Podręcznik uczestnika TISAX

Możliwość poddania się procesowi oceny TISAX i udostępnienia wyniku partnerowi

Opublikowany przez

ENX Association
Stowarzyszenie zgodne z przepisami prawa francuskiego z roku 1901,
wpisane do rejestru pod nr w923004198 w Sous-préfecture, Boulogne-Billancourt, Francja

Adresy
20 rue Barthélémy Danjou, 92100 Boulogne-Billancourt, Francja
Bockenheimer Landstraße 97-99, 60325 Frankfurt nad Menem, Niemcy

Autor

Florian Gleich

Dane do kontaktu

tisax@enx.com
+49 69 9866927-77

Wersja

Data:	06.03.2024 r.
Wersja:	2.7.1
Klasyfikacja:	Public
ENX doc ID:	602-PL

Informacja o prawach autorskich

Wszelkie prawa zastrzeżone przez ENX Association.
ENX, TISAX oraz ich odpowiednie logo są zastrzeżonymi znakami towarowymi ENX Association.
Wspomniane znaki towarowe stron trzecich stanowią własność ich właścicieli.

Spis treści

1. Informacje ogólne . . . 8
1.1. Cel . . . 8
1.2. Zakres . . . 8
1.3. Odbiorcy . . . 9
1.4. Struktura . . . 9
1.5. Sposób korzystania z tego dokumentu . . . 9
1.6. Zapraszamy do kontaktu . . . 9
1.7. Podręcznik uczestnika TISAX w innych językach i formatach . . . 10
1.7.1. O tłumaczeniu na język polski . . . 12
1.7.2. Informacje dotyczące formatu online . . . 13
1.7.3. Informacje dotyczące formatu offline . . . 13
1.7.4. Informacje dotyczące formatu PDF . . . 13
2. Wprowadzenie . . . 14
2.1. Dlaczego TISAX? . . . 14
2.2. Kto określa, co oznacza „bezpieczne”? . . . 14
2.3. Branża motoryzacyjna . . . 15
2.4. Jak skutecznie udowodnić bezpieczeństwo? . . . 15
3. Proces TISAX . . . 17
3.1. Informacje ogólne . . . 17
3.2. Rejestracja . . . 18
3.3. Ocena . . . 18
3.4. Wymiana . . . 19
4. Rejestracja (Etap 1) . . . 20
4.1. Informacje ogólne . . . 20
4.2. Są Państwo uczestnikiem TISAX . . . 20
4.3. Przygotowanie do rejestracji . . . 23
4.3.1. Kwestie prawne . . . 23
4.3.2. Zakres postępowania TISAX . . . 24
4.3.2.1. Opis zakresu . . . 25
4.3.2.2. Zakres standardowy . . . 25
4.3.2.3. Wybór lokalizacji . . . 26
4.3.2.4. Dostosowanie zakresu . . . 27
4.3.2.5. Lokalizacje w ramach zakresu . . . 28
4.3.2.6. Nazwa zakresu . . . 31
4.3.2.7. Osoby do kontaktu . . . 32

4.3.2.8. Publikacja i udostępnianie . . . 33
4.3.3. Cele oceny . . . 35
4.3.3.1. Lista celów oceny . . . 36
4.3.3.2. Cele oceny i ISA . . . 38
4.3.3.3. Cele oceny i etykiety TISAX . . . 38
4.3.3.4. Wybór celu oceny . . . 39
4.3.3.5. Potrzeby ochrony i poziomy oceny . . . 43
4.3.3.6. Cele oceny a Państwa dostawcy . . . 48
4.3.4. Opłata . . . 49
4.4. Portal ENX . . . 51
4.5. Proces rejestracji online . . . 51
4.5.1. Wymagany czas . . . 51
4.5.2. Miejsce rozpoczęcia . . . 52
4.5.3. Konto na portalu . . . 52
4.5.4. Rejestracja uczestnika . . . 52
4.5.5. Osoba do kontaktu ze strony uczestnika . . . 53
4.5.6. Warunki ogólne . . . 54
4.5.7. Rejestracja zakresu oceny . . . 54
4.5.8. Wiadomość e-mail z potwierdzeniem . . . 57
4.5.8.1. Participant ID (Identyfikator uczestnika) . . . 58
4.5.8.2. Scope ID (Identyfikator zakresu) . . . 59
4.5.9. Informacje dotyczące statusu . . . 60
4.5.10. Zmiany informacji podanych przez Państwa w trakcie rejestracji . . . 63
5. Ocena (Etap 2) . . . 64
5.1. Informacje ogólne . . . 64
5.2. Samoocena na podstawie ISA . . . 64
5.2.1. Pobieranie dokumentu ISA . . . 65
5.2.2. Rozumienie dokumentu ISA . . . 65
5.2.2.1. Katalogi kryteriów . . . 65
5.2.2.2. Rozdziały . . . 73
5.2.2.3. Pytania kontrolne . . . 74
5.2.2.4. Pola formularza samooceny . . . 74
5.2.2.5. Cel . . . 75
5.2.2.6. Wymagania . . . 76
5.2.2.7. Poziomy dojrzałości . . . 76
5.2.3. Prowadzenie samooceny . . . 78
5.2.4. Interpretacja wyniku samooceny . . . 79

5.2.4.1. Analiza . . . 79
5.2.4.2. Docelowy poziom dojrzałości (na poziomie pytań) . . . 83
5.2.4.3. Państwa wynik (na poziomie pytań) . . . 83
5.2.4.4. Wartość docelowa (na poziomie punktacji) . . . 86
5.2.4.5. Państwa wynik (na poziomie punktacji) . . . 88
5.2.4.6. Czy są Państwo gotowi? . . . 89
5.2.5. Działanie na podstawie wyniku samooceny . . . 91
5.3. Wybór dostawcy usług audytu . . . 92
5.3.1. Dane kontaktowe . . . 93
5.3.2. Zakres terytorialny . . . 93
5.3.3. Zapytania ofertowe . . . 93
5.3.4. Ocena ofert . . . 94
5.4. Proces oceny TISAX . . . 96
5.4.1. Informacje ogólne . . . 96
5.4.2. Spotkanie inauguracyjne . . . 96
5.4.3. Rodzaje ocen TISAX . . . 97
5.4.4. Elementy oceny TISAX . . . 97
5.4.5. Informacje na temat zgodności . . . 98
5.4.6. Państwa przygotowania do procesu oceny TISAX . . . 101
5.4.7. Ocena wstępna . . . 101
5.4.7.1. Pierwsze formalne spotkanie otwierające . . . 102
5.4.7.2. Procedura oceny . . . 102
5.4.7.3. Spotkanie kończące . . . 102
5.4.7.4. Raport z oceny TISAX . . . 102
5.4.8. Opracowanie planu działań korygujących . . . 103
5.4.9. Ocena planu działań korygujących . . . 104
5.4.9.1. Powody oceny planu działań korygujących . . . 105
5.4.9.2. Połączenie z oceną wstępną . . . 105
5.4.9.3. Wymagania dotyczące planu działań korygujących . . . 105
5.4.9.4. Tymczasowe etykiety TISAX . . . 106
5.4.10. Ocena kontrolna . . . 107
5.4.10.1. Ramy czasowe . . . 107
5.4.10.2. Warunki wstępne . . . 107
5.4.10.3. Wygaśnięcie tymczasowych etykiet TISAX . . . 107
5.4.11. Schemat procesu oceny TISAX . . . 107
5.4.12. Assessment ID (Identyfikator oceny) . . . 111
5.4.13. Raport z oceny TISAX . . . 112

5.4.14. Etykiety TISAX . . . 113
5.4.14.1. Hierarchia etykiet TISAX . . . 114
5.4.14.2. Okres ważności etykiet TISAX . . . 115
5.4.14.3. Odnowienie etykiet TISAX . . . 115
6. Wymiana (Etap 3) . . . 117
6.1. Założenie . . . 117
6.2. Platforma wymiany . . . 117
6.3. Ogólne warunki wstępne . . . 117
6.4. Trwałość wyników będących przedmiotem wymiany . . . 118
6.5. Poziomy udostępniania . . . 118
6.6. Publikacja Państwa wyniku oceny na platformie wymiany . . . 119
6.7. Udostępnianie własnego wyniku oceny konkretnemu uczestnikowi . . . 120
6.7.1. Warunki wstępne . . . 121
6.7.2. Sposób tworzenia zgody na udostępnianie . . . 122
6.8. Udostępnianie wyniku oceny poza TISAX . . . 123
6.8.1. Powody rygorystycznych regulacji mechanizmu wymiany . . . 123
6.8.2. Poradnik dotyczący publicznych komunikatów na temat TISAX . . . 123
6.8.3. Udostępnianie partnerowi, który nie jest jeszcze uczestnikiem TISAX . . . 123
6.8.4. Udostępnianie pracownikom Państwa partnera nieposiadającym bezpośredniego dostępu do portalu ENX . . . 124
7. Załączniki . . . 126
7.1. Załącznik: Przykładowa faktura . . . 126
7.2. Załącznik: Przykładowa wiadomość e-mail z potwierdzeniem . . . 127
7.3. Załącznik: Przykładowy wyciąg z zakresu TISAX . . . 128
7.4. Załącznik: Participant status (Status uczestnika) . . . 129
7.4.1. Informacje ogólne: Participant status (Status uczestnika) . . . 129
7.4.2. Participant status „Incomplete” (Status uczestnika „Niekompletny”) . . . 131
7.4.3. Participant status „Awaiting approval” (Status uczestnika „Oczekujący na zatwierdzenie”) . . . 132
7.4.4. Participant status „Preliminary” (Status uczestnika „Wstępny”) . . . 132
7.4.5. Participant status „Registered” (Status uczestnika „Zarejestrowany”) . . . 134
7.4.6. Participant status „Expired” (Status uczestnika „Po terminie ważności”) . . . 135
7.5. Załącznik: Assessment scope status (Status zakresu oceny) . . . 135
7.5.1. Informacje ogólne: Assessment scope status (Status zakresu oceny) . . . 135
7.5.2. Assessment scope status „Incomplete” (Status zakresu oceny „Niekompletny”) . . . 137
7.5.3. Assessment scope status „Awaiting your order” (Status zakresu oceny „Oczekujący na Państwa zlecenie”) . . . 138

7.5.4. Assessment scope status „Awaiting ENX approval” (Status zakresu oceny „Oczekujący na zatwierdzenie ENX”) . . . 138
7.5.5. Assessment scope status „Awaiting your payment” (Status zakresu oceny „Oczekujący na Państwa płatność”) . . . 140
7.5.6. Assessment scope status „Registered” (Status zakresu oceny „Zarejestrowany”) . . . 141
7.5.7. Assessment scope status „Active” (Status zakresu oceny „Aktywny”) . . . 141
7.5.8. Assessment scope status „Expired” (Status zakresu oceny „Po terminie ważności”) . . . 142
7.6. Załącznik: Assessment status (Status oceny) . . . 143
7.6.1. Informacje ogólne: Assessment status (Status oceny) . . . 143
7.6.2. Assessment status „Initial assessment ordered” (Status oceny „Ocena wstępna zlecona”) . . . 145
7.6.3. Assessment status „Initial assessment ongoing” (Status oceny „Ocena wstępna w toku”) . . . 145
7.6.4. Assessment status „Waiting for corrective action plan assessment” (Status oceny „Oczekiwanie na ocenę planu działań korygujących”) . . . 146
7.6.5. Assessment status „Waiting for follow-up” (Status oceny „Oczekiwanie na kontrolę”) . . . 146
7.6.6. Assessment status „Finished” (Status oceny „Zakończony”) . . . 147
7.7. Załącznik: Argumenty przeciwko „ocenom początkowym” i „analizom luk” . . . 147
7.8. Załącznik: Zakresy niestandardowe . . . 149
7.8.1. Zakres niestandardowy rozszerzony . . . 149
7.8.2. Zakres niestandardowy pełny . . . 149
7.9. Załącznik: Zarządzanie cyklem życia danych uczestników . . . 150
7.9.1. Utrata dostępu do danych uczestnika (portal ENX) . . . 150
7.9.2. Administrowanie osobami do kontaktu . . . 150
7.9.2.1. Dodawanie nowej osoby do kontaktu . . . 150
7.9.2.2. Usuwanie istniejącej osoby do kontaktu . . . 151
7.9.2.3. Aktualizacja danych istniejącej osoby do kontaktu . . . 151
7.9.3. Administrowanie lokalizacjami . . . 152
7.9.3.1. Wniosek o zmianę nazwy spółki . . . 152
7.9.3.2. Wniosek o zmianę lokalizacji . . . 153
7.9.3.3. Wniosek o zmianę nazwy ulicy . . . 154
7.9.3.4. Dodawanie kolejnej lokalizacji . . . 155
7.10. Załącznik: Ocena rozszerzenia zakresu . . . 155
7.11. Załącznik: Zarządzanie cyklem życia ISA . . . 156
7.12. Załącznik: Przydatne dokumenty . . . 156

7.13. Załącznik: Zarządzanie reklamacjami . . . 157
7.13.1. Powody reklamacji . . . 157
7.13.1.1. Reklamacje związane z ENX Association . . . 157
7.13.1.2. Reklamacje związane z dostawcami usług audytu . . . 157
7.13.1.3. Wymagania związane z reklamacjami . . . 158
7.13.2. Osoba do kontaktu w odniesieniu do reklamacji . . . 159
8. Historia dokumentu . . . 160

1. Informacje ogólne

1.1. Cel

Witamy w TISAX (Trusted Information Security Assessment Exchange).

Jeden z Państwa partnerów zażądał od Państwa udowodnienia, że stosowane przez Państwa zarządzanie bezpieczeństwem informacji jest zgodne z poziomem określonym w wymaganiach „Oceny bezpieczeństwa informacji” (Information Security Assessment, ISA). Chcą Państwo wiedzieć, jak spełnić to żądanie.

Niniejszy podręcznik pozwoli Państwu zrealizować żądanie partnera — lub zyskać przewagę w drodze uprzedzenia takich żądań partnera.

W tym podręczniku opisano etapy, przez jakie należy przejść w celu uzyskania pomyślnego wyniku oceny TISAX oraz udostępnienia wyniku oceny partnerowi.

Już samo ustanowienie i utrzymanie systemu zarządzania bezpieczeństwem informacji (ISMS) jest złożonym zadaniem. Udowodnienie partnerowi, że zarządzanie bezpieczeństwem informacji spełnia wymogi dla danego zadania czyni je jeszcze trudniejszym. Ten podręcznik nie ułatwi zarządzania bezpieczeństwem informacji. Ma natomiast ułatwić udowodnienie partnerowi własnych wysiłków.

1.2. Zakres

Niniejszy podręcznik dotyczy wszystkich procesów TISAX, w których mogą Państwo uczestniczyć.

Zawiera wszystkie informacje niezbędne, by przejść proces TISAX.

Ten podręcznik podpowiada, jak spełnić wymagania dotyczące bezpieczeństwa informacji będące kluczowym elementem oceny. Nie zawiera jednak informacji ogólnych dotyczących czynności niezbędnych do uzyskania pomyślnego wyniku oceny bezpieczeństwa informacji.

1.3. Odbiorcy

Głównymi odbiorcami tego podręcznika są spółki, które muszą lub pragną udowodnić określony poziom zarządzania bezpieczeństwem informacji zgodnie z wymaganiami „Oceny bezpieczeństwa informacji” (Information Security Assessment, ISA).

Informacje zawarte w tym podręczniku przydadzą się po czynnym rozpoczęciu procesów TISAX.

Skorzystają z nich także spółki żądające od swych dostawców udowodnienia określonych poziomów zarządzania bezpieczeństwem informacji. Podręcznik pozwoli im zrozumieć, co muszą zrobić dostawcy w celu realizacji tego żądania.

1.4. Struktura

Zaczniemy od krótkiego wprowadzenia TISAX, a później przejdziemy do instrukcji dotyczących konkretnych działań. Znajdą tu Państwo wszystkie elementy potrzebne do przejścia procesu -- w określonej kolejności.

Szacowany czas czytania tego dokumentu wynosi 75–90 minut.

1.5. Sposób korzystania z tego dokumentu

Wcześniej czy później prawdopodobnie zapragną Państwo zrozumieć większość kwestii zawartych w tym dokumencie. Aby odpowiednio się przygotować, zalecamy zapoznanie się z całym podręcznikiem.

Struktura podręcznika opiera się na trzech głównych etapach procesu TISAX, dzięki czemu można przejść do potrzebnego punktu, a z pozostałą częścią zapoznać się później.

Wykorzystane w podręczniku ilustracje ułatwiają rozumienie. Kolory na ilustracjach często mają dodatkowe znaczenie. Dlatego też zalecamy zapoznanie się z niniejszym dokumentem na ekranie komputera lub w postaci kolorowego egzemplarza papierowego.

Cenimy Państwa opinie. Jeśli Państwa zdaniem w niniejszym podręczniku czegoś brakuje lub coś trudno zrozumieć, prosimy o informację. Za takie opinie będziemy wdzięczni zarówno my sami, jak i wszyscy przyszli czytelnicy podręcznika.

Jeśli korzystali już Państwo z poprzedniej wersji podręcznika uczestnika TISAX, na końcu dokumentu w Punkt 8, “Historia dokumentu” znajdą Państwo przydatne uwagi.

1.6. Zapraszamy do kontaktu

Z przyjemnością poprowadzimy Państwa przez proces TISAX oraz udzielimy odpowiedzi na ewentualne pytania.

Prosimy o wiadomość e-mail na adres: tisax@enx.com

Lub o kontakt telefoniczny pod numerem: +49 69 9866927-77

Można się z nami skontaktować w zwykłych godzinach pracy w Niemczech (UTC+01:00).

Wszyscy posługujemy się językiem angielskim oraz niemieckim. Dla jednego z członków naszego zespołu rodzimym językiem jest włoski.

Prosimy o zapoznanie się z Punkt 7.13, “Załącznik: Zarządzanie reklamacjami”.

1.7. Podręcznik uczestnika TISAX w innych językach i formatach

Podręcznik uczestnika TISAX jest dostępny w następujących językach i formatach:

Język	Wersja	Format	Link
angielski	2.7.1	Online	https://www.enx.com/handbook/tisax-participant-handbook.html
		Offline	https://www.enx.com/handbook/tisax-participant-handbook-offline.html
		PDF	https://www.enx.com/handbook/TISAX%20Participant%20Handbook.pdf
niemiecki	2.7.1	Online	https://www.enx.com/handbook/tisax-teilnehmerhandbuch.html
		Offline	https://www.enx.com/handbook/tisax-teilnehmerhandbuch-offline.html
		PDF	https://www.enx.com/handbook/TISAX-Teilnehmerhandbuch.pdf
francuski	2.7	Online	https://www.enx.com/handbook/tph-fr.html
		Offline	https://www.enx.com/handbook/tph-fr-offline.html
		PDF	https://www.enx.com/handbook/tph-fr.pdf
chiński	2.7	Online	https://www.enx.com/handbook/tph-cn.html
		Offline	https://www.enx.com/handbook/tph-cn-offline.html
		PDF	https://www.enx.com/handbook/tph-cn.pdf
hiszpański	2.7	Online	https://www.enx.com/handbook/tph-es.html
		Offline	https://www.enx.com/handbook/tph-es-offline.html
		PDF	https://www.enx.com/handbook/tph-es.pdf
japoński	2.7	Online	https://www.enx.com/handbook/tph-jp.html
		Offline	https://www.enx.com/handbook/tph-jp-offline.html
		PDF	https://www.enx.com/handbook/tph-jp.pdf
brazylijski portugalski	2.7	Online	https://www.enx.com/handbook/tph-pt.html
		Offline	https://www.enx.com/handbook/tph-pt-offline.html
		PDF	https://www.enx.com/handbook/tph-pt.pdf

Język	Wersja	Format	Link
włoski	2.7.1	Online	https://www.enx.com/handbook/tph-it.html
		Offline	https://www.enx.com/handbook/tph-it-offline.html
		PDF	https://www.enx.com/handbook/tph-it.pdf
koreański	2.7	Online	https://www.enx.com/handbook/tph-kr.html
		Offline	https://www.enx.com/handbook/tph-kr-offline.html
		PDF	https://www.enx.com/handbook/tph-kr.pdf
czeski	2.7.1	Online	https://www.enx.com/handbook/tph-cz.html
		Offline	https://www.enx.com/handbook/tph-cz-offline.html
		PDF	https://www.enx.com/handbook/tph-cz.pdf
polski	2.7.1	Online	https://www.enx.com/handbook/tph-pl.html
		Offline	https://www.enx.com/handbook/tph-pl-offline.html
		PDF	https://www.enx.com/handbook/tph-pl.pdf

Ważna uwaga:

Wersją wiodącą jest wersja w języku angielskim.
Wersje w innych językach są tłumaczeniem wersji w języku angielskim.
W przypadku wątpliwości rozstrzygająca jest wersja anglojęzyczna.

1.7.1. O tłumaczeniu na język polski

Niniejszy Podręcznik uczestnika TISAX jest tłumaczeniem wersji w języku angielskim.

Wszystkie dokumenty leżące u podstaw TISAX opracowano w języku angielskim (np. wszystkie umowy i wymagania dotyczące dostawców usług audytu TISAX). w związku z tym Państwa partner lub dostawca usług audytu może używać niektórych związanych z TISAX terminów w języku angielskim.

Aby ułatwić rozumienie, w tłumaczeniu Podręcznika uczestnika TISAX zachowaliśmy oryginalny termin TISAX w języku angielskim lub podaliśmy go w nawiasach tuż po wersji tłumaczonej.

1.7.2. Informacje dotyczące formatu online

Każdy punkt posiada unikalny identyfikator (format: ID1234).
Niezależnie od języka, identyfikator odwołuje się do konkretnego punktu.

Aby przejść do konkretnego punktu, można:

- kliknąć prawym klawiszem myszy tytuł punktu i skopiować link, lub
- kliknąć tytuł punktu i skopiować link z paska adresu przeglądarki.

Większość rysunków jest dostępna w formacie większym od domyślnie wyświetlanego. Aby otworzyć większą wersję rysunku, należy go kliknąć.

1.7.3. Informacje dotyczące formatu offline

Format offline zachowuje większość cech formatu online. w szczególności ilustracje są zamieszczone w pliku HTML.
Aby użyć formatu offline, potrzebny jest tylko jeden plik.

W porównaniu do formatu online, format offline nie posiada:

- większych ilustracji,
- oryginalnych czcionek formatu online.
  Czcionki są zgodne z domyślnymi ustawieniami przeglądarki.

1.7.4. Informacje dotyczące formatu PDF

Korzystanie z pliku PDF na komputerze pozwala kliknąć wszystkie odnośniki.
Natomiast w przypadku wydruku wersji PDF, nie będzie np. numerów stron, w związku z czym trzeba będzie samodzielnie wyszukiwać odnośniki.

2. Wprowadzenie

Poniższe punkty wprowadzają koncepcję TISAX.

Jeśli się Państwu spieszy, można je pominąć i zacząć od Punkt 4.3, “Przygotowanie do rejestracji”.

2.1. Dlaczego TISAX?

Czy też raczej, dlaczego są Państwo tutaj?

Odpowiedź na to pytanie zaczniemy od kilku ogólnych przemyśleń na temat prowadzenia działalności, ze szczególnym naciskiem na ochronę informacji.

Proszę wyobrazić sobie własnego partnera. Posiada informacje poufne. Chce je udostępnić swojemu dostawcy — Państwu. Współpraca Państwa z partnerem tworzy wartość. Informacje udostępnione Państwu przez partnera są ważnym elementem takiego tworzenia wartości. w związku z tym partner pragnie je odpowiednio chronić. Chce mieć także pewność, że Państwo dokładają takiej samej należytej staranności w odniesieniu do przekazanych przez niego informacji.

Jak może jednak zapewnić, że takie informacje są w dobrych rękach? Nie może po prostu Państwu „uwierzyć”. Partner potrzebuje dowodu.

I teraz dwa pytania. Kto określa, co oznacza „bezpieczne” postępowanie z informacjami? I jak to udowodnić?

2.2. Kto określa, co oznacza „bezpieczne”?

Przed tymi pytaniami nie stają tylko Państwo i Państwa partner. Niemal wszyscy muszą znaleźć na nie odpowiedź, a większość odpowiedzi wykazuje pewne podobieństwa.

Zamiast za każdym razem od nowa samodzielnie opracowywać rozwiązanie powszechnego problemu, można skorzystać ze standardowego sposobu działania, który zmniejsza obciążenie wynikające z tworzenia od podstaw. Choć opracowanie standardu wymaga ogromnego wysiłku, robi się to tylko raz, a stosowanie danego standardu za każdym razem przynosi korzyść.

Z całą pewnością różne osoby różnie postrzegają właściwe działania w kontekście ochrony informacji. Jednakże ze względu na powyższe korzyści, większość firm decyduje się korzystać ze standardu. Standard to skondensowana forma wszystkich potwierdzonych i sprawdzonych dobrych praktyk na potrzeby danego wyzwania.

W Państwa przypadku aktualny stan wiedzy na potrzeby bezpiecznego postępowania z informacjami poufnymi wynika z takich norm, jak ISO/IEC 27001 (dotycząca systemów zarządzania bezpieczeństwem informacji, tj. ISMS), i ich wdrożenia. Dzięki takiej

normie nie muszą Państwo za każdym razem wynajdować koła na nowo. Co więcej, normy zapewniają wspólne podstawy wymiany danych poufnych przez dwie spółki.

2.3. Branża motoryzacyjna

Normy niezależne od branży opracowuje się jako rozwiązania uniwersalne, nie zaś dostosowane do konkretnych potrzeb firm motoryzacyjnych.

Przed laty w branży motoryzacyjnej powstały stowarzyszenia, których celem było — między innymi — dopracowanie i określenie standardów dopasowanych do jej konkretnych potrzeb. Jednym z takich stowarzyszeń jest „Verband der Automobilindustrie” (VDA). Kilku członków branży motoryzacyjnej w grupie roboczej ds. bezpieczeństwa informacji doszło do wniosku, że posiadają zbliżone potrzeby w kontekście dostosowania istniejących standardów zarządzania bezpieczeństwem informacji.

Wspólnym staraniem opracowali kwestionariusz obejmujący powszechnie przyjęte wymogi dotyczące bezpieczeństwa informacji w branży motoryzacyjnej. Nosi on nazwę „Ocena bezpieczeństwa informacji” (Information Security Assessment, ISA).

Dzięki ISA mamy odpowiedź na pytanie „Kto określa, co oznacza bezpieczne?”. Za pośrednictwem VDA branża motoryzacyjna przekazuje tę odpowiedź swym członkom.

2.4. Jak skutecznie udowodnić bezpieczeństwo?

Niektóre spółki wykorzystują ISA wyłącznie do potrzeb wewnętrznych, zaś inne do oceny dojrzałości zarządzania bezpieczeństwem informacji u swoich dostawców. Czasem na potrzeby relacji biznesowych wystarczy samoocena. Jednakże w niektórych przypadkach spółki prowadzą pełną ocenę zarządzania bezpieczeństwem informacji u swoich dostawców (wraz z audytami na miejscu).

W miarę wzrostu świadomości zapotrzebowania na zarządzanie bezpieczeństwem informacji i coraz powszechniejszego przyjęcia ISA jako narzędzia do oceny bezpieczeństwa informacji, coraz większa liczba partnerów otrzymywała podobne żądania ze strony różnych partnerów.

Partnerzy ci stosowali różne standardy i interpretowali je w różny sposób. Dostawcy musieli jednak zasadniczo udowodnić to samo, choć odmiennie.

Im większa liczba dostawców otrzymywała od swych partnerów wnioski o udowodnienie poziomu zarządzania bezpieczeństwem informacji, tym głośniejsze były skargi na wielokrotne wysiłki. Przedstawianie kolejnym audytorom tych samych środków zarządzania bezpieczeństwem informacji po prostu nie jest wydajne.

Jak można zwiększyć wydajność tego procesu? Czy nie byłoby lepiej, gdyby różni partnerzy mogli skorzystać z raportu dowolnego audytora?

Producenci oryginalnego sprzętu i dostawcy w grupie roboczej ENX odpowiedzialnej za utrzymanie ISA wysłuchali skarg dostawców. Obecnie zapewniają swym dostawcom oraz innym spółkom w branży motoryzacyjnej odpowiedź na pytanie „Jak udowodnić bezpieczeństwo?”.

Odpowiedzią jest TISAX, skrót od „Trusted Information Security Assessment Exchange”.

3. Proces TISAX

3.1. Informacje ogólne

Proces TISAX zwykle[1] rozpoczyna się od wniosku jednego z partnerów o udowodnienie określonego poziomu zarządzania bezpieczeństwem informacji zgodnie z wymogami „Oceny bezpieczeństwa informacji” (ISA). Aby zrealizować takie żądanie, należy ukończyć 3-etapowy proces TISAX. Niniejszy punkt zawiera informacje ogólne na temat etapów, przez jakie trzeba przejść.

3-etapowy proces TISAX składa się z następujących etapów:

Rysunek 1. Omówienie procesu TISAX

1. Etap 1
   Rejestracja
2. Etap 2
   Ocena
3. Etap 3
   Wymiana

1. Rejestracja
   Zbieramy informacje na temat Państwa firmy oraz elementów wchodzących w skład oceny.
2. Ocena
   Przechodzą Państwo proces ocen prowadzonych przez jednego z naszych dostawców usług audytu TISAX.
3. Wymiana
   Wyniki Państwa oceny udostępniają Państwo swojemu partnerowi.

Każdy etap składa się z etapów pomocniczych. Ich zarys znajduje się w trzech poniższych punktach, a szczegółowy opis w odpowiednich punktach w dalszej części dokumentu.

