğitimleri

Kişisel Veri Güvenliği Eğitimleri

Teknik Güvenlik Eğitimleri

Güvenlik Analizi Eğitimleri

Sızma Testi Eğitimleri

Eğitim Anlayışımız

Risk Yönetimini Eğitim Konuları

İç Denetim Eğitim Konuları

BT Denetimini Eğitim Konuları

Siber Güvenlik Eğitim Konuları

Risk Modelleme Eğitim Konuları

Yönetim Sistemleri Eğitim Konuları



TG6 Bulut Güvenliği Teknik İmplementasyon Eğitimi



3 gün

- ▶ İç denetçiler
- ▶ Ağ yönetim ekipleri
- ▶ Sistem yönetim ekipleri



AMAÇ

Bulut sistemlerinin güvenliğinin sağlanması için teknik anlamda takip edilmesi gereken çerçeve ve prosedürler ve alınması gereken tedbirlerin öğrenilmesi hedeflenmektedir.

KAPSAM

- ▶ Kimlik ve erişim yönetimi
- ▶ Hesaplama ve yapılandırma yönetimi
- ▶ Veri koruma ve otomasyon
- ▶ Ağ oluşturma ve loglama
- ▶ Uyumluluk, olay müdahale ve sızma testi

Kurumsal Güvenlik Eğitimleri

Bilgi Güvenliği Standardı Eğitimleri

Kişisel Veri Güvenliği Eğitimleri

Teknik Güvenlik Eğitimleri

Güvenlik Analizi Eğitimleri

Sızma Testi Eğitimleri

Eğitim Anlayışımız

Risk Yönetimi Eğitim Konuları

İç Denetim Eğitim Konuları

BT Denetim Eğitim Konuları

Siber Güvenlik Eğitim Konuları

Risk Modelleme Eğitim Konuları

Yönetim Sistemleri Eğitim Konuları



TG7 Log Yönetim Sistemleri Kurulum ve Teknik Uyarlama Eğitimi



1-2 gün

- ▶ İç denetçiler
- ▶ İç kontrol uzmanları
- ▶ Siber güvenlik ekipleri
- ▶ Ağ ve sistem yönetim ekipleri



AMAÇ

Kurum ve kuruluşların bilişim altyapısında bulunan sistemlerin üretmiş olduğu logların kapsamlı bir şekilde toplanması, birleştirilmesi, saklanması ve doğru analizler gerçekleştirilmesi gibi adımlardan oluşan log yönetiminin incelenmesi hedeflenmektedir.

KAPSAM

- ▶ Başarılı bir log yönetim sistemi nasıl yapılır
- ▶ Log kaynakları nelerdir
- ▶ Log kaynaklarının ve toplanacak logların seçimi
- ▶ Log yönetim araçlarının seçimi
- ▶ Log analizi, normalizasyonu ve korelasyon
- ▶ IPS/IDS (Network/Host Based) kurulumu ve konfigürasyonu
- ▶ SIEM kurulumu ve konfigürasyonu
- ▶ Alarm yönetimi

Kurumsal Güvenlik Eğitimleri

Bilgi Güvenliği Standardı Eğitimleri

Kişisel Veri Güvenliği Eğitimleri

Teknik Güvenlik Eğitimleri

Güvenlik Analizi Eğitimleri

Sızma Testi Eğitimleri

Eğitim Anlayışımız

Risk Yönetimi Eğitim Konuları

İç Denetim Eğitim Konuları

BT Denetimi Eğitim Konuları

Siber Güvenlik Eğitim Konuları

Risk Modelleme Eğitim Konuları

Yönetim Sistemleri Eğitim Konuları



TG8 Veri Kaybı Önleme (DLP) Yönetimi ve Teknik Uyumlaştırma Eğitimi



1-2 gün

- ▶ İç denetçiler
- ▶ İç kontrol uzmanları
- ▶ Siber güvenlik ekipleri



AMAÇ

Hassas verilere erişim ve bunlar üzerinde gerçekleştirilen işlemlerin izlenmesi, veri sızıntılarına yönelik tanımlama yapılabilmesi ve müdahalelerin gerçekleştirilebilmesi için kural oluşturmayı öğretmek hedeflenmektedir.

KAPSAM

- ▶ Veri sızıntı şekilleri
- ▶ DLP çalışma şekli
- ▶ DLP çeşitleri
- ▶ Fingerprint teknolojisi
- ▶ Veri şifreleme
- ▶ Microsoft Power Automate DLP ilke ayarları
- ▶ Uluslararası standartlarla uyumluluk ve GDPR kontrolleri

Kurumsal Güvenlik Eğitimleri

Bilgi Güvenliği Standardı Eğitimleri

Kişisel Veri Güvenliği Eğitimleri

Teknik Güvenlik Eğitimleri

Güvenlik Analizi Eğitimleri

Sızma Testi Eğitimleri

Eğitim Anlayışımız

Risk Yönetimi Eğitim Konuları

İç Denetim Eğitim Konuları

BT Denetimi Eğitim Konuları

Siber Güvenlik Eğitim Konuları

Risk Modelleme Eğitim Konuları

Yönetim Sistemleri Eğitim Konuları



TG9 Kimlik Yönetimi (IDM) Temel Eğitimi



1-2 gün

- ▶ Kimlik yönetimi ekipleri
- ▶ Siber güvenlik ekipleri

**AMAÇ**

Kimlik Yönetimi (IDM), insanlar, sistemler ve hizmetler için dijital kimliklerin (profillerin) yaşam döngüsünü yönetmek amacıyla toplu olarak kullanılan süreçler ve teknolojilerdir.

