TISAX Nedir?

TISAX (Trusted Information Security Assessment Exchange), otomotiv ekosisteminde bilgi güvenliğinin değerlendirilmesi ve karşılıklı kabul edilmesi amacıyla oluşturulmuş bir değerlendirme mekanizmasıdır.

TISAX Nedir?

TISAX (Trusted Information Security Assessment Exchange), otomotiv ekosisteminde bilgi güvenliğinin değerlendirilmesi ve karşılıklı kabul edilmesi amacıyla oluşturulmuş bir değerlendirme mekanizmasıdır.

- Otomotiv üreticileri ve tedarikçileri için geliştirilmiştir
- VDA ISA (Information Security Assessment) kataloğunu temel alır

Amaç:

Bilgi güvenliği seviyesinin şeffaf, doğrulanabilir ve paylaşılabilir olması

TISAX Değerlendirme Seviyeleri (AL)

TISAX kapsamında uygulanacak denetim yöntemi ve danışmanlık yaklaşımı; seçilen Değerlendirme Seviyesi (Assessment Level – AL) doğrultusunda belirlenmektedir.

AL seviyeleri bir sonraki sayfada belirtildiği gibi 3 seviyden oluşur.

TISAX sürecinde uygulanacak denetim yöntemi ve danışmanlık yaklaşımı; yalnızca değerlendirme seviyesine değil, aynı zamanda;

- Firmanın saha (lokasyon) sayısına,
- Yönetim sistemlerinin merkezi olarak mı yoksa saha bazlı mı yönetildiğine

bağlı olarak da şekillenmektedir.

Bu unsurlar, danışmanlık sürecinin kapsamını, denetim hazırlık çalışmalarını ve uygulanacak metodolojiyi doğrudan etkilemektedir.

AL1: Kurum İçi Öz Değerlendirme (Self Assessment)

Firma, TISAX gereksinimlerini kendi iç kaynaklarıyla değerlendirir	Harici veya akredite denetçi sürece dahil değildir	Kurum içi farkındalık ve ön değerlendirme amacıyla kullanılır	Düşük riskli bilgi paylaşımları için uygundur

Not: AL1 seviyesi, TISAX kaydı oluşturmak veya mevcut olgunluk seviyesini görmek isteyen firmalar için başlangıç niteliğindedir.

AL2: Uygunluk Kontrolü (Plausibility Check)

Değerlendirme Yöntemi

Değerlendirme dokümanlar ve kanıtlar üzerinden yapılır

Kontrol Şekli

Kontroller uzaktan veya sınırlı doğrulama yöntemiyle gerçekleştirilir

İnceleme Kapsamı

Süreçlerin ve dokümantasyonun tutarlılığı incelenir

Kullanım Alanı

Orta düzey gizlilik içeren projeler için tercih edilir

AL3: Yerinde Denetim (On-site Assessment)

En kapsamlı TISAX değerlendirme seviyesidir

- Akredite denetçi tarafından yerinde denetim yapılır
- Süreçler, teknik kontroller ve fiziksel güvenlik önlemleri gözlemlenir
- Yüksek gizlilik derecesine sahip ve kritik projeler için zorunludur

Kritik Projeler

Yüksek gizlilik derecesine sahip projeler için zorunlu seviye

Değerlendirme Seviyesinin Danışmanlığa Etkisi

Değerlendirme seviyesi yükseldikçe:

1

Danışmanlık Süreci

Danışmanlık süreci daha detaylı ve yapılandırılmış hâle gelir

2

Gereksinimler

Dokümantasyon ve uygulama gereksinimleri artar

3

Hazırlık

Denetim öncesi hazırlık süresi uzar

4

Kapsam

Denetim kapsamı ve doğrulama derinliği genişler

Tek Saha vs Çok Saha Yapısı

Tek Saha (Single Site)

- Daha dar ve yönetilebilir bir kapsam
- Tek saha üzerinden değerlendirme yapılır
- Denetim ve danışmanlık süreci daha kısa sürede tamamlanır

Çok Saha (Multi Site)

- Farklı sahalardan kaynaklı farklı risk profilleri oluşur
- Lokasyon bazlı uygulama ve kontrol farklılıkları bulunabilir
- Denetim planı daha karmaşık hâle gelir
- Saha bazında doldurulması gereken VDA ISA doküman sayısı artar