Uwaga:

Choć chcielibyśmy wskazać termin uzyskania wyniku oceny TISAX, prosimy o wyrozumiałość, ponieważ nie jesteśmy w stanie wiarygodnie tego przewidzieć. Całkowity czas trwania procesu TISAX zależy od zbyt wielu czynników. Niemożność przewidzenia terminu wynika z różnic wielkości spółek oraz celów oceny, a także gotowości systemu zarządzania bezpieczeństwem

informacji.

3.2. Rejestracja

Pierwszy etap to rejestracja TISAX.

Głównym celem rejestracji TISAX jest zebranie informacji na temat Państwa spółki. Aby ułatwić przekazywanie nam takich informacji, używamy procesu rejestracji online.

Jest on warunkiem wstępnym wszystkich kolejnych etapów. Wiąże się z opłatą.

W trakcie procesu rejestracji online:

- Poprosimy o dane do kontaktu i dane do rozliczeń.
- Muszą Państwo zaakceptować nasze warunki.
- Mogą Państwo określić zakres oceny bezpieczeństwa informacji.

Bezpośrednie rozpoczęcie tego etapu opisano w Punkt 4, “Rejestracja (Etap 1)”.

Proces rejestracji online szczegółowo opisano w Punkt 4.5, “Proces rejestracji online”. Jeśli jednak chcą Państwo zacząć od razu, proszę przejść do enx.com/en-US/TISAX/.

3.3. Ocena

Drugim etapem jest ocena bezpieczeństwa informacji.

Ma ona cztery etapy pomocnicze:

a. Przygotowanie do oceny
   Muszą się Państwo przygotować do oceny. Zakres przygotowań zależy od aktualnego poziomu dojrzałości systemu zarządzania bezpieczeństwem informacji. Przygotowania muszą być oparte na katalogu ISA.

b. Wybór dostawcy usług audytu
   Muszą Państwo wybrać jednego z naszych dostawców usług audytu TISAX.

c. Ocena(-y) bezpieczeństwa informacji
   Dostawca usług audytu przeprowadzi ocenę na podstawie zakresu oceny odpowiadającego wymaganiom Państwa partnera. Proces oceny będzie się składał co najmniej z audytu wstępnego.
   Jeśli spółka nie przejdzie oceny za pierwszym razem, proces oceny może wymagać dodatkowych etapów.

d. Wynik oceny
   Kiedy spółka pomyślnie przejdzie ocenę, dostawca usług audytu przekaże Państwu oficjalny raport z oceny TISAX. Wynik Państwa oceny opatrzymy także etykietami TISAX[2].

Bardziej szczegółowe informacje na temat tego etapu znajdują się w Punkt 5, “Ocena (Etap 2)”.

3.4. Wymiana

Trzecim i ostatnim etapem jest udostępnienie wyniku oceny Państwa partnerowi. Treść raportu z oceny TISAX podzielono na poziomy. To od Państwa zależy, do jakiego poziomu zyska dostęp Państwa partner.

Wynik Państwa oceny zachowuje ważność przez trzy lata. Jeśli po upływie tego czasu nadal będą Państwo dostawcą swojego partnera, będą Państwo musieli ponownie przejść ten trzyetapowy proces[3].

Bardziej szczegółowe informacje na temat tego etapu znajdują się w Punkt 6, “Wymiana (Etap 3)”.

Ponieważ znają już Państwo podstawy procesu TISAX, w poniższych punktach mogą się Państwo zapoznać z instrukcjami realizacji poszczególnych etapów.

4. Rejestracja (Etap 1)

Szacowany czas czytania punktu poświęconego rejestracji wynosi 30–40 minut.

4.1. Informacje ogólne

Rejestracja TISAX to pierwszy etap. Jest on warunkiem wstępnym wszystkich kolejnych etapów.

Poniższe punkty poprowadzą Państwa przez proces rejestracji:

1. Zaczniemy od wyjaśnienia istotnego nowego terminu.
2. Później wskażemy, jak się przygotować do procesu rejestracji online.
3. Następnie poprowadzimy przez proces rejestracji online.

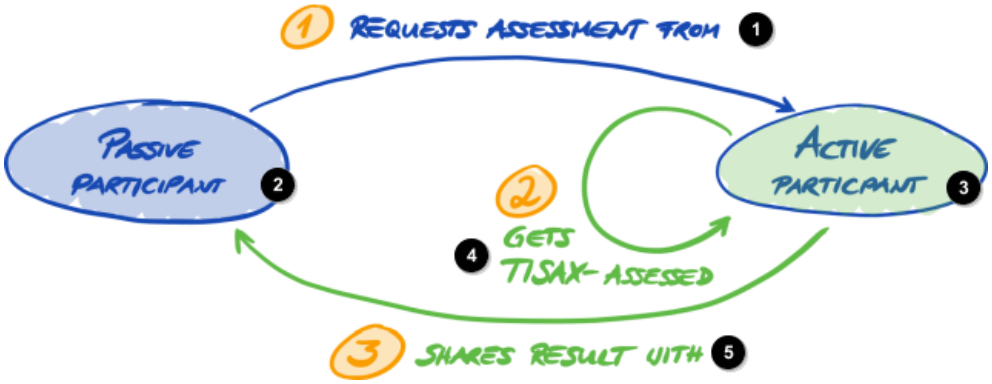
4.2. Są Państwo uczestnikiem TISAX

Przedstawmy najpierw nowy termin, który muszą Państwo rozumieć. Jak dotąd byli Państwo „dostawcą”. Są Państwo tutaj, by zrealizować wymóg swojego „klienta”. Sam TISAX nie rozróżnia jednak tych dwóch ról. w ramach TISAX wszyscy rejestrują się jako „uczestnik”. Państwo -- i Państwa partner — „uczestniczą” w wymianie wyników oceny bezpieczeństwa informacji.

Rysunek 2. Rejestracja, by zostać uczestnikiem TISAX

1. Państwa spółka
2. Rejestracja TISAX
3. Uczestnik TISAX

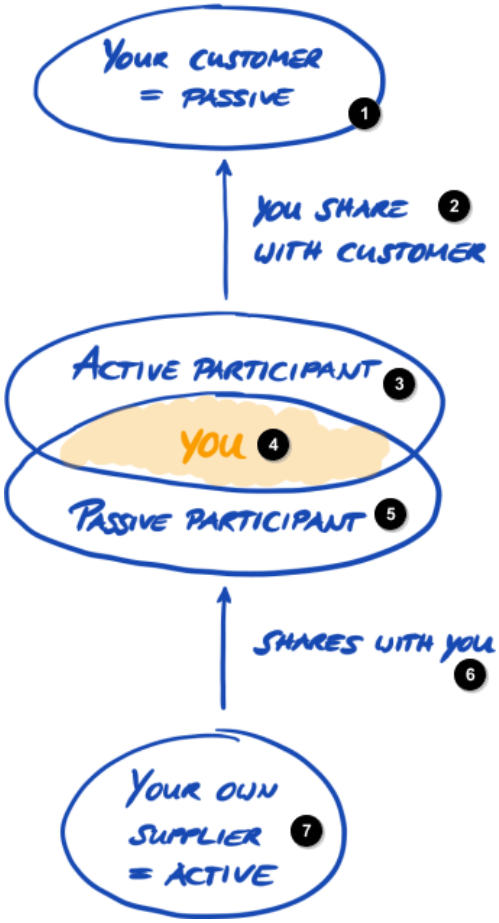
Aby od początku rozróżnić te dwie role, Państwa, czyli dostawcę, nazywamy „uczestnikiem czynnym”. Państwa partnera natomiast „uczestnikiem biernym”. Jako „uczestnik czynny” poddają się Państwo ocenie TISAX, której wynik udostępniają innym uczestnikom. „Uczestnik bierny” to podmiot, który zażądał od Państwa poddania się ocenie TISAX. „Uczestnik bierny” to podmiot otrzymujący wynik Państwa oceny.



Rysunek 3. Uczestnik bierny i uczestnik czynny

1. 1 Żąda oceny od
2. Uczestnik bierny
3. Uczestnik czynny
4. 2 Poddaje się ocenie TISAX
5. 3 Udostępnia wynik

Każda spółka może występować w obu rolach. Mogą Państwo udostępnić wynik oceny partnerowi, a jednocześnie żądać od własnych dostawców poddania się ocenie TISAX.



Rysunek 4. Uczestnicy TISAX mogą być jednocześnie czynni i bierni

1. Państwa klient
   = bierny
2. Udostępniają Państwo klientowi
3. Uczestnik czynny
4. Państwo
5. Uczestnik bierny
6. Udostępnia Państwu
7. Państwa dostawca
   = czynny

Żądanie od własnych dostawców poddania się ocenie TISAX sugeruje się szczególnie w przypadku, gdy Państwa dostawcy mają dostęp także do wymagających ochrony informacji Państwa partnera.

4.3. Przygotowanie do rejestracji

W tym punkcie znajdą Państwo zalecenia dotyczące sposobu *przygotowania się* do rejestracji. Sam proces rejestracji szczegółowo opisano w Punkt 4.5, “Proces rejestracji online”.

Przed rozpoczęciem procesu rejestracji online zalecamy:

- wcześniejsze zebranie informacji
- i podjęcie pewnych decyzji.

4.3.1. Kwestie prawne

Zwykle muszą Państwo podpisać dwie umowy. Pierwszą z nich jest umowa z ENX Association: „Warunki ogólne uczestnictwa TISAX” (OWU uczestnika TISAX). Drugą jest umowa między Państwem a jednym z naszych dostawców usług audytu TISAX. w kontekście rejestracji, omówimy tylko pierwszą z nich.

OWU uczestnika TISAX regulują nasze wzajemne relacje oraz Państwa stosunki z innymi uczestnikami TISAX. Określają one prawa i obowiązki wszystkich stron. Oprócz zwykłych postanowień, jakie występują w większości umów, szczegółowo określają one postępowanie z informacjami przekazywanymi i otrzymywanymi w ramach procesu TISAX. Najważniejszym celem tych zasad jest zapewnienie poufności wyników oceny TISAX. Ponieważ wszyscy uczestnicy TISAX podlegają tym samym zasadom, można liczyć na odpowiednią ochronę własnego wyniku oceny TISAX przez partnera (będącego uczestnikiem biernym).

Na dość wczesnym etapie procesu rejestracji online poprosimy Państwa o akceptację OWU uczestnika TISAX. Ponieważ jest to umowa, przed rozpoczęciem procesu rejestracji online zalecamy zapoznanie się z OWU uczestnika TISAX. Wynika to m.in. z faktu, że zależnie od własnej roli w firmie mogą być Państwo zmuszeni do uzyskania zgody prawnika firmowego lub zewnętrznego.

„Warunki ogólne uczestnictwa TISAX” można pobrać[4] z naszej strony internetowej pod adresem:
enx.com/en-US/TISAX/downloads/

PDF do pobrania:
enx.com/tisaxgtcen.pdf

W trakcie procesu rejestracji online poprosimy Państwa o zaznaczenie dwóch obowiązkowych pól wyboru:

- ☐ We accept the TISAX Participation General Terms and Conditions (Akceptujemy Warunki ogólne uczestnictwa TISAX)
- ☐ We confirm knowledge of Applicant’s release of Audit Providers’ professional duties of secrecy acc. to Sec. IX.5. and X.3 of the TISAX Participation General Terms and Conditions;

(🇵🇱 Potwierdzamy zaznajomienie się z wersją dla Wnioskodawcy zawodowych obowiązków zachowania tajemnicy Dostawców usług audytu zgodnie z punktem IX.5. i X.3 Warunków ogólnych uczestnictwa TISAX)

Drugie pole wyboru wynika z faktu, że część naszych dostawców usług audytu TISAX to biegli rewidenci. Obowiązują ich szczególne wymagania dotyczące zachowania tajemnicy zawodowej. Zwykle szczególne wymagania dotyczące zachowania tajemnicy zawodowej zakazują biegłym rewidentom wśród naszych dostawców usług audytu przekazywania nam informacji. Wykluczyłoby to opcje kontroli niezbędne nam do realizacji naszej roli zarządczej. Dlatego też potrzebujemy tej informacji. Przed zaznaczeniem pola warto zwrócić szczególną uwagę na te postanowienia.

Jeśli zwykle potrzebują Państwo zawrzeć z osobą mającą dostęp do informacji poufnych umowę o nieujawnianiu informacji, prosimy o zapoznanie się z odpowiednimi punktami naszych OWU. Prawdopodobnie znajdą tam Państwo odpowiedź na wszystkie swoje obawy. Co więcej, zwykle nie muszą nam Państwo przekazywać żadnych informacji poufnych.

Na zakończenie punktu dotyczącego kwestii prawnych przypominamy, że działanie systemu wymaga akceptacji jednakowych zasad przez wszystkie strony. w związku z tym nie możemy zaakceptować dodatkowych warunków ogólnych[5].

4.3.2. Zakres postępowania TISAX

W ramach drugiego etapu procesu TISAX, jeden z naszych dostawców usług audytu TISAX przeprowadzi ocenę bezpieczeństwa informacji. Musi jednak wiedzieć, gdzie zacząć, a gdzie przerwać. Właśnie dlatego muszą Państwo określić „zakres oceny”.

„Zakres oceny” określa zakres oceny bezpieczeństwa informacji. Dla uproszczenia, zakres oceny obejmuje każdą część Państwa firmy mającą dostęp do informacji poufnych Państwa partnera. Można go uznać za główny element opisu zadania dostawcy usług audytu. Wskazuje, co ma ocenić dostawca usług audytu.

Zakres oceny jest istotny z dwóch powodów:

a. Wynik oceny spełni wymogi partnera jedynie w przypadku, gdy dany zakres oceny obejmie wszystkie części firmy mające dostęp do informacji poufnych partnera.
b. Precyzyjnie określony zakres oceny jest ważnym warunkiem wstępnym konstruktywnych obliczeń kosztów prowadzonych przez naszych dostawców usług audytu TISAX.

Ważna uwaga:

ISO/IEC 27001 a TISAX

Przede wszystkim musimy rozróżnić dwa rodzaje zakresów:
1) zakres systemu zarządzania bezpieczeństwem informacji (ISMS) oraz

2) zakres oceny.
Nie muszą one być tożsame.

Na potrzeby procesu certyfikacji zgodności z normą ISO/IEC 27001, określają Państwo zakres swojego ISMS (w „określeniu zakresu”). Zakres ISMS można określić całkowicie dowolnie. Jednakże zakres oceny (zwany także „zakresem audytu”) musi być tożsamy z zakresem ISMS.

Na potrzeby TISAX również trzeba określić ISMS. Zakres oceny nie musi się z nim jednak pokrywać.

Na potrzeby procesu certyfikacji zgodności z normą ISO/IEC 27001, mogą Państwo dowolnie kształtować zakres oceny za pomocą określenia zakresu ISMS.

Natomiast w przypadku TISAX, zakres oceny jest wstępnie określony. Zakres oceny może być mniejszy od zakresu ISMS. Musi się jednak mieścić w zakresie ISMS.

4.3.2.1. Opis zakresu

Opis zakresu określa zakres oceny. Na potrzeby opisu zakresu trzeba wybrać jeden z dwóch rodzajów zakresu:

1. Standard scope (Zakres standardowy)
2. Custom scope (Zakres niestandardowy)
   a. Custom extended scope (Zakres niestandardowy rozszerzony)
   b. Full custom scope (Zakres niestandardowy pełny)

Zakres standardowy omówimy w następnym punkcie. Zakres standardowy jest właściwym wyborem dla ponad 99% uczestników. Dlatego zakresy niestandardowe omówimy w Punkt 7.8, “Załącznik: Zakresy niestandardowe”.

4.3.2.2. Zakres standardowy

Opis zakresu standardowego stanowi podstawę oceny TISAX. Inni uczestnicy TISAX akceptują jedynie wyniki oceny opartej na opisie zakresu standardowego.

Opis zakresu standardowego jest wstępnie określony i nie można go zmienić.

Główną zaletą zakresu standardowego jest brak konieczności opracowywania własnej definicji.

Oto opis zakresu standardowego (wersja 2.0):

The TISAX assessment scope defines the scope of the assessment. The assessment includes all processes, procedures and resources under responsibility of the assessed organization that are relevant to the security of the protection objects and their protection goals as defined in the listed assessment objectives at the listed locations.
The assessment is conducted at least in the highest assessment level listed in any of the listed assessment objectives. All assessment criteria listed in the listed assessment objectives are subject to the assessment.

Zakres oceny TISAX określa zakres oceny. Ocena obejmuje wszystkie procesy, procedury{nbsp}i{nbsp}zasoby, za jakie odpowiada oceniana firma, istotne dla bezpieczeństwa przedmiotów ochrony{nbsp}i{nbsp}celów takiej ochrony, jak określono na liście celów oceny{nbsp}w{nbsp}wymienionych lokalizacjach.
Ocenę prowadzi się na co najmniej najwyższym poziomie oceny wskazanym dla dowolnego{nbsp}z{nbsp}wymienionych celów oceny. Ocenie podlegają wszystkie kryteria oceny wymienione{nbsp}w{nbsp}wymienionych celach oceny.

Zdecydowanie zalecamy wybór zakresu standardowego. Wszyscy uczestnicy TISAX akceptują wyniki oceny bezpieczeństwa informacji opartej na zakresie standardowym.

4.3.2.3. Wybór lokalizacji

Kolejnym zadaniem po określeniu rodzaju zakresu jest wskazanie lokalizacji wchodzących w zakres oceny.

W przypadku małej spółki (jedna lokalizacja) to proste zadanie. Po prostu należy dodać lokalizację do zakresu oceny.

W przypadku dużej spółki można rozważyć rejestrację więcej niż jednego zakresu oceny.

Jeden zakres obejmujący wszystkie lokalizacje ma pewne zalety:

- Otrzymują Państwo jeden raport z oceny, jeden wynik oceny i jeden termin ważności.
- Mają Państwo prawo do obniżki kosztów oceny, ponieważ dostawca usług audytu TISAX tylko jeden raz ocenia procesy, procedury i zasoby na szczeblu centralnym.

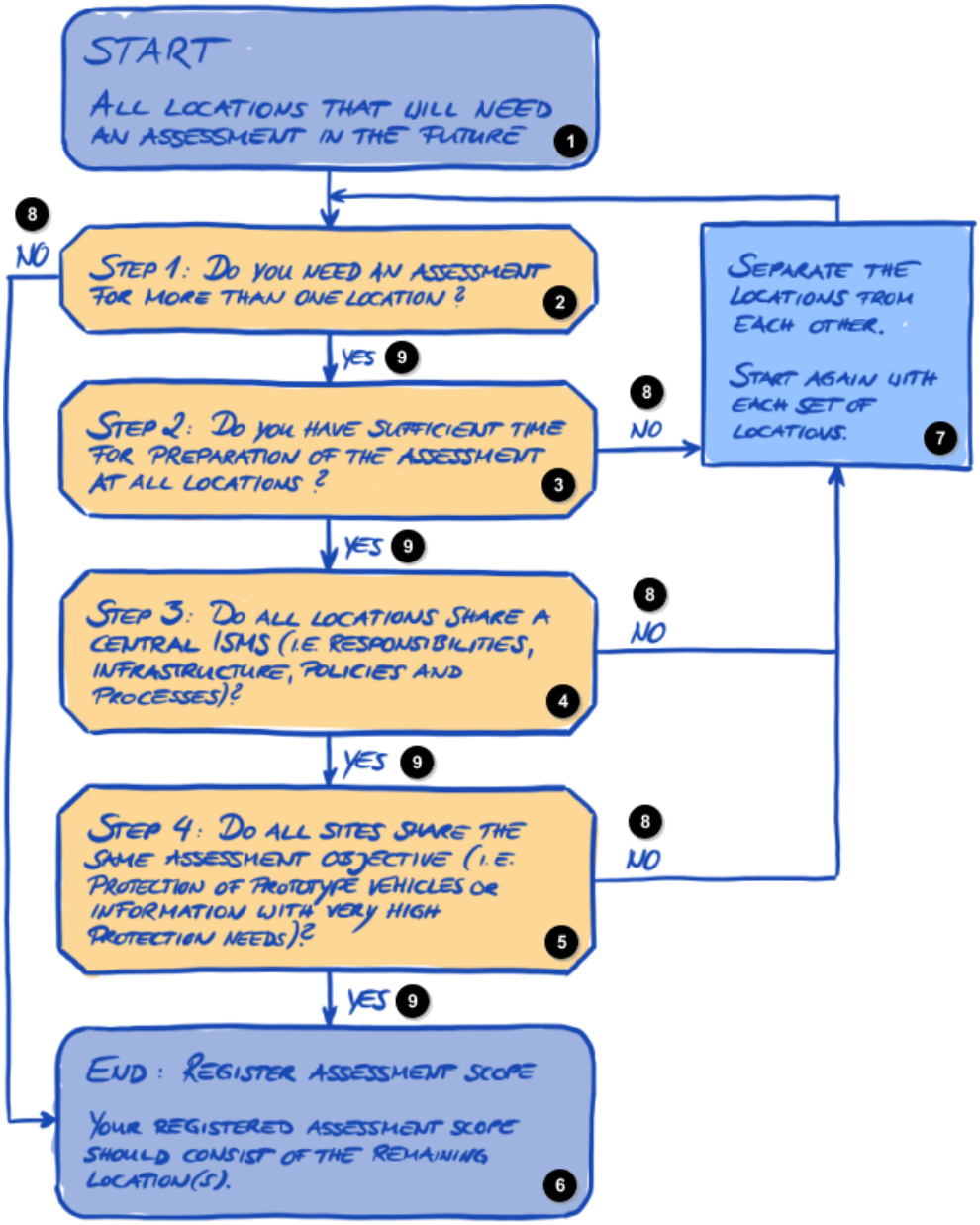
Jeden zakres może także mieć następujące wady:

- Wszystkie lokalizacje muszą mieć takie same cele oceny.
- Wynik oceny jest dostępny dopiero, kiedy dostawca usług audytu TISAX oceni wszystkie lokalizacje. Może to być istotne, jeśli pilnie potrzebują Państwo wyniku oceny.
- Wynik oceny zależy od pomyślnego wyniku oceny wszystkich lokalizacji. Jeśli nie uda się to jednej lokalizacji, nie otrzymają Państwo pozytywnego wyniku oceny. Ten problem można

obejść następująco: a) wyłączyć lokalizację z zakresu, b) usunąć problemy, c) dodać lokalizację w późniejszym terminie z oceną rozszerzenia zakresu.

4.3.2.4. Dostosowanie zakresu

Tylko Państwo mogą udzielić odpowiedzi na pytanie, czy będzie to jeden zakres, czy też kilka zakresów. Pomoc w udzieleniu na nie odpowiedzi znajdą Państwo na poniższym schemacie.



Rysunek 5. Drzewo decyzyjne dostosowania zakresu

1. ROZPOCZĘCIE
   Wszystkie lokalizacje wymagające oceny w przyszłości
2. Etap 1: Czy potrzebuję oceny dla więcej niż jednej lokalizacji?

3. Etap 2: Czy mam dość czasu, by przygotować się do oceny we wszystkich lokalizacjach?
4. Etap 3: Czy wszystkie lokalizacje posiadają ten sam centralny ISMS (tj. obowiązki, infrastrukturę, zasady i procesy?)
5. Etap 4: Czy wszystkie lokalizacje posiadają ten sam cel oceny (tj. ochrona prototypów pojazdów lub informacji wymagających bardzo wysokiej ochrony)?
6. Zakończenie: Rejestracja zakresu oceny
   Zarejestrowany zakres oceny powinien obejmować pozostałe lokalizacje.
7. Teraz proszę oddzielić lokalizacje od siebie.
   A później zacząć ponownie z każdym zbiorem lokalizacji.
8. Nie
9. Tak

Uwaga:

Proszę się nie bać tej decyzji. Zakres można zmienić do czasu, gdy dostawca usług audytu nie zakończy oceny.

Na przykład, podczas przygotowań do oceny mogą Państwo stwierdzić, że zakres nie jest właściwy -- i odpowiednio go zmienić. Albo dostawca usług audytu może sugerować zmianę zakresu na wcześniejszych etapach oceny.

Uwagi dodatkowe:

- W sensie technicznym nie można zmienić zakresu oceny określonego na etapie procesu rejestracji online w portalu ENX. Dostawca usług audytu może jednak zaktualizować zakres oceny podczas wczytywania wyniku oceny w portalu ENX.
- Zwiększenie zakresu powoduje podwyższenie opłaty, zaś wyłączenie niektórych lokalizacji z zakresu nie przekłada się na zwrot kosztów. Ponieważ dostawcy usług audytu obliczają koszty na podstawie pierwotnego zakresu, należy się spodziewać zmian.

4.3.2.5. Lokalizacje w ramach zakresu

Po podjęciu decyzji, jakie lokalizacje wchodzą w skład zakresu oceny, można dalej zbierać informacje dotyczące poszczególnych lokalizacji.

Dla każdej lokalizacji prosimy o takie informacje, jak nazwa i adres spółki. Prosimy także o dodatkowe informacje, które pozwolą naszym dostawcom usług audytu TISAX lepiej poznać strukturę Państwa spółki. Państwa odpowiedzi staną się podstawą szacowania ich nakładu pracy.

Należy się przygotować do podania następujących danych dla każdej z lokalizacji (czerwona gwiazdka * wskazuje obowiązkowe informacje w procesie online):

Pole	**Opcje**
Nazwa lokalizacji *	nd.
NUMER D&B D-U-N-S	nd.
Rodzaj lokalizacji *	Budynek/budynki należący/-e do spółki i tylko przez nią używany/-e Budynek/budynki wynajmowany/-e przez spółkę Piętro/biuro wynajmowane przez spółkę w budynku współdzielonym Biuro współdzielone z innymi spółkami Własne centrum danych Współdzielone centrum danych
Bierna ochrona lokalizacji *	Tak Nie
Branża *(Można wybrać kilka opcji)*	Technologie informacyjne ☐ Usługi IT ☐ Usługi telekomunikacyjne ☐ Rozwój oprogramowania
	Zarządzanie ☐ Doradztwo
	Media ☐ Marketing ☐ Agencja ☐ Usługi drukarskie ☐ Fotografia ☐ Usługi tłumaczeniowe

Pole	Opcje
	Prace badawczo-rozwojowe ☐ Testy pojazdów ☐ Symulacje pojazdów ☐ Budowa prototypów ☐ Miniaturowe modele samochodów ☐ Usługi rozwojowe ☐ Usługi rozwojowe CAx
	Produkcja ☐ Usługi produkcyjne ☐ Produkcja na zlecenie ☐ Dział produkcji ☐ Logistyka
	Sprzedaż i usługi posprzedażne ☐ Import, NSC ☐ Dystrybucja ☐ Usługi finansowe ☐ Ubezpieczenia ☐ Obsługa roszczeń
	Inna branża *(proszę podać)*
Liczba pracowników lokalizacji: ogółem *	0 1–10 11–100 101–1000 1001–5000 Ponad 5000
Liczba pracowników lokalizacji: IT *	0 1–10 11–25 26–50 Ponad 50

Pole	Opcje
Liczba pracowników lokalizacji: Bezpieczeństwo IT *	0 Na część etatu 1–5 6–25 Ponad 25
Liczba pracowników lokalizacji: Bezpieczeństwo lokalizacji *	0 Na część etatu 1–3 4–10 Ponad 10
Certyfikaty danej Lokalizacji	ISO 27001 Inne *(proszę podać)* ISAE 3402 SOC2

Tabela 1. Dane dotyczące lokalizacji

Uwaga:

W odniesieniu do „Branży”: należy wybrać zgodnie z własną wiedzą. w przypadku wyboru powyższych opcji nie ma prawidłowych i błędnych odpowiedzi. Jeśli nie mogą Państwo znaleźć opcji odpowiadającej rodzajowi własnego przedsiębiorstwa, proszę po prostu zaznaczyć odpowiednią opcję w „Inne”.

Dla każdej lokalizacji należy określić „location name” („nazwę lokalizacji”). Nazwa lokalizacji ułatwia odwoływanie się do niej podczas przypisywania do zakresu oceny.

Zalecamy przydzielanie nazw lokalizacji na podstawie poniższego wzorca:

Wzorzec: [Odnośnik geograficzny]

Przykład: dla fikcyjnej spółki „ACME”

- Frankfurt
  (dla lokalizacji w niemieckim **mieście** Frankfurt)

4.3.2.6. Nazwa zakresu

Dla każdego zakresu należy określić „scope name” („nazwę zakresu”). Głównym celem nazwy zakresu jest ułatwienie Państwu identyfikacji zakresu na poglądowej liście zakresów na portalu ENX. Należy przypisać nazwę, która ułatwi życie zarówno czytelnikowi, jak i kolegom po fachu. w komunikacji zewnętrznej należy użyć Identyfikatora zakresu.

Można podać dowolną nazwę. Nie należy jednak nadawać tej samej nazwy zakresu więcej niż jednemu zakresowi.

W przypadku późniejszego odnowienia oceny TISAX należy utworzyć nowy zakres (być może identyczny z aktualnym). w związku z tym zalecamy, by do nazwy zakresu dodać rok oceny.

Zalecamy przydzielanie nazw zakresów na podstawie poniższego wzorca:

Wzorzec:	[Odnośnik geograficzny lub *funkcjonalny*] [Rok oceny]
Przykłady:	dla fikcyjnej spółki „ACME”

- 2024
  (bez odnośnika geograficznego, jeśli spółka posiada tylko jedną lokalizację)
- Frankfurt 2024
  (dla zakresu obejmującego kilka lokalizacji w niemieckim **mieście** Frankfurt)
- Dolna Saksonia 2024
  (dla zakresu obejmującego wszystkie lokalizacje w niemieckim **kraju związkowym** Dolna Saksonia)
- Niemcy 2024
  (dla zakresu obejmującego wszystkie lokalizacje w *państwie* Niemcy)
- EMEA 2024
  (dla zakresu obejmującego wszystkie lokalizacje w *regionie* EMEA („Europa, Bliski Wschód, Afryka”))
- Opracowywanie prototypów 2024
  (odnośnik *funkcjonalny* dla zakresu obejmującego wszystkie lokalizacje zajmujące się opracowywaniem prototypów)

4.3.2.7. Osoby do kontaktu

W celu komunikacji z Państwem, zbieramy dane osób do kontaktu w Państwa firmie.

