EĞİTİM KATALOĞU

"Çalışanlarınızı eğitip işten ayrılmalarından daha kötü olan tek şey onları eğitmemek ve işte kalmalarını sağlamaktır."
Henry FORD

ICT Trend Academy Eğitim ve Danışmanlık Hizmetleri LTD. ŞTİ
Cevizli Mah. Tugay Yolu Cad. Piazza AVM No:69C/222
34846 Maltepe/İSTANBUL

- www.icttrendacademy.com.tr
- www.icttrendconsultancy.com.tr
- info@icttrendacademy.com.tr
- +90 850 466 0 428

BİLİŞİM STANDARTLARI EĞİTİMLERİ

ICT Trend Academy Eğitim ve Danışmanlık Hizmetleri LTD. ŞTİ
Cevizli Mah. Tugay Yolu Cad. Piazza AVM No:69C/222
34846 Maltepe/İSTANBUL

- www.icttrendacademy.com.tr
- www.icttrendconsultancy.com.tr
- info@icttrendacademy.com.tr
- +90 850 466 0 428

BİLGİ GÜVENLİĞİ VE SİBER GÜVENLİK FARKINDALIK EĞİTİMLERİ

ISO 20000-1:2019 BT Servis Yönetimi Farkındalık Eğitimi

Eğitimin Amacı

- Bu eğitimin amacı, ISO 20000-1:2019 Bilgi Teknolojileri Servis Yönetim Sistemi standardı hakkında katılımcılara genel farkındalık kazandırmak; BT servis yönetiminin temel prensiplerini, standardın yapısını ve kuruluşlara sağladığı faydaları özet seviyede aktarmaktır. Eğitim, servis yönetimi yaklaşımının organizasyon genelinde anlaşılmasını hedefler.

Katılımcı Profili

- Kuruluşlarında BT servis yönetimi süreçlerinde görev alan çalışanlar,
- ISO 20000-1 standardı hakkında temel bilgi sahibi olmak isteyen yöneticiler,
- BT ekipleri ve servis sağlayıcı firmaların çalışanları.

Eğitim Süresi

- 1 gün

Eğitim İçeriği

- BT Servis Yönetimi Temel Kavramları ve Önemi
- ISO/IEC 20000-1:2019 Standardına Genel Bakış
- Servis Yönetim Sistemi (SMS) Yaklaşımı
- Servis Yaşam Döngüsü ve Temel Servis Yönetimi Süreçleri
- Roller, Sorumluluklar ve Sürekli İyileştirme Yaklaşımı

ISO 22301:2019 İş Sürekliliği Yönetim Sistemi

Eğitimin Amacı

- ISO 22301 İş Sürekliliği Yönetim Sistemi eğitiminin temel amacı işletmenin olağan dışı bir durum karşısında gerekecek müdahale kapasitesini oluşturmaktır. ISO 22301 İSYS Standardı, kuruluşunuza potansiyel tehditleri tanımlayabilecek, etkilerini değerlendirebilecek ve kesintileri asgari seviyeye indirecek bir uluslararası anlayış sunar. Etkili bir İSYS uygulayan bir kuruluş, beklenmeyen kesintilerle karşılaştığında, sadece müşterilerini ve itibarını koruma konusunda yarar sağlamaz, ayrıca benzer zorluklara karşı rakipler karşısında avantaj sağlayabilir.

Katılımcı Profili

- İş Sürekliliği yönetici ve çalışanları,
- Bilgi Teknolojileri yönetici ve çalışanları,
- İş sürekliliği yönetim sisteminin uygulanması ve yönetiminden sorumlu personeller.

Eğitim Süresi

- 1 gün

Eğitim İçeriği

- İş sürekliliği tanımları ve İş Sürekliliği Yönetim Sistemi terimleri
- ISO 22301:2019 İş Sürekliliği Yönetim Sistemi Standardı
- Planlama ve kontrol
- İş etki analizi ve risk belirlemesi
- İş sürekliliği stratejisi

ISO 27001:2022 Bilgi Güvenliği Yönetim Sistemi

Eğitimin Amacı

- Bu eğitimde amaç, ISO 27001:2022 Bilgi Güvenliği Yönetim Sistemi (BGYS) tetkikçilerini bir Tetkik Planını yönetmek, planlamak, idare etmek ve uygulamak üzere yetiştirmek ve katılımcılara BGYS standardı hakkında ve sistemin tüm maddeleri için genel bilgilendirme yapmak, uygulamanın gerçekleştirilmesi ve sistemin kurulması için örneklerle açıklayıcı bilgiler sunmaktır.

Katılımcı Profili

- Kuruluşlarında ISO 27001 Bilgi Güvenliği Yönetim Sistemi kurmak veya kurulmuş sistemi yönetmek, iyileştirmek isteyen çalışanlar, ya da bilgi güvenliği alanında kendini geliştirmek isteyen herkes.

Eğitim Süresi

- 1 gün

Eğitim İçeriği

- Bilgi Güvenliği Temel Kavramları ve Bilgi Güvenliğinin Önemi
- ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardı Özeti
- Güvenlik Tehditleri ve İncelenebilirlikleri
- Güvenlik Risklerinin Yönetimi
- Güvenlik Kontrollerinin Seçimi

ISO 27005:2014 Bilgi Güvenliği Risk Yönetimi

Eğitimin Amacı

- Bu eğitimde Bilgi Teknolojileri Risk Yönetim çerçevesinin kurulması, işletilmesi ve yönetilmesini sağlamak amacıyla katılımcılara temel bilgiler verilmesi hedeflenmektedir. Katılımcıların eğitimin sonunda öğrendikleri bilgiler eşliğinde kurumlarında etkin risk yönetim uygulayabilecek seviyeye gelmeleri beklenmektedir. Eğitim içeriği ISO/IEC 27005:2014 Bilgi Güvenliği Risk Yönetimi dokümanı baz alınarak hazırlanmıştır. Örnek uygulamaların ve atölye çalışmalarının yer aldığı eğitimde bilgi güvenliği riskleri, tehditler ve açıkları detaylı olarak ele alınacaktır.

Katılımcı Profili

- İşletme bünyesindeki risk yöneticileri ve risk yönetim takım üyeleri, IT Risk yöneticileri, IT yöneticileri, bilgi güvenliği yöneticiler, IT yöneticileri, IT ve risk yönetiminden sorumlu orta seviye organizasyon yöneticileri, iç kontrol ve denetim ekip üyeleri, IT uzmanları ve danışmanlar.

Eğitim Süresi

- 1 gün

Eğitim İçeriği

- Risk Yönetimi ile ilgili terimler ve tanımlar
- Etkin Risk Yönetim Adımları
- Risk Analizi Kapsamın Belirlenmesi
- Varlıkların Belirlenmesi ve Varlık Envanterinin Oluşturulması
- Varlık Sınıflandırma ve Varlık Değerleme
- Risk Belirleme Şekilleri
- Risk Kategorileri

ISO 27701:2019 Kişisel Veri Yönetim Sistemi

Eğitimin Amacı

- ISO/IEC 27701; kuruluş bağlamındaki gizlilik yönetimi için ISO/IEC 27001 ve ISO/IEC 27002'nin bir eklentisi olacak şekilde Kişisel Veri Yönetim Sistemi (KVYS) oluşturulması, uygulanması, sürdürülmesi ve sürekli olarak iyileştirilmesine ilişkin gereklilikleri kapsar ve kılavuz bilgiler sunar. Bu belge; KVYS ile ilgili gereklilikleri belirtirken, kişisel veri işlenmesine ilişkin sorumluluğu ve hesap verebilirliği olan kişisel veri sorumluları ve kişisel veri işleyenlere de kılavuz bilgiler verir.
- Bu eğitimde amaç kuruluşlara Kişisel Veri Yönetim Sistemi (KVYS) konusunda kişisel veri ve kişisel veri güvenliği ile ilgili farkındalıklarının artırmak; örneklemlerle Standart ve denetim anlayışı konusunda yetkinlik kazandırmaktır.

