TISAX - Ocena systemu zarządzania bezpieczeństwem informacji w branży automotive

TÜV NORD

TISAX – co to znaczy?

Duże niemieckie grupy motoryzacyjne (VW, BMW i Daimler-Benz) coraz częściej wymagają od swoich dostawców przedstawienia dowodu posiadania znaku TISAX. **Dlaczego?**

W dobie cyfryzacji bezpieczeństwo informacji w coraz większym stopniu stanowi decydujący czynnik pozostania konkurencyjnym. Dotyczy to w szczególności przemysłu motoryzacyjnego – firmy wymieniają codziennie ogromną ilość wrażliwych danych, które należy chronić przed kradzieżą, utratą lub manipulacją. Bezpieczeństwo informacji było kiedyś traktowane jako indywidualny problem każdej firmy ale wraz z opracowaniem procedury testowania i wymiany informacji TISAX (Trusted Information Security Assessment Exchange) niebawem ulegnie to zmianie.

Aby uzyskać/utrzymać prawo do stosowania znaku TISAX, dostawcy branży automotive muszą co 3 lata udowodnić, że spełniają kryteria niezbędne do zapewnienia bezpieczeństwa informacji w swojej branży. Podstawą do tego jest katalog wymagań ISA (Information Security Assessments) opracowany przez VDA. Opiera się na istotnych aspektach i kryteriach uznawanej na całym świecie normy ISO 27001 a także zawiera specjalne katalogi kryteriów dla sektora motoryzacyjnego. Do tego dochodzi dobrze przemyślany proces testowania i wymiany. Platforma internetowa TISAX umożliwia uczestnikom wymianę danych z oceny oraz ułatwia kontakt pomiędzy uczestnikami a dostawcami usług testowych (jednostkami akredytowanymi przez TISAX). TISAX działa pod patronatem VDA i jest zarządzany przez stowarzyszenie ENX, które monitoruje jakość wykonania oceny oraz jej wyniki. TUV NORD CERT jest obecnie zatwierdzony przez ENX do obsługi zapytań z zakresu TISAX oraz prowadzenia procedury oceny.

Uczestnictwo w programie TISAX - dwa możliwe modele

Istnieją dwa modele, które każda z firm może zastosować zgodnie ze swoimi potrzebami:

- Uczestnik bierny /pasywny (np. Producent OEM, producent samochodów): prosi aby inna firma (np. dostawca) została poddana ocenie i wnioskuje o dostęp do jej wyników
- Aktywni uczestnicy lub auditowani (np. dostawcy): Firmy wobec których inne firmy (np. OEM lub klient) wymagają podejścia do oceny zgodnie z kryteriami katalogowymi lub przechodzą ocenę z własnej inicjatywy. Po ocenie aktywny uczestnik może umożliwić wybranym firmom (np. OEM) uzyskanie dostępu do wyników oceny.

Firmy uzyskują dostęp do portalu TISAX przez rejestrację jako uczestnik. Rejestracja jest również warunkiem wstępnym do zlecenia oceny przez akredytowaną organizację oceniającą. Takie organizacje są znane jako **XAP.**

Różne poziomy ochronne i poziomy oceny

Stowarzyszenie ENX jako operator programu TISAX ma jasno określony poziom i zakres oceny. TISAX rozróżnia trzy różne „poziomy ochrony" (normalny, wysoki i bardzo wysoki) określające wymagany poziom ochrony informacji. Ponadto TISAX rozróżnia trzy „poziomy oceny" określające głębokość oceny i metodę oceny:

- **Informacje z normalnym poziomem ochrony:** poziom oceny 1, realizowany w formie samooceny. Wyniki ocen z poziomem oceny 1 zwykle nie są stosowane w TISAX ale mogą być wymagane poza systemem lub do realizacji wyższych poziomów.
- **Informacje o wysokim poziomie ochrony:** poziom oceny 2, realizowany za obligatoryjnym pośrednictwem organizacji audytującej (XAP). Warunkiem wstępnym jest tu przeprowadzenie oceny zgodnej z poziomem 1 a inaczej mówiąc całościowa samoocena. Na poziomie 2 kroki oceny są następujące:
  - Spotkanie otwierające
  - Weryfikacja kompletności i kontrola wiarygodności samooceny i odpowiednich dowodów
  - Wywiad telefoniczny z osobą odpowiedzialną za SZBI bazujący na wymaganych dokumentach (inspekcja na miejscu w razie potrzeby, np. jeśli trzecia strona i/lub ochrona prototypu są włączone w ocenę)
- **Informacje o bardzo wysokim poziomie ochrony:** poziom oceny 3, przeprowadzony przez niezależnego