Prosimy o co najmniej jedną osobę do kontaktu ogólnie dla Państwa firmy jako uczestnika TISAX oraz po jednej na każdy zakres oceny. Mogą Państwo wskazać dodatkowe osoby do kontaktu.

Podczas przygotowań do rejestracji należy zdecydować, kto będzie osobą do kontaktu w Państwa firmie.

Prosimy o następujące dane osób do kontaktu:

	Dane osób do kontaktu	Obowiązkowe?	Przykład
1.	Zwrot grzecznościowy	Tak	Pani, Pan
2.	Stopień naukowy		Dr, inny
3.	Imię	Tak	John
4.	Nazwisko	Tak	Doe
5.	Stanowisko	Tak	Szef IT
6.	Dział	Tak	Technologie informacyjne
7.	Podstawowy numer telefonu	Tak	+49 69 986692777
8.	Pomocniczy numer telefonu		
9.	Adres e-mail	Tak	john.doe@acme.com
10.	Preferowany język	Tak	angielski (domyślnie)
11.	Inne języki		niemiecki, francuski
12.	Osobisty identyfikator adresowy		HPC 1234
13.	Ulica i numer domu	Tak	Bockenheimer Landstraße 97–99
14.	Kod pocztowy	Tak	60325
15.	Miejscowość	Tak	Frankfurt
16.	Kraj związkowy/stan/województwo		
17.	Państwo	Tak	Niemcy

Tabela 2. Dane osób do kontaktu

Ważna uwaga:

Zalecamy wyznaczenie co najmniej jednego zastępcy każdej osoby do kontaktu. w przypadku czasowej niedostępności osoby do kontaktu lub zakończenia jej zatrudnienia w firmie, danymi uczestnika firmy będzie mogła zarządzać inna osoba.
Konieczność wyznaczenia nowej osoby do kontaktu (przy braku aktualnie wyznaczonych zastępców) pociąga za sobą skomplikowany proces. Nasz proces zapewnia, że jedynie osoby mogące udowodnić swoje prawo do reprezentowania spółki mogą zatwierdzić wyznaczenie nowej głównej osoby do kontaktu.

4.3.2.8. Publikacja i udostępnianie

Głównym celem TISAX jest przekazanie wyniku Państwa oceny innym uczestnikom TISAX oraz udostępnienia wyniku Państwa oceny Państwa partnerowi/partnerom.

Decyzję o publikacji i udostępnianiu Państwa wyniku oceny mogą Państwo podjąć w trakcie procesu rejestracji lub w dowolnym późniejszym terminie.

Jeśli proces TISAX jest u Państwa etapem wstępnym, mogą Państwo podjąć decyzję o publikacji wyniku własnej oceny na potrzeby społeczności uczestników TISAX. w przeciwnym razie na tym etapie nie trzeba się do niczego przygotowywać.

Jeśli proces TISAX przechodzą Państwo na żądanie partnera, wcześniej czy później będą Państwo musieli udostępnić wynik oceny. Informacje na temat statusu mogą Państwo udostępnić partnerowi już na etapie rejestracji. Kiedy wynik oceny będzie dostępny, partner automatycznie otrzyma zgodę na dostęp[6].

Aby udostępnić informacje dotyczące statusu, potrzebne są dwa elementy:

1. Identyfikator uczestnika TISAX Państwa partnera

   Identyfikator uczestnika TISAX umożliwia identyfikację Państwa partnera jako uczestnika TISAX.

   Zwykle partner powinien podać Państwu swój Identyfikator uczestnika TISAX.

   Dla ułatwienia formularz rejestracyjny zawiera rozwijaną listę Identyfikatorów uczestnika wybranych spółek, które często otrzymują udostępniane wyniki oceny.[7]

2. Wymagany poziom udostępniania

   Poziom udostępniania określa poziom dostępu partnera do wyników Państwa oceny.

   Partner może zażądać określonego poziomu udostępniania lub Państwo mogą zdecydować, na jakim poziomie chcą Państwo zapewnić partnerowi dostęp do wyniku oceny.

   Bardziej szczegółowe informacje na temat poziomu udostępniania znajdują się w Punkt 6.5, “Poziomy udostępniania”.

Warto się upewnić, czy posiadają Państwo takie informacje.

Uwaga:

- Decyzję o publikacji wyniku oceny można podjąć w późniejszym terminie.
- Zgody na udostępnianie partnerowi można udzielić w późniejszym terminie.

Ważna uwaga:

Jeśli Państwo nie opublikują wyniku oceny lub go nie udostępnią, nikt nie będzie miał do niego dostępu.

Ważna uwaga:

Nie można cofnąć zgody na publikację lub udostępnianie.

Bardziej szczegółowe informacje znajdują się w Punkt 6.4, “Trwałość wyników będących przedmiotem wymiany”.

Uwaga:

Choć może się to wydawać dziwne, „wynik oceny” można udostępnić, nawet jeśli nie zaczęli Państwo jeszcze procesu oceny. Na tym wczesnym etapie po prostu udostępniają Państwo „status oceny”. Uczestnik, któremu udostępnią Państwo „wynik oceny”, będzie mógł sprawdzić, na jakim etapie procesu oceny się Państwo znajdują.

Niektóry uczestnicy TISAX muszą wydać specjalny komunikat, jeśli muszą Państwo pokazać etykiety TISAX, choć nie ukończyli Państwo jeszcze procesu oceny. w takim przypadku Państwa partner może chcieć zobaczyć Państwa „status oceny” na swoim koncie w portalu ENX.

Bardziej szczegółowe informacje na temat statusu oceny znajdują się w Punkt 7.6, “Załącznik: Assessment status (Status oceny)”.

Bardziej szczegółowe informacje na temat publikacji i udostępniania wyniku oceny znajdują się w Punkt 6, “Wymiana (Etap 3)”.

4.3.3. Cele oceny

Cele oceny należy określić w procesie rejestracji. Cel oceny (assessment objective) określa obowiązujące wymagania, jakie musi spełnić Państwa system zarządzania bezpieczeństwem informacji (ISMS). Cel oceny całkowicie zależy od rodzaju danych, jakie przetwarzają Państwo w imieniu partnera.

W kolejnych punktach opiszemy cele oceny i podpowiemy, jak je poprawnie wybrać.

Wykorzystanie celów oceny ułatwia związaną z TISAX komunikację z partnerem oraz dostawcami usług audytu TISAX, ponieważ odnoszą się one do określonych danych wejściowych procesu oceny TISAX.

Uwaga:

Niektórzy partnerzy mogą żądać oceny TISAX na określonym „poziomie oceny” (assessment level, AL), zamiast określać cel oceny.

Bardziej szczegółowe informacje na temat poziomów oceny znajdują

> się w punkcie Punkt 4.3.3.5, “Potrzeby ochrony i poziomy oceny” (podpunkt „Informacje dodatkowe”).

4.3.3.1. Lista celów oceny

Obecnie istnieje dwanaście celów oceny TISAX. Trzeba wybrać co najmniej jeden z nich. Można wybrać więcej niż jeden.

Cel oceny należy uznać za wzorzec porównawczy systemu zarządzania bezpieczeństwem informacji. Cel oceny stanowi kluczowe dane wejściowe procesu TISAX. Wszyscy dostawcy usług audytu TISAX opierają strategię oceny przede wszystkim na celu oceny.

Aktualne cele oceny TISAX są następujące:

Lp.	Nazwa	Opis
1.	Info high	Handling of information with high protection needs Postępowanie z informacjami wymagającymi wysokiej ochrony
2.	Info very high	Handling of information with very high protection needs Postępowanie z informacjami wymagającymi bardzo wysokiej ochrony
3.	Confidential	Handling of information with high protection needs in the context of confidentiality (access to confidential information) Postępowanie z informacjami wymagającymi wysokiej ochrony w kontekście poufności (dostęp do informacji poufnych)
4.	Strictly confidential	Handling of information with very high protection needs in the context of confidentiality (access to strictly confidential information) Postępowanie z informacjami wymagającymi bardzo wysokiej ochrony w kontekście poufności (dostęp do informacji ściśle poufnych)
5.	High availability	Handling of information with high protection needs in the context of *availability* (high availability of information) Postępowanie z informacjami wymagającymi wysokiej ochrony w kontekście *dostępności* (wysoka dostępność informacji)

Lp.	Nazwa	Opis
6.	Very high availability	Handling of information with very high protection needs in the context of *availability* (very high availability of information) Postępowanie z informacjami wymagającymi bardzo wysokiej ochrony w kontekście *dostępności* (bardzo wysoka dostępność informacji)
7.	Proto parts	Protection of Prototype Parts and Components Ochrona prototypów części i komponentów
8.	Proto vehicles	Protection of Prototype Vehicles Ochrona prototypów pojazdów
9.	Test vehicles	Handling of Test Vehicles Postępowanie z pojazdami testowymi
10.	Proto events	Protection of Prototypes during Events and Film or Photo Shoots Ochrona prototypów podczas wydarzeń, kręcenia filmów lub fotografowania
11.	Data	Data protection according to Article 28 („Processor”) of the European General Data Protection Regulation (GDPR) Ochrona danych zgodnie z art. 28 („Podmiot przetwarzający”) europejskiego Ogólnego rozporządzenia o ochronie danych (RODO)
12.	Special data	Data protection according to Article 28 („Processor”) of the European General Data Protection Regulation (GDPR) with special categories of personal data as specified in Article 9 of the GDPR Ochrona danych zgodnie z art. 28 („Podmiot przetwarzający”) europejskiego Ogólnego rozporządzenia o ochronie danych (RODO) dla szczególnych kategorii danych osobowych, jak określono w art. 9 RODO

Tabela 3. Aktualne cele oceny TISAX

Na przykład: jeśli prowadzą Państwo jazdy próbne na drogach publicznych, do Państwa celów oceny należy cel oceny „Test vehicles”.

Uwaga:

Cele oceny „Info high” i „Info very high” można wybrać jedynie do 31 marca

2024 r.

Cele oceny „Confidential” i „Strictly confidential” można wybrać od 1 kwietnia 2024 r.

Bardziej szczegółowe informacje na temat tej zmiany znajdują się w następującym artykule na naszej stronie internetowej: CHANGES TO TISAX LABELS ACCOMPANYING ISA 6 RELEASE enx.com/en-US/news/Changes-to-TISAX-Labels-ISA-six-Release/

Ważna uwaga:

Danymi wejściowymi procesu TISAX jest zasadniczo „cel oceny”. Niektórzy partnerzy mogą żądać oceny TISAX na określonym „poziomie oceny” (AL).

Bardziej szczegółowe informacje na temat stosunku między potrzebą ochrony a poziomami oceny znajdują się w Punkt 4.3.3.5, “Potrzeby ochrony i poziomy oceny”.

4.3.3.2. Cele oceny i ISA

ISA zawiera trzy katalogi kryteriów (bezpieczeństwo informacji, ochrona prototypów, ochrona danych). Każdy katalog kryteriów składa się z tzw. „pytań kontrolnych” i powiązanych wymogów.

Każdy cel oceny określa:

- odpowiedni/-e katalog/-i kryteriów ISA
- pytania kontrolne, na które muszą Państwo udzielić odpowiedzi
- wymogi, które muszą Państwo spełnić

W przypadku niektórych celów oceny obowiązuje jedynie podzbiór pytań kontrolnych i wymagań.

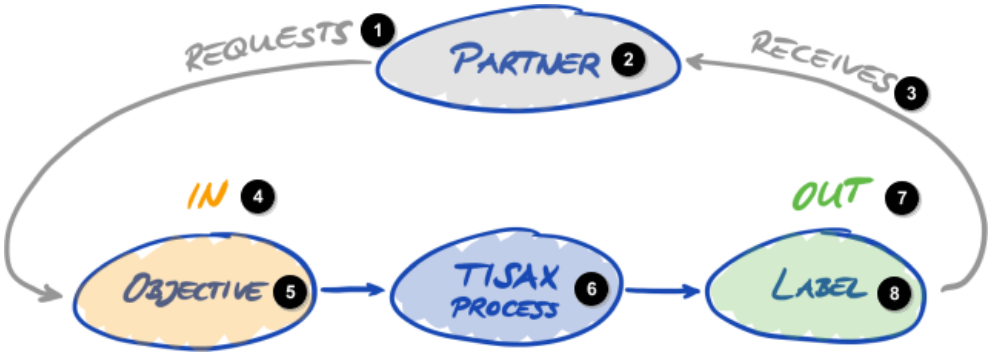
Bardziej szczegółowe informacje kontekstowe na temat celów oceny TISAX oraz odpowiednich pytań kontrolnych i wymagań znajdują się w Punkt 5.2.2, “Rozumienie dokumentu ISA”.

4.3.3.3. Cele oceny i etykiety TISAX

Partner może wspomnieć o „etykietach TISAX”. „Cele oceny” i „etykiety TISAX” są niemal tym samym. Różnica polega na tym, że proces oceny zaczyna się od „celów oceny”, a w przypadku pomyślnego wyniku oceny otrzymuje się odpowiednie „etykiety TISAX”.

Przykład: partner żąda od Państwa uzyskania etykiety TISAX „Info high”. w tej sytuacji wybierają Państwo cel oceny „Info high”.

Poniższa ilustracja przedstawia dane wejściowe i wyjściowe procesu TISAX:



Rysunek 6. Cele oceny i etykiety TISAX

1. Żąda
2. Partner
3. Otrzymuje
4. DANE WEJ.
5. Cel
6. Proces TISAX
7. DANE WYJ.
8. Etykieta

Bardziej szczegółowe informacje na temat etykiet TISAX znajdują się w Punkt 5.4.14, “Etykiety TISAX”.

4.3.3.4. Wybór celu oceny

W optymalnym przypadku partner dokładnie wskazuje cele oceny, które mają Państwo osiągnąć.

Cele oceny należy określić wedle własnego uznania w następujących przypadkach:

a. pragną Państwo uzyskać ocenę TISAX, zanim partner o to poprosi, lub
b. partner nie informuje, który cel oceny należy osiągnąć.

Ważna uwaga:

Na tym etapie zachęcamy do uwzględnienia pozostałych partnerów. Czy posiadają Państwo obecnie partnerów o takich samych lub wyższych wymaganiach? Czy przewidują Państwo, że w przyszłości partnerzy będą mieli wyższe wymagania?

> Być może warto rozważyć wybór celów oceny o wyższych potrzebach ochrony. Pozwoli to zapobiec problemom w przypadku wyższych wymagań innych partnerów.

Jeśli muszą Państwo wybrać cel oceny wedle własnego uznania, być może warto uwzględnić następujące aspekty:

Lp.	Cel oceny	Informacje
1.	Info high	Potrzeby dotyczące ochrony (wysoka, bardzo wysoka) można uzyskać z klasyfikacji dokumentu partnera.
2.	Info very high	
3.	Confidential	Dla wszystkich spółek otrzymujących i przetwarzających informacje o wysokiej potrzebie ochrony w kontekście poufności lub klasyfikowane zwykle jako poufne zgodnie ze schematem klasyfikacji przyjętym przez spółkę (np. Biała księga VDA „Harmonizacja poziomów klasyfikacji”). Tę etykietę TISAX należy wybrać szczególnie w przypadku, gdy ujawnienie informacji osobom nieuprawnionym mogłoby spowodować znaczne szkody (np. szkody dla reputacji, skutki karne lub szkody finansowe).
4.	Strictly confidential	Dla wszystkich spółek otrzymujących i przetwarzających informacje o bardzo wysokiej potrzebie ochrony w kontekście poufności lub klasyfikowane zwykle jako ściśle poufne lub tajne zgodnie ze schematem klasyfikacji przyjętym przez spółkę (np. Biała księga VDA „Harmonizacja poziomów klasyfikacji”). Tę etykietę TISAX należy wybrać szczególnie w przypadku, gdy ujawnienie informacji osobom nieuprawnionym mogłoby spowodować szkody zagrażające lub katastrofalne (np. poważne szkody dla reputacji, poważne skutki karne lub bardzo wysokie szkody finansowe).

Lp.	Cel oceny	Informacje
5.	High availability	W przypadku wszystkich spółek, dla których zdolność klientów do produkcji lub realizacji zależy od dostępności produktów lub usług spółki i gdzie brak realizacji obowiązków spowodowałby znaczące szkody dla klientów w krótkim czasie. Przykład: dostawcy surowców produkcyjnych działający w trybie „just-in-time”
6.	Very high availability	W przypadku wszystkich spółek, dla których zdolność klientów do produkcji i realizacji zależy od krótkoterminowej dostępności produktów i usług spółki i gdzie brak realizacji obowiązków spowodowałby znacząco wysokie szkody dla klientów w bardzo krótkim czasie. Przykład: dostawcy działający w trybie „just-in-time”, gdzie brak realizacji obowiązków mógłby w krótkim czasie prowadzić do kompleksowego przestoju produkcji o bardzo długim czasie ponownego uruchomienia.
7.	Proto parts	W przypadku spółek produkujących, przechowujących lub wykorzystujących dostarczone przez klienta komponenty lub części klasyfikowane jako wymagające ochrony we własnych lokalizacjach. Ocena obejmuje wymogi dotyczące ochrony fizycznej i ochrony z uwzględnieniem otoczenia, wymogów organizacyjnych i konkretnych wymogów postępowania z prototypami.

Lp.	Cel oceny	Informacje
8.	Proto vehicles	W przypadku spółek produkujących, przechowujących lub wykorzystujących dostarczone przez klienta pojazdy klasyfikowane jako wymagające ochrony we własnych lokalizacjach. Ocena obejmuje wymogi dotyczące ochrony fizycznej i ochrony z uwzględnieniem otoczenia (w tym istnienia chronionych garaży i warsztatów), wymogów organizacyjnych i konkretnych wymogów postępowania z prototypami. Po uzyskaniu pomyślnego wyniku oceny automatycznie otrzymują Państwo etykietę TISAX „Ochrona prototypów części i komponentów”.
9.	Test vehicles	Dla wszystkich spółek prowadzących testy i jazdy próbne (np. jazdy próbne na drogach publicznych lub torach testowych) dostarczonymi przez klienta samochodami klasyfikowanymi jako wymagające ochrony. Ocena obejmuje wymogi organizacyjne, szczegółowe wymogi dotyczące postępowania z prototypami, w tym kamuflaż, oraz postępowania z pojazdami podczas jazd próbnych po drogach publicznych lub torach testowych. W skład oceny nie muszą wchodzić wymogi dotyczące ochrony fizycznej i ochrony z uwzględnieniem otoczenia. w przypadku odpowiedniego wyposażenia lokalizacji zalecamy także wybór celu „Ochrona prototypów pojazdów”.

Lp.	Cel oceny	Informacje
10.	Proto events	Dla wszystkich spółek prowadzących prezentacje lub wydarzenia (np. badania rynkowe, wydarzenia, wydarzenia marketingowe) oraz uczestniczących w kręceniu filmów lub robieniu zdjęć przy użyciu dostarczonych przez klienta samochodów klasyfikowanych jako wymagające ochrony. Ocena obejmuje wymogi organizacyjne i szczegółowe wymogi dotyczące postępowania z prototypami, w tym wymogi dotyczące prezentacji, wydarzeń, kręcenia filmów i robienia zdjęć w pomieszczeniach chronionych i miejscach publicznych. W skład oceny nie muszą wchodzić wymogi dotyczące ochrony fizycznej i ochrony z uwzględnieniem otoczenia. w przypadku odpowiedniego wyposażenia lokalizacji zalecamy także wybór celu „Ochrona prototypów pojazdów”.
11.	Data	Jeśli przetwarzają Państwo dane osobowe jako podmiot przetwarzający zgodnie z art. 28 RODO, prawdopodobnie muszą Państwo zaznaczyć „Data”.
12.	Special data	Jeśli przetwarzają Państwo szczególne kategorie danych osobowych (np. dotyczące stanu zdrowia lub wyznania) jako podmiot przetwarzający zgodnie z art. 28 RODO, prawdopodobnie muszą Państwo zaznaczyć „Special data”.

Tabela 4. Porady dotyczące wyboru celu oceny

Dalsze wyjaśnienia:

- Jeśli partner przekazał Państwu szczegółowe wymagania, zwykle nie trzeba z nim omawiać celów oceny. Jeśli partner nie przekazał Państwu szczegółowych wymagań, gorąco zachęcamy do konsultacji z nim przed rozpoczęciem procesu oceny.
- ISA opisuje (ewentualne) różnice wdrożenia dla „wysokich” i „bardzo wysokich” potrzeb ochrony dla poszczególnych wymogów.
  Bardziej szczegółowe informacje na ten temat znajdują się w Rysunek 11, “Zrzut ekranu: Główne elementy pytań w katalogu kryteriów ISA „Bezpieczeństwo informacji””.

4.3.3.5. Potrzeby ochrony i poziomy oceny

Państwa partner posiada różne rodzaje informacji, z których niektóre mogą wymagać wyższego

poziomu ochrony od innych. ISA uwzględnia ten fakt, rozróżniając trzy „potrzeby ochrony” (🇬🇧 „protection needs”): standardową, wysoką i bardzo wysoką. Państwa partner klasyfikuje własne informacje i zwykle przypisuje potrzeby ochrony.

Im wyższe potrzeby ochrony, tym bardziej Państwa partner jest zainteresowany zapewnieniem bezpieczeństwa przetwarzania jego informacji przez Państwa. Dlatego też TISAX rozróżnia trzy „poziomy oceny” (AL). Poziom oceny określi, jaką metodę oceny musi zastosować dostawca usług audytu. Wyższy poziom oceny wymaga większego wysiłku podczas oceny. To skutkuje wyższą starannością i rzetelnością oceny.

Poniższa tabela przedstawia poziomy oceny dotyczące celów oceny TISAX:

Lp.	Cel oceny TISAX	Poziom oceny (AL)
1.	Info high	AL 2
2.	Info very high	AL 3
3.	Confidential	AL 2
4.	Strictly confidential	AL 3
5.	High availability	AL 2
6.	Very high availability	AL 3
7.	Proto parts	AL 3
8.	Proto vehicles	AL 3
9.	Test vehicles	AL 3
10.	Proto events	AL 3
11.	Data	AL 2
12.	Special data	AL 3

Tabela 5. Przełożenie celów oceny TISAX na poziomy oceny

Poziom oceny 1 (AL 1):

Oceny na poziomie oceny 1 służą głównie do celów wewnątrzfirmowych w rozumieniu samooceny (🇬🇧 self-assessment).

W trakcie oceny na poziomie oceny 1, audytor sprawdza istnienie wypełnionej samooceny. Nie ocenia treści samooceny. Nie wymaga dalszych dowodów.

Wyniki oceny na poziomie oceny 1 mają niski poziom zaufania, a tym samym nie wykorzystuje się ich w ramach TISAX. Może się jednak zdarzyć, że partner zażąda takiej samooceny poza TISAX.

Poziom oceny 2 (AL 2):

W trakcie oceny na poziomie oceny 2, dostawca usług audytu sprawdza wiarygodność przeprowadzonej przez Państwa samooceny (dla wszystkich lokalizacji w zakresie oceny). Wsparciem tego procesu jest sprawdzenie dowodów[8] i rozmowa z osobą odpowiedzialną za bezpieczeństwo informacji.

Dostawca usług audytu zwykle prowadzi taką rozmowę w formie konferencji przez Internet. Na Państwa żądanie może ją przeprowadzić osobiście.

Jeżeli nie chcą Państwo przekazywać dostawcy usług audytu wszystkich dowodów, mogą Państwo wystąpić o kontrolę na miejscu. Dzięki temu dostawca usług audytu może sprawdzić Państwa dowody przeznaczone wyłącznie dla Państwa oczu.

Uwaga:

Ocenę na poziomie oceny 2 można przeprowadzić odmienną metodą. Zamiast kontroli wiarygodności dostawca usług audytu prowadzi pełną ocenę zdalną. Tę metodę określa się czasem „**poziomem oceny 2,5**”.

W porównaniu do oceny na poziomie oceny 2, audytor *weryfikuje*, czy Państwa ISMS spełnia obowiązujące wymogi. w przeciwieństwie jednak do oceny na poziomie oceny 3, audytor nie prowadzi działań na miejscu określonych w kolejnym punkcie dotyczącym poziomu oceny 3.

Formalnie taka ocena zostanie uznana za ocenę AL 2.

Zaletą AL 2,5 jest zgodność metodologiczna tego podejścia z AL 3. Dzięki temu w późniejszym terminie przy niewielkim wysiłku można zaktualizować do pełnoprawnej oceny AL 3. w celu aktualizacji audytor musi jedynie przeprowadzić działania na miejscu określone poniżej w punkcie dotyczącym AL 3.

Ocenę na poziomie oceny 2,5 zalecamy w następujących przypadkach:

1. Aktualnie potrzebują Państwo jedynie etykiet TISAX implikujących ocenę AL 2, ale nie mogą Państwo wykluczyć możliwości, że inni partnerzy będą wymagać etykiet TISAX implikujących ocenę AL 3. Ocena AL 2,5 umożliwia późniejszą aktualizację do AL 3.
2. Mają Państwo trudności z opracowaniem odpowiednio wiarygodnej samooceny. Na potrzeby wiarygodności samoocena musi być rozstrzygająca, zrozumiała i uzasadniona. Opracowanie takiej samooceny może wymagać znacznych wysiłków wewnątrzfirmowych, nawet dla spółek posiadających zasadniczo dobrą pozycję.

Bardziej szczegółowe informacje na temat podwyższenia poziomu oceny znajdują się w Punkt 7.10, “Załącznik: Ocena rozszerzenia zakresu”.

Ta alternatywa jest opcjonalna i niewymagana do spełnienia wymogów AL 2. Różnica między AL 2 a AL 2,5 nie będzie widoczna dla partnerów, którym udostępnią Państwo wynik oceny.

Poziom oceny 3 (AL 3):

W trakcie oceny na poziomie oceny 3, dostawca usług audytu prowadzi kompleksową weryfikację zgodności Państwa firmy z obowiązującymi wymogami. Audytor opracowuje ocenę na podstawie Państwa samooceny i przekazanych dokumentów. w przeciwieństwie jednak do poziomu oceny 2, audytor weryfikuje wszystkie dane. Audytor:

- bada dokumenty i dowody,
- prowadzi zaplanowane rozmowy z właścicielami procesów,
- obserwuje warunki lokalne,
- obserwuje realizację procesów,
- prowadzi *nie*planowane rozmowy z uczestnikami procesów.

Uwaga:

Poniższy tekst odnosi się do kilku koncepcji wyjaśnionych w dalszej części niniejszego dokumentu.

W przypadku AL 3, dostawca usług audytu musi odwiedzić Państwa lokalizację. Jeżeli z takich czy innych przyczyn jest to czasowo niemożliwe lub wymagałoby nieuzasadnionego wysiłku, dostawca usług audytu może przeprowadzić czynności oceny na miejscu **metodą oceny zdalnej przy wsparciu wideo**.

Dostawca usług audytu musi to ująć w raporcie z oceny TISAX jako drobną niezgodność. Kiedy tylko dostawca usług audytu będzie mógł się stawić w Państwa lokalizacji/lokalizacjach, musi przeprowadzić ocenę kontrolną obejmującą wszystkie niemożliwe wcześniej czynności na miejscu. Co więcej, ocenę kontrolną należy zaplanować, nawet jeżeli nie zakończyli Państwo jeszcze pozostałych działań kontrolnych.

W porównaniu z oczekiwaniem na dostępność dostawcy usług audytu na potrzeby czynności na miejscu, to podejście pozwala udostępnić partnerowi tymczasowe etykiety TISAX.

Poziomy oceny i metody oceny

Poniższa tabela zawiera uproszczony przegląd metod audytu związanych z poszczególnymi poziomami oceny:

Metoda oceny	Poziom oceny 1 (AL 1)	Poziom oceny 2 (AL 2)	Poziom oceny 3 (AL 3)
Samoocena	Tak	Tak	Tak
Dowody	Nie	Kontrola wiarygodności	Dokładna weryfikacja
Rozmowy	Nie	W formie konferencji internetowej[9]	Osobiście, na miejscu
Kontrola na miejscu	Nie	Na Państwa żądanie	Tak

Tabela 6. Stosowanie metod oceny do różnych poziomów oceny

Informacje dodatkowe:

- Różnice między AL 2 a AL 3
  Te dwa podejścia wykazują znaczne różnice metodologiczne. W przypadku ocen na poziomie oceny 2 audytor nic weryfikuje wszystkiego. Sprawdza jedynie wiarygodność. w związku z tym dostawca usług audytu nie może wykorzystać wyników oceny na poziomie oceny 2 w charakterze podstawy do aktualizacji do poziomu oceny 3. Aktualizacja do poziomu oceny 3 wymaga zasadniczo tyle samo wysiłku, co nowa ocena początkowa.
- Kontrola wiarygodności a weryfikacja
  W dużym uproszczeniu kontrola wiarygodności oznacza sprawdzenie, czy coś istnieje i czy właściwie *wygląda*. Natomiast weryfikacja oznacza faktyczną kontrolę, czy coś jest takie, za jakie się podaje.
- Klasyfikacja informacji i potrzeby ochrony
  U różnych partnerów mogą występować różne powiązania między klasyfikacją informacji (np. poufnych lub tajnych) a potrzebami ochrony. w związku z tym, pomimo najlepszych chęci, nie możemy przedstawić Państwu prostej tabeli przypisującej stosowaną przez Państwa partnera klasyfikację informacji określonym potrzebom ochrony.
- Nie wystarczy znać poziomu oceny
  Niektórzy partnerzy mogą żądać oceny TISAX na określonym poziomie oceny. Trzeba pamiętać, że sama znajomość poziomu oceny nie wystarczy do rozpoczęcia procesu TISAX. Poziom oceny ma sens jedynie w połączeniu z katalogiem kryteriów ISA i odpowiednią potrzebą ochrony. Partnerzy zwykle żądają uzyskania etykiety TISAX (katalog kryteriów plus potrzeba ochrony). Ponieważ jednak potrzeby ochrony przekładają się na poziomy

oceny 1:1, wystarczy znać katalog/katalogi kryteriów oraz poziom oceny.