Katılımcı Profili

- Bu belge; bir BGYS bünyesinde kişisel veri sorumlusu olan ve/veya kişisel verileri, kişisel veri işleyen sıfatıyla işleyen kamu şirketleri ve özel şirketler, devlet oluşumları, kâr amacı gütmeyen kuruluşlar dâhil, her tipteki ve büyüklükteki kuruluş için geçerlidir.

Eğitim Süresi

- 1 gün

Eğitim İçeriği

- Kişisel veri nedir?
- Özel Nitelikli Kişisel Veri nedir?
- Kişisel veri koruma ve ilgili mevzuatlar (KVKK, GDPR, vb.)
- 6698 Sayılı Kişisel Verilerin Korunması Kanunu (KVKK)
- ISO 27701-ISO 27001 ilişkisi
- KVKK Yönetmelikleri
- Kişisel Verileri Koruma Politikası
- Veri Sorumlusu kimdir?
- Veri İşleme Temsilcisi
- Aydınlatma Yükümlülüğü
- Açık Rıza
- Kişisel veri tehditleri
- Kişisel veri riskleri
- Kişisel veri farkındalığı

ISO 42001:2023 Yapay Zeka Yönetim Sistemi

Eğitimin Amacı

- Bu eğitimin amacı, ISO/IEC 42001:2023 Yapay Zeka Yönetim Sistemi standardı hakkında katılımcılara temel farkındalık kazandırmak; yapay zekâ sistemlerinin sorumlu, güvenilir ve etik şekilde yönetilmesine yönelik yönetim sistemi yaklaşımını tanıtmaktır.

Katılımcı Profili

- Yapay zekâ kullanan veya kullanmayı planlayan kuruluşların yöneticileri,
- BT ve dijital dönüşüm ekipleri,
- Veri ve yazılım ekipleri, bilgi güvenliği,
- Uyum, risk ve iç denetim ekipleri ile standart hakkında genel bilgi edinmek isteyen tüm çalışanlar.

Eğitim Süresi

- 1 gün

Eğitim İçeriği

- Yapay zekâ temel kavramları ve organizasyonlar için önemi
- ISO/IEC 42001:2023 standardının amacı, kapsamı ve yapısı
- Yapay Zeka Yönetim Sistemi (AIMS) yaklaşımı ve temel bileşenleri
- Yapay zekâ yaşam döngüsü ve temel risk alanları
- Etik, şeffaflık, insan gözetimi ve sorumlu yapay zekâ prensipleri
- Sürekli iyileştirme yaklaşımı ve belgelendirme sürecine genel bakış

Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Bilgi ve İletişim Güvenliği Rehberi

Eğitimin Amacı

- Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, tüm kamu kurum ve kuruluşları ile kritik altyapı sektörlerinden "Elektronik Haberleşme", "Enerji", "Su Yönetimi", "Ulaştırma", "Bankacılık ve Finans" sektörleri ve nüfus, sağlık, güvenlik gibi alanlarda "Kritik Kamu Hizmetleri" sunan işletmelerin alması gereken tedbirleri belirlemek amacıyla Bilgi ve İletişim Güvenliği Rehberi yayınladı. Rehber kurumların hazırlıklarını ivedilikle tamamlaması ve yıl sonuna kadar denetimden geçmelerini öngörüyor. Bilgi ve iletişim güvenliği rehberi kurumların bu süreçte izlemesi gereken yolları detaylı bir şekilde anlatıyor. Bu eğitimde amaç kurumları bu süreçte bilinçlendirmek denetimlere hazırlamaktır.

Katılımcı Profili

- Elektronik Haberleşme, Enerji, Su Yönetimi", Ulaştırma, Bankacılık ve Finans sektörleri ve nüfus, sağlık, güvenlik gibi alanlarda Kritik Kamu Hizmetleri sunan kamu ve özel kurumlar

Eğitim Süresi

- 2 gün

Eğitim İçeriği

- Genelge'nin kapsamı ve Genelge'de açıklanan bilgi güvenliği tedbirleri nelerdir?
- Bilgi ve İletişim Güvenliği Rehberi hangi kurum ve kuruluşları kapsamaktadır?
- Bilgi ve İletişim Güvenliği Rehberi İçeriği
- Bilgi ve İletişim Güvenliği Rehberi Uygulama Süreci
- Varlık Envanteri Boşluk Analizi
- Varlık Gruplarına Yönelik Güvenlik Tedbirleri
- Uygulama ve Teknoloji Alanlarına Yönelik Güvenlik Tedbirleri
- Sıkılaştırma Tedbirleri
- Rehberde kullanılan formlar/dokümanlar
- Bilgi ve İletişim Güvenliği Denetim Rehberi İçeriği
- Bilgi ve İletişim Güvenliği Rehberi ile ISO 27001 BGYS İlişkisi
- Genelge ve Rehberler için Uyum Süreleri

Cyber GRC (Yönetişim, Risk ve Uyum) Yönetimi

Eğitimin Amacı

- Bu eğitimin amacı; katılımcılara Cyber GRC (Yönetişim, Risk ve Uyum) yaklaşımına ilişkin temel farkındalık kazandırmak, bilgi güvenliği ve siber risklerin iş süreçleri, yönetişim ve uyum gereksinimleriyle olan ilişkisini üst seviyeden ele almaktır.
- Eğitim kapsamında, ISO/IEC 27005 Bilgi Güvenliği Risk Yönetimi yaklaşımı esas alınarak; risk, tehdit, açıklık ve kontrol kavramlarının temel mantığı aktarılacak, risk yönetiminin yalnızca teknik bir konu olmadığı, kurumsal ve yönetsel bir sorumluluk olduğu vurgulanacaktır.
- Eğitim sonunda katılımcıların, kurumlarında yürütülen risk ve uyum çalışmalarını doğru okuyabilen, sorgulayabilen ve yönlendirebilen bir farkındalık seviyesine ulaşmaları hedeflenmektedir.

