

TÜV NORD CERT – Bilgi Güvenliği Yönetim Sistemlerinin TISAX’a göre değerlendirilmesi



TISAX Nedir?

VDA tarafından geliştirilen Bilgi Güvenliği Değerlendirmesi kataloğunu kullanarak otomotiv sektörü için ortak bilgi güvenliği değerlendirilmesi ve paylaşımı yapılmasını sağlayan bir standarttır. Güvenlik değerlendirmelerine ait doğrulamalar merkezi bir otoritenin (ENX -European Network eXchange) akredite ettiği kuruluşlar tarafından yapılmakta ve sonuçlar ENX tarafından saklanmaktadır. Sonuçlar üreticiden tedarikçiye kadar tüm servis sağlayıcılar tarafından tanınır. Değerlendirme sonuçlarını kimlerin görebileceği denetlenen firmanın kontrolündedir.

TISAX'da;

- 1) ISO27001 temelli bilgi güvenliği kontrolleri,
- 2) Prototip koruma ile ilgili kontrolleri,
- 3) Üçüncü parti kuruluş faaliyetleri ile ilgili kontrolleri ve
- 4) Veri koruma (GDPR) ile ilgili kontrolleri

içeren kataloglar yer alır. Kataloglarda yer alan her bir kontrolün etkinliği 0-5 arasında tanımlanan olgunluk seviyesi ile değerlendirilmelidir.

Neden Gereklidir?

Otomotiv sektörü için, Bilgi Güvenliği Yönetim Sisteminin etkinliği TISAX standardına göre değerlendirilebilir. Bu değerlendirmeler artık pek çok otomotiv üreticisi tarafından istenmektedir.

Değerlendirmeler, Alman Otomotiv Endüstrisi Kuruluşu (VDA) tarafından geliştirilen bilgi güvenliği değerlendirilmesi (VDA ISA) gereksinim kataloglarına göre yapılmaktadır.

İki olası katılımcı rolü

Bilgi güvenliği değerlendirmelerinin paylaşımında kuruluşların ihtiyaçlarına göre iki farklı rol vardır:

- Pasif katılımcılar (örneğin. OEM'ler, otomotiv üreticileri): Bu katılımcılar, diğer kuruluşların (örn. tedarikçi) TISAX değerlendirmesi almasını şart koşar, sonrasında da değerlendirme sonuçlarını talep eder.
- Aktif katılımcılar ya da denetlenenler (örn. tedarikçiler): Başka bir kuruluş tarafından (örn. OEM ya da müşteri) belirlenen kriter kataloğuna göre denetim alması istenir. Bazen de kuruluş kendi inisiyatifi ile bu değerlendirmeyi alabilir. Değerlendirmenin ardından, aktif katılımcı seçtiği kuruluşlara (örn. OEM'ler) kendisinin değerlendirme sonuçlarına erişim izni verir.

TISAX platformuna şu adresten erişilebilir :

<https://enx.com/tisax/tisax-en.html>

Kuruluşlar TISAX sistemini katılımcı olarak kayıt olduktan sonra kullanabilirler. Kayıt aynı zamanda akredite bir değerlendirme kuruluşu tarafından değerlendirilebilmek için de ön koşuldur. Değerlendirici kuruluşlar XAP (TISAX Audit Provider - TISAX Denetim Sağlayıcı) olarak bilinirler.

Farklı koruma ve değerlendirme seviyeleri

Kuruluşun nasıl değerlendirileceğini belirleyen farklı koruma seviyeleri ve bunlarla ilişkili değerlendirme seviyeleri vardır:

1. Seviye Değerlendirme daha çok kuruluşun kendi ihtiyaçları içindir ve kuruluş burada kendi kendini değerlendirir.

Yüksek seviyeli koruma gerekliliğinde, sürece bir XAP'nin dahil olması zorunludur. Burada, kuruluş önce kendi kendini değerlendirir (1. Seviye Değerlendirme). Ardından, 2. Seviye Değerlendirmeyi XAP yapar. Bu kontrol değerlendirmesi aşağıdaki adımlardan oluşur:

- Açılış toplantısı
- Kuruluşun yaptığı 1. Seviye değerlendirmenin ve ilgili kanıtlarının XAP tarafından uygunluk ve anlamlık kontrolünün yapılması
- BGYS'den sorumlu kişilerle telefon mülakatlarının yapılması (eğer üçüncü parti kuruluşlar ve/ya prototip koruma söz konusu ise yerinde saha ziyareti gereklidir).