- Hierarchia poziomów oceny
  Wyższe poziomy oceny zawsze obejmują niższe poziomy oceny. Na przykład, jeśli Państwa ocena opiera się na poziomie oceny 3, automatycznie spełnia wszystkie wymogi dla poziomu oceny 2.
- Nasze zalecenie dotyczące poziomów oceny
  Jeśli muszą Państwo wybrać cel oceny (a tym samym, w sposób dorozumiany, odpowiedni poziom oceny) wedle własnego uznania, zalecamy wybór celów oceny implikujących poziom oceny 3. Oceny TISAX na poziomie oceny 3 zasadniczo nie wymagają więcej wysiłku niż na poziomie oceny 2.
  Dostawcy posiadający kilku partnerów często wybierają cele oceny implikujące poziom oceny 3. Dzięki temu są przygotowani na wszystkie przyszłe żądania i nie muszą się martwić różnymi poziomami oceny.
- Dalsze względy komercyjne
  W odniesieniu do poziomów oceny, całkowity koszt oceny TISAX obejmuje sumę Państwa wysiłków wewnątrzfirmowych oraz koszt oceny. Nawet jeśli ocena na poziomie oceny 2 może być tańsza, może się wiązać z większym wysiłkiem wewnątrzfirmowym. Wynika to z faktu, że ocena na poziomie oceny 2 zwykle wymaga bardziej kompleksowej samooceny i lepszej dokumentacji wewnętrznej. w przypadku ocen na poziomie oceny 3 wykazanie sposobu działania i udostępnienie podstawowej dokumentacji często stanowi dla audytora wystarczające dowody. Bez kontroli na miejscu, audytor żąda jednak dokładnej dokumentacji. w związku z tym, nierzadko wybiera się poziom oceny 3 zamiast poziomu oceny 2. Taką decyzję podejmują jednak zwykle mniejsze firmy.

4.3.3.6. Cele oceny a Państwa dostawcy

TISAX nie musi wymagać od Państwa nałożenia jednakowych wymogów na wszystkich swoich dostawców. Cel oceny „Bezpieczeństwo informacji o *bardzo* wysokich potrzebach ochrony" NIE oznacza automatycznie, że Państwa dostawcy muszą zrealizować ten sam cel oceny. Nie oznacza nawet, że w ogóle muszą posiadać etykiety TISAX.

Mimo to jednak trzeba sprawdzić, czy korzystanie z usług poszczególnych dostawców zwiększa ryzyko lub wprowadza nowe.

Oto dwa mocno uproszczone przykłady:

1. Zgodnie z polityką Państwa firmy, danych o bardzo wysokich potrzebach ochrony nie można przesyłać w zwykłej wiadomości e-mail. w związku z tym dostawca Państwa serwisu poczty elektronicznej nie musi uzyskać etykiety TISAX o bardzo wysokich potrzebach ochrony.
   Do podobnego wniosku można dojść, jeśli wysyłają Państwo jedynie szyfrowane wiadomości e-mail, a dostawca serwisu poczty elektronicznej nie widzi żadnych danych o bardzo wysokich potrzebach ochrony.

2. Wydruki danych o bardzo wysokich potrzebach ochrony utylizują Państwo w niszczarce. w takim przypadku dostawca usług utylizacji odpadów nie musi spełniać takich samych wymogów, jak Państwo.

Jednakże z oceny ryzyka może wynikać, że Państwa dostawca również musi spełnić wymogi dotyczące bardzo wysokich potrzeb ochrony. w takim przypadku etykiety TISAX stanowią opcję odpowiedniego udowodnienia Państwu tego faktu.

4.3.4. Opłata

Pobieramy opłatę. Nasz cennik informuje Państwa o obowiązujących opłatach, możliwych rabatach i naszych warunkach płatności.

Cennik można pobrać z naszej strony internetowej pod adresem:
enx.com/en-US/TISAX/downloads/
PDF do pobrania:
enx.com/pricelist.pdf

W trakcie przygotowań do rejestracji trzeba uwzględnić pewne aspekty związane z fakturami:

- Wybór adresu do faktury
  Domyślnie wyślemy fakturę na adres podany przez Państwa jako własną lokalizację uczestnika. Mogą Państwo jednak podać inny adres na potrzeby doręczenia faktury.

Ważna uwaga:

Proszę sprawdzić poprawność adresu do faktury. Zgodnie z przepisami o rachunkowości adres na fakturze musi dokładnie odpowiadać adresowi Państwa firmy (do faktury). z przyczyn związanych z zapewnieniem zgodności, po wystawieniu faktury nie możemy zmienić adresu do faktury.

- Numer ref. zlecenia
  Jeśli na wystawionej przez nas fakturze potrzebują Państwo konkretnego numeru zlecenia lub podobnego, mogą Państwo podać nam numer ref. zlecenia.
- Numer płatnika VAT
  Jeżeli dotyczy, wszystkie pobierane przez nas opłaty podlegają opodatkowaniu niemieckim podatkiem od wartości dodanej (VAT).
  Ten numer jest nam potrzebny do przetwarzania płatności z UE. Numer płatnika VAT jest obowiązkowy w przypadku, gdy Państwa adres do faktury znajduje
  się w jednym z poniższych państw:
  Austria, Belgia, Bułgaria, Chorwacja, Cypr (część grecka), Czechy, Dania, Estonia, Finlandia, Francja, Niemcy, Grecja, Węgry, Irlandia, Włochy, Łotwa, Litwa, Luksemburg, Malta, Holandia, Polska, Portugalia, Słowacja, Słowenia, Hiszpania, Szwecja, Wielka Brytania
- Zarządzanie dostawcami

Ważna uwaga:

Przypominamy, że ze względu na wzajemne relacje wszystkich uczestników TISAX, nie możemy akceptować jakichkolwiek dodatkowych warunków (jak ogólne warunki zakupu, kodeksy postępowania).

Dodatkowe informacje na temat procesu fakturowania:

- Nie akceptujemy indywidualnych warunków zakupu.
- Akceptujemy:
  - Przelewy środków na rachunek bankowy podany na fakturze,
  - Płatności kartą kredytową (w procesie rejestracji za pośrednictwem naszego dostawcy usług płatniczych „Stripe”)
- Wystawiona przez nas faktura będzie zawierać następujące odnośniki do Państwa rejestracji:
  - Imię i nazwisko oraz adres e-mail głównej osoby do kontaktu ze strony uczestnika
  - Nazwa zakresu oceny

  Przykładową fakturę znajdą Państwo w załączniku Punkt 7.1, “Załącznik: Przykładowa faktura”.
- Większość informacji wymaganych zwykle przez Państwa w celu przetwarzania wystawionej przez nas faktury podajemy bezpośrednio na fakturze. Te i inne informacje są dostępne w dokumencie „Informacje dla członków i partnerów biznesowych”. Prosimy o przesłanie nam wiadomości e-mail, a my przekażemy aktualną wersję tego dokumentu.

Uwaga:

Mamy świadomość, że proces zatwierdzenia płatności wewnętrznych w spółce bywa długotrwały. Dlatego też Państwa kolejny etap w ramach procesu TISAX nie zależy od otrzymania przez nas płatności. Przypominamy jednak, że jeśli nie otrzymamy płatności, nie będziemy mogli udostępnić wyniku Państwa oceny.
Dlatego sugerujemy, by dopilnowali Państwo, abyśmy wysłali fakturę do odpowiedniego adresata i by zawierała ona, w razie potrzeby, numer referencyjny zlecenia. Być może sprawdzą Państwo także wewnętrznie, czy zapłacono fakturę.

Ważna uwaga:

My — ENX Association — wystawiamy fakturę na opłatę. Jest to jedynie część

całkowitego kosztu oceny TISAX. Fakturę na koszt oceny/ocen wystawia dostawca usług audytu TISAX.

Bardziej szczegółowe informacje na temat kosztów związanych z dostawcą usług audytu mogą Państwo znaleźć w Punkt 5.3.4, “Ocena ofert”.

Ważna uwaga:

Opłata jest należna niezależnie od tego, czy Państwo:

- będą kontynuować proces TISAX, czy też nie.
- pomyślnie przejdą proces oceny TISAX.

W związku z tym doręczenie faktury może nastąpić, zanim rozpoczną Państwo ocenę wstępną.

4.4. Portal ENX

Następny punkt zawiera opis procesu rejestracji online, podczas którego wprowadzają Państwo dane zebrane zgodnie z wytycznymi w poprzednim punkcie. Przed rozpoczęciem procesu rejestracji online pokrótce wyjaśnimy cel i zalety portalu ENX.

Portal ENX pozwala nam prowadzić bazę danych wszystkich uczestników TISAX i odgrywa ważną rolę w całym procesie TISAX. Podczas rejestracji TISAX wprowadzają Państwo dane, których dostawcy usług audytu TISAX będą mogli użyć (za Państwa zgodą) do obliczenia oferty i zaplanowania procedur oceny. Po przejściu procesu oceny TISAX za pomocą platformy wymiany na portalu ENX udostępnią Państwo wynik Państwa oceny swojemu partnerowi.

Portal nazywa się „Portal ENX”, nie zaś „Portal TISAX”, ponieważ używamy go także do zarządzania innymi działaniami biznesowymi (np. siecią ENX).

4.5. Proces rejestracji online

Jeśli podczas przygotowań skorzystali Państwo z powyższych porad (Punkt 4.3, “Przygotowanie do rejestracji”), są Państwo gotowi rozpocząć proces rejestracji online.

4.5.1. Wymagany czas

Długość tego procesu w znacznej mierze zależy od liczby rejestrowanych zakresów i lokalizacji. Pierwsza rejestracja uczestnika posiadającego jeden zakres o jednej lokalizacji potrwa co najmniej 20 minut.

Zalecamy ukończenie rejestracji w trakcie jednej sesji, ponieważ aktualnie nie można bez trudu wrócić do niej kilka etapów dalej. Jeśli mimo to potrzebują Państwo przerwy, skontaktujemy

się z Państwem w celu uzupełnienia brakujących danych.

4.5.2. Miejsce rozpoczęcia

Rejestrację należy rozpocząć na naszej stronie internetowej pod adresem:
enx.com/en-us/Account/Login/Register?returnUrl=%2FTISAX%2Ftisax-initial-registration%2F

Zasadniczo należy po prostu postępować zgodnie z instrukcjami wyświetlonymi na ekranie. Mimo to jednak poniżej przedstawimy krótki opis procesu.

4.5.3. Konto na portalu

Pierwszy etap to utworzenie własnego konta na portalu ENX. Konto na portalu pozwoli zarządzać „danymi uczestnika” Państwa spółki.

Uwaga:

Prosimy o kontakt, jeśli portal ENX zgłosi, że już wykorzystano Państwa adres e-mail. Ten komunikat może wskazywać, że z takich czy innych przyczyn znajdują się już Państwo w naszym systemie.

Uwaga:

Jak już wspomniano, konta na portalu nie muszą być „osobami do kontaktu ze strony uczestnika” ani „osobami do kontaktu w odniesieniu do zakresu” (patrz niżej), czynnie uczestniczącymi w procesie oceny.

I na odwrót, „osoba do kontaktu ze strony uczestnika” lub „osoba do kontaktu w odniesieniu do zakresu” nie obejmuje automatycznie takich samych praw do zarządzania danymi uczestnika, jak konto na portalu. Oznacza to, że pracownicy nazywani „osobą do kontaktu ze strony uczestnika” lub „osobą do kontaktu w odniesieniu do zakresu” nie mogą automatycznie uzyskać dostępu do danych uczestnika na portalu ENX.

Jeśli pragną Państwo przypisać prawo do zarządzania danymi uczestnika osobie do kontaktu utworzonej na portalu ENX (niezależnie od ewentualnej przypisanej jej roli), taką osobę do kontaktu należy zaprosić. Bardziej szczegółowe informacje na ten temat znajdują się w ostatniej uwadze w Punkt 4.5.5, “Osoba do kontaktu ze strony uczestnika”.

4.5.4. Rejestracja uczestnika

Drugi etap to rejestracja spółki jako uczestnika TISAX. „Uczestnik TISAX” to spółka, która wymienia wyniki oceny z innymi uczestnikami.

4.5.5. Osoba do kontaktu ze strony uczestnika

Jest to osoba odpowiedzialna za wszystkie tematy w ramach oceny bezpieczeństwa informacji w spółce. Mogą to być Państwo lub inny pracownik spółki.

Zwykle potrzebujemy jedynie głównej osoby do kontaktu ze strony uczestnika. Jeżeli pragną Państwo, abyśmy całą korespondencję własną i dostawców usług audytu TISAX w odniesieniu do tej rejestracji kierowali także do innych osób, proszę dodać kolejne osoby do kontaktu ze strony uczestnika.

Ważna uwaga:

Zalecamy wyznaczenie co najmniej jednego zastępcy każdej osoby do kontaktu. w przypadku czasowej niedostępności osoby do kontaktu lub zakończenia jej zatrudnienia w firmie, danymi uczestnika firmy będzie mogła zarządzać inna osoba.
Konieczność wyznaczenia nowej osoby do kontaktu (przy braku aktualnie wyznaczonych zastępców) pociąga za sobą skomplikowany proces. Nasz proces zapewnia, że jedynie osoby mogące udowodnić swoje prawo do reprezentowania spółki mogą zatwierdzić wyznaczenie nowej głównej osoby do kontaktu.

Uwaga:

Osoby do kontaktu mogą Państwo dodać lub usunąć w późniejszym terminie (również po zakończeniu procesu rejestracji online, a nawet ocen).

Uwaga:

W odniesieniu do osób do kontaktu ze strony uczestnika można użyć adresów e-mail grupy (np. „info@acme.com” lub „IT@acme.com”).

Jest to zgodne z wymogami ISA dotyczącymi logowania użytkowników.

Uwaga:

Mogą Państwo zdecydować, czy każda osoba do kontaktu ma mieć dostęp do danych uczestnika Państwa spółki. Mogą Państwo:

1. Po prostu dodać osobę do kontaktu. Osoba do kontaktu zostanie zapisana w naszym systemie, lecz nie może się logować ani zarządzać danymi.
2. Lub zaprosić osobę do kontaktu. w takim przypadku portal ENX wyśle do takiej osoby do kontaktu wiadomość e-mail z zaproszeniem. Osoba do

kontaktu musi kliknąć zawarty w tej wiadomości link z zaproszeniem. Po utworzeniu osobistego konta na portalu ENX osoba do kontaktu będzie mogła zarządzać danymi uczestnika spółki.

Aby utworzyć nową osobę do kontaktu: Zarejestruj się w > MY TISAX (MÓJ TISAX) > ADMINISTRATORS (ADMINISTRATORZY) > Create new TISAX Administrator (Utwórz nowego administratora TISAX)

Aby zaprosić osobę do kontaktu: Zarejestruj się w > MY TISAX > (MÓJ TISAX) > ADMINISTRATORS (ADMINISTRATORZY) > Przejdź na koniec wiersza tabeli dotyczącego osoby do kontaktu i kliknij przycisk strzałki w dół > Edytuj Administratora TISAX > Przejdź do punktu „ENX PORTAL ACCESS” (DOSTĘP DO PORTALU ENX) > Ustaw „INVITE THIS CONTACT” (ZAPROŚ TĘ OSOBĘ DO KONTAKTU)" na „Yes” (Tak) > Kliknij „Save Contact” (Zapisz kontakt)

4.5.6. Warunki ogólne

Trzecim etapem jest akceptacja „Warunków ogólnych uczestnictwa TISAX”.

Warto odwołać się do uwag wyjaśniających w Punkt 4.3.1, “Kwestie prawne”.

4.5.7. Rejestracja zakresu oceny

Czwartym etapem jest rejestracja zakresu oceny w ramach oceny bezpieczeństwa informacji.

Prosimy Państwa o:

1. przypisanie nazwy zakresu oceny.
   Głównym celem nazwy zakresu jest ułatwienie Państwu identyfikacji zakresu na poglądowej liście zakresów na portalu ENX.
   Warto odwołać się do uwag wyjaśniających w Punkt 4.3.2.6, “Nazwa zakresu”.
2. wybór rodzaju zakresu oceny.
   (standardowy, niestandardowy)
   Warto odwołać się do uwag wyjaśniających w Punkt 4.3.2, “Zakres postępowania TISAX”.
3. określenie głównej osoby do kontaktu w odniesieniu do zakresu.
   Jest to osoba odpowiedzialna za ocenę danego zakresu. Mogą to być Państwo lub inny pracownik spółki.
   Zwykle potrzebujemy jedynie głównej osoby do kontaktu w odniesieniu do zakresu. Jeżeli pragną Państwo, abyśmy całą korespondencję własną w odniesieniu do tego konkretnego zakresu kierowali także do innych osób, mogą Państwo dodać kolejne osoby do kontaktu ze strony uczestnika.
4. wybór celu/celów oceny.
   Warto odwołać się do uwag wyjaśniających w Punkt 4.3.3, “Cele oceny”.

5. dodanie lokalizacji zakresu oceny.
   Poprosimy Państwa o określenie wszystkich lokalizacji wchodzących w zakres oceny.
   Warto odwołać się do uwag wyjaśniających w Punkt 4.3.2, “Zakres postępowania TISAX”.

Uwaga:

Utworzonej nowej lokalizacji nie można edytować. Prosimy o kontakt w przypadku drobnych zmian (zmiana nazwy spółki, błędy literowe w nazwie ulicy, kodzie pocztowym, nazwie miejscowości itp.). Wprowadzimy niezbędne korekty.

Ważna uwaga:

Niniejsza uwaga odnosi się jedynie do sytuacji odnawiania etykiet TISAX.

Prosimy o wykorzystanie istniejących rejestrów lokalizacji utworzonych i używanych podczas rejestracji poprzedniego zakresu. Nie należy tworzyć nowego rejestru lokalizacji o tym samym adresie.

Wynika to z faktu, że niektórzy uczestnicy TISAX automatycznie przetwarzają wyniki oceny swoich partnerów. Synchronizują własny system z portalem ENX. Nawet niewielkie różnice mogą uniemożliwić pomyślną synchronizację. Co więcej, pozwala to uniknąć zaśmiecania danych uczestników zbędnymi powieleniami.

6. wybór poziomu publikacji i udostępniania (opcjonalnie).
   Już na tym etapie mogą Państwo podjąć decyzję o przekazaniu wyniku Państwa oceny innym uczestnikom TISAX oraz udostępnieniu wyniku Państwa oceny Państwa partnerowi/partnerom. Zwykle wyrażają Państwo zgodę, abyśmy co najmniej wykazali, że są Państwo uczestnikiem i że pomyślnie przeszli Państwo proces TISAX.
   Ten etap można bezpiecznie pominąć podczas rejestracji wstępnej. Dostęp do wyniku własnej oceny można zdefiniować w późniejszym terminie.
   Warto odwołać się do uwag wyjaśniających w Punkt 4.3.2.8, “Publikacja i udostępnianie”.

Ważna uwaga:

Zgody na publikację lub udostępnianie nie można cofnąć.
Bardziej szczegółowe informacje znajdują się w Punkt 6.4, “Trwałość wyników będących przedmiotem wymiany”.

7. określenie adresata faktury.
   Poprosimy Państwa o określenie adresata swojej faktury/faktur.
   Warto odwołać się do uwag wyjaśniających w Punkt 4.3.4, “Opłata”.

Uwaga:

Tu nie można zbyt wiele zepsuć. Jeśli w późniejszym terminie stwierdzą Państwo, że zarejestrowali Państwo nieco odmienny zakres (zapomnieli o lokalizacji, posiadają Państwo inny cel oceny itp.), dostawca usług audytu może przeprowadzić ocenę.

Przykład: audytor określa, że zakres musi zawierać dodatkową lokalizację, której początkowo Państwo nie ujęli w zakresie. Audytor będzie kontynuował, a później zaktualizuje Państwa zakres oceny na portalu ENX podczas wczytywania Państwa wyniku oceny.

Uwaga:

Każdy zakres oceny przechodzi pewien cykl. Na tym etapie zakres oceny ma status „Niekompletny”, „Oczekujący na Państwa zlecenie” lub „Oczekujący na zatwierdzenie ENX”.

Bardziej szczegółowe informacje na temat statusu zakresu oceny znajdują się w Punkt 7.5.1, “Informacje ogólne: Assessment scope status (Status zakresu oceny)”.

Uwaga:

Dużym korporacjom posiadającym wiele lokalizacji TISAX oferuje uproszczoną ocenę grupy. Tę opcję można rozważyć, jeśli:

- Państwa zakres obejmuje co najmniej trzy lokalizacje[10] oraz
- Państwa system zarządzania bezpieczeństwem jest w szczytowej formie i zorganizowany centralnie[11].

Uproszczona ocena grupy wymaga większego wysiłku początkowego. Opłacalność rośnie jednak ze wzrostem liczby lokalizacji.

Bardziej szczegółowe informacje na temat „uproszczonej oceny grupy” znajdują się w dokumencie „Uproszczona ocena grupy TISAX”.

Dokument „Uproszczona ocena grupy TISAX” można pobrać z naszej strony internetowej pod adresem:
enx.com/en-US/TISAX/downloads/

PDF do pobrania:
enx.com/sga.pdf

Uwaga:

Zarejestrowanego zakresu oceny nie można samodzielnie zmienić.

Jeśli są nas Państwo w stanie wiarygodnie zapewnić, że NIE przesłali Państwo jeszcze „Wyciągu z zakresu TISAX” naszym dostawcom usług audytu, prosimy o kontakt. Wprowadzimy niezbędne korekty.

Jeżeli już przesłali Państwo „Wyciąg z zakresu TISAX” dostawcom usług audytu, mogą Państwo po prostu utworzyć nową/-e lokalizację/-e na portalu ENX (jeżeli dotyczy), a wszelkie zmiany omówić ze swoim dostawcą usług audytu. Dostawca usług audytu przeprowadzi ocenę na podstawie zmian i aktualizację informacji dotyczących zakresu oceny na portalu ENX.

Uwaga:

Nie mogą Państwo usunąć zakresu oceny na portalu ENX. Prosimy o kontakt, jeśli pomyłkowo utworzyli Państwo zakres oceny. Usuniemy go w Państwa imieniu.

4.5.8. Wiadomość e-mail z potwierdzeniem

Kiedy ukończą Państwo wszystkie powyższe etapy obowiązkowe, sprawdzimy Państwa wniosek. Później prześlemy wiadomość e-mail z potwierdzeniem.

Ta wiadomość zawiera dwa ważne elementy:

- Listę danych kontaktowych wszystkich dostawców usług audytu TISAX
  Muszą Państwo wybrać jednego z naszych dostawców usług audytu TISAX, który przeprowadzi ocenę Państwa zakresu oceny. Mogą Państwo użyć danych kontaktowych do złożenia zapytań ofertowych.
  Bardziej szczegółowe informacje na temat wyboru dostawcy usług audytu znajdują się w Punkt 5.3, “Wybór dostawcy usług audytu”.
- „Wyciąg z zakresu TISAX” w postaci załączonego pliku PDF

  Zawiera on:

  - Informacje zapisane przez nas w naszej bazie danych
  - Państwa Identyfikator uczestnika
    Bardziej szczegółowe informacje znajdują się w Punkt 4.5.8.1, “Participant ID (Identyfikator uczestnika)” poniżej.
  - Państwa Identyfikator(y) zakresu
    Bardziej szczegółowe informacje znajdują się w Punkt 4.5.8.2, “Scope ID (Identyfikator zakresu)” poniżej.

Przykład naszej wiadomości e-mail z potwierdzeniem znajduje się w Punkt 7.2, “Załącznik: Przykładowa wiadomość e-mail z potwierdzeniem”.

Przykład „Wyciągu z zakresu TISAX” znajduje się w Punkt 7.3, “Załącznik: Przykładowy wyciąg z zakresu TISAX”.

Wiadomość e-mail z potwierdzeniem zwykle otrzymają Państwo od nas w ciągu trzech dni roboczych.

Jeśli nie otrzymają Państwo od nas wiadomości w ciągu siedmiu dni roboczych, proszę sprawdzić, czy a) przekazali Państwo wszystkie informacje oraz b) status zakresu oceny to „Oczekujący na zatwierdzenie ENX”. Przetwarzanie Państwa rejestracji rozpoczniemy dopiero po uzyskaniu wszystkich informacji. Jeśli Państwa zdaniem mamy wszystkie informacje, lecz się z Państwem nie skontaktowaliśmy, prosimy o kontakt.

Wiadomość e-mail z potwierdzeniem prześlemy głównej osobie do kontaktu ze strony uczestnika.

Uwaga:

Każdy zakres oceny przechodzi pewien cykl. Na tym etapie zakres oceny ma status „Oczekujący na zatwierdzenie ENX”.

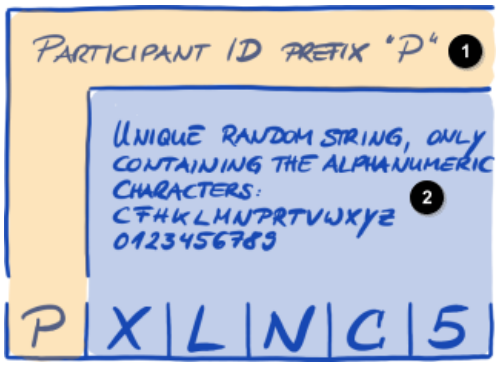
Bardziej szczegółowe informacje na temat statusu zakresu oceny znajdują się w Punkt 7.5.5, “Assessment scope status „Awaiting your payment” (Status zakresu oceny „Oczekujący na Państwa płatność”)”.

Kolejne dwa podpunkty zawierają szczegółowe informacje na temat celu Państwa Identyfikatora uczestnika oraz Identyfikatora zakresu.

4.5.8.1. Participant ID (Identyfikator uczestnika)

Identyfikator uczestnika:

- umożliwia identyfikację uczestnika TISAX.
- jest unikalny dla każdego uczestnika.
- jest przydzielany Państwu po zakończeniu procesu rejestracji.
- jest warunkiem wstępnym zlecenia oceny bezpieczeństwa informacji dowolnemu z naszych dostawców usług audytu TISAX.
- ma następującą postać:



Rysunek 7. Format Identyfikatora uczestnika[1]

1. Prefiks „P” Identyfikatora uczestnika
2. Unikalny ciąg losowy, zawierający jedynie znaki alfanumeryczne:
   CFHKLMNPRTVWXYZ
   0123456789

Uwaga:

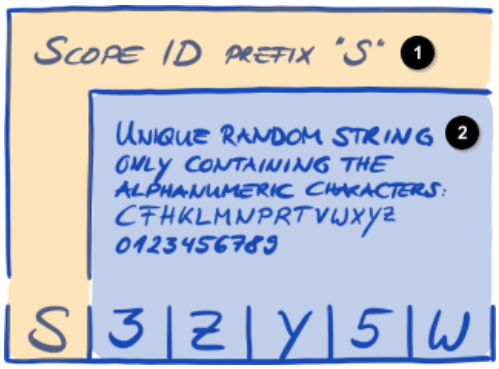
Własny identyfikator uczestnika można znaleźć na dwa sposoby:

1. Sprawdzając „Wyciąg z zakresu TISAX”.
   Bardziej szczegółowe informacje znajdują się w Punkt 4.5.8, “Wiadomość e-mail z potwierdzeniem” powyżej.
2. Należy się zalogować na portalu ENX, przejść do głównego paska nawigacji i zaznaczyć „DASHBOARD” („PULPIT”). Tam znajdą Państwo swój Identyfikator uczestnika.

4.5.8.2. Scope ID (Identyfikator zakresu)

Identyfikator zakresu:

- służy do identyfikacji zakresu oceny.
- jest unikalny dla każdego zakresu oceny.
- jest przydzielany Państwu po zakończeniu procesu rejestracji.
- jest warunkiem wstępnym możliwości zlecenia oceny bezpieczeństwa informacji dowolnemu z naszych dostawców usług audytu TISAX.
- ma następującą postać:



Rysunek 8. Format Identyfikatora zakresu

1. Prefiks „S” Identyfikatora zakresu
2. Unikalny ciąg losowy, zawierający jedynie znaki alfanumeryczne:
   CFHKLMNPRTVWXYZ
   0123456789

Uwaga:

Własny identyfikator zakresu można znaleźć na dwa sposoby:

1. Sprawdzając „Wyciąg z zakresu TISAX”.
   Bardziej szczegółowe informacje znajdują się w Punkt 4.5.8, “Wiadomość e-mail z potwierdzeniem” powyżej.
2. Należy się zalogować na portalu ENX, przejść do głównego paska nawigacji i zaznaczyć „MY TISAX” (MÓJ TISAX), a później „SCOPES AND ASSESSMENTS” (ZAKRESY I OCENY). Tam znajdą Państwo swój Identyfikator zakresu.

Uwaga:

Każdy zakres oceny (zidentyfikowany na podstawie identyfikatora zakresu) przechodzi pewien cykl.