Eğitimin amacı, bahse konu kimlik yaşam döngüsünün tesis edilebilmesi için katılımcılara temel kavramlar, teknolojiler, yöntemler ve faaliyetler hakkında bilgi vermektir.

KAPSAM

- ▶ Kimlik ve erişim yönetimine ilişkin temel kavramlar ve süreçler
- ▶ Kimlik yönetimi yaşam döngüsü
- ▶ Erişim yönetimi kontrolleri ve modeli
- ▶ Roller ve sorumluluklar
- ▶ Kimlik ve erişim yönetimi teknolojileri
- ▶ Kimlik ve erişim yönetimi uygulama metodolojileri
- ▶ Güvenlik gereksinimleri ve mevzuata uyum süreçleri

Kurumsal Güvenlik Eğitimleri

Bilgi Güvenliği Standardı Eğitimleri

Kişisel Veri Güvenliği Eğitimleri

Teknik Güvenlik Eğitimleri

Güvenlik Analizi Eğitimleri

Sızma Testi Eğitimleri

Eğitim Anlayışımız

Risk Yönetimi Eğitim Konuları

İç Denetim Eğitim Konuları

BT Denetim Eğitim Konuları

Siber Güvenlik Eğitim Konuları

Risk Modelleme Eğitim Konuları

Yönetim Sistemleri Eğitim Konuları



GA1 Ağ Trafiği Analizi Eğitimi

GA1/3



3 gün

- ▶ Ağ yönetimi ekipleri
- ▶ Adli bilişim ekipleri
- ▶ Siber güvenlik uzmanları



AMAÇ

Ağ trafiğinde yakalanan paketleri okuyup yorumlama, trafiği değerlendirme, çeşitli protokollere hakim olma ve anormallikleri tespit edebilme kabiliyetlerini kazandırmayı; böylelikle hem ağ performansı sorunlarının hem de ağ trafiğinde saldırıların tespit edilip engellenmesine yardımcı olmayı hedeflemektedir.

KAPSAM

- ▶ Ağ trafiği analizine giriş
- ▶ Yaygın protokoller
- ▶ PKI, TLS, SSL, CA, sertifika zinciri kavramları
- ▶ Kayıt ortamları
- ▶ PCAP
- ▶ TCPDUMP aracı ile ağ trafiği analizi
- ▶ Wireshark ile trafik analizi, kayıt dosyaları, zaman damgaları, filtreler
- ▶ Wireshark gelişmiş filtreler, paket birleştirme, ağ trafiğinden dosya analizi

Kurumsal Güvenlik Eğitimleri

Bilgi Güvenliği Standardı Eğitimleri

Kişisel Veri Güvenliği Eğitimleri

Teknik Güvenlik Eğitimleri

Güvenlik Analizi Eğitimleri

Sızma Testi Eğitimleri

Eğitim Anlayışımız

Risk Yönetimi Eğitim Konuları

İç Denetim Eğitim Konuları

BT Denetim Eğitim Konuları

Siber Güvenlik Eğitim Konuları

Risk Modelleme Eğitim Konuları

Yönetim Sistemleri Eğitim Konuları



GA2 Adli Analiz ve Zararlı Yazılım Analizi



3 gün

- ▶ İç denetçiler
- ▶ Siber güvenlik uzmanları
- ▶ Ağ yönetim ekipleri



AMAÇ

Kurum ve kuruluşların bilişim altyapısında meydana gelebilecek veya şüphe uyandıran bilişim olayları karşısında alınması gereken reaksiyon, uygulanması gereken metodoloji ve teknik analiz adımları hakkında bilgi sağlanması hedeflenmektedir.

KAPSAM

- ▶ İşletim sistemlerinde dosyalama sistemleri
- ▶ Veri çıkarma şekilleri
- ▶ Dizi sorguları, veri madenciliği ve e-posta adli analizi
- ▶ Kayıt defteri ve USB analizi
- ▶ Kayıt dosyası analizi
- ▶ Web tarayıcı analizi
- ▶ TCP/IP ağlarda protokol analizi
- ▶ Şifreli trafik analizi
- ▶ Derinlemesine paket incelemesi(DPI)
- ▶ Ağ trafiği analizinde donanımsal bileşenler
- ▶ TCP/IP protokol ailesi adli bilişim analizi
- ▶ Ağ güvenliği cihazları ve temel çalışma yapıları
- ▶ E-posta iletişimde adli bilişim analizi
- ▶ Kablosuz ağlarda adli bilişim analizi
- ▶ Zararlı yazılım tipleri
- ▶ Zararlı yazılımların kurumsal ağlara giriş ve yayılma yöntemleri
- ▶ Web tabanlı zararlı yazılımlar
- ▶ Zararlı yazılımlar için statik analiz ve uygulama örnekleri
- ▶ Zararlı yazılımlar için dinamik analiz ve uygulama örnekleri
- ▶ Sunucu ve sistemlerde hafıza inceleme
- ▶ Uygulamalı Sandbox kurulumu ve örnek bir zararlı yazılım incelemesi

Kurumsal Güvenlik Eğitimleri

Bilgi Güvenliği Standardı Eğitimleri

Kişisel Veri Güvenliği Eğitimleri

Teknik Güvenlik Eğitimleri

Güvenlik Analizi Eğitimleri

Sızma Testi Eğitimleri



GA3 Blue Team Eğitimi



3 gün

- ▶ Ağ yönetimi ekipleri
- ▶ Siber güvenlik ekipleri



AMAÇ

Kişinin güvenlik cihazlarını yapılandırabilme ve sistem güvenlik sıkılaştırmalarını yapabileceği konusunda tecrübe sahibi olması hedeflenmektedir.