Katılımcı Profili

- Üst ve orta kademe yöneticiler
- İş birimi yöneticileri
- IT ve Bilgi Güvenliği yöneticileri
- Risk yönetimi, iç kontrol ve uyum ekipleri
- İç denetim ve IT denetim ekipleri
- Cyber GRC ve bilgi güvenliği konularında farkındalık kazanmak isteyen yöneticiler ve uzmanlar

Eğitim Süresi

- 1 gün

Eğitim İçeriği

- Cyber GRC (Yönetişim, Risk ve Uyum) kavramı ve temel bileşenleri
- Siber risklerin iş riski üzerindeki etkileri
- Yönetişim bakış açısıyla bilgi güvenliği ve risk yönetimi
- Bilgi güvenliği risk yönetimine ilişkin temel terimler ve tanımlar
- ISO/IEC 27005 kapsamında risk yönetimi yaklaşımının genel yapısı
- Risk, tehdit, açıklık (zafiyet) ve kontrol kavramlarının ilişkisi
- Varlık, gizlilik, bütünlük ve erişilebilirlik (CIA) kavramlarına üst seviye bakış
- Risk yönetimi sürecinin temel adımları (kapsam, risk belirleme, değerlendirme, kontrol, izleme)
- Risk, kontrol ve uyum (ISO 27001, KVKK vb.) arasındaki ilişki
- Yönetim ve denetim perspektifinden Cyber GRC farkındalığı
- Kısa vaka örnekleri ile risk yönetimi yaklaşımının değerlendirilmesi

Kişisel Verilerin Korunması Kanunu (KVKK) Farkındalık Eğitimi

Eğitimin Amacı

- Bu eğitimin amacı; katılımcılara 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) kapsamında kişisel verilerin korunmasına ilişkin temel kavramlar, yükümlülükler ve sorumluluklar hakkında farkındalık kazandırmaktır.
- Eğitim kapsamında; kişisel verilerin hukuka uygun işlenmesi, saklanması, aktarılması ve imhasına ilişkin temel prensipler, çalışanların ve yöneticilerin KVKK sürecindeki rolleri üst seviyeden ele alınacaktır.
- Eğitim sonunda katılımcıların, günlük iş süreçlerinde kişisel veri içeren faaliyetleri ayırt edebilen, riskleri fark edebilen ve kurumsal KVKK politikalarına uygun davranış geliştirebilen bir farkındalık seviyesine ulaşmaları hedeflenmektedir.

Katılımcı Profili

- Üst ve orta kademe yöneticiler
- Tüm çalışanlar
- İnsan Kaynakları, Satınalma, Satış ve Pazarlama ekipleri
- IT ve Bilgi Güvenliği ekipleri
- Hukuk, uyum ve risk yönetimi ekipleri
- İç denetim ekipleri
- KVKK konusunda farkındalık kazanmak isteyen tüm paydaşlar

Eğitim Süresi

- 1 gün

Eğitim İçeriği

- Kişisel veri ve özel nitelikli kişisel veri kavramları
- KVKK'nın amacı, kapsamı ve temel ilkeleri
- Veri sorumlusu ve veri işleyen kavramları
- Kişisel verilerin işlenme şartları ve hukuki sebepler
- Açık rıza kavramı ve uygulamada sık yapılan hatalar
- Kişisel verilerin aktarımı (yurt içi / yurt dışı) farkındalığı
- Veri güvenliği yükümlülükleri ve çalışan sorumlulukları
- Kişisel veri ihlali nedir, nasıl hareket edilmelidir?
- Veri sahiplerinin hakları ve başvuru süreçleri
- VERBİS kaydı ve envanter farkındalığı
- Kişisel verilerin saklanması, silinmesi ve imhasına farkındalık
- KVKK idari para cezaları ve örnek kararlar
- Gerçek vaka örnekleri ile KVKK farkındalığı

Siber Güvenlik ve Bilgi Güvenliği Farkındalık Eğitimi

Eğitimin Amacı

- Bu eğitimin amacı; katılımcılara Siber Güvenlik ve Bilgi Güvenliği kavramlarına ilişkin temel farkındalık kazandırmak, bilgi varlıklarının korunmasının yalnızca teknik ekiplerin değil, tüm çalışanların ve yöneticilerin ortak sorumluluğu olduğu bilincini oluşturmaktır.
- Eğitim kapsamında; bilgi güvenliğinin temel ilkeleri, güncel siber tehditler, insan faktörünün önemi ve güvenli davranış kültürü üst seviyeden ele alınacaktır.
- Eğitim sonunda katılımcıların, günlük iş yaşamında karşılaşabilecekleri siber riskleri tanıyabilen, doğru tepkiyi verebilen ve kurumsal bilgi güvenliği politikalarına uygun davranış geliştirebilen bir farkındalık seviyesine ulaşmaları hedeflenmektedir.

Katılımcı Profili

- Üst ve orta kademe yöneticiler
- Tüm çalışanlar
- İş birimi yöneticileri
- IT ve Bilgi Güvenliği ekipleri
- Risk, iç kontrol ve uyum ekipleri
- İç denetim ekipleri
- Siber ve bilgi güvenliği konularında farkındalık kazanmak isteyen tüm paydaşlar

Eğitim Süresi

- 1 gün

Eğitim İçeriği

- Bilgi güvenliği ve siber güvenlik kavramları
- Bilgi varlıkları ve korunmasının önemi
- Gizlilik, Bütünlük ve Erişilebilirlik (CIA) ilkeleri
- Bilgi Güvenliği Yönetim Sistemi'ne genel bakış
- Güncel siber tehditler ve saldırı türleri
- Sosyal mühendislik ve oltalama (phishing) saldırıları
- İnsan faktörü ve güvenli kullanıcı davranışları
- Parola güvenliği ve erişim farkındalığı
- Mobil cihaz, uzaktan çalışma ve bulut güvenliği farkındalığı
- Bilgi güvenliği ihlalleri ve olası etkileri
- KVKK ve kişisel verilerin korunmasına farkındalık düzeyinde bakış
- Gerçek vaka örnekleri ile siber güvenlik farkındalığı

BT STANDARTLARI UYGULAMA VE DOKÜMAN EĞİTİMLERİ

ISO 20000-1:2019 BT Servis Yönetim Sistemi

Eğitimin Amacı

- Bu eğitimin amacı, ISO/IEC 20000-1:2019 BT Servis Yönetim Sistemi standardının kuruluşlarda uygulanması, dokümante edilmesi ve belgelendirmeye hazır hale getirilmesi için gerekli bilgi ve becerilerin kazandırılmasıdır. Eğitim kapsamında, servis yönetim sisteminin kurulumu, süreçlerin tanımlanması, dokümantasyon yapısının oluşturulması ve uygulamada karşılaşılan temel sorunlara yönelik rehberlik sağlanır.

Katılımcı Profili

- BT servis yönetimi süreçlerinde görev alan yöneticiler, süreç sahipleri, servis yöneticileri,
- BT operasyon ekipleri,
- Kalite ve iç denetim ekipleri
- ISO 20000-1 belgelendirme sürecinde aktif rol alacak çalışanlar.

Eğitim Süresi

- 2 gün

Eğitim İçeriği

- ISO 20000-1:2019 Standardının Uygulama Yaklaşımı
- Servis Yönetim Sistemi Dokümantasyon Yapısı
- Servis Envanteri ve Kapsam Belirleme Çalışmaları
- Temel BT Servis Yönetimi Süreçlerinin Uygulanması
- Roller, Sorumluluklar ve Organizasyonel Yapı
- Performans İzleme ve Sürekli İyileştirme
- Belgelendirme Süreci ve Denetim Hazırlıkları

ISO 22301:2019 İş Sürekliliği Yönetim Sistemi

Eğitimin Amacı

- ISO 22301 İş Sürekliliği Yönetim Sistemi eğitiminin temel amacı işletmenin olağan dışı bir durum karşısında gerekecek müdahale kapasitesini oluşturmaktır. ISO 22301 İSYS Standardı, kuruluşunuza potansiyel tehditleri tanımlayabilecek, etkilerini değerlendirebilecek ve kesintileri asgari seviyeye indirecek bir uluslararası anlayış sunar. Etkili bir İSYS uygulayan bir kuruluş, beklenmeyen kesintilerle karşılaştığında, sadece müşterilerini ve itibarını koruma konusunda yarar sağlamaz, ayrıca benzer zorluklara karşı rakipler karşısında avantaj sağlayabilir.