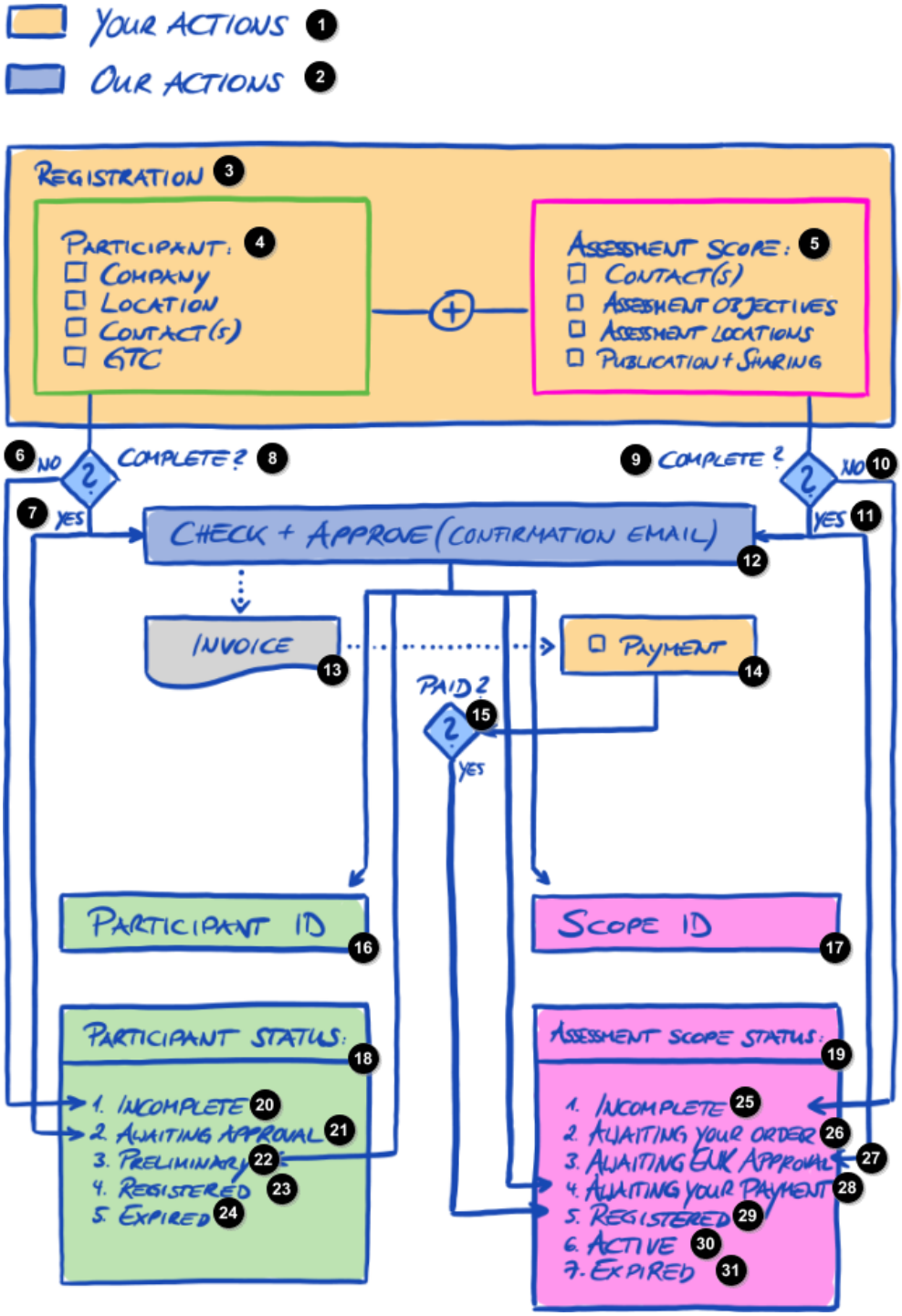
Bardziej szczegółowe informacje na temat statusu zakresu oceny znajdują się w Punkt 7.5, “Załącznik: Assessment scope status (Status zakresu oceny)”.

4.5.9. Informacje dotyczące statusu

Na tym etapie Państwa pozycję w procesie TISAX opisujemy za pomocą dwóch statusów:

1. Status uczestnika
2. Status zakresu oceny

Poniższy schemat przedstawia warunki wymagane w celu uzyskania danego statusu:



Rysunek 9. Warunki uzyskania statusu uczestnika i statusu zakresu oceny

1. Państwa czynności
2. Nasze czynności
3. Rejestracja

4. Uczestnik:
[ ] Spółka
[ ] Lokalizacja
[ ] Osoba/osoby do kontaktu
[ ] GTC

5. Zakres oceny:
[ ] Osoba/osoby do kontaktu
[ ] Cele oceny
[ ] Lokalizacje poddawane ocenie
[ ] Publikacja + udostępnianie

6. Nie

7. Tak

8. Ukończono?

9. Ukończono?

10. Nie

11. Tak

12. Kontrola + zatwierdzenie (wiadomość e-mail z potwierdzeniem)

13. Faktura

14. [ ] Płatność

15. Zapłacono?

16. Identyfikator uczestnika

17. Identyfikator zakresu

18. Status uczestnika:

19. Status zakresu oceny:

20. 1. Niekompletny

21. 2. Oczekujący na zatwierdzenie

22. 3. Wstępny

23. Zarejestrowany

24. Po terminie ważności

25. 1. Niekompletny

26. 2. Oczekujący na Państwa zlecenie

27 3. Oczekujący na zatwierdzenie ENX

28 4. Oczekujący na Państwa płatność

29 5. Zarejestrowany

30 6. Aktywny

31 7. Po terminie ważności

Definicje statusów oraz czynności niezbędne w celu przejścia do kolejnego statusu znajdują się w załączniku.

Bardziej szczegółowe informacje na temat:

- statusu uczestnika znajdują się w Punkt 7.4, “Załącznik: Participant status (Status uczestnika)”.
- statusu zakresu oceny znajdują się w Punkt 7.5, “Załącznik: Assessment scope status (Status zakresu oceny)”.

4.5.10. Zmiany informacji podanych przez Państwa w trakcie rejestracji

Uwaga:

Wszystkie odpowiedzi dotyczące cyklu życia danych znajdują się w Punkt 7.9, “Załącznik: Zarządzanie cyklem życia danych uczestników”. Zawiera on instrukcje na wypadek sytuacji, gdy pragną Państwo zmienić lub zaktualizować takie dane, jak nazwa firmy lub dane kontaktowe.

Gratulacje, są Państwo teraz zarejestrowanym uczestnikiem TISAX. Są Państwo gotowi, by przejść do kolejnego etapu procesu TISAX.

5. Ocena (Etap 2)

Szacowany czas czytania punktu poświęconego ocenie wynosi 30–35 minut.

5.1. Informacje ogólne

Ocena TISAX to drugi etap. Tu wykonują Państwo najwięcej pracy w celu uzyskania oceny TISAX.

Poniższe punkty poprowadzą Państwa przez proces oceny:

1. Na początek wyjaśnimy, jak można za pomocą samooceny ISA sprawdzić, czy są Państwo przygotowani do oceny TISAX.
2. Przekażemy porady dotyczące sposobu wyboru jednego z naszych dostawców usług audytu TISAX.
3. Następnie opiszemy Państwa drogę przez proces oceny.
4. Na koniec wyjaśnimy „rezultat procesu”: wynik oceny i powiązane z nim etykiety TISAX.

5.2. Samoocena na podstawie ISA

Aby przygotować się do oceny TISAX, potrzebują Państwo przede wszystkim sprawnego systemu zarządzania bezpieczeństwem informacji (ISMS). Aby ustalić, czy Państwa ISMS odpowiada spodziewanemu poziomowi dojrzałości, muszą Państwo przeprowadzić samoocenę na podstawie ISA.

„Ocena bezpieczeństwa informacji” (Information Security Assessment, ISA) to katalog kryteriów opublikowanych przez Verband der Automobilindustrie e.V. (VDA), niemieckie stowarzyszenie przemysłu motoryzacyjnego. Stanowi on standard branży motoryzacyjnej stosowany do oceny bezpieczeństwa informacji.

W poniższych punktach przedstawiono wskazówki praktyczne na potrzeby przeprowadzenia samooceny na podstawie ISA.

Wyjaśnienia, przykłady oraz zrzuty ekranów zawarte w tym podręczniku pochodzą z wersji 5 ISA.

Uwaga:

Informacje na temat zmian w porównaniu do poprzednich wersji ISA znajdują się w pliku Excel pt. „Historia zmian” (Change history).

Uwaga:

> Informacje na temat wersji ISA obowiązującej w odniesieniu do Państwa oceny w przypadku, gdy VDA opublikuje nową wersję, znajdą Państwo w Punkt 7.11, “Załącznik: Zarządzanie cyklem życia ISA”.

5.2.1. Pobieranie dokumentu ISA

Samoocenę należy zacząć od pobrania dokumentu ISA.

Można go pobrać z naszej strony internetowej pod adresem:
enx.com/en-US/TISAX/downloads/

Bezpośrednie pobieranie pliku PDF:
portal.enx.com/isa5-en.xlsx

Dokument ISA jest dostępny także w języku niemieckim:
enx.com/de-de/TISAX/downloads/

5.2.2. Rozumienie dokumentu ISA

Przed rozpoczęciem samooceny warto zapoznać się z poniższymi wyjaśnieniami. Stanowią one uzupełnienie oficjalnych wyjaśnień i definicji zawartych w dokumencie ISA, skupione na wykorzystaniu do celów oceny TISAX.

5.2.2.1. Katalogi kryteriów

ISA posiada obecnie trzy „katalogi kryteriów”[12]:

1.	Bezpieczeństwo informacji	Information Security
2.	Ochrona prototypów	Prototype Protection
3.	Ochrona danych	Data Protection

Każdy katalog kryteriów posiada własny arkusz Excel:

Rysunek 10. Zrzut ekranu: katalogi kryteriów ISA jako arkusze Excel

Który katalog kryteriów odnosi się do Państwa? To zależy od Państwa celu/celów oceny.

Każdy cel oceny określa obowiązujące wymagania z określonego katalogu kryteriów. w przypadku niektórych celów oceny obowiązują wymagania jedynie z _jednego_ katalogu kryteriów, w przypadku innych z _więcej niż jednego_ katalogu kryteriów.

Wspomniane cele oceny przekładają się na te katalogi kryteriów:

Lp.	Cel oceny (🇬🇧 Assessment objective)	Katalog(i) kryteriów ISA
1.	Info high	Information Security (🇵🇱 Bezpieczeństwo informacji)
2.	Info very high	Information Security (🇵🇱 Bezpieczeństwo informacji)
3.	Confidential	Information Security (🇵🇱 Bezpieczeństwo informacji)
4.	Strictly confidential	Information Security (🇵🇱 Bezpieczeństwo informacji)
5.	High availability	Information Security (🇵🇱 Bezpieczeństwo informacji)
6.	Very high availability	Information Security (🇵🇱 Bezpieczeństwo informacji)
7.	Proto parts	Prototype Protection (🇵🇱 Ochrona prototypów)
8.	Proto vehicles	Prototype Protection (🇵🇱 Ochrona prototypów)
9.	Test vehicles	Prototype Protection (🇵🇱 Ochrona prototypów)
10.	Proto events	Prototype Protection (🇵🇱 Ochrona prototypów)
11.	Data	Information Security (🇵🇱 Bezpieczeństwo informacji) Data Protection (🇵🇱 Ochrona danych)
12.	Special data	Information Security (🇵🇱 Bezpieczeństwo informacji) Data Protection (🇵🇱 Ochrona danych)

Tabela 7. Powiązania między celami oceny TISAX a katalogami kryteriów ISA

Przykład: jeśli jako cel oceny wybrali Państwo „Ochronę danych”, będą Państwo musieli udzielić odpowiedzi na pytania w katalogach kryteriów „Bezpieczeństwo informacji” ORAZ „Ochrona danych”.

Być może zauważyli Państwo, że na każdy katalog kryteriów przypada więcej niż jeden cel oceny. Jak ustalić, które wymagania dotyczą poszczególnych celów oceny?

Poniższa tabela wskazuje obowiązujące wymagania:

Lp.	Cel oceny (🇬🇧 Assessment objective)	Obowiązujące wymagania
1.	Info high	▪ Katalog kryteriów „Information Security” (🇵🇱 „Bezpieczeństwo informacji”) ◦ Kolumna „Requirements (must)” (🇵🇱 „Wymagania (musi)”) ◦ Kolumna „Requirements (should)” (🇵🇱 „Wymagania (powinien)”) ◦ Kolumna „Additional requirements for high protection needs” (🇵🇱 „Dodatkowe wymagania na potrzeby wysokiej ochrony”)
2.	Info very high	▪ Katalog kryteriów „Information Security” (🇵🇱 „Bezpieczeństwo informacji”) ◦ Kolumna „Requirements (must)” (🇵🇱 „Wymagania (musi)”) ◦ Kolumna „Requirements (should)” (🇵🇱 „Wymagania (powinien)”) ◦ Kolumna „Additional requirements for high protection needs” (🇵🇱 „Dodatkowe wymagania na potrzeby wysokiej ochrony”) ◦ Kolumna (🇵🇱)„Dodatkowe wymagania na potrzeby bardzo wysokiej ochrony”
3.	Confidential	▪ Katalog kryteriów „Information Security” (🇵🇱 „Bezpieczeństwo informacji”) ◦ Kolumna „Requirements (must)” (🇵🇱 „Wymagania (musi)”) ◦ Kolumna „Requirements (should)” (🇵🇱 „Wymagania (powinien)”) ◦ Kolumna „Additional requirements for high protection needs” (🇵🇱 „Dodatkowe wymagania na potrzeby wysokiej ochrony”) (ale jedynie oznaczone literą „**C**” jak **C**onfidentiality (🇵🇱 **C**onfidentiality, czyli poufność))

Lp.	Cel oceny (Assessment objective)	Obowiązujące wymagania
4.	Strictly confidential	▪ Katalog kryteriów „Information Security” („Bezpieczeństwo informacji”) ◦ Kolumna „Requirements (must)” („Wymagania (musi)”) ◦ Kolumna „Requirements (should)” („Wymagania (powinien)”) ◦ Kolumna „Additional requirements for high protection needs” („Dodatkowe wymagania na potrzeby wysokiej ochrony”) (ale jedynie oznaczone literą „**C**” jak **C**onfidentiality (**C**onfidentiality, czyli poufność)) ◦ Kolumna ( )„Dodatkowe wymagania na potrzeby bardzo wysokiej ochrony” (ale jedynie oznaczone literą „**C**” jak **C**onfidentiality (**C**onfidentiality, czyli poufność))
5.	High availability	▪ Katalog kryteriów „Information Security” („Bezpieczeństwo informacji”) ◦ Kolumna „Requirements (must)” („Wymagania (musi)”) ◦ Kolumna „Requirements (should)” („Wymagania (powinien)”) ◦ Kolumna „Additional requirements for high protection needs” („Dodatkowe wymagania na potrzeby wysokiej ochrony”) (ale jedynie oznaczone literą „**A**” jak **A**vailability (**A**vailability, czyli dostępność))

Lp.	Cel oceny (Assessment objective)	Obowiązujące wymagania
6.	Very high availability	▪ Katalog kryteriów „Information Security” („Bezpieczeństwo informacji”) ◦ Kolumna „Requirements (must)” („Wymagania (musi)”) ◦ Kolumna „Requirements (should)” („Wymagania (powinien)”) ◦ Kolumna „Additional requirements for high protection needs” („Dodatkowe wymagania na potrzeby wysokiej ochrony”) (ale jedynie oznaczone literą „**A**” jak **A**vailability (**A**vailability, czyli dostępność)) ◦ Kolumna ( )„Dodatkowe wymagania na potrzeby bardzo wysokiej ochrony” (ale jedynie oznaczone literą „**A**” jak **A**vailability (**A**vailability, czyli dostępność))
7.	Proto parts	▪ Katalog kryteriów „Prototype Protection” („Ochrona prototypów”) Ale jedynie w następujących rozdziałach: 8.1 Physical and Environmental Security (8.1 Bezpieczeństwo fizyczne i środowiska) 8.2 Organizational Requirements (8.2 Wymagania organizacyjne) 8.3 Handling of vehicles, components and parts (8.3 Postępowanie z pojazdami, komponentami i częściami) ◦ Kolumna „Requirements (must)” („Wymagania (musi)”) ◦ Kolumna „Requirements (should)” („Wymagania (powinien)”)

Lp.	Cel oceny (🇬🇧 Assessment objective)	Obowiązujące wymagania
8.	Proto vehicles	▪ Katalog kryteriów „Prototype Protection” (🇵🇱 „Ochrona prototypów”) Ale jedynie w następujących rozdziałach: 8.1 Physical and Environmental Security (🇵🇱 8.1 Bezpieczeństwo fizyczne i środowiska) 8.2 Organizational Requirements (🇵🇱 8.2 Wymagania organizacyjne) 8.3 Handling of vehicles, components and parts (🇵🇱 8.3 Postępowanie z pojazdami, komponentami i częściami) ◦ Kolumna „Requirements (must)” (🇵🇱 „Wymagania (musi)”) ◦ Kolumna „Requirements (should)” (🇵🇱 „Wymagania (powinien)”) ◦ Kolumna „Additional requirements for vehicles classified as requiring protection” (🇵🇱 „Dodatkowe wymagania na potrzeby pojazdów klasyfikowanych jako wymagające ochrony”)
9.	Test vehicles	▪ Katalog kryteriów „Prototype Protection” (🇵🇱 „Ochrona prototypów”) Ale jedynie w następujących rozdziałach: 8.2 Organizational Requirements (🇵🇱 8.2 Wymagania organizacyjne) 8.3 Handling of vehicles, components and parts (🇵🇱 8.3 Postępowanie z pojazdami, komponentami i częściami) 8.4 Requirements for trial vehicles (🇵🇱 8.4 Wymagania dotyczące pojazdów próbnych) ◦ Kolumna „Requirements (must)” (🇵🇱 „Wymagania (musi)”) ◦ Kolumna „Requirements (should)” (🇵🇱 „Wymagania (powinien)”)

Lp.	Cel oceny (Assessment objective)	Obowiązujące wymagania
10.	Proto events	▪ Katalog kryteriów „Prototype Protection” („Ochrona prototypów”) Ale jedynie w następujących rozdziałach: 8.2 Organizational Requirements (8.2 Wymagania organizacyjne) 8.3 Handling of vehicles, components and parts (8.3 Postępowanie z pojazdami, komponentami i częściami) 8.5 Requirements for events and shootings (8.5 Wymagania dotyczące wydarzeń oraz filmów i zdjęć) ◦ Kolumna „Requirements (must)” („Wymagania (musi)”) ◦ Kolumna „Requirements (should)” („Wymagania (powinien)”)
11.	Data	▪ Katalog kryteriów „Information Security” („Bezpieczeństwo informacji”) ◦ Kolumna „Requirements (must)” („Wymagania (musi)”) ◦ Kolumna „Requirements (should)” („Wymagania (powinien)”) ◦ Kolumna „Additional requirements for high protection needs” („Dodatkowe wymagania na potrzeby wysokiej ochrony”) (ale jedynie oznaczone literą „**C**” jak **C**onfidentiality (**C**onfidentiality, czyli poufność)) ▪ Katalog kryteriów „Data Protection” („Ochrona danych”) ◦ Kolumna „Requirements (must)” („Wymagania (musi)”)

Lp.	Cel oceny (Assessment objective)	Obowiązujące wymagania
12.	Special data	▪ Katalog kryteriów „Information Security” („Bezpieczeństwo informacji”) ◦ Kolumna „Requirements (must)” („Wymagania (musi)”) ◦ Kolumna „Requirements (should)” („Wymagania (powinien)”) ◦ Kolumna „Additional requirements for high protection needs” („Dodatkowe wymagania na potrzeby wysokiej ochrony”) (ale jedynie oznaczone literą „**C**” jak **C**onfidentiality (**C**onfidentiality, czyli poufność)) ◦ Kolumna („Dodatkowe wymagania na potrzeby bardzo wysokiej ochrony” (ale jedynie oznaczone literą „**C**” jak **C**onfidentiality (**C**onfidentiality, czyli poufność)) ▪ Katalog kryteriów „Data Protection” („Ochrona danych”) ◦ Kolumna „Requirements (must)” („Wymagania (musi)”)

Tabela 8. Wymogi obowiązujące w przypadku celów oceny

Uwaga:

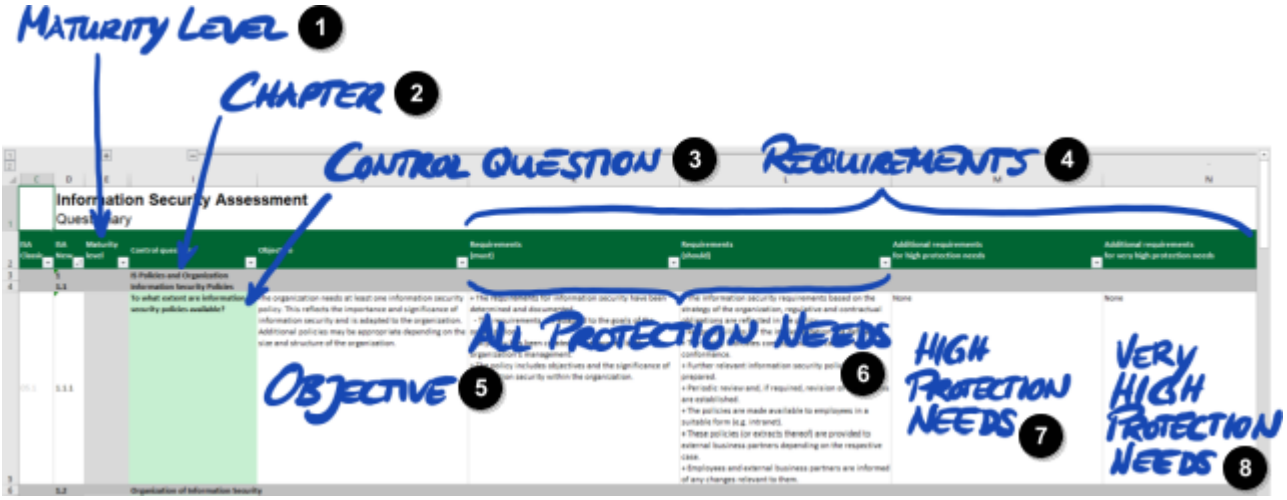
Każdy wymóg w dwóch kolumnach „Dodatkowe wymagania na potrzeby wysokiej ochrony” oraz „Dodatkowe wymagania na potrzeby bardzo wysokiej ochrony” oznaczono literą „**C**” jak **C**onfidentiality (**C**onfidentiality, czyli poufność) lub „**I**” jak **I**ntegrity (**I**ntegrity, czyli integralność) lub „**A**” jak **A**vailability (**A**vailability, czyli dostępność) lub dowolną kombinacją tych trzech liter.

Kiedy powyższa tabela zawęża wymagania w tych dwóch kolumnach do oznaczonych *jedną* z powyższych liter, zawsze uwzględnia wymagania oznaczone także *więcej niż tą* literą.

Przykład: wszystkie wymagania oznaczone literą „(C)”, „(C, I, A)” lub „(C, I)” obowiązują w przypadku, gdy w powyższej tabeli wskazano „C” (np. w celu

> oceny „Special data”).

Poniższy zrzut ekranu przedstawia główne elementy pytań kontrolnych w katalogu kryteriów „Bezpieczeństwo informacji”. (Pozostałe katalogi kryteriów zawierają jedynie podzbiór tych elementów.) Wszystkie elementy wyjaśnimy poniżej.



Rysunek 11. Zrzut ekranu: Główne elementy pytań w katalogu kryteriów ISA „Bezpieczeństwo informacji”

1. Poziom dojrzałości
2. Rozdział
3. Pytanie kontrolne
4. Wymagania
5. Cel
6. Wszystkie potrzeby dotyczące ochrony
7. Potrzeby wysokiej ochrony
8. Potrzeby bardzo wysokiej ochrony

5.2.2.2. Rozdziały

Każdy katalog kryteriów dzieli pytania na rozdziały.

Przykład: „2 Zasoby ludzkie”

Ten podział opiera się na typowych obowiązkach w spółce. Działy wskazano w kolumnie „Typowa osoba odpowiedzialna za wdrożenie procesu” (w powyższym przykładzie jest to „HR”).

5.2.2.3. Pytania kontrolne

Pytania dla każdego katalogu kryteriów znajdą Państwo w odpowiednich arkuszach Excel.

Przykład: „4.1.2 w jakim zakresie zabezpieczony jest dostęp użytkownika do usług sieciowych, systemów IT oraz aplikacji IT?”

Pytania kontrolne, na które muszą Państwo udzielić odpowiedzi, nazywane są też „kontrolami”. To „słowa audytora”. Termin „kontrola” używany jest także w normach ISO, na których opiera się ISA.

5.2.2.4. Pola formularza samooceny

Między kolumną „Maturity level” („Poziom dojrzałości”) a „Control question” („Pytanie kontrolne”) znajdują się pola formularza, które należy wypełnić podczas samooceny:

Pole formularza	Cel	Obowiązkowe?
Implementation description (Opis wdrożenia) (Kolumna F)	Tu należy pokrótce opisać rozwiązania wdrożone w firmie w związku z danym pytaniem kontrolnym.	Tak
Reference Documentation (Dokumentacja odniesienia) (Kolumna G)	Tu należy wskazać, w jakich dokumentach potwierdzają Państwo wdrożenie.	Tak
Findings/Result (Ustalenia/Wynik) (Kolumna H)	Tu można zapisać wszelkie ustalenia, w których Państwa zdaniem istnieje luka między stanem optymalnym a obecnym.	Nie

Tabela 9. Pola formularza samooceny i ich cel

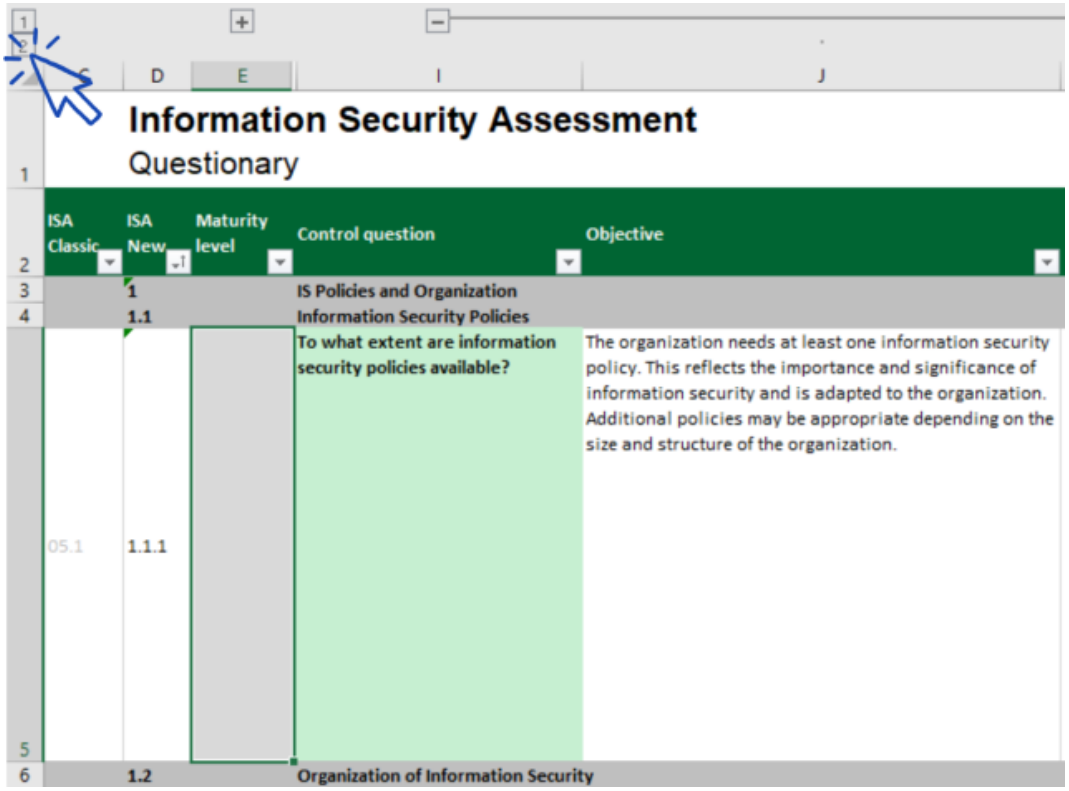
Obowiązkowy jest jedynie krótki opis wdrożenia oraz odwołanie do Państwa dokumentacji. Te informacje pomogą dostawcom usług audytu TISAX lepiej zrozumieć Państwa spółkę i przygotować ocenę.

W celu wsparcia Państwa samooceny istnieją również inne kolumny opcjonalne:

- Measures/recommendations (Środki/zalecenia) (Kolumna R)
- Date of assessment (Data oceny) (Kolumna S)
- Date of completion (Data ukończenia) (Kolumna T)
- Responsible department (Odpowiedzialny dział) (Kolumna U)
- Contact (Osoba do kontaktu) (Kolumna V)

Ważna uwaga:

Kiedy otworzą Państwo pobrany plik Excel i zaznaczą jeden z arkuszy katalogów kryteriów (np. Bezpieczeństwo informacji), prawdopodobnie nie zobaczą Państwo od razu pól formularza samooceny. By je wyświetlić, należy kliknąć przycisk grupowania dla poziomu „2”[13]. Przycisk znajduje się powyżej komórki C1, nieco w lewo od niej. Za jego pomocą można rozwinąć widok pól formularza samooceny.



Można także przewinąć w dół klawiszami strzałek. Wynika to z faktu, że ze względu na duże wymiary komórek przewijanie paskiem do przewijana może wymagać doskonałej sprawności motorycznej. Również w przypadku użycia funkcji przewijania urządzenia wskazującego można przypadkowo pominąć większe komórki.

5.2.2.5. Cel

W prawo od komórki „Pytanie kontrolne” znajduje się kolumna „Cel” (kolumna J). Jej treść opisuje, co trzeba osiągnąć w odniesieniu do tego aspektu swojego zarządzania bezpieczeństwem informacji.