KAPSAM

- ▶ MITRE ATT&CK framework
- ▶ Linux sıkılaştırması
- ▶ Windows sıkılaştırması
- ▶ IPS/IDS temelleri ve konfigürasyonu
- ▶ SIEM temelleri ve konfigürasyonu
- ▶ Sistem ve veritabanı güvenliği
- ▶ Ağ cihazları güvenliği ve yapılandırılması
- ▶ Network topolojisi ve yapılandırılması
- ▶ Network trafik analizi
- ▶ AD güvenliği ve policy oluşturulması
- ▶ Log analizi

Kurumsal Güvenlik Eğitimleri

Bilgi Güvenliği Standardı Eğitimleri

Kişisel Veri Güvenliği Eğitimleri

Teknik Güvenlik Eğitimleri

Güvenlik Analizi Eğitimleri

Sızma Testi Eğitimleri

Eğitim Anlayışımız

Risk Yönetimi Eğitim Konuları

İç Denetim Eğitim Konuları

BT Denetim Eğitim Konuları

Siber Güvenlik Eğitim Konuları

Risk Modelleme Eğitim Konuları

Yönetim Sistemleri Eğitim Konuları



ST1 Offensive Security Certified Professional (OSCP) Hazırlık Eğitimi

ST1/6



5 gün

- ▶ Ağ yönetimi ekipleri
- ▶ Siber güvenlik ekipleri



AMAÇ

OSCP sertifikası almak isteyen siber güvenlik uzmanlarının sınava hazırlıklarının sağlanması hedeflenmektedir.

KAPSAM

- ▶ Pasif bilgi toplama
- ▶ Aktif bilgi toplama
- ▶ Güvenlik açığı taraması
- ▶ AD sızma testleri
- ▶ Windows Buffer Overflow saldırıları
- ▶ Linux Buffer Overflow saldırıları
- ▶ Exploitlerle çalışmak
- ▶ Dosya transferleri
- ▶ Hak yükseltme
- ▶ İstemci tarafı saldırıları
- ▶ Web uygulama saldırıları
- ▶ Şifre saldırıları
- ▶ Port yönlendirme ve tünel açma
- ▶ Metasploit framework
- ▶ Antivirüs yazılımlarını atlama

Kurumsal Güvenlik Eğitimleri

Bilgi Güvenliği Standardı Eğitimleri

Kişisel Veri Güvenliği Eğitimleri

Teknik Güvenlik Eğitimleri

Güvenlik Analizi Eğitimleri

Sızma Testi Eğitimleri

Eğitim Anlayışımız

Risk Yönetimi Eğitim Konuları

İç Denetim Eğitim Konuları

BT Denetim Eğitim Konuları

Siber Güvenlik Eğitim Konuları

Risk Modelleme Eğitim Konuları

Yönetim Sistemleri Eğitim Konuları



ST2 Certified Ethical Hacker (CEH) Eğitimi

ST2/6



5 gün

- ▶ İç denetçiler
- ▶ İç kontrol uzmanları
- ▶ Siber güvenlik uzmanları



AMAÇ

CEH sertifikası almak isteyen siber güvenlik uzmanlarının sınava hazırlığının sağlanması hedeflenmektedir.

KAPSAM

- ▶ Footprinting ve bilgi toplama
- ▶ Network taraması
- ▶ E-numeration
- ▶ Açıklık analizi
- ▶ Sistem ele geçirme
- ▶ Kötü amaçlı yazılım tehditleri
- ▶ Sniffing
- ▶ Sosyal mühendislik
- ▶ Dos saldırıları
- ▶ Oturum çalma saldırıları
- ▶ IDS, güvenlik duvarları ve Honeypot atlatma
- ▶ Web uygulamaları istismarı
- ▶ SQL enjeksiyonu
- ▶ Kablosuz ağ istismarları
- ▶ Mobil platform istismarları
- ▶ IoT hacking ve OT hacking
- ▶ Bulut bilişim
- ▶ Kriptografi

Kurumsal Güvenlik Eğitimleri

Bilgi Güvenliği Standardı Eğitimleri

Kişisel Veri Güvenliği Eğitimleri

Teknik Güvenlik Eğitimleri

Güvenlik Analizi Eğitimleri

Sızma Testi Eğitimleri

Eğitim Anlayışımız

Risk Yönetimi Eğitim Konuları

İç Denetim Eğitim Konuları

BT Denetim Eğitim Konuları

Siber Güvenlik Eğitim Konuları

Risk Modelleme Eğitim Konuları

Yönetim Sistemleri Eğitim Konuları



ST3 Web Uygulamalarına Yönelik Testler



3 gün

- ▶ İç denetçiler
- ▶ İç kontrol uzmanları
- ▶ Siber güvenlik uzmanları



AMAÇ

Kurum ve kuruluşların, web uygulamalarının güvenliğini sağlamak amacıyla gerçekleştirdiği sızma testlerinin gerçekleştirilme metodolojisi, ihtiyaç duyulan bilgi birikimi düzeyi, kullanılan araçlar ve gerçekleştirilen faaliyetler hakkında bilgi sağlanması hedeflenmektedir.