Katılımcı Profili

- İş Sürekliliği yönetici ve çalışanları,
- Bilgi Teknolojileri yönetici ve çalışanları,
- İş sürekliliği yönetim sisteminin uygulanması ve yönetiminden sorumlu personeller.

Eğitim Süresi

- 2 gün

Eğitim İçeriği

- İş sürekliliği tanımları ve İş Sürekliliği Yönetim Sistemi terimleri
- ISO 22301:2019 İş Sürekliliği Yönetim Sistemi Standardı
- Planlama ve kontrol
- İş etki analizi ve risk belirlemesi
- İş sürekliliği stratejisi
- İş sürekliliği prosedürlerinin oluşturulması ve gerçekleştirilmesi
- Tatbik etme ve test işlemi
- İzleme, ölçme, analiz ve değerlendirme
- İç denetim ve düzeltici faaliyetler

ISO 27001:2022 Bilgi Güvenliği Yönetim Sistemi

Eğitimin Amacı

- Bu eğitimde amaç, ISO 27001:2022 Bilgi Güvenliği Yönetim Sistemi (BGYS) tetkikçilerini bir Tetkik Planını yönetmek, planlamak, idare etmek ve uygulamak üzere yetiştirmek ve katılımcılara BGYS standardı hakkında ve sistemin tüm maddeleri için genel bilgilendirme yapmak, uygulamanın gerçekleştirilmesi ve sistemin kurulması için örneklerle açıklayıcı bilgiler sunmaktır.

Katılımcı Profili

- Kuruluşlarında ISO 27001 Bilgi Güvenliği Yönetim Sistemi kurmak veya kurulmuş sistemi yönetmek, iyileştirmek isteyen çalışanlar, ya da bilgi güvenliği alanında kendini geliştirmek isteyen herkes.

Eğitim Süresi

- 2 gün

Eğitim İçeriği

- Bilgi Güvenliği Temel Kavramları ve Bilgi Güvenliğinin Önemi
- ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardı Özeti
- Güvenlik Tehditleri ve İncelenebilirlikleri
- Güvenlik Risklerinin Yönetimi
- Güvenlik Kontrollerinin Seçimi
- Bilgi Güvenliği Yönetim Sistemi Denetimi
- Uygunsuzluk ve Düzeltici Önleyici Faaliyet Raporu
- Liste, Rapor, Plan Örnekleri
- Örnek Denetim Uygulaması

ISO 27005:2014 Bilgi Güvenliği Risk Yönetimi

Eğitimin Amacı

- Bu eğitimde Bilgi Teknolojileri Risk Yönetim çerçevesinin kurulması, işletilmesi ve yönetilmesini sağlamak amacıyla katılımcılara temel bilgiler verilmesi hedeflenmektedir. Katılımcıların eğitimin sonunda öğrendikleri bilgiler eşliğinde kurumlarında etkin risk yönetim uygulayabilecek seviyeye gelmeleri beklenmektedir. Eğitim içeriği ISO/IEC 27005:2014 Bilgi Güvenliği Risk Yönetimi dokümanı baz alınarak hazırlanmıştır. Örnek uygulamaların ve atölye çalışmalarının yer aldığı eğitimde bilgi güvenliği riskleri, tehditler ve açıkları detaylı olarak ele alınacaktır.

Katılımcı Profili

- İşletme bünyesindeki risk yöneticileri ve risk yönetim takım üyeleri, IT Risk yöneticileri, IT yöneticileri, bilgi güvenliği yöneticiler, IT yöneticileri, IT ve risk yönetiminden sorumlu orta seviye organizasyon yöneticileri, iç kontrol ve denetim ekip üyeleri, IT uzmanları ve danışmanlar.

Eğitim Süresi

- 2 gün

Eğitim İçeriği

- Risk Yönetimi ile ilgili terimler ve tanımlar
- Etkin Risk Yönetim Adımları
- Risk Analizi Kapsamın Belirlenmesi
- Varlıkların Belirlenmesi ve Varlık Envanterinin Oluşturulması
- Varlık Sınıflandırma ve Varlık Değerleme
- Risk Belirleme Şekilleri
- Risk Kategorileri
- Tehditlerin ve Açıklıkların Belirlenmesi
- Olasılık Değerlendirme
- Tehdit/Açıklık/Olasılık için Atölye Çalışması
- Etki Analizi
- Risk Seviye Değerinin Hesaplanması
- Risk Derecelendirme
- Uygun Kontrollerin Seçimi ve Uygulanması
- Risk izleme ve gözden geçirme
- Risk Değerlendirme Uygulamasına Yönelik Atölye Çalışması

ISO 27701:2019 Kişisel Veri Yönetim Sistemi

Eğitimin Amacı

- ISO/IEC 27701; kuruluş bağlamındaki gizlilik yönetimi için ISO/IEC 27001 ve ISO/IEC 27002'nin bir eklentisi olacak şekilde Kişisel Veri Yönetim Sistemi (KVYS) oluşturulması, uygulanması, sürdürülmesi ve sürekli olarak iyileştirilmesine ilişkin gereklilikleri kapsar ve kılavuz bilgiler sunar. Bu belge; KVYS ile ilgili gereklilikleri belirtirken, kişisel veri işlenmesine ilişkin sorumluluğu ve hesap verebilirliği olan kişisel veri sorumluları ve kişisel veri işleyenlere de kılavuz bilgiler verir.
- Bu eğitimde amaç kuruluşlara Kişisel Veri Yönetim Sistemi (KVYS) konusunda kişisel veri ve kişisel veri güvenliği ile ilgili farkındalıklarının artırmak; örneklemlerle Standart ve denetim anlayışı konusunda yetkinlik kazandırmaktır.

Katılımcı Profili

- Bu belge; bir BGYS bünyesinde kişisel veri sorumlusu olan ve/veya kişisel verileri, kişisel veri işleyen sıfatıyla işleyen kamu şirketleri ve özel şirketler, devlet oluşumları, kâr amacı gütmeyen kuruluşlar dâhil, her tipteki ve büyüklükteki kuruluş için geçerlidir.