Przykład (dla pytania kontrolnego 4.1.2): „Dostęp do systemów IT mogą uzyskać jedynie osoby po bezpiecznej identyfikacji (uwierzytelnieniu). w tym celu tożsamość użytkownika ustala się bezpiecznie za pomocą odpowiednich procedur.”

5.2.2.6. Wymagania

Wymagania określają, co mają Państwo zrealizować w celu realizacji celu.

Wymagania podzielono na cztery kolumny:

1. Requirements (must) (Wymagania (musi)) (Kolumna K)
2. Requirements (should) (Wymagania (powinien)) (Kolumna L)
3. Additional requirements for high protection needs (Dodatkowe wymagania na potrzeby wysokiej ochrony) (Kolumna M)
4. Additional requirements for very high protection needs (Dodatkowe wymagania na potrzeby bardzo wysokiej ochrony) (Kolumna N)

Należy spełnić wszystkie wymagania na potrzeby ochrony, którą chcą Państwo uzyskać (można ją znaleźć w celu oceny).

W przypadku niektórych celów oceny obowiązuje jedynie podzbiór wymagań. Bardziej szczegółowe informacje na temat obowiązujących wymagań znajdują się w Tabela 8, “Wymogi obowiązujące w przypadku celów oceny” w Punkt 5.2.2.1, “Katalogi kryteriów”, a szczególnie w note na końcu niniejszego punktu.

Bardziej szczegółowe informacje na temat przyjętych w ISA definicji poziomów wymagań „musi” i „powinien” znajdą Państwo w „Kluczowych terminach” w arkuszu Excel pt. „Definicje”.

Ważna uwaga:

Przypominamy, że każdy wymóg należy interpretować w kontekście i duchu celu. Nawet realizacja wymagania co do joty nie gwarantuje, że dostawca usług audytu potwierdzi jego realizację w kontekście i duchu celu (kolumna J).

Wymagania i ich treść opierają się na teoretycznym wdrożeniu przez fikcyjną, przeciętną firmę nieznanej wielkości.

Dostawca usług audytu zawsze musi zważyć cel względem unikalnej interpretacji w Państwa firmie. To, co właściwe dla przeciętnej firmy, nie musi wystarczyć w Państwa sytuacji.

Bardziej szczegółowe informacje znajdują się w Punkt 5.2.5, “Działanie na podstawie wyniku samooceny”.

5.2.2.7. Poziomy dojrzałości

ISA wykorzystuje koncepcję „maturity levels” („poziomy dojrzałości”) do oceny jakości wszystkich aspektów Państwa systemu zarządzania bezpieczeństwem informacji. Im bardziej rozbudowany jest Państwa system zarządzania bezpieczeństwem informacji, tym wyższy

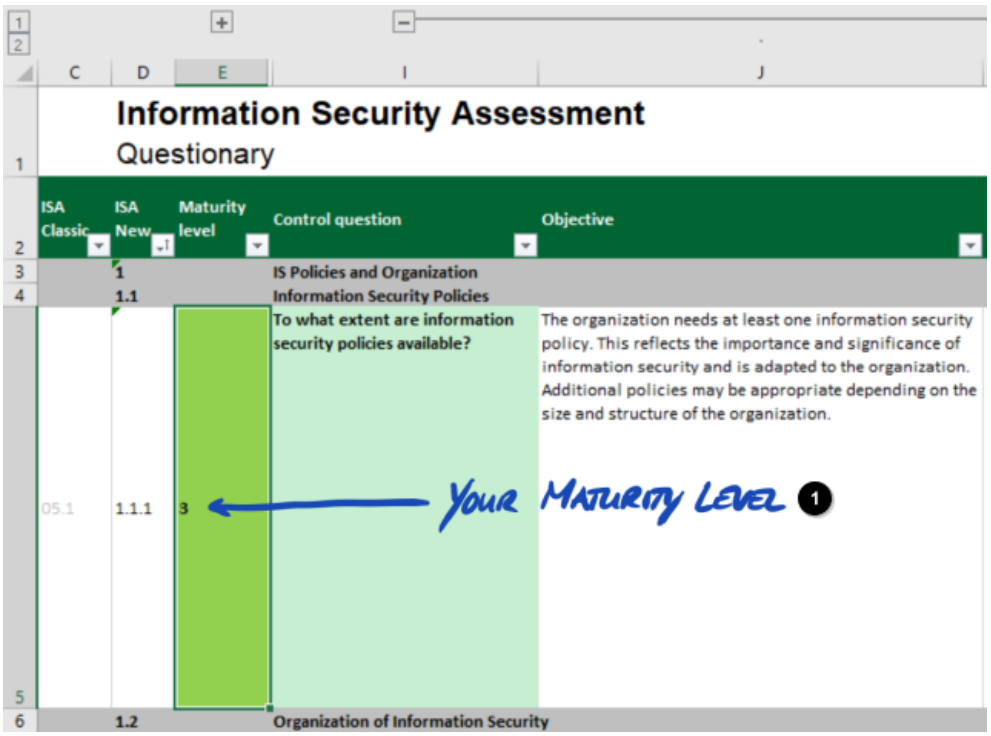
będzie Państwa poziom dojrzałości.

ISA wyróżnia sześć poziomów dojrzałości. Szczegółową definicję znajdą Państwo w arkuszu Excel „Maturity levels” („Poziomy dojrzałości”). Na potrzeby skonsolidowanego przeglądu poziomów dojrzałości cytujemy nieformalne opisy zawarte w ISA:

Maturity level (Poziom dojrzałości)	**Jednym słowem**	**Opis**
0	Incomplete (Niekompletny)	Proces nie jest dostępny, nie przestrzega się go lub nie umożliwia realizacji celu.
1	Performed (Realizowany)	Realizuje się nieudokumentowany lub niekompletnie udokumentowany proces oraz istnieją wskaźniki, że pozwala zrealizować cel.
2	Managed (Zarządzany)	Stosuje się proces umożliwiający realizację celów. Są dostępne dokumentacja i dowody wdrożenia procesu.
3	Established (Ustanowiony)	Stosuje się standardowy proces włączony w system ogólny. Dokumentuje się zależności od innych procesów i tworzy odpowiednie powierzchnie styku. Istnieją dowody na zrównoważone i czynne stosowanie procesu przez dłuższy czas.
4	Predictable (Przewidywalny)	Stosuje się ustanowiony proces. Skuteczność procesu monitoruje się w trybie ciągłym, zbierając kluczowe wskaźniki. Określa się wartości graniczne, przy których proces uznaje się za niewystarczająco skuteczny i wymagający korekty. (Kluczowe wskaźniki efektywności)
5	Optimizing (Optymalizacja)	Stosuje się przewidywalny proces, którego głównym celem jest ciągłe doskonalenie. Doskonalenie wspiera się czynnie przy pomocy dedykowanych zasobów.

Tabela 10. Nieformalny opis poziomów dojrzałości

Poziom dojrzałości własnego systemu zarządzania bezpieczeństwem informacji należy ocenić zgodnie z pytaniem. Proszę wprowadzić swój poziom dojrzałości w kolumnie „Maturity level” („Poziom dojrzałości”) (kolumna E).



Rysunek 12. Zrzut ekranu: przykład wyboru poziomu dojrzałości w dokumencie ISA (arkusz Excel „Bezpieczeństwo informacji”)

1 Państwa poziom dojrzałości

Bardziej szczegółowe informacje na temat docelowych poziomów dojrzałości i ich wpływu na wynik Państwa oceny znajdują się w Punkt 5.2.4, “Interpretacja wyniku samooceny”.

Lepsze rozumienie zapewnia Państwu teraz gotowość do rozpoczęcia samooceny.

5.2.3. Prowadzenie samooceny

Proszę otworzyć plik Excel i na podstawie przeglądu wszystkich pytań kontrolnych w każdym katalogu kryteriów związanym z Państwa celem/celami oceny określić poziom dojrzałości odpowiadający aktualnemu stanowi Państwa systemu zarządzania bezpieczeństwem informacji. w tym celu należy się oprzeć na własnej ocenie. Na tym etapie nie ma poprawnych lub błędnych odpowiedzi.

Po zakończeniu samooceny kolumna „Wynik” (H) w arkuszu Excel „Wyniki (ISA5)” powinna być całkowicie wypełniona cyframi (0–5) lub „nd.” (tzn. „nie dotyczy”).

No.	Subject	Target maturity level	Result
1.1.1	To what extent are information security policies available?	3	3
1.2.1	To what extent is information security managed within the organization?	3	3
1.2.2	To what extent are information security responsibilities organized?	3	3
1.2.3	To what extent are information security requirements taken into account in projects?	3	3
1.2.4	To what extent are responsibilities between external IT service providers and the own organization defined?	3	3
1.3.1	To what extent are information assets identified and recorded?	3	3
1.3.2	To what extent are information assets classified and managed in terms of their protection needs?	3	3
1.3.3	To what extent is it ensured that only evaluated and approved external IT services are used for processing the organization's information assets?	3	3
1.4.1	To what extent are information security risks managed?	3	3
1.5.1	To what extent is compliance with information security ensured in procedures and processes?	3	3
1.5.2	To what extent is the ISMS reviewed by an independent entity?	3	3
1.6.1	To what extent are information security events processed?	3	3

1 GREEN = ✓

Rysunek 13. Zrzut ekranu: przykład arkusza „Wyniki (ISA5)” w dokumencie ISA

1 Zielony

W przypadku pytań dotyczących ISA prosimy o kontakt.

5.2.4. Interpretacja wyniku samooceny

W kolejnych pięciu podpunktach wyjaśniono sposób analizy i interpretacji Państwa wyniku samooceny. Analiza wykaże, czy są Państwo gotowi do oceny TISAX, czy też jeszcze nie.

5.2.4.1. Analiza

Państwa punktacja stanowi podsumowanie wyniku samooceny.

Punktację („Wynik skorygowany docelowym poziomem dojrzałości”) można znaleźć w arkuszu Excel „Wyniki (ISA5)” (komórka D6). Termin „skorygowany” wyjaśnimy w dalszej części dokumentu.

Information Security Assessment Results

VDA Verband der Automobilindustrie

Result with cutback to target maturity level:	3,00	Maximum score:	3,00

Details: YOUR RESULT SCORE 1 MAXIMUM RESULT SCORE

No.	Subject	Target maturity level	Result 2
1.1.1	To what extent are information security policies available?	3	3
1.2.1	To what extent is information security managed within the organization?	3	3
1.2.2	To what extent are information security responsibilities organized?	3	3

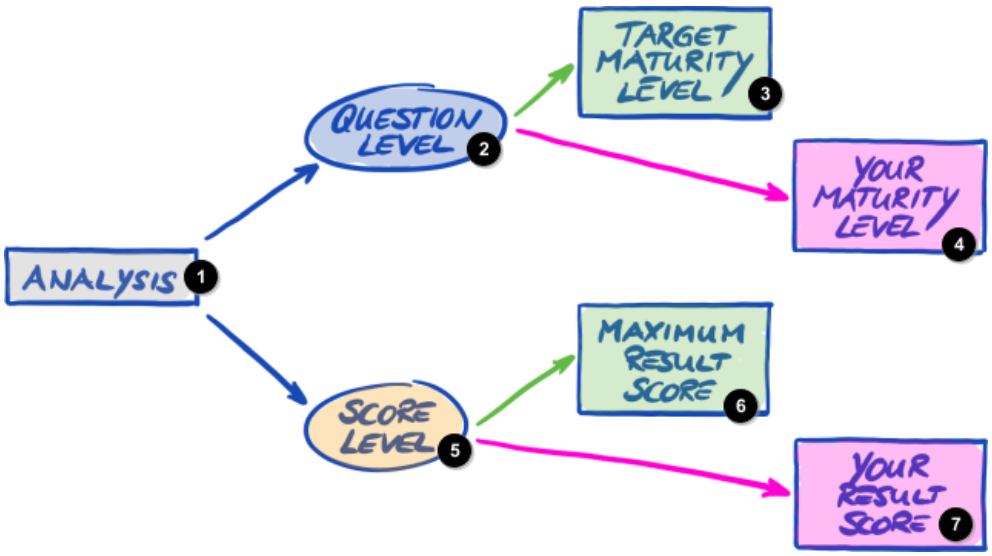
Rysunek 14. Zrzut ekranu: Państwa punktacja i maksymalna punktacja (arkusz Excel „Wyniki (ISA5)”, komórka D6 i G6)

1. Państwa punktacja
2. Maksymalna punktacja

Aby zrozumieć, a później zinterpretować Państwa wynik samooceny i punktację, należy rozróżnić dwa poziomy analizy:

1. Poziom pytań
   Ten poziom zawiera wszystkie pytania. Dla każdego pytania istnieje docelowy poziom dojrzałości oraz Państwa poziom dojrzałości.
2. Poziom punktacji
   Na tym poziomie istnieje ogólny wynik podsumowujący wyniki dla wszystkich pytań. Istnieje punktacja maksymalna oraz punktacja uzyskana przez Państwa.

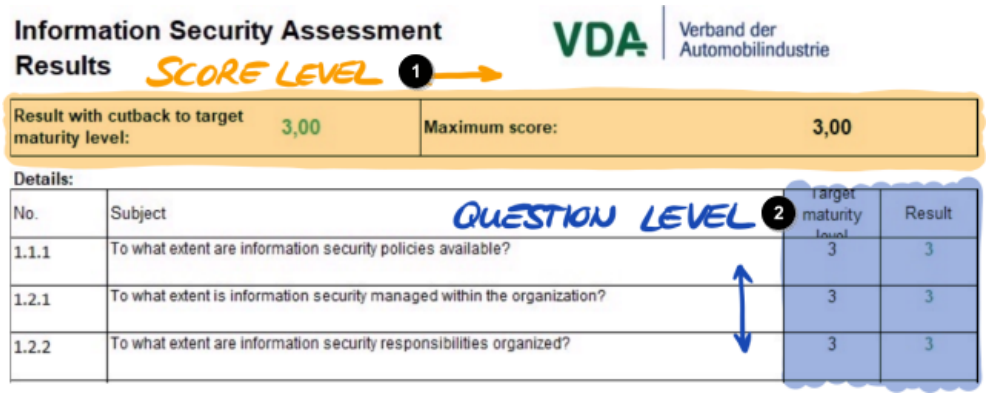
Na poniższym rysunku przedstawiono poziomy analizy:



Rysunek 15. Analiza wyniku samooceny na poziomie pytań i poziomie punktacji

1. Analiza
2. Poziom pytań
3. Docelowy poziom dojrzałości
4. Państwa poziom dojrzałości
5. Poziom punktacji
6. Maksymalna punktacja
7. Państwa punktacja

Poniższy rysunek przedstawia, gdzie znaleźć wyniki na poziomie punktacji oraz na poziomie pytań:



Rysunek 16. Poziom punktacji i poziom pytań w arkuszu Excel „Wyniki (ISA5)”

1. Poziom punktacji
2. Poziom pytań

Kolejny rysunek przedstawia uproszczony widok poziomów analizy, definicje wartości docelowych ISA oraz Państwa wyników:

Rysunek 17. Wartości docelowe i Państwa wyniki na poziomie pytań i poziomie punktacji

1. Docelowy poziom dojrzałości
2. Państwa poziom dojrzałości
3. Poziom pytań
4. Q (Question) (pytanie)
5. TML (Target maturity level) (docelowy poziom dojrzałości)
6. YML (Your maturity level) (Państwa poziom dojrzałości)
7. Maksymalna punktacja
8. Państwa punktacja
9. Poziom punktacji

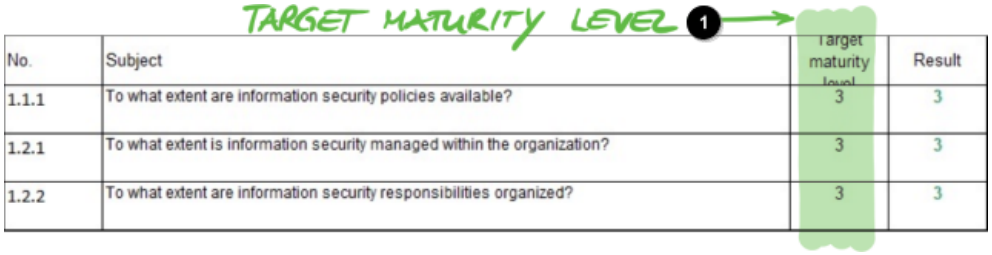
W poniższych punktach szczegółowo wyjaśniono wynik i jego analizę.

5.2.4.2. Docelowy poziom dojrzałości (na poziomie pytań)

ISA określa „docelowy poziom dojrzałości” 3 dla każdego pytania.

Bardziej szczegółowe informacje na temat definicji każdego poziomu dojrzałości znajdują się w Punkt 5.2.2, “Rozumienie dokumentu ISA”.

ISA określa docelowe poziomy dojrzałości w arkuszu Excel „Wyniki (ISA5)” (począwszy od kolumny G, wiersz 22; patrz poniższy rysunek).



No.	Subject	Target maturity level	Result
1.1.1	To what extent are information security policies available?	3	3
1.2.1	To what extent is information security managed within the organization?	3	3
1.2.2	To what extent are information security responsibilities organized?	3	3

Rysunek 18. Definicja docelowego poziomu dojrzałości w arkuszu Excel „Wyniki (ISA5)”

1 Docelowy poziom dojrzałości

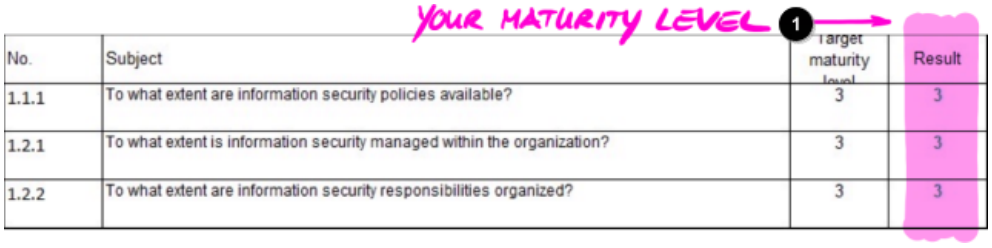
5.2.4.3. Państwa wynik (na poziomie pytań)

Aby otrzymać etykiety TISAX, zwykle potrzebują Państwo dla każdego pytania poziomów dojrzałości co najmniej równych docelowemu poziomowi dojrzałości.

Przykład: jeśli docelowy poziom dojrzałości dla pytania X wynosi „3”, Państwa poziom dojrzałości dla tego pytania powinien wynosić co najmniej „3”. Jeśli Państwa poziom dojrzałości dla tego pytania jest niższy niż „3”, mogą Państwo nie dostać etykiet TISAX.

Tak samo jest w przypadku wszystkich pytań. Jeśli docelowy poziom dojrzałości dla dwóch pytań wynosi „3”, nie mogą Państwo skompensować poziomu dojrzałości „2” dla jednego pytania poziomem dojrzałości „4” dla drugiego.

Dokument ISA automatycznie przenosi Państwa poziomy dojrzałości z arkusza Excel „Bezpieczeństwo informacji” (kolumna E) do arkusza „Wyniki (ISA5)” (począwszy od kolumny H, wiersz 23):



No.	Subject	Target maturity level	Result
1.1.1	To what extent are information security policies available?	3	3
1.2.1	To what extent is information security managed within the organization?	3	3
1.2.2	To what extent are information security responsibilities organized?	3	3

Rysunek 19. Państwa poziomy dojrzałości w arkuszu Excel „Wyniki (ISA5)”

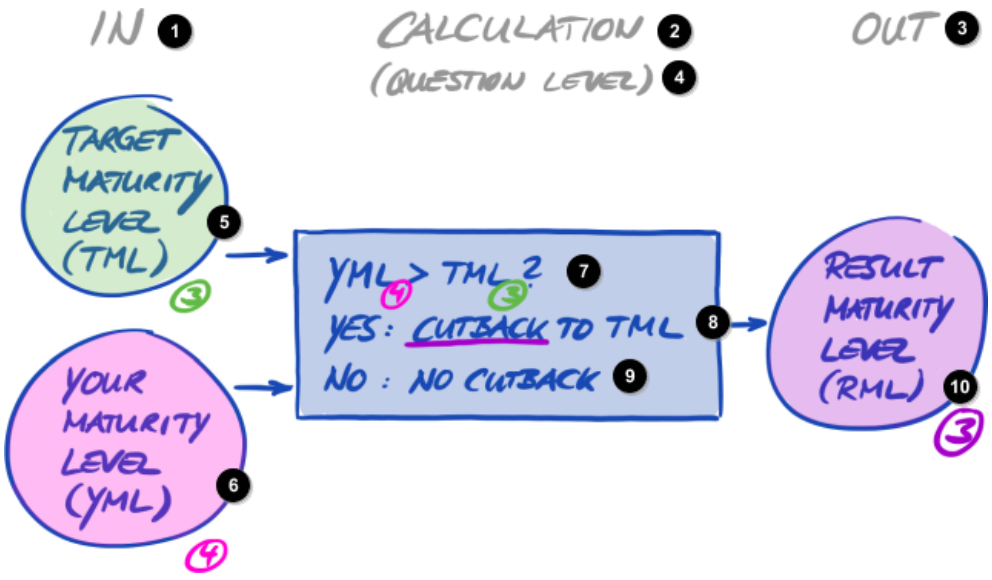
1. Państwa docelowy poziom dojrzałości

Państwa poziom dojrzałości oblicza się, zanim dokument ISA podsumuje go w Państwa punktacji. Zasadniczo Państwa poziom dojrzałości „koryguje się” do docelowego poziomu dojrzałości. Dzięki temu pytania, dla których Państwa poziom dojrzałości jest *wyższy* od docelowego poziomu dojrzałości nie kompensują pytań, dla których Państwa poziom dojrzałości jest *niższy* od docelowego poziomu dojrzałości.

Oto w jaki sposób ISA oblicza Państwa wynik na poziomie pytań:

- Porównuje Państwa poziom dojrzałości z docelowym poziomem dojrzałości pytania.
- Jeśli Państwa poziom dojrzałości jest wyższy od docelowego poziomu dojrzałości, „koryguje go” do docelowego poziomu dojrzałości.
- Jeśli Państwa poziom dojrzałości jest niższy niż Państwa docelowy poziom dojrzałości lub mu równy, dla danego pytania nie zachodzą żadne zmiany.

Przykład (patrz poniższy rysunek): docelowy poziom dojrzałości wynosi „3”. Państwa poziom dojrzałości wynosi „4”. Państwa „wynik skorygowany” dla tego pytania wyniesie „3”.

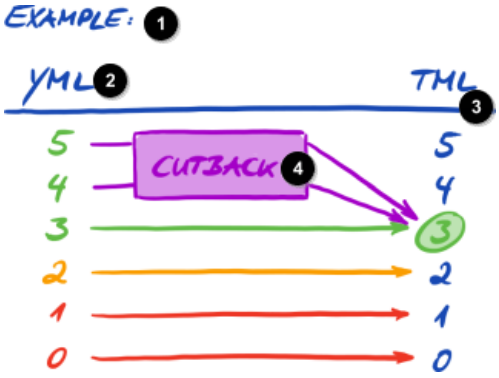


Rysunek 20. Skorygowane obliczenie poziomu dojrzałości wyniku

1. Dane wej.
2. Obliczenie
3. Dane wyj.
4. (Poziom pytań)
5. Docelowy poziom dojrzałości (TML)
6. Państwa poziom dojrzałości (YML)

7. YML > TML?
8. Tak: Korekta do TML
9. Nie: Brak korekty
10. Poziom dojrzałości wyniku (RML)

Poniższy rysunek pokazuje, że jeśli Państwa poziom dojrzałości jest wyższy od docelowego poziomu dojrzałości, ISA skoryguje go w dół (kolory zielony, pomarańczowy i czerwony odpowiadają kolorom zastosowanym w kolumnie „Wynik", patrz Rysunek 19, "Państwa poziomy dojrzałości w arkuszu Excel „Wyniki (ISA5)"").



Rysunek 21. Ilustracja przedstawiająca korektę z kolorami używanymi w arkuszu Excel „Wyniki (ISA5)"

1. Przykład:
2. YML
3. TML
4. Korekta

Poniżej znajduje się kolejny sposób przedstawienia poziomów dojrzałości na poziomie pytań. Kolory kółek ilustrują docelowy poziom dojrzałości lub „odległość" do niego (np. kółko ma kolor pomarańczowy, kiedy poziom dojrzałości wynosi „-1" względem docelowego poziomu dojrzałości). Symbole zaznaczenia wskazują Państwa poziom dojrzałości.

Rysunek 22. Poziomy dojrzałości na poziomie pytań

1. Poziom dojrzałości
2. Pytanie
3. Korekta
4. Docelowy poziom dojrzałości (TML)
5. Co najmniej jeden powyżej TML
6. Jeden poniżej TML
7. Co najmniej dwa poniżej TML
8. Państwa poziom dojrzałości (YML)
9. Korekta do TML

Uwaga:

Pomyślny wynik oceny TISAX można uzyskać nawet przy braku uzyskania docelowego poziomu dojrzałości dla wszystkich pytań. w takich przypadkach główne pytanie brzmi, czy posiadają Państwo ryzyko. Jeśli poziom dojrzałości jest niższy od wartości docelowej, lecz nie ma ryzyka, może to wystarczyć.

5.2.4.4. Wartość docelowa (na poziomie punktacji)

ISA określa „idealny” ogólny poziom dojrzałości — „maksymalną punktację” (lub „Maksymalny wynik”, komórka G6).

Information Security Assessment Results

VDA Verband der Automobilindustrie

Result with cutback to target maturity level:	3,00	Maximum score:	3,00

MAXIMUM RESULT SCORE

Details:

No.	Subject	Target maturity level	Result 1
1.1.1	To what extent are information security policies available?	3	3
1.2.1	To what extent is information security managed within the organization?	3	3
1.2.2	To what extent are information security responsibilities organized?	3	3

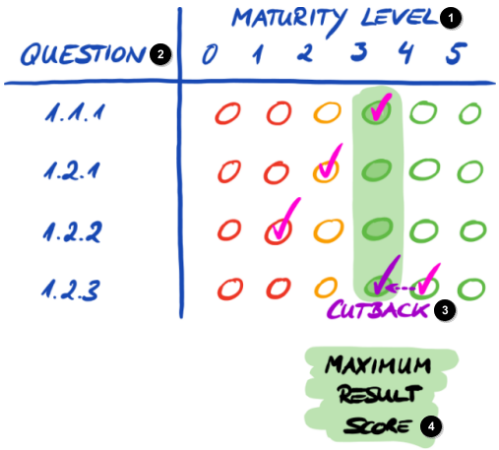
Rysunek 23. Maksymalna punktacja (arkusz Excel „Wyniki (ISA5)”)

1. Maksymalna punktacja

W teorii ten ogólny poziom dojrzałości jest średnią wszystkich docelowych poziomów dojrzałości (na poziomie pytań). Dawałoby to maksymalną punktację „3,0”.

Jednakże „3,0” jest jedynie w przypadku, gdy do Państwa sytuacji odnoszą się wszystkie pytania. Jeśli jednak do Państwa sytuacji nie odnosi się jakieś pytanie, średnia się zmienia, a maksymalna punktacja jest niższa od „3,0”.

Na podstawie powyższego widoku (Rysunek 22, “Poziomy dojrzałości na poziomie pytań”), poniżej mogą Państwo sprawdzić, co wchodzi w skład średniej dla maksymalnej punktacji:



Rysunek 24. Maksymalna punktacja (na poziomie punktacji)

1. Poziom dojrzałości
2. Pytanie
3. Korekta
4. Maksymalna punktacja

5.2.4.5. Państwa wynik (na poziomie punktacji)

Państwa ogólna punktacja („Wynik skorygowany do docelowego poziomu dojrzałości”, komórka D6):

- podsumowuje ogólny poziom dojrzałości Państwa systemu zarządzania bezpieczeństwem informacji.
- jest średnią wszystkich Państwa poziomów dojrzałości (na poziomie pytań).
- może być niższa niż maksymalna punktacja lub jej równa.
- powinna być jak najbliższa maksymalnej punktacji. Im Państwa punktacja jest niższa od punktacji maksymalnej, tym niższe prawdopodobieństwo otrzymania etykiet TISAX.

Information Security Assessment Results

VDA Verband der Automobilindustrie

Result with cutback to target maturity level:	3,00	Maximum score:	3,00

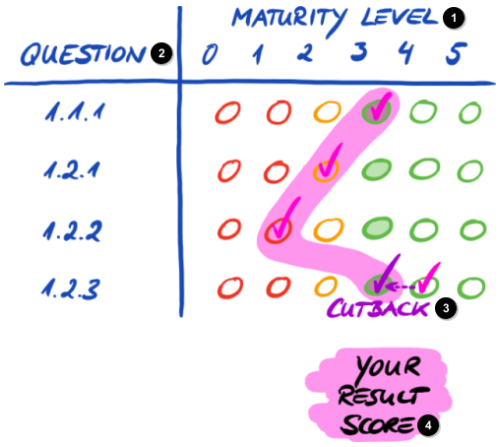
Details: YOUR RESULT SCORE ❶

No.	Subject	Target maturity level	Result
1.1.1	To what extent are information security policies available?	3	3
1.2.1	To what extent is information security managed within the organization?	3	3
1.2.2	To what extent are information security responsibilities organized?	3	3

Rysunek 25. Państwa punktacja (arkusz Excel „Wyniki (ISA5)”)

❶ Państwa punktacja

Na podstawie powyższego widoku (Rysunek 22, “Poziomy dojrzałości na poziomie pytań”), poniżej mogą Państwo sprawdzić, co wchodzi w skład średniej dla punktacji:



Rysunek 26. Państwa punktacja (na poziomie punktacji)

❶ Poziom dojrzałości

❷ Pytanie

3 Korekta

4 Państwa punktacja

Punktacja wskazuje, czy Państwo:

- są gotowi do oceny TISAX.
- mogą liczyć na etykiety TISAX.