KAPSAM

- ▶ Web uygulama mimarisi
- ▶ Ağ servis uygulamaları
- ▶ HTTP protokolü
- ▶ HTTPS protokolü
- ▶ Web sunucu katmanına yönelik saldırılar
- ▶ XSS (Cross Site Scripting) açıklıkları
- ▶ Erişim kontrol açıklıkları
- ▶ Dizin aşım açıklıkları
- ▶ İstemci tarafı kontrollerin aşılması
- ▶ Local/Remote file inclusion
- ▶ Uygulama sunucu yönetim açıklıkları
- ▶ Oturum yönetim açıklıkları
- ▶ Cookie riskleri
- ▶ File upload riskleri
- ▶ CSRF saldırıları
- ▶ Redirection açıklıkları
- ▶ URL ve referer başlıkları
- ▶ HTML comment
- ▶ Uygulama sunucu katmanı injection açıklıkları
- ▶ SQL injection saldırıları
- ▶ XPATH, LDAP, SMTP injection
- ▶ Web servisleri
- ▶ Mantık hataları ve kötüye kullanım senaryoları
- ▶ Jmeter ile yük testi (DDOS saldırı yöntemi)
- ▶ İşletim sistemini ele geçirme
- ▶ Web uygulamaları güvenlik denetim metodolojisi
- ▶ Güvenli yazılım geliştirme metodolojileri
- ▶ Burp Suit modüllerinin kullanımı

Kurumsal Güvenlik Eğitimleri

Bilgi Güvenliği Standardı Eğitimleri

Kişisel Veri Güvenliği Eğitimleri

Teknik Güvenlik Eğitimleri

Güvenlik Analizi Eğitimleri

Sızma Testi Eğitimleri



ST3/6

ST4 Ethical Hacker Bootcamp

**3 gün**

► Siber güvenlik ekipleri

**AMAÇ**

Öğrenilen sızma testi kabiliyetlerinin gerçek yaşamda karşılaşılabilecek güncel uygulama ve işletim sistemlerine sahip örnekleriyle uygulamalı olarak pekiştirilmesini hedeflemektedir.

KAPSAM

- Lab ortamı kurulumu
- Linux işletim sistemi
- Bilgi toplama
- Tarayıcıların kullanımı
- Uygulama: Python kodu ile tarayıcı oluşturma
- Açıklık analizi
- Uygulama: Sistem istismarı ve ele geçirme
- Uygulama: Windows 10 manual istismarı
- Uygulama: Hak yükseltme
- Uygulama: Keylogger çalıştırma
- Uygulama: Python ile Backdoor oluşturma
- Web Uygulamaları sızma testleri
- Uygulama: Python ile Login kaba kuvvet saldırısı
- MITM atakları
- Uygulama LFI/RFI atakları

Kurumsal Güvenlik Eğitimleri

Bilgi Güvenliği Standardı Eğitimleri

Kişisel Veri Güvenliği Eğitimleri

Teknik Güvenlik Eğitimleri

Güvenlik Analizi Eğitimleri

Sızma Testi Eğitimleri

Eğitim Anlayışımız

Risk Yönetimi Eğitim Konuları

İç Denetim Eğitim Konuları

BT Denetim Eğitim Konuları

Siber Güvenlik Eğitim Konuları

Risk Modelleme Eğitim Konuları

Yönetim Sistemleri Eğitim Konuları



ST5 ICS/SCADA Güvenliği Eğitimi



2-3 gün

- ▶ İç denetçiler
- ▶ Ağ ve sistem yönetim ekipleri



AMAÇ

Endüstriyel kontrol/SCADA sistemleri güvenliğinin sağlanması, ilgili kontrollerin tasarlanması ve denetlenmesi konularında kapsamlı bir bilgilendirme yapılması amaçlanmaktadır. Eğitim içeriği, kullanılan sistemlere ve sektörler göre özelleştirilebilir.

KAPSAM

- ▶ Erişim kontrolü
- ▶ Denetim ve hesap verebilirlik
- ▶ Güvenlik değerlendirmesi ve yetkilendirme
- ▶ Konfigürasyon yönetimi
- ▶ Acil durum planlaması
- ▶ Kimlik ve kimlik doğrulama (Tanımlama ve yetkilendirme)
- ▶ Olay müdahale
- ▶ Bakım
- ▶ Medya (Ortam) koruması
- ▶ Fiziksel ve çevresel güvenlik
- ▶ Planlama
- ▶ Bilgi/Sistem güvenliği planı
- ▶ Bilgi/Sistem güvenliği mimarisi
- ▶ Risk değerlendirme
- ▶ Sistem ve iletişim güvenliği
- ▶ Sistem ve bilgi bütünlüğü
- ▶ Program yönetimi
- ▶ Bilgi güvenliği programının planlanması
- ▶ Kritik altyapı planı

Kurumsal Güvenlik Eğitimleri

Bilgi Güvenliği Standardı Eğitimleri

Kişisel Veri Güvenliği Eğitimleri

Teknik Güvenlik Eğitimleri

Güvenlik Analizi Eğitimleri

Sızma Testi Eğitimleri

Eğitim Anlayışımız

Risk Yönetimi Eğitim Konuları

İç Denetim Eğitim Konuları

BT Denetim Eğitim Konuları

Siber Güvenlik Eğitim Konuları

Risk Modelleme Eğitim Konuları

Yönetim Sistemleri Eğitim Konuları



ST6 SCADA Pentesting

**2-3 gün**

- ▶ İç denetçiler
- ▶ Siber güvenlik ekipleri
- ▶ Ağ yönetim ekipleri

**AMAÇ**

Endüstriyel kontrol/SCADA sistemlerinde bulunabilecek açıklıkların tespiti ve kapatılması amacıyla uygulanacak metodoloji, kullanılan araçlar ve yöntemlerin öğretilmesi hedeflenmektedir. Eğitim içeriği, kullanılan sistemlere ve sektörlere göre özelleştirilebilir.