Eğitim Süresi

- 2 gün

Eğitim İçeriği

- Kişisel veri nedir?
- Özel Nitelikli Kişisel Veri nedir?
- Kişisel veri koruma ve ilgili mevzuatlar (KVKK, GDPR, vb.)
- 6698 Sayılı Kişisel Verilerin Korunması Kanunu (KVKK)
- ISO 27701-ISO 27001 ilişkisi
- KVKK Yönetmelikleri
- Kişisel Verileri Koruma Politikası
- Veri Sorumlusu kimdir?
- Veri İşleme Temsilcisi
- Aydınlatma Yükümlülüğü
- Açık Rıza
- Kişisel veri tehditleri
- Kişisel veri riskleri
- Kişisel veri farkındalığı
- KVKK yönetim süreci ve uygulamaları
- Pratik Çalışmalar
- Atölye Çalışmaları

ISO 42001:2023 Yapay Zeka Yönetim Sistemi

Eğitimin Amacı

- Bu eğitimin amacı, ISO/IEC 42001:2023 Yapay Zeka Yönetim Sistemi standardının kuruluşlarda kurulması, uygulanması, dokümante edilmesi ve belgelendirmeye hazır hale getirilmesi için gerekli bilgi ve uygulama yaklaşımını kazandırmaktır. Eğitim kapsamında, yapay zekâ sistemlerine yönelik yönetişim, risk yönetimi ve yaşam döngüsü kontrolleri uygulama örnekleriyle ele alınır.

Katılımcı Profili

- Yapay zekâ projelerinde görev alan yöneticiler,
- BT ve dijital dönüşüm ekipleri, veri bilimi ve yazılım ekipleri,
- Bilgi güvenliği, KVKK/uyum, risk ve iç denetim ekipleri
- ISO 42001 belgelendirme sürecinde aktif rol alacak çalışanlar.

Eğitim Süresi

- 2 gün

Eğitim İçeriği

- ISO 42001:2023 Standardının Yapısı ve Kapsamı
- Yapay Zeka Yönetim Sistemi (AIMS) Kurulumu
- Yapay Zeka Risk Yönetimi Yaklaşımı
- Yapay Zeka Yaşam Döngüsü Yönetimi
- AIMS Dokümantasyon Yapısı
- Operasyonel Kontroller ve Uygulama Süreçleri
- Performans İzleme ve Sürekli İyileştirme
- Belgelendirme Süreci ve Denetim Hazırlığı

Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Bilgi ve İletişim Güvenliği Rehberi

Eğitimin Amacı

- Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, tüm kamu kurum ve kuruluşları ile kritik altyapı sektörlerinden "Elektronik Haberleşme", "Enerji", "Su Yönetimi", "Ulaştırma", "Bankacılık ve Finans" sektörleri ve nüfus, sağlık, güvenlik gibi alanlarda "Kritik Kamu Hizmetleri" sunan işletmelerin alması gereken tedbirleri belirlemek amacıyla Bilgi ve İletişim Güvenliği Rehberi yayınladı. Rehber kurumların hazırlıklarını ivedilikle tamamlaması ve yıl sonuna kadar denetimden geçmelerini öngörüyor. Bilgi ve iletişim güvenliği rehberi kurumların bu süreçte izlemesi gereken yolları detaylı bir şekilde anlatıyor. Bu eğitimde amaç kurumları bu süreçte bilinçlendirmek denetimlere hazırlamaktır.

Katılımcı Profili

- Elektronik Haberleşme, Enerji, Su Yönetimi", Ulaştırma, Bankacılık ve Finans sektörleri ve nüfus, sağlık, güvenlik gibi alanlarda Kritik Kamu Hizmetleri sunan kamu ve özel kurumlar

Eğitim Süresi

- 2 gün

Eğitim İçeriği

- Genelge'nin kapsamı ve Genelge'de açıklanan bilgi güvenliği tedbirleri nelerdir?
- Bilgi ve İletişim Güvenliği Rehberi hangi kurum ve kuruluşları kapsamaktadır?
- Bilgi ve İletişim Güvenliği Rehberi İçeriği
- Bilgi ve İletişim Güvenliği Rehberi Uygulama Süreci
- Varlık Envanteri Boşluk Analizi
- Varlık Gruplarına Yönelik Güvenlik Tedbirleri
- Uygulama ve Teknoloji Alanlarına Yönelik Güvenlik Tedbirleri
- Sıkılaştırma Tedbirleri
- Rehberde kullanılan formlar/dokümanlar
- Bilgi ve İletişim Güvenliği Denetim Rehberi İçeriği
- Bilgi ve İletişim Güvenliği Rehberi ile ISO 27001 BGYS İlişkisi
- Genelge ve Rehberler için Uyum Süreleri

6998 Sayılı Kişisel Verilerin Korunması Kanunu (KVKK) Uygulama Eğitimi

Eğitimin Amacı

- Bu eğitimin amacı, 6698 sayılı Kişisel Verilerin Korunması Kanunu kapsamında kuruluşların hukuki ve teknik uyum yükümlülüklerini yerine getirebilmesi, KVKK uygulamalarının hayata geçirilmesi ve gerekli dokümantasyon altyapısının oluşturulması için katılımcılara uygulamaya yönelik bilgi ve beceri kazandırmaktır. Eğitim süresince, KVKK uyum sürecinin baştan sona nasıl yönetileceği ele alınır.

Katılımcı Profili

- Üst ve orta kademe yöneticiler
- Tüm çalışanlar
- İnsan Kaynakları, Satınalma, Satış ve Pazarlama ekipleri
- IT ve Bilgi Güvenliği ekipleri
- Hukuk, uyum ve risk yönetimi ekipleri
- İç denetim ekipleri
- KVKK konusunda farkındalık kazanmak isteyen tüm paydaşlar

Eğitim Süresi

- 2 gün

Eğitim İçeriği

- 6698 sayılı KVKK'nın amacı, kapsamı ve temel kavramlar
- Veri sorumlusu ve veri işleyen yükümlülükleri
- Kişisel veri işleme şartları ve hukuki dayanaklar
- Özel nitelikli kişisel verilerin işlenmesi ve alınması gereken tedbirler
- Aydınlatma yükümlülüğü ve aydınlatma metni hazırlanması
- Açık rıza kavramı ve açık rıza metinlerinin oluşturulması
- Veri işleme envanteri ve kişisel veri haritalandırma çalışmaları
- VERBİS kayıt süreci ve uygulamada dikkat edilmesi gereken hususlar
- Kişisel verilerin aktarılması (yurt içi / yurt dışı) ve alınacak önlemler
- Kişisel verilerin saklanması, imhası ve saklama–imha politikası
- Teknik ve idari tedbirlerin belirlenmesi ve uygulanması
- Kişisel veri ihlali yönetimi ve ihlal bildirim süreçleri
- Veri sahiplerinin hakları ve başvuru süreçlerinin yönetimi
- KVKK kapsamında sözleşmeler ve taahhütnameler
- KVKK dokümantasyon yapısı ve zorunlu dokümanlar
- İç denetim, izleme ve sürekli iyileştirme yaklaşımı
- KVKK denetimleri, yaptırımlar ve iyi uygulama örnekleri

BİLİŞİM STANDARTLARI İÇ DENETÇİ EĞİTİMLERİ

ISO 20000-1:2019 BT Servis Yönetimi Sistemi İç Denetçi Eğitimi

Eğitimin Amacı

- Bu eğitimin amacı, ISO/IEC 20000-1:2019 BT Servis Yönetimi standardı kapsamında kuruluşların gerçekleştirmesi gereken iç denetim faaliyetlerini planlayabilecek, yürütebilecek ve raporlayabilecek iç denetçilerin yetiştirilmesidir. Eğitim süresince, standardın maddeleri, iç denetim prensipleri ve uygulamalı denetim teknikleri ele alınır. Eğitimi başarıyla tamamlayan katılımcılar, ISO 20000-1 kapsamında iç denetim gerçekleştirebilecek bilgi ve yetkinliği kazanır.
- Eğitim sonunda bir sınav yapılacak olup, ilgili standart konusunda İç Tetkik gerçekleştirmek isteyen tüm katılımcılar bu sınavdan başarılı oldukları takdirde eğitim programına ait **"İç Tetkikçi Sertifikası"** almaya hak kazanacaklardır.