Çok Sahalı Yapının Danışmanlığa Etkisi

01

Her saha için kapsam doğrulanır ve saha bazında VDA ISA kontrolleri doldurulur

02

Risk analizi ve varlık envanteri çalışmalarının kapsamı genişler

03

Saha sayısı arttıkça iç denetim faaliyetleri ve çalışma eforu artar

04

Merkezi kontroller ile sahalara özel kontroller beraber ele alınır

05

Dokümantasyon yapısı tekil değil, hiyerarşik olarak tasarlanır

Danışmanlık Hizmeti

Danışmanlık Yaklaşımı ve Kapsamı

Seçilen TISAX denetim hedefine ve Değerlendirme Seviyesine (Assessment Level – AL) uygun olarak; kuruluşun organizasyonel yapısı, süreçleri ve kontrolleri denetime hazır hâle getirilir.

Danışmanlık hizmeti, farkındalıktan denetim kapanışına kadar uçtan uca sunulur.

Danışmanlık Hizmeti - Uygulama ve Destek Çalışmaları

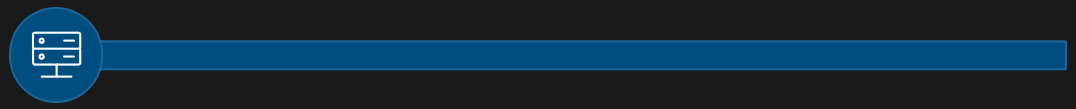
- TISAX ve VDA ISA gereksinimlerine yönelik farkındalık eğitiminin verilmesi
- Seçilen denetim hedefine uygun organizasyon yapısının kurulması
- Bilgi varlıklarının ve destekleyici varlıkların belirlenmesi ve sınıflandırılması
- Kurum genelinde risk değerlendirme çalışmalarının tamamlanması

Aşağıdaki kontrol alanlarına göre mevcut durumun değerlendirilmesi ve gereksinimlere uygun iyileştirme önerilerinin oluşturulması:

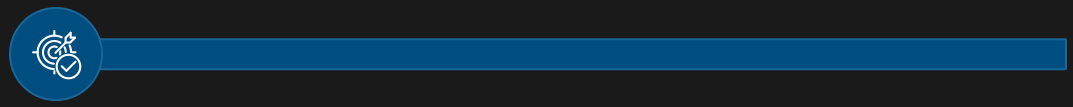
Fiziksel Güvenlik	Kimlik ve Erişim Yönetimi (Identity Management)	İnsan Kaynakları (Human Resources)
IT Security & Cyber Security	Tedarikçi İlişkileri (Supplier Relationships)	Mevzuat ve Uyum (Compliance)
Prototip Koruma (Prototype Protection)	Veri Koruma (Data Protection)	

- TISAX / VDA ISA gereksinimlerine uygun dokümantasyonun hazırlanması
- VDA ISA kataloğunun saha bazında doldurulması

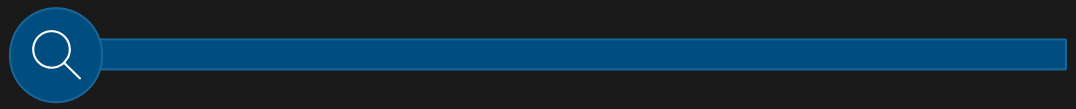
Danışmanlık Hizmeti - ENX Portal ve Denetim Yönetimi



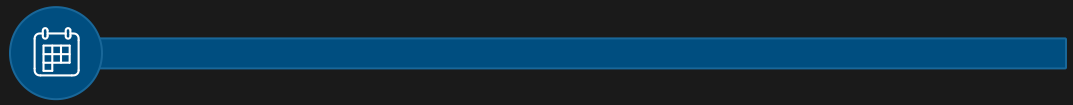
ENX portal kaydının oluşturulması ve süreç yönetimi



TISAX kapsam ve hedeflerinin portal üzerinde doğru şekilde tanımlanması



Akredite denetçi firma seçim sürecinde destek



Denetim planlamasının danışmanlık süreciyle uyumlu yürütülmesi

Danışmanlık Hizmeti – Doğrulama, Denetim ve Kapanış

01

VDA ISA kriterlerine uygun iç denetimin gerçekleştirilmesi

02

Gerçek denetim senaryolarını içeren denetim simülasyonu

03

Denetim sırasında veya sonrasında oluşan bulguların kapatılmasına destek

04

Sürecin Yönetimin Gözden Geçirmesi (YGG) ile tamamlanması

Danışmanlık Hizmeti Çıktıları

- Denetim hedefine ve AL seviyesine uygun yapılandırılmış organizasyon
- Uygulanmış ve kanıtları oluşturulmuş teknik ve idari kontroller / Gerekli olan dökümanların oluşturulması
- Saha bazında doldurulmuş VDA ISA kataloğu
- Denetime hazır, sürdürülebilir TISAX yapısı