KAPSAM

- ▶ EKS ağının ve mimari analizi
- ▶ Zafiyet tarama analizi
- ▶ Zararlı yazılım analizi
- ▶ Kablosuz ağ ve bileşenleri testleri
- ▶ Ağında sömürü testleri

Kurumsal Güvenlik Eğitimleri

Bilgi Güvenliği Standardı Eğitimleri

Kişisel Veri Güvenliği Eğitimleri

Teknik Güvenlik Eğitimleri

Güvenlik Analizi Eğitimleri

Sızma Testi Eğitimleri

Eğitim Anlayışımız

Risk Yönetimi Eğitim Konuları

İç Denetim Eğitim Konuları

BT Denetimi Eğitim Konuları

Siber Güvenlik Eğitim Konuları

Risk Modelleme Eğitim Konuları

Yönetim Sistemleri Eğitim Konuları



Risk Modelleme Eđitimleri



RM1 R ile Gelişmiş Analitik Yöntemler Eğitimi

RM1/11



5 gün

- ▶ Risk yönetimi uzmanları
- ▶ Tahsis, izleme ve pazarlama analitiği uzmanları
- ▶ İç denetçiler

**AMAÇ**

Temel R programlama dili eğitimiyle birlikte klasik ve modern metotları veri madenciliği ile birleştirerek verideki kalıpları keşfetmeye ve geleceğe dair tahmin yapılmasını sağlayacak yöntemlere ilişkin R uygulamalarının aktarılması hedeflenmektedir.

KAPSAM

- ▶ Temel R eğitimi
- ▶ Karar ve döngü yapıları
- ▶ Betimleyici istatistikler
- ▶ Regresyon
- ▶ Karar ağacı
- ▶ Kümeleme ve sınıflandırma
- ▶ Vaka çalışmaları:
 - ▶ Kredi riski skorlama
 - ▶ Müşteri terk analizi



RM2 R'da Temerrüt Olasılığı Modellemesi ve Model Validasyonu Eğitimi

RM2/11



5 gün

- ▶ Risk yönetimi uzmanları
- ▶ Tahsis, izleme ve pazarlama analitiği uzmanları
- ▶ İç denetçiler

**AMAÇ**

Uygulamalı temel R programlama dili eğitiminin ardından oluşturulacak veri seti ile birlikte Temerrüt Olasılığı Modellemesi ve Model Validasyonunun nasıl uygulanabileceği ve çıkarımların yorumlanmasının aktarılması amaçlanmaktadır.

KAPSAM

- ▶ Temel R eğitimi
- ▶ Veri setinin R ortamına aktarımı ve veri kontrolleri
- ▶ Değişken eleme yöntemleri
- ▶ Eksik değer atama yöntemleri
- ▶ Model kalibrasyonu ve derecelendirme cetvelinin oluşturulması
- ▶ Model performans ve stabilite testleri
- ▶ Lojistik regresyon metotları



RM3 IRB (İçsel Derecelendirmeye Dayalı-İDD) Yaklaşımı Eğitimi

RM3/11

 3 gün

- ▶ İç denetçiler
- ▶ Risk yönetimi uzmanları
- ▶ Tahsis ve izleme uzmanları

**AMAÇ**

İçsel derecelendirme sistemi tasarımı, uygulamaları, denetimi ve validasyonu hakkında geniş kapsamlı bilgilerin aktarılması amaçlanmaktadır.

KAPSAM

- ▶ IRB yaklaşımına genel bakış
- ▶ Kredi riski modelleri için temel konseptler
- ▶ Rating (PD) Model geliştirme
- ▶ LGD model geliştirme
- ▶ EAD/CCF model geliştirme
- ▶ Düşük temerrüt portföyler
- ▶ Risk parametresi validasyonu
- ▶ Süreçlerde kredi riski modellerinin kullanımı
- ▶ Raporlama gereksinimleri

RM4 Üst Seviye Yöneticileri İçin Finansal Risk Yönetimi Regülasyonları Eğitimi

RM4/11

**1 gün**

- ▶ YK üyeleri
- ▶ Üst yönetim
- ▶ Bölüm/Daire başkanları

**AMAÇ**

İçsel derecelendirme sistemi, Basel II , Basel IV ve IFRS 9 regülasyonları için üst yöneticilerin ihtiyaç duyacağı konular hakkında bilgi aktarımları amaçlanmaktadır.

KAPSAM

- ▶ Finansal Risk Yönetimi Regülasyonları: Genel konseptler
- ▶ Basel II ve IRB
- ▶ IRB kullanım testi ve kullanıcı prosedürleri
- ▶ IFRS 9: Beklenen kredi zararı ve ileriye dönük beklentiler
- ▶ Basel IV
- ▶ Finansal Risk Yönetimi regülasyonlarına ilişkin sektör iyi uygulamaları



RM5 Denetçiler İçin IRB (İçsel Derecelendirmeye Dayalı-İDD) Yaklaşımı Eğitimi



2 gün

- ▶ İç denetçiler
- ▶ İç kontrol uzmanları
- ▶ Teftiş uzmanları

**AMAÇ**

İçsel derecelendirme sisteminin incelenmesi esnasında uygulanacak denetim ve validasyon tekniklerinin ekiplere kazandırılması amaçlanmaktadır.