Katılımcı Profili

- BT servis yönetimi süreçlerinde görev alan çalışanlar, Süreç ve servis sahipleri,
- Kalite ve iç denetim ekipleri,
- BT yöneticileri,
- ISO 20000-1 belgelendirme sürecinde görev alacak personel ile iç denetçi olmak isteyen tüm katılımcılar.

Eğitim Süresi

- 3 gün

Eğitim İçeriği

- ISO 20000-1:2019 standardına genel bakış ve iç denetimin rolü
- İç denetim kavramı, amaçları ve ISO yönetim sistemlerindeki yeri
- İç denetçinin sahip olması gereken yetkinlikler ve etik ilkeler
- Denetim programı ve denetim planının hazırlanması
- Denetim kapsamı, kriterleri ve denetim ekibinin belirlenmesi
- Açılış ve kapanış toplantılarının yürütülmesi
- Denetimde soru sorma teknikleri ve mülakat yöntemleri
- Objektif delil kavramı ve delil toplama yöntemleri
- ISO 20000-1 ana madde gerekliliklerinin denetimi
- BT servis yönetimi süreçlerinin denetim yaklaşımı
- Uygunsuzluk türleri (majör, minör, gözlem) ve karar verme
- Uygunsuzlukların ilgili standart maddeleriyle ilişkilendirilmesi
- Düzeltici faaliyetlerin tanımlanması ve takibi
- Denetim raporunun hazırlanması ve sonuçların sunulması
- İç denetim sonrası izleme ve sürekli iyileştirme yaklaşımı
- Denetim planı hazırlanması
- Denetim soru listesi oluşturulması
- Örnek denetim senaryosu üzerinden denetim uygulaması
- Uygunsuzluk tespiti ve sınıflandırılması
- Düzeltici faaliyet formu doldurma

ISO 22301:2019 İş Sürekliliği Yönetim Sistemi

Eğitimin Amacı

- ISO 22301 İş Sürekliliği Yönetim Sistemi eğitiminin temel amacı işletmenin olağan dışı bir durum karşısında gerekecek müdahale kapasitesini oluşturmaktır. ISO 22301 İSYS Standardı, kuruluşunuza potansiyel tehditleri tanımlayabilecek, etkilerini değerlendirebilecek ve kesintileri asgari seviyeye indirecek bir uluslararası anlayış sunar. Etkili bir İSYS uygulayan bir kuruluş, beklenmeyen kesintilerle karşılaştığında, sadece müşterilerini ve itibarını koruma konusunda yarar sağlamaz, ayrıca benzer zorluklara karşı rakipler karşısında avantaj sağlayabilir. Eğitim sonunda bir sınav yapılacak olup, ilgili standart konusunda İç Tetkik gerçekleştirmek isteyen tüm katılımcılar bu sınavdan başarılı oldukları takdirde eğitim programına ait **"İç Tetkikçi Sertifikası"** almaya hak kazanacaklardır.

Katılımcı Profili

- İş Sürekliliği yönetici ve çalışanları,
- Bilgi Teknolojileri yönetici ve çalışanları,
- İş sürekliliği yönetim sisteminin uygulanması ve yönetiminden sorumlu personeller.
- ISO 22301:2019 Standardında İç denetçi kariyeri yapmak isteyenler.

Eğitim Süresi

- 3 gün

Eğitim İçeriği

- İş sürekliliği tanımları ve İş Sürekliliği Yönetim Sistemi terimleri
- ISO 22301:2019 İş Sürekliliği Yönetim Sistemi Standardı
- Planlama ve kontrol
- İş etki analizi ve risk belirlemesi
- İş sürekliliği stratejisi
- İş sürekliliği prosedürlerinin oluşturulması ve gerçekleştirilmesi
- Tatbik etme ve test işlemi
- İzleme, ölçme, analiz ve değerlendirme
- İç denetim ve düzeltici faaliyetler

ISO 27001:2022 Bilgi Güvenliği Yönetim Sistemi

Eğitimin Amacı

- İç denetim ISO standartları sertifikasyonun ayrılmaz bir parçasıdır. Kurumlar ISO standartları kapsamında yapmış oldukları dış denetimlerin yansıra İç denetim faaliyeti de gerçekleştirmeleri gerekmektedir. Sertifikalı ISO 27001 İç Denetçi Eğitimi'nde ISO 27001 standart maddeleri hakkında bilgi verilecek ve iç denetim süreçleri anlatılacaktır. Eğitim sonunda bir sınav yapılacak olup, ilgili standart konusunda İç Tetkik gerçekleştirmek isteyen tüm katılımcılar bu sınavdan başarılı oldukları takdirde eğitim programına ait **"İç Tetkikçi Sertifikası"** almaya hak kazanacaklardır.

Katılımcı Profili

- Özel ve kamu sektör çalışanları
- Akademisyenler
- Üniversite öğrencileri
- Üniversite mezunu iş arama sürecinde olanlar

Eğitim Süresi

- 3 gün

Eğitim İçeriği

- Denetçinin sahip olması gereken özellikler
- Açılış ve kapanış toplantıları
- Soru sorma teknikleri
- Objektif delil kriterleri
- ISO 27001 Ana ve Ek-A kontrol maddeleri
- Grup Çalışmaları:
    - Denetim Planı hazırlama
    - Soru listesi hazırlama
    - Denetimin tatbiki
    - Uygunsuzluk olup olmadığına karar verme, ilgili maddeyi bulma
    - Düzeltici faaliyet formu doldurma

ISO 27701:2019 Kişisel Veri Yönetim Sistemi

Eğitimin Amacı

- Eğitimin amacı; katılımcıları, ISO/IEC 27701:2022 Kişisel Veri Yönetim Sistemi Standardına göre iç denetim teknikleri konusunda bilgilendirmek, denetim gerekliliklerini kavramış ve etkin bir şekilde denetim gerçekleştirebilecek kuruluş içi denetçiler yetiştirmektir. Eğitim sonunda bir sınav yapılacak olup, ilgili standart konusunda İç Tetkik gerçekleştirmek isteyen tüm katılımcılar bu sınavdan başarılı oldukları takdirde eğitim programına ait **"İç Tetkikçi Sertifikası"** almaya hak kazanacaklardır.

Katılımcı Profili

- ISO/IEC 27001:2022 Bilgi Güvenliği Yönetim Sistemi'ni uygulamaya başlayacak, geçiş yapacak olan kuruluş çalışanları
- ISO/IEC 27001:2022 Bilgi Güvenliği Yönetim Sistemi'ni uygulayan tüm sistem sorumluları ve yöneticiler, danışmanlar, denetçi adayları ve bu konuda kariyer yapmak isteyenler.