Jeśli Państwa punktacja („Wynik skorygowany do docelowych poziomów dojrzałości”) jest niższa od „3,0”, Państwa poziom dojrzałości nie odpowiada docelowemu poziomowi dojrzałości dla co najmniej jednego pytania. w takim przypadku prawdopodobnie muszą Państwo ulepszyć swój system zarządzania bezpieczeństwem informacji, zanim będą Państwo gotowi do oceny TISAX.

Uwaga:

Dla punktacji ogólnej istnieją formalne wartości graniczne dopuszczalnej „odległości” między Państwa punktacją a maksymalną punktacją („Wynik skorygowany do docelowych poziomów dojrzałości”).

Jeśli Państwa punktacja jest o ponad:

- 10% niższa, ogólny wynik oceny to „drobna niezgodność”.
- 30% niższa, ogólny wynik oceny to „poważna niezgodność”.

Ważna uwaga:

Uzyskanie punktacji („Wynik skorygowany do docelowych poziomów dojrzałości”) na poziomie „3” nie gwarantuje pomyślnego wyniku oceny TISAX bez ustaleń wykluczających. Proszę pamiętać, że dostawca usług audytu może na pewne kwestie patrzeć odmiennie od Państwa.

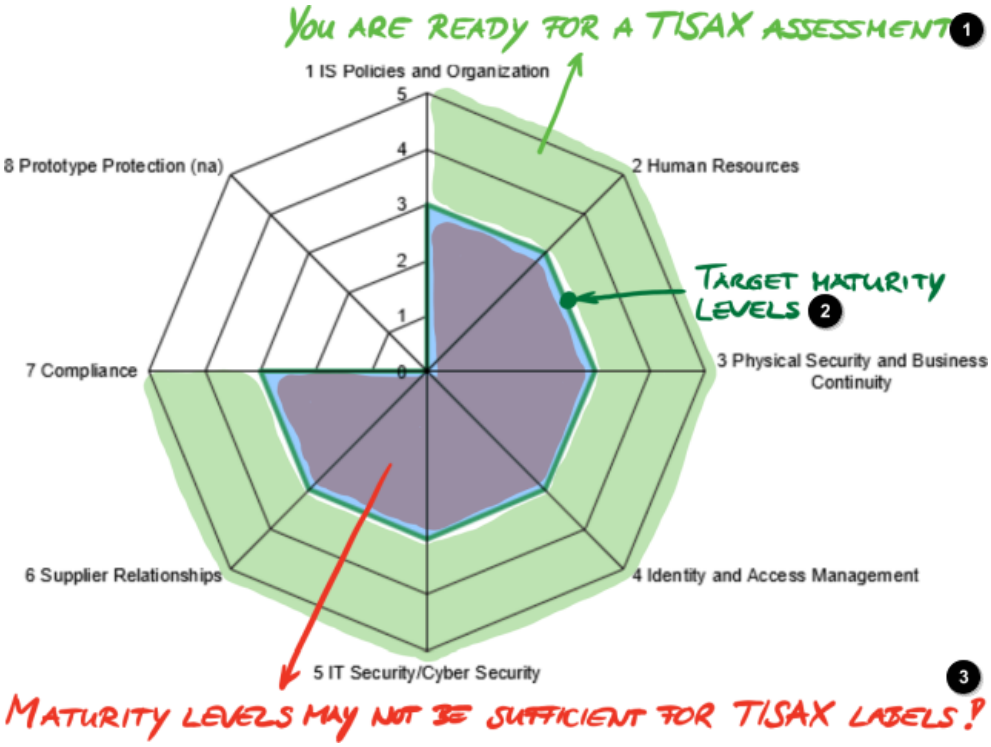
5.2.4.6. Czy są Państwo gotowi?

Celem powyższej analizy jest ustalenie Państwa gotowości do oceny TISAX.

Z całą pewnością są Państwo gotowi do oceny TISAX, jeśli Państwa punktacja („Wynik skorygowany do docelowych poziomów dojrzałości) wynosi „3,0” lub jest bliska tej wartości. w takim przypadku wszystkie wartości w kolumnie „Wyniki” (H) mają kolor zielony (nie pomarańczowy ani czerwony).

Jeśli nie są zielone, wynik samooceny wymaga podjęcia działań (patrz Punkt 5.2.5, “Działanie na podstawie wyniku samooceny”).

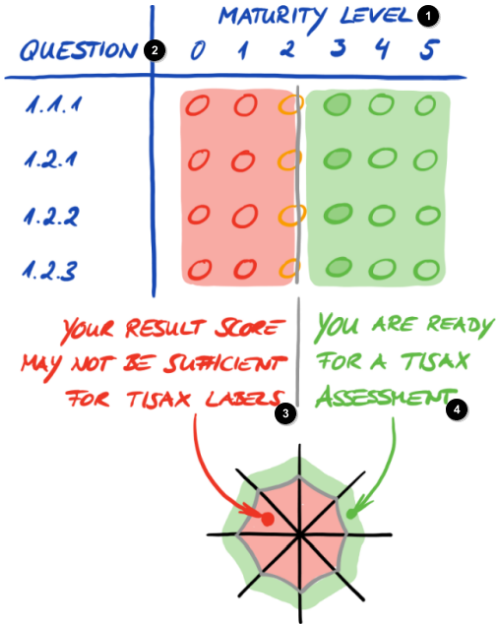
Poniższy rysunek przedstawia schemat „pajęczynę” ISA w arkuszu Excel „Wyniki (ISA5)”. Zielona linia wskazuje docelowy poziom dojrzałości dla rozdziału. Jeśli Państwa poziomy dojrzałości znajdują się na lub powyżej tej linii, są Państwo gotowi do oceny TISAX. Jeśli są poniżej tej linii, może to nie wystarczyć do otrzymania etykiet TISAX.



Rysunek 27. Zrzut ekranu: Realizacja docelowego poziomu dojrzałości na schemacie pajęczyny ISA (arkusz Excel „Wyniki (ISA5)”).

1. Są Państwo gotowi do oceny TISAX
2. Docelowe poziomy dojrzałości
3. Poziomy dojrzałości mogą nie wystarczyć na potrzeby etykiet TISAX!

Po „rozwinięciu” schematu pajęczyny ISA do poziomu pytań uzyskają Państwo podobny zielony /czerwony widok na poziomie pytań:



Rysunek 28. „Rozwinięcie" schematu pajęczyny ISA

1. Poziom dojrzałości
2. Pytanie
3. Państwa punktacja może nie wystarczyć do uzyskania etykiet TISAX
4. Są Państwo gotowi do oceny TISAX

5.2.5. Działanie na podstawie wyniku samooceny

Państwa wynik samooceny może wykazywać konieczność ulepszenia Państwa systemu zarządzania bezpieczeństwem informacji, zanim będą Państwo gotowi do otrzymania etykiet TISAX.

Być może wiedzą już Państwo, jak usunąć niektóre luki między Państwa poziomem dojrzałości a docelowym poziomem dojrzałości. w przypadku innych mogą Państwo potrzebować porad zewnętrznych. Wówczas mogą Państwo poprosić naszych dostawców usług audytu TISAX o usługi doradcze. TISAX umożliwia takie konsultacje, lecz ich nie wymaga. Przypominamy, że dostawca usług audytu, który świadczy na Państwa rzecz usługi doradcze, nie może prowadzić Państwa oceny TISAX.

Ważna uwaga:

Dla wielu firm najważniejszą przeszkodę stanowi *brak* podjęcia odpowiednich działań na podstawie wyniku samooceny *przed* rozpoczęciem oceny. Warto odpowiednio ocenić wysiłki niezbędne w celu uzyskania systemu zarządzania bezpieczeństwem informacji zgodnego z wymogami. Wiele firm musi formalnie utworzyć duży projekt w celu przygotowania się do oceny TISAX.

Uwaga:

Szukając pomocy zewnętrznej w przejściu procesu TISAX, znajdą Państwo szereg firm oferujących usługi konsultingowe i szkoleniowe. Żadna z nich nie jest związana z nami.

Obecnie:

- nie oferujemy oficjalnych szkoleń bezpośrednio ani za pośrednictwem osób trzecich.
- nie wydajemy jakichkolwiek oświadczeń dotyczących jakości usług osób trzecich, a tym samym zalecamy ostrożność.

Uwaga:

Odradzamy występowanie o lub zlecenia takich pozycji, jak „ocena początkowa” lub „analiza luk”. Choć rozumiemy chęć takiego przygotowania się do oceny, niemal zawsze lepiej od razu rozpocząć ocenę.

Bardziej szczegółowe wyjaśnienie przyczyn, dla których odradzamy oceny początkowe, znajduje się w Punkt 7.7, “Załącznik: Argumenty przeciwko „ocenom początkowym” i „analizom luk””.

5.3. Wybór dostawcy usług audytu

Ocenę TISAX mogą prowadzić wyłącznie dostawcy usług audytu, z którymi podpisaliśmy umowę[14]. Dostawcom usług audytu TISAX wolno prowadzić oceny TISAX Państwa firmy pod warunkiem braku jakichkolwiek wcześniejszych zleceń konsultingowych na Państwa rzecz.

Wszyscy nasi dostawcy usług audytu TISAX mają obowiązek prowadzić oceny TISAX jedynie dla firm będących zarejestrowanymi uczestnikami TISAX.

Ważna uwaga:

Po rejestracji zakresu oceny TISAX, *powinni* Państwo zacząć nawiązywać kontakt z naszymi dostawcami usług audytu. Czas realizacji usług zależeć będzie od ich dostępności. Kontakt z nimi *po* zakończeniu przez Państwa przygotowań może niepotrzebnie wydłużyć okres oczekiwania.

Uwaga:

Każdy zakres oceny przechodzi pewien cykl. Na tym etapie Państwa zakres oceny musi mieć status „Zatwierdzony” lub „Zarejestrowany”

> Bardziej szczegółowe informacje na temat statusu zakresu oceny znajdują się w Punkt 7.5.5, “Assessment scope status „Awaiting your payment” (Status zakresu oceny „Oczekujący na Państwa płatność”)”.

5.3.1. Dane kontaktowe

Po rejestracji zakresu oceny TISAX mogą Państwo nawiązać kontakt z wszystkimi dostawcami usług audytu TISAX i poprosić o oferty. Ich dane kontaktowe znajdują się w otrzymanej przez Państwa wiadomości e-mail z potwierdzeniem rejestracji[15] (patrz Punkt 4.5.8, “Wiadomość e-mail z potwierdzeniem”).

> Uwaga:
>
> Zapytanie ofertowe do naszych dostawców usług audytu TISAX można przesłać dopiero PO rejestracji. Dostawcy usług audytu sprawdzą, czy dokonano rejestracji. Mają obowiązek odrzucić wnioski bez rejestracji.
>
> Z tego samego powodu dane kontaktowe dostawców usług audytu otrzymują Państwo dopiero w wiadomości e-mail z potwierdzeniem rejestracji, a nie na ogólnodostępnej stronie internetowej.

5.3.2. Zakres terytorialny

Choć obecnie wielu naszych dostawców usług audytu ma siedzibę w Niemczech, wszyscy oni mogą prowadzić oceny TISAX na całym świecie. Większość z nich posiada nawet pracowników w wielu krajach.

Nasza strona internetowa zawiera podstronę, gdzie można wybrać kraj, a później sprawdzić, który dostawca usług audytu posiada miejscowych sprzedawców i/lub audytorów (enx.com/en-US/TISAX/xap/).

5.3.3. Zapytania ofertowe

Aby dostawcy usług audytu TISAX mogli precyzyjnie obliczyć nakład pracy związany z oceną, należy zawsze załączyć „Wyciąg z zakresu TISAX”.

Rysunek 29. Miniaturka wyciągu z zakresu (pierwsza strona)

Bardziej szczegółowe informacje znajdują się w Punkt 4.5.8, “Wiadomość e-mail z potwierdzeniem”.

Uwaga:

Do kluczowych cech naszych dostawców usług audytu TISAX należy bezstronność. Sprawdzą oni, czy nie występuje konflikt interesów. Przed kontaktem z nimi warto rozważyć tę kwestię. Jeśli Państwa firma ma jakiekolwiek powiązania z dostawcą usług audytu, nie może liczyć, że taki dostawca przeprowadzi jej ocenę.

5.3.4. Ocena ofert

Mogą Państwo wybrać dowolnego z naszych dostawców usług audytu TISAX. Wszyscy są związani taką samą umową. Wszyscy prowadzą oceny na podstawie tych samych kryteriów i za pomocą takich samych metod audytu. w kontekście wyniku audytu nie będzie różnic wynikających z wyboru takiego lub innego dostawcy usług audytu. Wszyscy uczestnicy TISAX zaakceptują Państwa wynik oceny.

Oprócz oczywistych czynników, takich jak cena, reputacja i sympatia, mogą Państwo zwrócić uwagę na następujące aspekty oferty:

- Dostępność:
  Kiedy może się zacząć proces oceny? Może to być ważny aspekt, jeśli chcą Państwo uzyskać ocenę TISAX w trybie pilnym.
- Koszty dojazdu na wizyty na miejscu:
  Dostawcy usług audytu posiadający biura w Państwa kraju mogą naliczać niższe koszty dojazdu.
- Język:
  Czy Państwo i każdy inny uczestnik rozmów z audytorem w Państwa firmie będą mogli się z nim porozumiewać w swoim języku ojczystym?
- Zakres oferty:

Jakie oceny wchodzą w zakres?
Bardziej szczegółowe informacje na temat ocen znajdują się w Punkt 5.4.3, “Rodzaje ocen TISAX”.
Zwykle oferty obejmują ocenę wstępną oraz ocenę planu działań korygujących. Ponieważ trudno przewidzieć nakład pracy podczas ocen kontrolnych, zwykle ofertę na nie składa się po zakończeniu pozostałych ocen.

Ostatecznie sprowadza się to do zaufania. Będą Państwo musieli nawiązać z dostawcą usług audytu relacje oparte na zaufaniu, ponieważ uzyska on wgląd w sprawy Państwa firmy.

Uwaga:

Odradzamy występowanie o lub zlecenia takich pozycji, jak „ocena początkowa” lub „analiza luk”. Choć rozumiemy chęć takiego przygotowania się do oceny, niemal zawsze lepiej od razu rozpocząć ocenę.

Bardziej szczegółowe wyjaśnienie przyczyn, dla których odradzamy oceny początkowe, znajduje się w Punkt 7.7, “Załącznik: Argumenty przeciwko „ocenom początkowym” i „analizom luk””.

Uwaga:

Choć chcielibyśmy wskazać kwoty wynagrodzenia pobieranego przez naszych dostawców usług audytu, prosimy o wyrozumiałość, ponieważ nie jesteśmy w stanie podać takich informacji. Koszty zależą od zbyt wielu czynników. Co więcej, dostawcy usług audytu mają swobodę naliczania stawek komercyjnych.

Możemy podać dość zgrubne szacunki dotyczące liczby roboczodni, za jakie naliczą wynagrodzenie nasi dostawcy usług audytu. w przypadku przeciętnej, małej firmy o jednej lokalizacji należy się spodziewać opłaty za trzy i pół do czterech roboczodni za ocenę na poziomie oceny 2 oraz pięciu do sześciu roboczodni za ocenę na poziomie oceny 3.

Uwaga:

Każda ocena przechodzi pewien cykl.

Bardziej szczegółowe informacje na temat statusu oceny znajdują się w Punkt 7.6, “Załącznik: Assessment status (Status oceny)”.

Po wyborze jednego z naszych dostawców usług audytu TISAX, mogą Państwo wreszcie rozpocząć proces oceny TISAX.

5.4. Proces oceny TISAX

5.4.1. Informacje ogólne

Proces oceny TISAX składa się z kilku rodzajów ocen. w większości przypadków będzie to więcej niż jedna ocena.

Proces oceny należy postrzegać jako sekwencję powiązanych ze sobą etapów, podczas których:

- Zapewniają Państwo optymalną formę systemu zarządzania bezpieczeństwem informacji.
- Dostawca usług audytu sprawdza, czy Państwa system zarządzania bezpieczeństwem informacji spełnia określony zestaw wymagań. Może znaleźć luki.
- Następnie Państwo usuwają luki w podanych terminach.
- Później dostawca usług audytu ponownie sprawdza, czy usunęli Państwo luki.

Te etapy powtarzają się do czasu usunięcia wszystkich luk.

Należy pamiętać, że to *Państwo* rozpoczynają każdy etap pomocniczy w procesie oceny. To Państwo kontrolują cały proces oceny. Tym samym w oczywisty sposób mogą Państwo w dowolnej chwili przerwać proces oceny i z niego zrezygnować.[16]

Proces oceny TISAX posiada następującą strukturę nadrzędną:

- Spotkanie inauguracyjne
  Wspólnie z dostawcą usług audytu planują Państwo szczegóły procesu oceny
- Faza 1 oceny
  Dostawca usług audytu sprawdza Państwa samoocenę
- Faza 2 oceny
  Dostawca usług audytu prowadzi ocenę/oceny.

5.4.2. Spotkanie inauguracyjne

Proces oceny TISAX rozpoczyna się spotkaniem inauguracyjnym. To czas planowania szczegółów procesu oceny. Spotkanie inauguracyjne odbywa się zwykle za pomocą telekonferencji. Dostawca usług audytu poprowadzi Państwa przez to spotkanie.

Program spotkania obejmuje, między innymi, następujące kwestie:

- Kim są uczestnicy spotkania?
- Jaka spółka jest przedmiotem oceny?
- Jak działa proces oceny TISAX?
- Jaki jest zakres oceny i czy jest właściwy?

- Nie ma konfliktów interesów?
- Jak wygląda dobra samoocena?
- Kto odpowiada za co?
- Jak się komunikujemy?
- Kiedy ma miejsce ocena (wraz z planowaniem innych terminów)?
- Kto musi uczestniczyć w ocenie/ocenach?
- z kim można kontaktować się w razie reklamacji?

Okres od spotkania inauguracyjnego do dostarczenia Państwa samooceny trwa zwykle od jednego do trzech miesięcy. Jednak nawet sześć miesięcy nie jest niczym niezwykłym. Okres zależy od poziomu Państwa przygotowań. TISAX nie określa długości tego okresu. Mogą Państwo dowolnie długo przygotowywać samoocenę oraz spółkę do oceny.

5.4.3. Rodzaje ocen TISAX

Proces oceny TISAX składa się z trzech poniższych rodzajów ocen TISAX:

- Ocena wstępna (Initial assessment)
- Ocena planu działań korygujących (Corrective action plan assessment)
- Ocena kontrolna (Follow-up assessment) [17]

Ocena początkowa występuje zawsze. Pozostałe dwie oceny TISAX mogą wystąpić i można je kilkakrotnie powtarzać. Będą się odbywać do czasu:

- usunięcia przez Państwa wszystkich luk
- lub opuszczenia przez Państwa procesu oceny TISAX
- lub zakończenia maksymalnego okresu dziewięciu miesięcy od końca spotkania kończącego ocenę wstępną (kiedy to konieczna jest kolejna ocena wstępna).

Wszystkie oceny TISAX opiszemy w dalszej części dokumentu.

Uwaga:

Każda ocena przechodzi pewien cykl.

Bardziej szczegółowe informacje na temat statusu oceny znajdują się w Punkt 7.6, “Załącznik: Assessment status (Status oceny)”.

5.4.4. Elementy oceny TISAX

Każda ocena TISAX składa się z następujących elementów:

- Formalne spotkanie otwierające[18][19]
  - Jego celem jest omówienie wszystkich kwestii organizacyjnych.
  - Nie musi to być spotkanie stacjonarne.
  - Te kwestie można omawiać podczas jednego spotkania lub w czasie kilku spotkań.
  - Jest to „kontener logiczny” na wszystkie organizacyjne tematy oceny *początkowej*.
- Procedura oceny
  - Dostawca usług audytu sprawdza wszystkie wymagania.
  - Metody oceny wybiera się zgodnie z danym poziomem oceny.
- Formalne spotkanie kończące[20]
  - Kończy ono ocenę TISAX.
  - Dostawca usług audytu przedstawia własne ustalenia.
  - Dostawca usług audytu przekazuje wynik oceny.
  - Nie musi to być spotkanie stacjonarne.
  - Jest to „kontener logiczny” na wszystkie organizacyjne kwestie *po* ocenie.

Po „spotkaniu kończącym” dostawca usług audytu opracowuje i wysyła Państwu projekt zaktualizowanego „raportu z oceny TISAX”. Jeśli Państwa zdaniem dostawca usług audytu coś błędnie zrozumiał, mogą Państwo zgłosić zastrzeżenia.[21] Następnie dostawca usług audytu wydaje ostateczny „raport z oceny TISAX”.

Wszystkie te elementy opiszemy w dalszej części dokumentu.

5.4.5. Informacje na temat zgodności

Zanim przejdziemy do dalszego opisu procesu oceny TISAX, pragniemy wyjaśnić Państwu kluczowe pojęcie, które pozwoli Państwu zrozumieć kolejne punkty.

Celem oceny TISAX jest stwierdzenie, czy Państwa system zarządzania bezpieczeństwem informacji spełnia określony zestaw wymagań. Dostawca usług audytu sprawdza, czy Państwa system zarządzania bezpieczeństwem informacji „spełnia” (🇬🇧 „conforms”) wymagania.

Etap 1: Kontrole prowadzi się dla każdego obowiązującego wymagania oddzielnie.

Jeśli Państwa podejście „spełnia” wszystkie wymagania, pomyślnie przechodzą Państwo ocenę i otrzymują etykiety TISAX, które odpowiadają celom Państwa oceny.

Wszystko poniżej pełnej, czyli idealnej, zgodności z wymogami nazywa się ustaleniem (🇬🇧 finding). TISAX rozróżnia cztery rodzaje ustaleń:

Lp.	Rodzaj	Definicja	Reakcja	Przykłady
1.	*Poważna* niezgodność (*Major* non-conformity)	*Poważna* niezgodność: ▪ powoduje znaczne, bezpośrednie ryzyko dla bezpieczeństwa Państwa informacji ▪ **lub** powoduje wątpliwości dotyczące ogólnej skuteczności Państwa systemu bezpieczeństwa informacji	Mają Państwo obowiązek: ▪ bezzwłocznie zająć się *poważnymi* niezgodnościami przy użyciu odpowiednich środków kompensujących, ▪ bez zbędnej zwłoki wdrożyć działania korygujące	▪ Niezgodności systemowe ▪ Niedociągnięcia wdrożenia, które prowadzą do powstania krytycznego ryzyka dla bezpieczeństwa informacji poufnych ▪ Niedociągnięcia wdrożenia, które nie zostały usunięte przy pomocy odpowiednich działań korygujących
2.	*Drobna* niezgodność (*Minor* non-conformity)	*Drobna* niezgodność: ▪ *nie* powoduje znacznego, bezpośredniego ryzyka dla bezpieczeństwa Państwa informacji ▪ **ani** *nie* powoduje wątpliwości dotyczących ogólnej skuteczności Państwa systemu bezpieczeństwa informacji	Mają Państwo obowiązek: ▪ bez zbędnej zwłoki wdrożyć działania korygujące	▪ Błędy odosobnione lub sporadyczne ▪ Niezgodność lub niedociągnięcia wdrożenia wymogów lub zasad

Lp.	Rodzaj	Definicja	Reakcja	Przykłady
3.	Spostrzeżenie (Observation)	Spostrzeżenie to niezgodność z wymogami Państwa zasad, która nie stwarza bezpośredniego ryzyka dla bezpieczeństwa Państwa informacji, choć może się to zdarzyć w przyszłości.	Mają Państwo obowiązek: ▪ uważnie zbadać, monitorować i oceniać ewentualne ryzyko ▪ określić sposób postępowania w przypadku spostrzeżenia	nd.
4.	Pole do poprawy (Room for improvement)	Odstępstwo, które nie należy do powyższych rodzajów ani nie stwarza ryzyka dla bezpieczeństwa Państwa informacji, a mimo to stanowi wyraźne pole do poprawy.	Mogą Państwo podjąć decyzję, czy chcą się Państwo zająć tym ustaleniem i w jaki sposób.	nd.

Tabela 11. Cztery rodzaje ustaleń

Etap 2: Wszystkie wyniki poprzedniego kroku „zgodności z wymogami” łączy się w całkowity wynik oceny.

Całkowity wynik oceny może mieć postać:

a. Spełnia (Conform)
Całkowity wynik oceny to „spełnia”. Spełniono wszystkie wymagania.

b. Drobna niezgodność (Minor non-conform)
Całkowity wynik oceny to „drobna niezgodność”, jeśli dla co najmniej jednego wymagania uzyskano „drobną niezgodność”.

c. Poważna niezgodność (Major non-conform)
Całkowity wynik oceny to „poważna niezgodność”, jeśli dla co najmniej jednego wymagania uzyskano „poważną niezgodność”.
(Pod nieobecność zatwierdzonego planu działań korygujących, każda niezgodność prowadzi do całkowitego wyniku oceny „poważna niezgodność”.)

Jeśli Państwa całkowity wynik oceny to:

- „drobna niezgodność”, mogą Państwo otrzymać *tymczasowe* etykiety TISAX do czasu usunięcia wszystkich niezgodności.
- „poważna niezgodność”, przed otrzymaniem etykiet TISAX muszą Państwo usunąć dany problem.
  Za pomocą odpowiednich środków kompensujących i działań korygujących zatwierdzonych przez dostawcę usług audytu można zmienić całkowity wynik oceny z „poważnej niezgodności” na „drobną niezgodność”, a tym samym otrzymać tymczasowe etykiety TISAX.

Należy pamiętać, że Państwa całkowity wynik oceny poprawi się w trakcie całego procesu oceny TISAX.

Oto uproszczony przykład: Ocena wstępna przyniosła całkowity wynik oceny „poważna niezgodność”. Później zmniejszają Państwo związane z nią ryzyko. To zmienia Państwa całkowity wynik oceny z „poważnej niezgodności” na „drobną niezgodność”. Po eliminacji ryzyka Państwa końcowy całkowity wynik oceny to „spełnia”.

Poniżej wyjaśnimy to znacznie bardziej szczegółowo. Bardziej szczegółowe informacje na temat etykiet TISAX znajdą Państwo w dalszej części w Punkt 5.4.14, “Etykiety TISAX”.

5.4.6. Państwa przygotowania do procesu oceny TISAX

Dostawca usług audytu opracuje ocenę na podstawie Państwa samooceny. Dlatego też proszę uwzględnić konieczność wcześniejszego przekazania samooceny dostawcy usług audytu. Terminy takiego przekazania zostaną ustalone na spotkaniu inauguracyjnym.

Dobrze przygotowany dostawca usług audytu skróci czas niezbędny do przeprowadzenia oceny. Oprócz samooceny, przed rozpoczęciem oceny poprosi także o powiązane dokumenty. Mogą to być dokumenty przywołane przez Państwa w samoocenie lub inne dokumenty uznane za istotne przez dostawcę usług audytu.

Na podstawie tych informacji, Państwa dostawca usług audytu zaplanuje procedurę oceny.

5.4.7. Ocena wstępna

Jest to pierwsza ocena TISAX, która wyznacza formalne rozpoczęcie procesu oceny TISAX.

Ważna uwaga:

Ocena wstępna wyznacza początek dwóch ważnych okresów:

1. Maksymalny okres ważności etykiet TISAX wynosi trzy lata.
2. Na usunięcie niezgodności mają Państwo najwyżej dziewięć miesięcy. Jeśli w tym okresie nie usuną Państwo wszystkich niezgodności, nie otrzymają Państwo etykiet TISAX. Jeśli jednak nie zmieszczą się Państwo w tym terminie, mogą Państwo przejść bezpośrednio do kolejnej

oceny wstępnej.

Początkiem obu okresów jest dzień spotkania kończącego ocenę wstępną.

Uwaga:

Oprócz dwóch powyższych okresów nie ma innych ograniczeń czasowych. Na przykład ani zakończenie procesu rejestracji online, ani kontakt z naszymi dostawcami usług audytu, ani nawet przeprowadzenie spotkania inauguracyjnego nie pociąga za sobą żadnych terminów. Rozpoczęcie oceny wstępnej zależy od Państwa.

5.4.7.1. Pierwsze formalne spotkanie otwierające

Podobnie jak wszystkie oceny TISAX, ocena wstępna zaczyna się formalnym spotkaniem otwierającym. Formalne spotkanie otwierające prowadzone jest zwykle w formie telekonferencji lub konferencji internetowej. w przypadku małych spółek, posiadających pewne doświadczenie zdobyte podczas wcześniejszych audytów, nie trwa ono długo.

To spotkanie ma następujące cele:

- sprawdzenie warunków wstępnych oceny
- przedstawienie lidera projektu oceny i zespołu oceny
- opracowanie planu oceny

5.4.7.2. Procedura oceny

Dostawca usług audytu prowadzi ocenę wstępną zgodnie z opracowanym planem. Szczegóły oceny zależą od Państwa celów oceny. Ocena obejmuje przede wszystkim telekonferencje, rozmowy na miejscu oraz kontrole na miejscu o różnym poziomie szczegółowości[22].

Dostawca usług audytu przedstawia wszystkie ustalenia podczas oceny wstępnej.

5.4.7.3. Spotkanie kończące

Podczas spotkania kończącego dostawca usług audytu ponownie podsumowuje wszystkie ustalenia.

5.4.7.4. Raport z oceny TISAX

Po spotkaniu kończącym dostawca usług audytu opracowuje i wysyła Państwu projekt „raportu z oceny TISAX”. Jeśli Państwa zdaniem dostawca usług audytu coś błędnie zrozumiał, mogą Państwo zgłosić zastrzeżenia.[23] Wówczas dostawca usług audytu wydaje „raport z oceny TISAX”.