KAPSAM

- ▶ Basel II ve IRB
- ▶ Kredi riski modelleri için temel konseptler
- ▶ PD model denetimi
- ▶ LGD model denetimi
- ▶ EAD/CCF model denetimi
- ▶ Validasyon süreci denetimi
- ▶ Model kullanım süreci denetimi

RM5/11

RM6 Denetçiler İçin Kredi Riski Yönetimi Eğitimi



2 gün

- ▶ İç denetçiler
- ▶ İç kontrol uzmanları
- ▶ Teftiş uzmanları

**AMAÇ**

Kredi riski yönetimde kullanılan yöntemler, teknikler ve model denetimi süreci hakkında kapsamlı bilgi kazandırılması ve ekip yetkinliklerinin artırılması hedeflenmektedir.

KAPSAM

- ▶ Kredi riski için temel konseptler
- ▶ Kredi riski ölçüm teknikleri
- ▶ Kredi riski model denetimi
- ▶ Kredi riski kontrol süreç ve sistem denetimleri
- ▶ Yönetişim konuları

RM6/11

RM7 İSEDES (İçsel Sermaye Yeterliliği Değerlendirme Süreci) Eğitimi



2 gün

► Risk yönetimi uzmanları

**AMAÇ**

İSEDES yönetmeliği ve Basel II doğrultusunda ekonomik sermaye hesaplamaları, stres testi uygulamaları ve süreç hakkında farkındalık oluşturulması hedeflenmiştir.

KAPSAM

- Basel II ve İSEDES
- İSEDES filozofisi ve yapısı
- Bireysel risk değerlendirmesi
- Ekonomik sermaye ve stres testi
- Dokümantasyon

RM7/11

RM8 Denetçiler İçin Validasyon Eğitimi



2 gün

- ▶ İç denetçiler
- ▶ İç kontrol uzmanları
- ▶ Teftiş uzmanları

**AMAÇ**

Kurumların alacak riskine ilişkin geliştirdiği veya kullanmakta olduğu modellerin incelenmesi esnasında kullanılacak niteliksel ve niceliksel yöntemlerin ekiplere kazandırılması hedeflenmektedir.

KAPSAM

- ▶ Validasyonun temel ilkeleri
- ▶ Piyasa riski ölçüm modeli ve validasyon denetimi
- ▶ Kredi riski modellerinin geçerliliği ve denetimi, temel validasyon kuralları

RM8/11

**1 gün**

- ▶ İç denetçiler
- ▶ Risk yönetimi uzmanları
- ▶ İzleme ve finansal muhasebe ekipleri

**AMAÇ**

Alacak riskine ilişkin karşılık hesaplamasını ve buna ilişkin geliştirilebilecek yöntemleri düzenleyen IFRS 9 standardının temel ve önemli noktalarının detaylı bir şekilde ve örnekler üzerinden aktarımının yapılması hedeflenmektedir.

KAPSAM

- ▶ Sınıflandırma ve ölçüm
- ▶ Değer düşüklüğü
- ▶ Kredi riskinde önemli derecede artış
- ▶ Kredi riski parametreleri
- ▶ Geriye dönük testler
- ▶ IFRS 9 implementasyon denetimi

RM10 Risk İzleme ve Tahsilat Analitiği Eğitimi

**1 gün**

- ▶ İç denetçiler
- ▶ Risk yönetimi uzmanları
- ▶ İzleme ve finansal muhasebe ekipleri

**AMAÇ**

Kurumların risk izleme ve tahsilat fonksiyonlarının analitik yöntemlerle desteklenerek daha etkin yönetimi için gerekli sektör iyi uygulamaları hakkında temel yetkinliklerin kazandırılması hedeflenmektedir.

KAPSAM

- ▶ Erken uyarı sistemleri
- ▶ Karar destek sistemlerinin izleme süreçlerinde kullanımı
- ▶ Tahsilat skorkartları
- ▶ İzleme ve raporlama faaliyetleri
- ▶ Yönetişim konuları

RM10/11

RM11 Doğal Afetlerin Risk Yönetimine Etkileri Eğitimi

**1 gün**

- ▶ İç denetçiler
- ▶ Risk yönetimi uzmanları
- ▶ Tahsil ve İzleme uzmanları

**AMAÇ**

Özellikle Covid-19 ile birlikte gündemde olan salgın, deprem, kuraklık gibi doğal afetlerin risk yönetimine etkilerinin, afet öncesi ve afet sonrası alınması gereken temel aksiyon noktalarının değerlendirilmesi amaçlanmaktadır.

KAPSAM

- ▶ Kredi risk modellerine etkiler
- ▶ Tahsis ve izleme sistemlerine etkiler
- ▶ Doğal afet sonrası portföy yönetim stratejileri
- ▶ Sorunlu alacak azaltım stratejileri
- ▶ İzleme ve erken uyarı fonksiyonlarının önemi
- ▶ Doğal afetlerden alınan dersler

Yönetim Sistemleri Eğitimleri

Eğitim
Anlayışımız

Risk Yönetimi
Eğitim Konuları

İc Denetim
Eğitim Konuları

BT Denetimi
Eğitim Konuları

Siber Güvenlik
Eğitim Konuları

Risk Modelleme
Eğitim Konuları

Yönetim Sistemleri
Eğitim Konuları



YS1 ISO 9001 Kalite Yönetim Sistemi Temel Bilgilendirme Eğitimi

**2 gün**

- ▶ Süreç ve kalite yönetimi uzmanları
- ▶ Yönetim sistemi uzmanları

**AMAÇ**

ISO 9001 Kalite Yönetim Sistemi, bir kuruluşun müşterilerinin ve çalışmalarından etkilenen diğer paydaşların beklentileri, ihtiyaçları ve mevzuat şartlarını karşılama yoluyla müşteri memnuniyetinin artırılmasını öngörmektedir.