TISAX - Ocena systemu zarządzania bezpieczeństwem informacji

dostawcę audytu (XAP). Kroki testowe są tu podobne do tych na poziomie 2 oceny z tą różnicą że istotne aspekty są uwzględniane podczas inspekcji na miejscu. Oczywiście całościowa samoocena również musi być przedstawiona:

- Spotkanie otwierające
- Weryfikacja kompletności i kontrola wiarygodności samooceny i odpowiednich dowodów
- Ocena efektywności oraz stopnia dojrzałości SZBI przez inspekcje na miejscu u zainteresowanych stron (wywiady ekspertów na miejscu, inspekcje w istotnych obszarach organizacji).

Po obydwu ocenach na poziomie 2 i poziomie 3, wyniki oraz wymagane działania korekcyjne są omawiane i podsumowywane w raporcie wstępnym.

Po wstępnej ocenie opisanej powyżej, aby uzyskać znak TISAX, należy przeprowadzić kolejne dwa etapy oceny:

- Opracowanie przez firmę auditowaną planu dla działań korekcyjnych i jego przegląd przez XAP. Plan jest wyjaśniony i podsumowany w raporcie uzupełniającym, który zasadniczo ma formę aktualizacji raportu wstępnego.
- Implementacja działań korekcyjnych przez firmę auditowaną i ich ocena przez XAP. Tworzony jest także raport, który następnie jest przesyłany do platformy ENX jako raport końcowy. Maksymalny czas od pierwszego spotkania otwierającego do raportu końcowego to 9 miesięcy i jeśli się on wydłuży cały proces musi się zacząć od początku.

Każda firma sama decyduje kto będzie miał dostęp do wyników jej oceny. Jakość procesu oceny oraz jego wyniki są przeglądane przez stowarzyszenie ENX, które później przyznaje znak TISAX na okres 3 lat. Po tym czasie cała procedura musi być powtórzona od początku.

Dla kogo jest TISAX?

Oceny na zgodność ze standardem TISAX zostały opracowane dla dostawców oraz usługodawców sektora automotive, którzy pracują z danymi wrażliwymi. Znak TISAX jest rozpoznawany przez wszystkich członków VDA włączając w to takie firmy jak Audi, Volkswagen, BMW i wiele innych. W niektórych przypadkach ocena na zgodność z TISAX jest już obowiązkowa dla dostawców.

Korzyści z programu TISAX

- Wszystkie kryteria oceny są istotne z punktu widzenia sektora automotive
- Wysoka jakość oceny i spójne wyniki
- Wystandaryzowana, rzetelna ocena i procedura raportowania
- Wyniki są zarówno porównywalne jak i znaczące
- Można uniknąć duplikowania i powtarzania ocen
- Redukcja ryzyka i ustanowienie systemu zarządzania ryzykiem
- Akceptacja zarządu oraz większe zaufanie dla sektora automotive
- Wzmocnienie lojalności klienta oraz promocja nowego biznesu
- Silny nacisk na potrzeby klientów

Nasze know-how dla Twojego sukcesu

Przez wiele lat TUV NORD CERT był zatwierdzony przez Niemiecką jednostkę certyfikującą DAkkS dla prowadzenia audytów i certyfikacji Systemów Zarządzania Bezpieczeństwem Informacji (SZBI) i na bazie tej potwierdzonej wiedzy specjalistycznej uzyskał również zatwierdzenie przez ENX jako akredytowany dostawca auditu TISAX (XAP) dla sektora automotive.

Skontaktuj się z nami, pomożemy Ci przystąpić do programu TISAX!

Jesteśmy po to, aby udzielić Państwu wyczerpujących informacji.

Przemysław Szczurek
Product Manager ds. Bezpieczeństwa Informacji
Tel.: 605 594 996
p.szczurek@tuv-nord.pl

Magdalena Brudzyńska
Doradca Klienta ds. Bezpieczeństwa Informacji
tel.: 781 700 029
m.brudzynska@tuv-nord.pl

TUV NORD Polska
ul. Mickiewicza 29
40-085 Katowice
e-mail: biuro@tuv-nord.pl
www.tuv-nord.pl