GAP Analiz Hizmeti

GAP Analizi:

Kuruluşun mevcut durumunun TISAX gereksinimlerini ne ölçüde karışaldığı tespit edilir ve uygulanması gereken teknik ve idari tedbirler raporlanır

VDA ISA kataloğu doldurularak mevcut olgunluk seviyesi ve puanı hesaplanır

Çıktılar:

- Analiz Raporu
- Teknik ve idari kontroller için aksiyon listesi

Eğitim Hizmetleri

TISAX Uygulama Eğitimi (1 Gün)

- TISAX & VDA ISA genel yapı
- ISA doküman yapısı ve kontrol beklentileri
- Kontrollerin karşılanmasına yönelik metodoloji

Amaç: Kurumsal farkındalık

TISAX Uygulama + Workshop (2 Gün)

- TISAX ISA beklentilerine göre kontrol gereksinimleri
- Kontrollerin uygulanmasına yönelik örnek senaryolar
- Kurum ve saha yapısına özel pratik çalışmalar

Amaç: Kuruma özel TISAX yol haritası oluşturmak

atak01 – GRC (Governance, Risk & Compliance) Platformu

ATAK01 GRC, TISAX başta olmak üzere bilgi güvenliği, risk ve uyum süreçlerinin merkezi olarak yönetilmesini, izlenmesini ve sürdürülebilir hâle getirilmesini sağlayan entegre bir GRC platformudur.

Platform; danışmanlık sürecinde kurulan yapının denetim sonrası da canlı kalmasını hedefler.

atak01 – (Governance) – Yönetişim

- Politika, prosedür ve talimatların tek merkezden yönetimi
- Dokümanlar için: Versiyonlama, Onay / yayın akışı, Değişiklik geçmişi
- Merkezi kontroller ile saha bazlı kontrollerin ayrıştırılması
- Organizasyon yapısı, rol ve sorumlulukların izlenebilir hâle getirilmesi

👉 Yönetim sistemleri kişilere değil, kurumsal yapıya bağlanır.

atak01 – (Risk) – Risk ve Varlık Yönetimi

- Bilgi ve destekleyici varlıkların merkezi tanımlanması
- Saha bazlı ve merkezi risk değerlendirme yapısı
- Risklerin: Seviyelendirilmesi, Sahiplerinin atanması, Azaltıcı kontrollerle ilişkilendirilmesi
- Risk aksiyonlarının durum bazlı takibi

👉 Riskler Excel'de değil, canlı sistem üzerinde yönetilir.

atak01 – (Compliance) – Uyum ve Denetim Yönetimi

- VDA ISA / TISAX uyumlu kontrol yapısı
- Uygulanabilirlik bildirgesinin doldurulması ve izlenmesi
- İç denetim planlama ve yürütme desteği
- Denetim bulgularının ve düzeltici faaliyetlerin takibi
- Denetim geçmişi ve kanıtların merkezi tutulması

👉 Denetimler "anlık hazırlık" değil, sürekli hazır olma yaklaşımıyla yönetilir.

Çok Sahalı Yapılar İçin atak01 GRC Avantajı

Saha sayısı arttıkça karmaşıklığın kontrol altına alınması

Merkezi görünürlük + saha bazlı detay

Denetçi örneklemesini destekleyen yapı

ISA doküman yükünün sistematik yönetimi

👉 Çok sahalı firmalarda efor ve maliyet ciddi şekilde azalır.

atak01 – Aksiyon ve Süreç Takibi

- Teknik ve idari kontroller için aksiyon tanımlama
- Sorumlu, termin ve durum bazlı izleme
- Geciken veya kritik aksiyonlar için görünürlük
- Denetim bulgularının kapanış sürecinin izlenmesi

atak01 – Raporlama & Yönetici Görünürlüğü

Uyum ve risk seviyeleri için gösterge panelleri

TISAX / VDA ISA bazlı özet raporlar

Üst yönetim için tek bakışta durum görünürlüğü