ISO 9001 eğitimi ile kalite yönetim sisteminin temel kavramları ile gerekliliklerinden bahsedilerek kuruluşlar için öneminin anlaşılması amaçlanmaktadır.

KAPSAM

- ▶ Kalite Yönetim Sistemi'nin önemi ve faydaları
- ▶ Kalite Yönetim Sistemi temel kavramları
- ▶ ISO 9001 Yönetim Sistemi temel gereklilikleri
- ▶ Planla-Uygula-Kontrol et-Önlem al yönetimi anlayışı
- ▶ Süreç yaklaşımı
- ▶ Kalite Yönetim Sistemi'nin planlanması
- ▶ Operasyonel süreçlerin Kalite Yönetim Sistemi'ne etkisi
- ▶ Performans değerlendirme ve sürekli iyileştirme

YS2 IATF 16949 Otomotiv Kalite Yönetim Sistemi Temel Bilgilendirme Eğitimi

YS2/7



2 gün

- ▶ Süreç ve kalite yönetimi uzmanları
- ▶ Yönetim sistemi uzmanları

**AMAÇ**

IATF 16949 Otomotiv Kalite Yönetim Sistemi, otomotiv üretimi ve yan sanayi kuruluşlarının otomotiv ile ilgili ürünlerin tasarımı, geliştirilmesi, üretimi, montajı ve servis hizmetleri içi kalite sistem gerekliliklerini belirlemektedir.

ISO 9001 tabanlı IATF 16949 eğitimi ile otomotiv sektöründe uluslararası alanda standardize olmuş kalite yönetimi farkındalığının artırılması amaçlanmaktadır.

KAPSAM

- ▶ Otomotiv Kalite Yönetim Sistemi'nin önemi ve faydaları
- ▶ Otomotiv Kalite Yönetim Sistemi temel kavramları
- ▶ IATF 16949 Yönetim Sistemi temel gereklilikleri
- ▶ ISO 9001 hakkında genel bilgilendirme
- ▶ Otomotiv Kalite Yönetim Sistemi uygulamaları

YS3 ISO 14001 Çevre Yönetim Sistemi Temel Bilgilendirme Eğitimi

**2 gün**

- ▶ Süreç ve kalite yönetimi uzmanları
- ▶ Yönetim sistemi uzmanları

**AMAÇ**

ISO 14001 Çevre Yönetim Sistemi, kuruluşun hammaddeden, nihai ürünün müşteriye sunulmasına kadar olan süreç içerisindeki çevresel faktörlerin belirlenmesi ve bu faktörlere yönelik önlemlerin alınarak çevresel etkinin en aza indirilmesini amaçlayan bir yönetim standardıdır.

ISO 14001 eğitiminde çevre yönetim sistemlerinin gereklilikleri ve temel kavramlar ile farkındalığın artırılması amaçlanmaktadır.

KAPSAM

- ▶ Çevre Yönetim Sistemi'nin önemi ve faydaları
- ▶ Çevre Yönetim Sistemi temel kavramları
- ▶ ISO 14001 Çevre Yönetim Sistemi temel gereklilikleri
- ▶ Çevre boyut ve etkileri değerlendirmesi
- ▶ Planla-Uygula-Kontrol Et-Önlem Alı yönetimi anlayışı
- ▶ Çevre Yönetim Sistemi ve dokümantasyon

YS3/7



YS4 ISO 45001 İSG Yönetim Sistemi Temel Bilgilendirme Eğitimi

**2 gün**

- ▶ İş sağlığı ve güvenliği uzmanları
- ▶ Yönetim sistemi uzmanları

**AMAÇ**

ISO 45001 İş Sağlığı ve Güvenliği Yönetim Sistemi, çalışanların iş sağlığı ve güvenliğini artırmaya, iş kazalarını, meslek hastalıklarını azaltmaya, ulusal ve uluslararası yasal düzenlemelere uyum sağlanmasına yardımcı olan bir yönetim standardıdır.

ISO 45001 eğitimi ile etkin bir yönetim yapısı ve gereklilikleri hakkında farkındalık yaratmak amaçlanmaktadır.

KAPSAM

- ▶ İş Sağlığı ve Güvenliği Yönetim Sistemi tanımı
- ▶ İş Sağlığı ve Güvenliği Yönetim Sistemi'nin önemi ve faydaları
- ▶ Temel iş sağlığı ve güvenliği kavramları
- ▶ ISO 45001 temel gereklilikleri
- ▶ Tehditlerin belirlenmesi ve risklerin analizi
- ▶ İSG Yönetim Sistemi ve dokümantasyon

YS4/7



YS5 ISO 19011 Uyumlu Yönetim Sistemleri İç Tetkikçi Eğitimi

**2 gün**

- ▶ Yönetim sistemi uzmanları
- ▶ İç denetçiler

**AMAÇ**

ISO 19011 Uyumlu Yönetim Sistemleri İç Tetkikçi Eğitimi'nin amacı; yönetim sistemlerinin planlanmış düzenlemelere, standartların şartlarına ve kuruluş tarafından oluşturulan yönetim sistemi şartlarına uyulmasını ve yönetim standartlarının etkinliğinin devamlılığını belirlemek için gerçekleştirilen tetkiklere yönelik iç tetkik sorumlularının eğitilmesi amaçlanmaktadır.