Eğitim Süresi

- 3 gün

Eğitim İçeriği

- Gizlilik Prensipleri (ISO 29100 çerçevesinde)
- Kişisel Veriler ve Kişisel Verilerin Yönetimi ile İlgili Normatif veya Kılavuz Yayınlar
- ISO/IEC 27001 ve ISO/IEC 27002 Özeti
- ISO/IEC 27701 Genişletilmiş Maddeleri (27001 ve 27002'ye göre)
- ISO/IEC 27701 Veri Sorumlusu ve Veri İşleyen Gereksinimleri
- ISO/IEC 29134:2017 Çerçevesinde Gizlilik Etki Değerlendirmesi Yöntemi
- ISO 19011:2018 Çerçevesinde Denetim Metodolojisi
- Denetim Prensipleri
- Denetim İçin Yetkinlikler
- Denetime Hazırlık
- Kanıt Toplama Teknikleri
- Denetimin Gerçekleştirilmesi
- Denetim Bulgularının Sunumu ve Raporlanması
- KVYS Denetimi Uygulamaları

ISO 42001:2023 Yapay Zeka Yönetim Sistemi

Eğitimin Amacı

- Bu eğitimin amacı, ISO/IEC 42001:2023 Yapay Zeka Yönetim Sistemi (AIMS) standardı kapsamında kuruluşların gerçekleştirmesi gereken iç denetim faaliyetlerini planlayabilecek, yürütebilecek ve raporlayabilecek iç denetçilerin yetiştirilmesidir. Eğitim süresince, AIMS standardı maddeleri, yapay zekâya özgü riskler ve iç denetim teknikleri uygulamalı olarak ele alınır. Eğitimi başarıyla tamamlayan katılımcılar, ISO 42001 kapsamında iç denetim gerçekleştirebilecek yetkinliğe sahip olur.
- Eğitim sonunda bir sınav yapılacak olup, ilgili standart konusunda İç Tetkik gerçekleştirmek isteyen tüm katılımcılar bu sınavdan başarılı oldukları takdirde eğitim programına ait **"İç Tetkikçi Sertifikası"** almaya hak kazanacaklardır.

Katılımcı Profili

- Yapay zekâ projelerinde görev alan yöneticiler,
- BT ve dijital dönüşüm ekipleri,
- Veri bilimi ve yazılım ekipleri,
- Bilgi güvenliği, uyum, risk ve iç denetim ekipleri
- ISO 42001 belgelendirme sürecinde iç denetçi olarak görev almak isteyen tüm katılımcılar.

Eğitim Süresi

- 3 gün

Eğitim İçeriği

- Bilgi güvenliği terminolojisi
- Bilgi güvenliği yönetim sistemi
- Denetim kavramı, tipleri ve kaynak gerekliliği
- Denetçi sorumlulukları ve görevleri
- Bir denetimi planlama, yürütme, raporlama ve takip için denetçinin rolünün açıklanması
- Soru sorma, görüşme yapma, denetim bulguları, raporlama
- Denetim psikolojisi ve zorlukları yönetme
- Uygunsuzluk tespiti
- Takip faaliyetleri
- Sınav

BİLİŞİM STANDARTLARI BAŞDENETÇİ EĞİTİMLERİ

ICT Trend Academy Eğitim ve Danışmanlık Hizmetleri LTD. ŞTİ
Cevizli Mah. Tugay Yolu Cad. Piazza AVM No:69C/222
34846 Maltepe/İSTANBUL

- www.icttrendacademy.com.tr
- www.icttrendconsultancy.com.tr
- info@icttrendacademy.com.tr
- +90 850 466 0 428

ISO 20000-1:2019 Bilgi Teknolojileri Servis Yönetimi Sistemi Baş Denetçi Eğitimi

Eğitimin Amacı

- Bu eğitimin amacı, ISO/IEC 20000-1:2019 Bilgi Teknolojileri Servis Yönetimi Sistemi kapsamında baş denetçi (lead auditor) olarak görev alabilecek denetçileri yetiştirmektir. Eğitim süresince katılımcıların, ISO 20000-1 standardı gerekliliklerini derinlemesine kavramaları, bir denetimi planlayabilmeleri, yönetebilmeleri, uygulayabilmeleri ve raporlayabilmeleri hedeflenir. Eğitim, belgelendirme denetimlerinde baş denetçi olarak görev alabilecek yetkinliğin kazandırılmasına yöneliktir.
- Eğitimin son günü yapılan sınavı geçen adaylar Exemplar Global onaylı **Baş Tetkikçi Sertifikası** almaya hak kazanırlar.

Katılımcı Profili

- Özel ve kamu sektöründe BT servis yönetimi alanında çalışanlar
- ISO 20000-1 iç denetçi veya denetim tecrübesi bulunan profesyoneller
- Kalite, süreç, denetim ve uyum ekipleri
- Denetçi veya baş denetçi olmak isteyen danışmanlar
- Üniversite mezunları ve kariyerine denetim alanında yön vermek isteyenler

Eğitim Süresi

- 4 gün

Eğitim İçeriği

- BT Servis Yönetimi Temel Kavramları ve Servis Yaklaşımı
- ISO/IEC 20000-1:2019 Standardının Detaylı İncelenmesi
- BT Servis Yönetimi Süreçleri ve Kontroller
- Denetim Kavramları, Türleri ve Standartları
- Baş Denetçi Yetkinlikleri ve Liderlik Rolü
- Denetim Planlama ve Uygulama Süreci
- Denetimin Gerçekleştirilmesi
- Uygunsuzluk Yönetimi ve Raporlama
- Denetim Raporları ve Belgelendirme Süreci
- Uygulamalı Çalışmalar ve Örnek Denetim
- Sınav ve Değerlendirme

ISO 22301:2019 İş Sürekliliği Yönetim Sistemi

Eğitimin Amacı

- Eğitimin amacı, ISO 22301:2019 şartlarına uygun olarak etkin İş Sürekliliği Yönetim Sistemi denetimleri yapılması ve yönetilmesi için gerekli bilgi ve becerileri sağlamaktır.
- ISO 22301:2019 ISYS Baş Tetkikçi Eğitimi; denetleme süreçlerini ele alan 4 günlük eğitimde katılımcıların Exemplar Global onaylı Baş Denetçi Belgesi almasına yönelik bir eğitimdir. Eğitimin son günü yapılan sınavı geçen adaylar Exemplar Global onaylı **Baş Tetkikçi Sertifikası** almaya hak kazanırlar

Katılımcı Profili

- İş Sürekliliği yönetici ve çalışanları,
- Bilgi Teknolojileri yönetici ve çalışanları,
- İş sürekliliği yönetim sisteminin uygulanması ve yönetiminden sorumlu personeller.
- ISO 22301:2019 Standardında İç denetçi kariyeri yapmak isteyenler.