Çok yüksek seviyeli koruma gerekliliğinde, değerlendirme 3. seviyeye göre yapılır ve süreçte XAP mutlaka olmalıdır. Burada, kontrol değerlendirme adımları 2. seviyeye benzerdir; ancak yerinde saha ziyareti zorunludur. 3. Seviye Değerlendirme için de ön koşul kuruluşun önce kendi kendini değerlendirmesidir (Seviye 1):

- Açılış toplantısı
- Kuruluşun yaptığı 1. Seviye değerlendirmenin ve ilgili kanıtlarının XAP tarafından uygunluk ve anlamlık kontrolünün yapılması
- BGYS'nin olgunluk seviyesi ve etkinliğinin yerinde denetim ile değerlendirilmesi

2. ve 3. seviye değerlendirmelerinden sonra, bulgular (örn. olgunluk seviyeleri) ve düzeltici faaliyetler ile ilgili gereklilikler taslak bir raporda tartışılır ve özetlenir.

TISAX etiketi alabilmek için, aşağıdaki iki değerlendirme adımının yapılması gerekmektedir:

- Denetlenen kuruluşun düzeltici faaliyet planlarını yapması ve bu planların XAP tarafından gözden geçirilmesi. Sonuçlar taslak rapor güncellenerek yayınlanır.
- Düzeltici faaliyetlerin denetlenen kuruluş tarafından devreye alınması ve sonuç aksiyonlarının XAP tarafından değerlendirilmesi. Burada rapor bir kez daha güncellenir ve ENX platformuna nihai rapor olarak yüklenir. Kapanış toplantısından itibaren nihai raporun üretilmesine kadar olan süre en fazla dokuz aydır. Bu süre aşılsa tüm süreç yeniden başlar.

Her kuruluş sonuçları kimlerin görebileceğine karar verebilir. Hem değerlendirme süreci hem de sonuçların kalitesi ENX tarafından gözden geçirilir ve ardından kuruluşa üç yıl geçerliliği olan TISAX etiketi verilir. Üç yıldan sonra tüm süreç tekrar edilmelidir.

TISAX değerlendirmeleri için hedef kitle

TISAX'a göre yapılan değerlendirmeler, otomotiv sektöründe olan ve hassas verilerle çalışan tedarikçiler ve servis sağlayıcılar için geliştirilmiştir. TISAX etiketleri Audi, Volkswagen, BMW ve diğer pek çok VDA üyeleri tarafından tanınmaktadır. Bazı durumlarda TISAX değerlendirmeleri yapılması tedarikçiler açısından zorunludur.

TISAX'ın avantajları

- Tüm değerlendirme kriterlerinin otomotiv sektörüne özel olması
- Yüksek değerlendirme kalitesi ve tutarlı sonuçlar
- Standartlaştırılmış değerlendirme ve raporlama prosedürleri
- Karşılaştırılabilir ve anlamlı sonuçlar
- Otomotiv sektöründe tanınan ve güvenilen değerlendirme sonuçları
- Risklerin azaltılması ve risk yönetim sistemi oluşturma
- Artan müşteri sadakati ve yeni iş fırsatları
- Müşteri ihtiyaçlarına daha fazla odaklanma

TÜV NORD, TISAX XAP olarak sizlere destek olabilir

TÜV NORD CERT GmbH, Alman akderitasyon otoritesi DAkkS tarafından Bilgi Güvenliği Yönetim Sistemi (BGYS) denetim ve sertifikasyonu yapmak için uzun yıllardan beri yetkilendirilmiş, alanında yetkin ve çok deneyimli bir kuruluştur.

Bu deneyimi ENX tarafından da onaylanmış olan TÜV NORD, otomotiv sektörüne TISAX akredite denetim sağlayıcı (XAP) olarak uzman Türk denetçileri ile hizmet vermektedir.

DAHA GENİŞ BİLGİ VE SORULARINIZ İÇİN:

TÜV Teknik Kontrol ve Belgelendirme A.Ş.

Ayazmadere Cad., Pazar Sok, No 2-4, Bareli Plaza, Kat 4, Gayrettepe, Beşiktaş, TR-34349 İstanbul

Tel: +90 212 293 26 42

Fax: +90 212 293 38 44

tuv-nord@tuv-turkey.com