KAPSAM

- ▶ Standard maddelerinin yorumlanması
- ▶ Yönetim sistemleri temel kavramları ve gereksinimler
- ▶ ISO 19011 standardının tanıtımı
- ▶ Tetkik çeşitleri ve tanımları
- ▶ Tetkikin faydaları
- ▶ Tetkikin yönetimi
- ▶ Tetkikin planlanması
- ▶ Kontrol ve soru listelerinin hazırlanması
- ▶ Tetkikin sonuçlandırılması ve rapor yazımı
- ▶ Tetkik görevlisinin sorumlulukları

YS5/7

YS6 Sosyal Sorumluluk Standartları Temel Bilgilendirme (ISO 26000, SA 8000) Eğitimi

**2 gün**

- ▶ Yönetim sistemi uzmanları
- ▶ Kurumsal iletişim uzmanları
- ▶ İnsan kaynakları uzmanları

**AMAÇ**

ISO 26000 standardı, sosyal sorumluluk alanında uluslararası çapta kabul görmüş bir rehberdir.

Sosyal Sorumluluk Standartları Temel Bilgilendirme eğitimi ile sosyal sorumluluk olgusunun tanınması ve sosyal sorumluluk ilkelerinin oluşturulmasına yönelik farkındalığın artırılması amaçlanmaktadır.

KAPSAM

- ▶ Sosyal sorumluluk standardı önemi ve faydaları
- ▶ Sosyal sorumluluk temel kavramları
- ▶ Sürdürülebilir kalkınma
- ▶ Sosyal sorumluluk yönetimi
- ▶ Sosyal sorumluluk ilkeleri
- ▶ Paydaşların katılımı
- ▶ Sosyal sorumluluk ana konuları ve uygulamaları:
 - ▶ Organizasyonel yönetim
 - ▶ İnsan hakları
 - ▶ Çalışan uygulamaları
 - ▶ Çevre
 - ▶ Adil çalışma uygulamaları
 - ▶ Tüketici meseleleri
 - ▶ Toplumsal katılım ve gelişme

YS6/7

**2 gün**

- ▶ Yönetim sistemleri uzmanları
- ▶ Süreç ve kalite uzmanları

**AMAÇ**

Entegre Yönetim Sistemi, ISO 9001, ISO 14001 ve ISO 45001 yönetim sistemlerinin tek çatı altında toplandığı ve gerekliliklerin eş zamanlı karşılanabildiği bütünsel bir yönetim sistemi uygulamasıdır.

Entegre Yönetim Sistemleri Temel Bilgilendirme eğitimi ile uygulamalarınızı ve gerekli dokümantasyonu daha etkili ve tek bir yapı halinde nasıl sürdürülebileceğinin aktarılması amaçlanmaktadır.

KAPSAM

- ▶ Entegre Yönetim Sistemi önemi ve faydaları
- ▶ ISO 9001, ISO 14001, ISO 45001 standartlarının tanıtımı, temel kavramları ve entegre uygulamaları
- ▶ Yönetim sistemlerinin planlanması
- ▶ Yönetim sistemlerinin uygulanması ve işletilmesi
- ▶ Dokümantasyon süreçleri
- ▶ Performans değerlendirme ve iç tetkik
- ▶ Yönetimin gözden geçirmesi

EY | Daha iyi bir çalışma dünyası oluřturmak

EY olarak amacımız; müşterilerimiz, çalışanlarımız ve toplum için değer yaratırken aynı zamanda sermaye piyasalarında güvenin ve daha iyi bir çalışma dünyasının oluşmasına katkıda bulunmaktır.

Dünya çapında 150'den fazla ülkede, sahip olduğumuz veri ve teknoloji ile hizmet veren ekiplerimizle, denetimde güveni sağlarken müşterilerimizin gelişmesine ve dönüşmesine destek oluyoruz.

Bağımsız denetim, danışmanlık, hukuk, kurumsal finansman, strateji ve vergi hizmetlerimizle iş dünyasının karşılaştığı zorluklara yeni çözümler sunacak doğru soruları soruyoruz.

EY adı küresel organizasyonu temsil eder ve Ernst & Young Global Limited'in her biri ayrı birer tüzel kişiliğe sahip olan, bir veya daha çok, üye firmasını temsil edebilir. Sınırlı sorumlu bir Birleşik Krallık şirketi olan Ernst & Young Global Limited müşteri hizmeti sunmamaktadır. Kişisel Verileri Koruma Kanunu (KVKK) kapsamında; EY'ın kişisel verileri nasıl topladığı, kullandığı ve bireylerin sahip olduğu haklara dair bilgilere ey.com/tr_tr/privacy-statement adresinden ulaşabilirsiniz. EY üye şirketleri yerel kanunların yasakladığı bölgelerde hukuk hizmeti sunmaz. Daha fazla bilgi için lütfen ey.com adresini ziyaret edin.

© 2024 EY Türkiye.
Tüm Hakları Saklıdır.

Sadece genel bilgi verme amacıyla sunulan bu yayın muhasebe, vergi, hukuk veya diğer profesyonel hizmetler alanında geçerli bir kaynak olarak kullanılması amacıyla hazırlanmamıştır. Belirli bir konuya ilişkin olarak ilgili danışmana başvurulmalıdır.

ey.com/tr
[linkedin.com/ernstandyoung](https://www.linkedin.com/company/ernstandyoung)
[facebook.com/ErnstYoungTurkiye](https://www.facebook.com/ErnstYoungTurkiye)
[instagram.com/eyturkiye](https://www.instagram.com/eyturkiye)
twitter.com/EY_Turkiye

İletişim

www.ey.com/tr_tr