Eğitim Süresi

- 4 gün

Eğitim İçeriği

- İş Sürekliliği Temel Kavramları
- ISO/IEC 22301 İş Sürekliliği Yönetim Sistemi Standardı Özeti
- Denetim Türleri ve Şekilleri
- Denetim Aşamaları ve Kapsamı
- Denetim için Gerekli Standartlar
- Baş Denetçi Özellikleri
- Denetim Ekibinin Yönlendirilmesi ve Yönetimi
- Denetim Soru Listesinin Hazırlanması ve Değerlendirilmesi
- Denetim Planı ve Raporlanması
- Uygunsuzluk ve Düzeltici Önleyici Faaliyet Raporu
- Liste, Rapor, Plan Örnekleri
- Örnek Denetim Uygulaması

ISO 27001:2022 Bilgi Güvenliği Yönetim Sistemi

Eğitimin Amacı

- Bu eğitimde amaç, ISO 27001:2022 Bilgi Güvenliği Yönetim Sistemi (BGYS) tetkikçilerini bir Tetkik Planını yönetmek, planlamak, idare etmek ve uygulamak üzere yetiştirmek ve katılımcılara BGYS standardı hakkında ve sistemin tüm maddeleri için genel bilgilendirme yapmak, uygulamanın gerçekleştirilmesi ve sistemin kurulması için örneklerle açıklayıcı bilgiler sunmaktır.
- ISO 27001:2022 BGYS Baş Tetkikçi Eğitimi; Bilgi güvenliği standartlarını, kurum ve kuruluşların bilgi güvenlik risklerini, tehditleri ve açıklarını sistematik olarak denetleme süreçlerini ele alan 4 günlük eğitimde katılımcıların Exemplar Global onaylı Baş Denetçi Belgesi almasına yönelik bir eğitimdir. Eğitimin son günü yapılan sınavda başarılı olan adaylar Exemplar Global onaylı **Baş Tetkikçi Sertifikası** almaya hak kazanırlar.

Katılımcı Profili

- Özel ve kamu sektör çalışanları
- Akademisyenler
- Üniversite öğrencileri
- Üniversite mezunu iş arama sürecinde olanlar

Eğitim Süresi

- 4 gün

Eğitim İçeriği

- Bilgi Güvenliği Temel Kavramları ve Bilgi Güvenliğinin Önemi
- ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardı Özeti
- Güvenlik Tehditleri ve İncelenebilirlikleri
- Güvenlik Risklerinin Yönetimi
- Güvenlik Kontrollerinin Seçimi
- Bilgi Güvenliği Yönetim Sistemi Denetimi
- Denetim Türleri ve Şekilleri
- Denetim Aşamaları ve Kapsamı
- Denetim için Gerekli Standartlar
- Baş Denetçi Özellikleri
- Denetim Ekibinin Yönlendirilmesi ve Yönetimi
- Denetim Soru Listesinin Hazırlanması ve Değerlendirilmesi
- Denetim Planı ve Raporlanması
- Uygunsuzluk ve Düzeltici Önleyici Faaliyet Raporu
- Liste, Rapor, Plan Örnekleri
- Örnek Denetim Uygulaması

ISO 27701:2019 Kişisel Veri Yönetim Sistemi

Eğitimin Amacı

- Bu eğitimde amaç, ISO 27701:2019 Kişisel Veri Gizliliği Yönetim Sistemi (KVYS) tetkikçilerini bir tetkik planını yönetmek, planlamak, idare etmek ve uygulamak üzere yetiştirmek ve katılımcılara KVYS standardı hakkında ve sistemin tüm maddeleri için genel bilgilendirme yapmak, uygulamanın gerçekleştirilmesi ve sistemin kurulması için örneklerle açıklayıcı bilgiler sunmaktır.
- ISO 27701:2019 KVYS Baş Tetkikçi Eğitimi; Bilgi güvenliği standartlarını, kurum ve kuruluşların bilgi güvenlik risklerini, tehditleri ve açıklarını sistematik olarak denetleme süreçlerini ele alan 5 günlük eğitimde katılımcıların Exemplar Global onaylı Baş Denetçi Belgesi almasına yönelik bir eğitimdir. Eğitimin son günü yapılan sınavı geçen adaylar Exemplar Global onaylı **Baş Tetkikçi Sertifikası** almaya hak kazanırlar.

Katılımcı Profili

- ISO/IEC 27001:2022 Bilgi Güvenliği Yönetim Sistemi'ni uygulamaya başlayacak, geçiş yapacak olan kuruluş çalışanları
- ISO/IEC 27001:2022 Bilgi Güvenliği Yönetim Sistemi'ni uygulayan tüm sistem sorumluları ve yöneticiler, danışmanlar, denetçi adayları ve bu konuda kariyer yapmak isteyenler.

Eğitim Süresi

- 4 gün

Eğitim İçeriği

- Gizlilik Prensipleri (ISO 29100 çerçevesinde)
- Kişisel Veriler ve Kişisel Verilerin Yönetimi ile İlgili Normatif veya Kılavuz Yayınlar
- ISO/IEC 27001 ve ISO/IEC 27002 Özeti
- ISO/IEC 27701 Genişletilmiş Maddeleri (27001 ve 27002'ye göre)
- ISO/IEC 27701 Veri Sorumlusu ve Veri İşleyen Gereksinimleri
- ISO/IEC 29134:2017 Çerçevesinde Gizlilik Etki Değerlendirmesi Yöntemi
- ISO 19011:2018 Çerçevesinde Denetim Metodolojisi
- Denetim Prensipleri
- Denetim İçin Yetkinlikler
- Denetime Hazırlık
- Kanıt Toplama Teknikleri
- Denetimin Gerçekleştirilmesi
- Denetim Bulgularının Sunumu ve Raporlanması
- Akreditasyon Kuralları Çerçevesinde Denetim Süreci
- Soru Bankası Oluşturma Uygulaması
- Vaka Analizleri
- KVYS Denetimi Uygulamaları

ISO 42001:2023 Yapay Zeka Yönetim Sistemi

Eğitimin Amacı

- Bu eğitimin amacı, ISO/IEC 42001:2023 Yapay Zeka Yönetim Sistemi kapsamında baş denetçi (Lead Auditor) olarak görev alabilecek profesyonelleri yetiştirmektir. Eğitim süresince katılımcıların, yapay zekâ yönetim sistemi gerekliliklerini derinlemesine anlamaları, bir denetimi planlayabilmeleri, yönetebilmeleri, uygulayabilmeleri ve raporlayabilmeleri hedeflenir. Eğitim, belgelendirme denetimlerinde baş denetçi olarak görev alabilecek yetkinliğin kazandırılmasına yöneliktir.
- Eğitimin son günü yapılan sınavı geçen adaylar Exemplar Global onaylı **Baş Tetkikçi Sertifikası** almaya hak kazanırlar.

Katılımcı Profili

- Yapay zekâ, veri, yazılım ve BT alanlarında çalışan profesyoneller
- Bilgi güvenliği, KVKK/uyum, risk ve iç denetim ekipleri
- ISO yönetim sistemleri denetim tecrübesi olanlar
- Denetçi veya baş denetçi olarak kariyerini geliştirmek isteyen danışmanlar
- Üniversite mezunları ve denetim alanında uzmanlaşmak isteyenler

Eğitim Süresi

- 4 gün

Eğitim İçeriği

- Yapay Zeka ve Sorumlu Yapay Zeka Temel Kavramları
- ISO/IEC 42001:2023 Standardının Detaylı İncelenmesi
- Yapay Zeka Yönetim Sistemi (AIMS) Yapısı ve Kontroller
- Denetim Kavramları, Standartları ve Türleri
- Baş Denetçi Yetkinlikleri ve Liderlik Rolü
- Denetim Planlama ve Denetim Programı Yönetimi
- Denetimin Gerçekleştirilmesi
- Yapay Zeka Riskleri ve Uygunsuzluk Yönetimi
- Denetim Raporlama ve Belgelendirme Süreci
- Uygulamalı Denetim ve Vaka Çalışmaları
- Sınav ve Değerlendirme