Na tym etapie aktualny całkowity wynik oceny ma postać:

- Spełnia lub
- Poważna niezgodność
  Nieusunięte (drobne) niezgodności zawsze prowadzą do całkowitego wyniku oceny „poważna niezgodność”. Całkowity wynik oceny „drobna niezgodność” otrzymają Państwo dopiero po opracowaniu działań pozwalających wdrożyć środki w celu usunięcia niezgodności.
  Bardziej szczegółowe informacje na temat sposobu postępowania w tej kwestii znajdują się w Punkt 5.4.9.4, “Tymczasowe etykiety TISAX”.

Jeśli Państwa całkowity wynik oceny to „spełnia” już podczas oceny wstępnej, mogą Państwo pominąć dalszą część oceny i przejść do wymiany swojego wyniku.

Jeśli Państwa całkowity wynik oceny to „poważna niezgodność”, Państwa kolejnym zadaniem jest opracowanie planu podejścia do ustaleń oraz usunięcia luk stwierdzonych przez dostawcę usług audytu. Oficjalna nazwa tego planu to „plan działań korygujących” (🇬🇧 „corrective action plan”).

Uwaga:

Jeśli przed rozpoczęciem oceny będą Państwo świadomi sytuacji prowadzącej do niezgodności, której nie uda się Państwu usunąć przed oceną, mogą Państwo zaplanować działanie korygujące (z terminem realizacji) i przedstawić je dostawcy usług audytu podczas oceny. Teoretycznie może to prowadzić do całkowitego wyniku oceny „drobna niezgodność”. Byłaby to jednak *rzadka* sytuacja.

5.4.8. Opracowanie planu działań korygujących

Państwa „plan działań korygujących” (🇬🇧 „corrective action plan”) wskazuje plan postępowania w kontekście ustaleń z oceny wstępnej. Państwa dostawca usług audytu oceni właściwość Państwa „planu działań korygujących” (patrz kolejny punkt).

W celu opracowania „planu działań korygujących” należy uwzględnić następujące wymagania:

- Ustalenie
  - Muszą Państwo określić, do którego ustalenia odnosi się działanie korygujące.
- Przyczyna źródłowa
  - Muszą Państwo określić i wskazać przyczynę źródłową ustalenia.
- Działania korygujące
  - Dla każdej niezgodności muszą Państwo określić co najmniej jedno „działanie korygujące”, które wdroży środki zmierzające do usunięcia niezgodności.
- Data wdrożenia

- Dla każdego działania korygującego muszą Państwo określić datę wdrożenia.
- Okres wdrożenia powinien zapewniać wystarczający czas na dokładne wdrożenie środków.

- Środki kompensujące
  - w odniesieniu do wszystkich niezgodności prowadzących do powstania krytycznego ryzyka należy określić środki kompensujące w celu złagodzenia niezgodności do czasu wdrożenia działań korygujących.
- Okres wdrożenia
  - w przypadku wszystkich działań korygujących, których wdrożenie trwa ponad trzy miesiące, należy uzasadnić okres wdrożenia.
  - w przypadku wszystkich działań korygujących wymagających ponad sześciu miesięcy należy dodatkowo przedstawić dowody na potwierdzenie niemożności szybszego wdrożenia.
  - Okres wdrożenia działania korygującego nie może przekraczać dziewięciu miesięcy.

Po zakończeniu planu działań korygujących mogą Państwo wystąpić o „ocenę planu działań korygujących”.

Ważna uwaga:

Zalecamy jak najszybsze rozpoczęcie wdrożenia. Nie trzeba czekać na wynik „oceny planu działań korygujących”.
„Ocena planu działań korygujących” zwykle ma miejsce po przekazaniu dostawcy usług audytu swojego planu działań korygujących.

Uwaga:

TISAX posiada jedynie wymagania dotyczące treści, a nie formy planów działań korygujących.
Większość naszych dostawców usług audytu oferuje szablony na potrzeby planów działań korygujących.

5.4.9. Ocena planu działań korygujących

Celem „oceny planu działań korygujących” jest weryfikacja, czy Państwa „plan działań korygujących” (patrz powyżej) spełnia wymagania TISAX.

Przekazują Państwo „plan działań korygujących” swojemu dostawcy usług audytu. Państwa dostawca usług audytu ocenia plan zgodnie z wymogami (patrz poniżej). Jeśli Państwa plan spełnia wymagania, dostawca usług audytu wydaje zaktualizowany „raport z oceny TISAX”.

Taka ocena zwykle nie trwa zbyt długo. w większości przypadków będzie to telekonferencja lub

konferencja internetowa. Czasami przybiera postać wiadomości e-mail.

5.4.9.1. Powody oceny planu działań korygujących

Powody „oceny planu działań korygujących” są następujące:

- Niezgodności pozostałe po
  - ocenie wstępnej
  - ocenie kontrolnej
  - ocenie rozszerzenia zakresu
- „Plan działań korygujących”, który poddano ocenie, lecz który nie spełniał wymagań
- Zmiana czynników, na których opiera się obliczanie okresów wdrożenia planu działań korygujących

5.4.9.2. Połączenie z oceną wstępną

„Ocena planu działań korygujących” nie musi być niezależnym wydarzeniem. Swój „plan działań korygujących” mogą Państwo przedstawić już na spotkaniu kończącym ocenę wstępną. w takim przypadku dostawca usług audytu może bezpośrednio przeprowadzić „ocenę planu działań korygujących”.

Jeśli połączą Państwo „ocenę planu działań korygujących” z oceną wstępną, a Państwa „plan działań korygujących” spełni wymagania, mogą Państwo ustalić z dostawcą usług audytu brak konieczności „raportu z oceny wstępnej”. Zamiast niego Państwa dostawca usług audytu może opracować po prostu „raport z oceny planu działań korygujących”. Ten raport pozwala otrzymać tymczasowe etykiety TISAX.

5.4.9.3. Wymagania dotyczące planu działań korygujących

Dostawca usług audytu oceni Państwa „plan działań korygujących” na podstawie następujących wymagań:

- Odpowiednie środki
  - Dostawca usług audytu oceni, czy działanie korygujące jest odpowiednie, tj. czy usunie przyczynę źródłową niezgodności.
- Do zmniejszania krytycznego ryzyka służą odpowiednie środki kompensujące[24]
- Odpowiednie okresy wdrożenia
  - Okresy wdrożenia rozpoczynają się w dniu spotkania kończącego ocenę wstępną
- Żaden okres wdrożenia nie przekracza:
  - trzech miesięcy bez dodatkowego uzasadnienia
  - sześciu miesięcy bez dodatkowego uzasadnienia i dowodów

- dziewięciu miesięcy

5.4.9.4. Tymczasowe etykiety TISAX

Jeśli Państwa całkowity wynik oceny to „drobna niezgodność”, otrzymują Państwo tymczasowe etykiety TISAX.

Państwa partner zasadniczo akceptuje tymczasowe etykiety TISAX pod warunkiem, że w późniejszym terminie otrzymają Państwo stałe etykiety TISAX. Może się to przydać, kiedy muszą Państwo w trybie pilnym udowodnić partnerowi skuteczność własnego systemu zarządzania bezpieczeństwem informacji.

Warunkiem wstępnym otrzymania tymczasowych etykiet TISAX jest raport z oceny planu działań korygujących z całkowitym wynikiem oceny „drobna niezgodność”.

Tymczasowe etykiety TISAX są równe stałym etykietom TISAX. Jedyną różnicą jest krótszy okres ważności tymczasowych etykiet TISAX.

Tymczasowe etykiety TISAX mogą zachować ważność przez najwyżej dziewięć miesięcy od spotkania kończącego ocenę wstępną. Okres ważności tymczasowych etykiet TISAX zależy od najdłuższego okresu wdrożenia działań korygujących.

Przykłady:

- Posiadają Państwo tylko jedną niezgodność. Muszą Państwo przeprowadzić przegląd polityki. Związany z tym okres wdrożenia wynosi *dwa* miesiące.
  W takim przypadku Państwa tymczasowe etykiety TISAX są ważne przez *dwa* miesiące.
- Posiadają Państwo niezgodność wspomnianego przeglądu polityki. Na dodatek w odniesieniu do występującej niezgodności w ramach działania korygującego muszą Państwo zbudować nową ścianę. Ze względu na czas niezbędny do uzyskania od gminy wymaganych pozwoleń, związany z tym okres wdrożenia wynosi *osiem* miesięcy.
  W takim przypadku Państwa tymczasowe etykiety TISAX są ważne przez *osiem* miesięcy.

Bardziej szczegółowe informacje na temat wymogów dotyczących okresów wdrożenia znajdują się w Punkt 5.4.9.3, “Wymagania dotyczące planu działań korygujących”

Uwaga:

„Ocena planu działań korygujących” ma charakter opcjonalny.

Mogą Państwo przejść bezpośrednio do oceny kontrolnej, jeśli:

- nie potrzebują Państwo tymczasowych etykiet TISAX oraz
- mają Państwo pewność wdrożenia działań korygujących bez zatwierdzenia planu przez dostawcę usług audytu

Po zakończeniu wszystkich działań korygujących należy wystąpić o „ocenę kontrolną”.

5.4.10. Ocena kontrolna

„Ocena kontrolna” sprawdza, czy usunięto wszystkie stwierdzone wcześniej niezgodności. Zwykle o ocenę kontrolną występuje się w chwili, gdy istnieje pewność dotycząca usunięcia wszystkich niezgodności.

Można jednak poddać się dowolnej liczbie ocen kontrolnych. Jeśli podczas oceny kontrolnej dostawca usług audytu stwierdzi istniejące, a nawet nowe niezgodności, po prostu aktualizują Państwo swój plan działań korygujących i ponownie rozpoczynają tę część procesu oceny.

Ta ocena może mieć postać spotkania stacjonarnego, telekonferencji lub konferencji internetowej.

5.4.10.1. Ramy czasowe

Państwa dostawca usług audytu może przeprowadzić ocenę(-y) kontrolną(-e) w ciągu najwyżej dziewięciu miesięcy od zakończenia oceny wstępnej[25].

5.4.10.2. Warunki wstępne

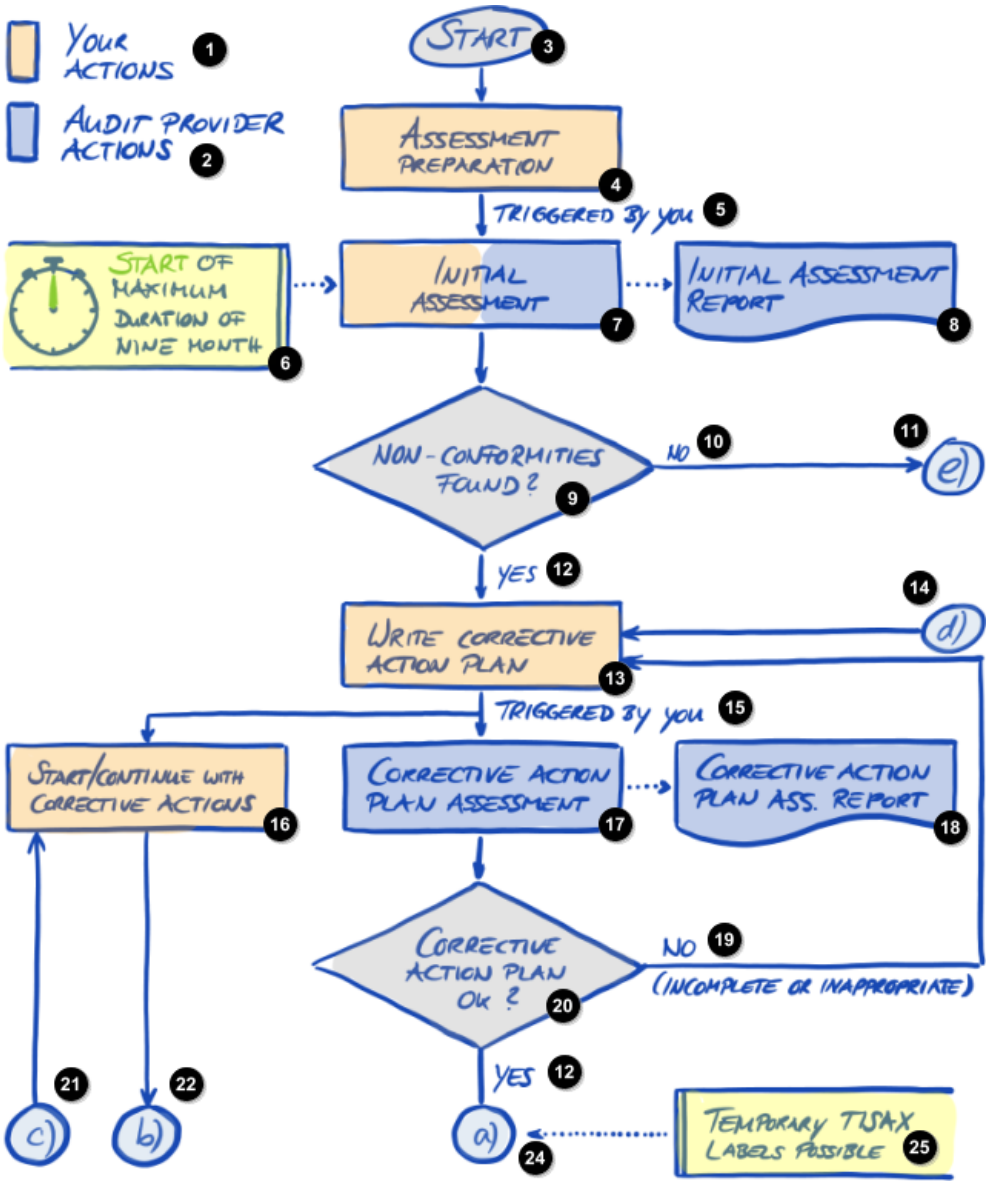
Jeśli nie potrzebują Państwo tymczasowych etykiet TISAX, mogą Państwo od razu poprosić o ocenę kontrolną. Przed oceną kontrolną nie jest potrzebna „ocena planu działań korygujących”.

5.4.10.3. Wygaśnięcie tymczasowych etykiet TISAX

Jeśli potrzebują Państwo tymczasowych etykiet TISAX, mogą Państwo sprawdzić, czy nie ma luk uniemożliwiających ich otrzymanie. w związku z tym zalecamy wystąpienie o ocenę kontrolną znacznie przed ostatecznym terminem[26]. Zapas czasu wynika z potrzeby usunięcia wszelkich drobnych ustaleń stwierdzonych podczas oceny kontrolnej.

5.4.11. Schemat procesu oceny TISAX

Poprzednie punkty podsumowano na poniższym schemacie procesu:



Rysunek 30. Schemat procesu oceny TISAX (część 1/2)

1. Państwa czynności
2. Czynności dostawcy usług audytu
3. Rozpoczęcie
4. Przygotowanie do oceny
5. Inicjowane przez Państwa
6. Rozpoczęcie maks. okresu dziewięciu miesięcy
7. Ocena wstępna
8. Raport z oceny wstępnej
9. Stwierdzono niezgodności?

10 Nie

11 e)

12 Tak

13 Opracowanie planu działań korygujących

14 d)

15 Inicjowane przez Państwa

16 Rozpoczęcie/kontynuacja z działaniami korygującymi

17 Ocena planu działań korygujących

18 Raport z oceny planu działań korygujących

19 Nie (niekompletny lub nieodpowiedni)

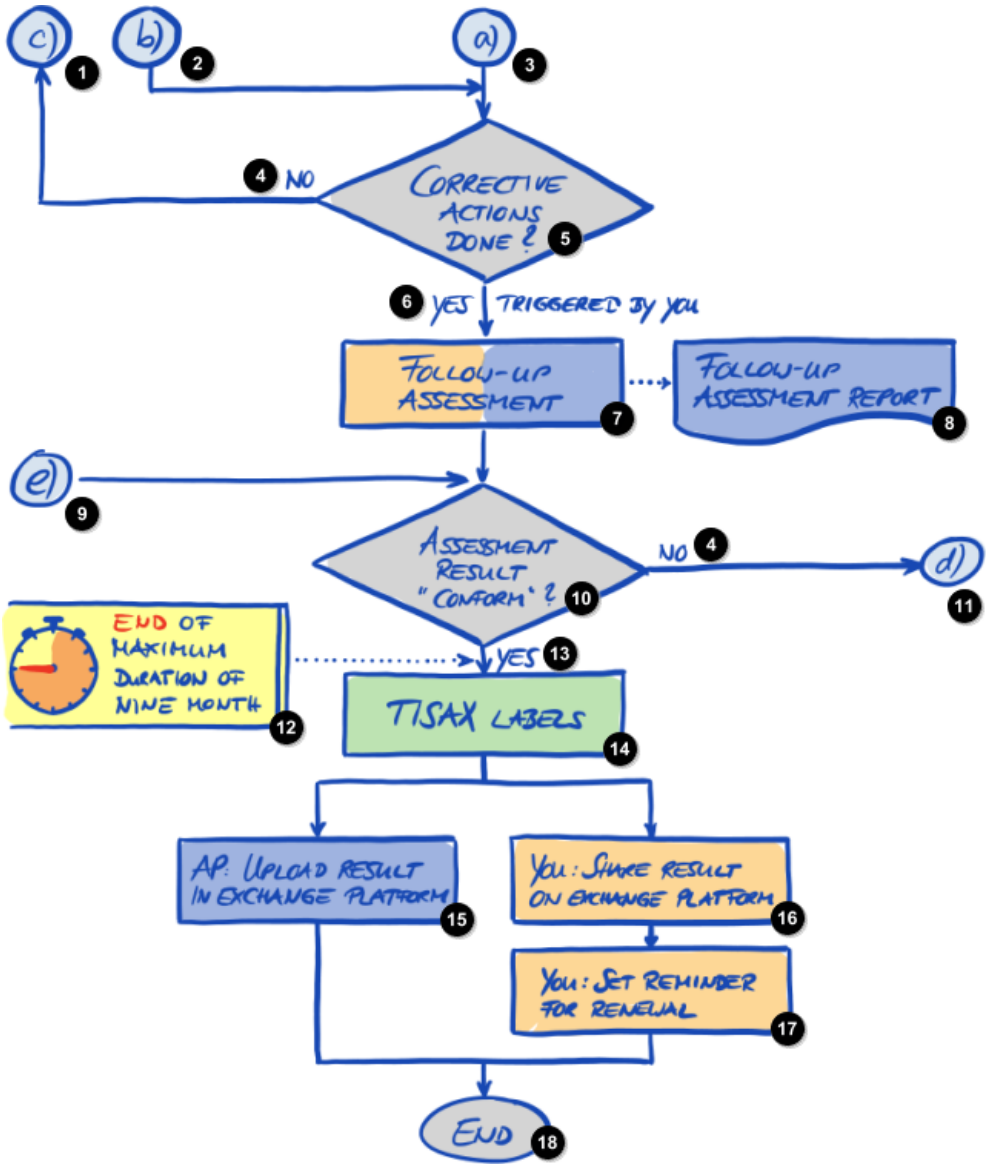
20 Plan działań korygujących w porządku?

21 c)

22 b)

24 a)

25 Możliwość otrzymania tymczasowych etykiet TISAX



Rysunek 31. Schemat procesu oceny TISAX (część 2/2)

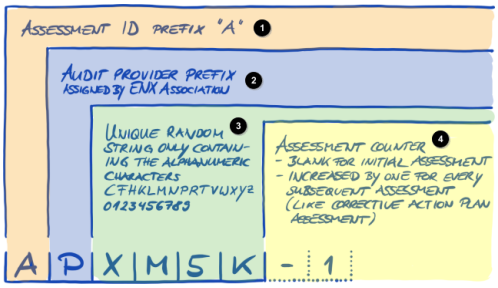
1. c)
2. b)
3. a)
4. Nie
5. Wykonano działania korygujące?
6. Tak, inicjowane przez Państwa
7. Ocena kontrolna
8. Raport z oceny kontrolnej
9. e)

10. Wynik oceny „spełnia”?
11. d)
12. Koniec maks. okresu dziewięciu miesięcy
13. Tak
14. Etykiety TISAX
15. Dostawca usług audytu: wczytuje wynik na platformę wymiany
16. Państwo: udostępniają wynik na platformie wymiany
17. Państwo: ustawiają przypomnienie o terminie odnowienia
18. Zakończenie

5.4.12. Assessment ID (Identyfikator oceny)

Każda ocena TISAX dotycząca zakresu oceny posiada „Identyfikator oceny”. Ten identyfikator odnosi się do Państwa wyniku oceny oraz odpowiadającego mu raportu z oceny TISAX.

Oto jak wygląda Identyfikator oceny:



Rysunek 32. Format Identyfikatora oceny

1. Prefiks „A” Identyfikatora oceny
2. Prefiks dostawcy usług audytu przypisany przez ENX Association
3. Unikalny ciąg losowy, zawierający jedynie znaki alfanumeryczne:
   CFHKLMNPRTVWXYZ
   0123456789
4. Licznik ocen
   – Puste dla oceny wstępnej
   – Zwiększane co jeden dla każdej kolejnej oceny (jak ocena planu działań korygujących)

Identyfikator oceny stosuje się zwykle podczas komunikacji dostawcy usług audytu z Państwem.

5.4.13. Raport z oceny TISAX

„Raport z oceny TISAX” (🇬🇧 „TISAX assessment report”):

- (aktualizuje i) wydaje się po każdej ocenie TISAX.
- dokumentuje ustalenia Państwa dostawcy usług audytu.
- zawiera całkowity wynik oceny (spełnia, drobna niezgodność, poważna niezgodność).
- zawiera wszystkie inne informacje związane z Państwa oceną TISAX (w tym cel oceny, zakres, zaangażowane osoby i lokalizacje).

„Raport z oceny TISAX” może należeć do jednego z poniższych rodzajów (zależnie od rodzaju oceny):

- Raport z oceny *wstępnej* (🇬🇧 *Initial* assessment report)
- Raport z oceny *planu działań korygujących* (🇬🇧 *Corrective action plan* assessment report)
- Raport z oceny *kontrolnej* (🇬🇧 *Follow-up* assessment report) [27]

„Raport z oceny TISAX” zawsze ma taką samą strukturę[28]. Po każdym rodzaju oceny dostawca usług audytu po prostu poszerza ten szablon. Oznacza to, że zajmują się Państwo jedynie ostatnią wersją raportu z oceny TISAX, która zawsze zawiera treść poprzednich wersji.

Partnerowi mają Państwo obowiązek udostępnić pierwsze punkty „raportu z oceny TISAX”.

Jedną z najważniejszych cech TISAX jest możliwość podjęcia samodzielnej decyzji, jakie części raportu z oceny TISAX chcą Państwo udostępnić partnerowi lub dowolnemu innemu uczestnikowi. Konstrukcja raportu z oceny TISAX umożliwia taką formę wybiórczego udostępniania. Każdy punkt rozszerza poziom szczegółowości.

Poniżej przedstawiamy strukturę „raportu z oceny TISAX”:

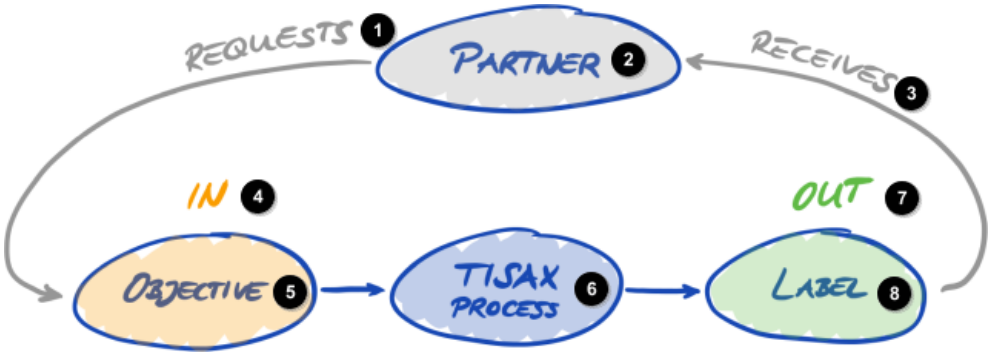
- A. Informacje związane z oceną
  Nazwa spółki, zakres oceny, Identyfikator zakresu, Identyfikator oceny, poziom oceny, cel(e) oceny, data(-y) oceny, dostawca usług audytu
  Ten punkt nie zawiera wyniku oceny.
- B. Wyniki zbiorcze
  Przeznaczone dla kadry kierowniczej zestawienie wyniku oceny (spełnia, drobna niezgodność, poważna niezgodność), liczba ustaleń, abstrakcyjna kategoryzacja wynikającego z tego ryzyka
- C. Podsumowanie wyniku oceny
  Podsumowanie wyniku oceny z podziałem na rozdziały (np. „9 Kontrola dostępu”) oraz katalogi kryteriów (np. „Bezpieczeństwo informacji”)
- D. Poziomy dojrzałości ISA VDA (zakładka Wyniki)
  Poziom dojrzałości dla każdego wymagania

- E. Szczegółowe wyniki oceny
  Szczegółowy opis wszystkich ustaleń, związanych z nimi wyników oceny ryzyka, wymaganych środków, okresu wdrożenia

Na etapie „wymiany” (szczegółowo opisanym poniżej) decydują Państwo, do jakiego poziomu Państwa partner zyska dostęp do treści Państwa raportu z oceny TISAX.

5.4.14. Etykiety TISAX

Ten temat pokrótce omówiliśmy w punkcie poświęconym przygotowaniom do rejestracji. Jak wyjaśniono, wcześniejszy cel oceny staje się teraz etykietą TISAX.



Rysunek 33. Cele oceny i etykiety TISAX

1. Żąda
2. Partner
3. Otrzymuje
4. DANE WEJ.
5. Cel
6. Proces TISAX
7. DANE WYJ.
8. Etykieta

Etykiety TISAX:

- są wynikiem procesu oceny TISAX.
- podsumowują Państwa wynik oceny.
- stanowią oświadczenie, że Państwa system zarządzania bezpieczeństwem informacji spełnia określony zestaw wymagań.

Wykorzystanie etykiet TISAX ułatwia związaną z TISAX komunikację z partnerem oraz dostawcami usług audytu TISAX, ponieważ odnoszą się one do określonych danych

wyjściowych procesu oceny TISAX.

5.4.14.1. Hierarchia etykiet TISAX

Cele oceny i odpowiadające im etykiety TISAX są powiązane w dość prosty sposób. Trzeba jednak pamiętać o jeszcze jednej ważnej rzeczy: *niektóre* etykiety TISAX są związane z hierarchią. Oznacza to, że otrzymując daną etykietę TISAX, automatycznie otrzymują Państwo wszystkie etykiety TISAX „niższego” rzędu.

Przykład: w przypadku celu oceny „Very high availability” otrzymują Państwo odpowiadającą mu etykietę TISAX „Very high availability”. Ponieważ jednak cel oceny „Very high availability” stanowi nadzbiór „High availability”, automatycznie otrzymują Państwo także etykietę TISAX „High availability”.

Obecnie w przypadku etykiet TISAX obowiązuje następująca hierarchia:

- „Info high” jest nadzbiorem „Confidential” i „High availability”.
- „Info very high” jest nadzbiorem „Strictly confidential” i „Very high availability”.
- „Strictly confidential” jest nadzbiorem „Confidential”.
- „Very high availability” jest nadzbiorem „High availability”.
- „Special data” jest nadzbiorem „Data”.

Uwaga:

Etykiety TISAX można otrzymać także ze skutkiem wstecznym. Kiedy wprowadzamy nową etykietę będącą podzbiorem otrzymanych przez Państwa etykiet TISAX, automatycznie otrzymują Państwo nową etykietę.

Przykład: etykietę TISAX „Info high” otrzymali Państwo w czasie, gdy nie istniała jeszcze etykieta „High availability”. Po wprowadzeniu etykiety High availability, nasz system automatycznie przypisał ją do Państwa.

Tą hierarchię można określić przez porównanie odpowiednich wymagań wskazanych w Tabela 8, “Wymogi obowiązujące w przypadku celów oceny”.

Nie każdemu uczestnikowi może się to wydawać ważne. Wyobraźmy sobie jednak, że jeden partner żąda od Państwa okazania etykiety TISAX „Very high availability”, a drugi „High availability”. w takim przypadku posiadanie obu etykiet TISAX ułatwia wszystkim życie, ponieważ nie trzeba wiedzieć, że „High availability” stanowi podzbiór „Very high availability”. Szczególnie prawdziwe może to być w przypadku partnerów, u których posiadanie określonych etykiet TISAX jest elementem rygorystycznego procesu zakupów. Zwykle nikt nie ma ochoty wyjaśniać, że „Very high availability” jest „lepsza” od „High availability”. Można po prostu przedstawić wszystkie posiadane etykiety TISAX, a osoba prowadząca ocenę może odhaczyć wymóg „musi posiadać etykietę TISAX «High availability»”.

5.4.14.2. Okres ważności etykiet TISAX

Etykiety TISAX zasadniczo zachowują ważność przez trzy lata. Okres ważności rozpoczyna się z końcem procesu oceny (jeszcze przed wydaniem raportu z oceny TISAX).

Okres ważności etykiet może być krótszy w przypadku istotnych zmian zakresu oceny TISAX.

Przykłady: przeniesienie firmy, nowe lokalizacje. (Instrukcje dotyczące sposobu postępowania w takich przypadkach znajdują się w Punkt 7.9.3.2, “Wniosek o zmianę lokalizacji” oraz Punkt 7.9.3.4, “Dodawanie kolejnej lokalizacji”.)

Uwaga:

Posiadane etykiety TISAX można wyświetlić jedynie na portalu ENX. Nie ujmuje się ich w raporcie z oceny TISAX.

5.4.14.3. Odnowienie etykiet TISAX

Aby zachować etykiety TISAX na długi czas, trzeba je odnawiać[29] co trzy lata.

Oznacza to właściwie konieczność ponownego przejścia procesu TISAX (rejestracji zakresu oceny, ponownego poddania się ocenie TISAX, udostępnienia wyniku oceny). Rejestracja jest nieco prostsza, ponieważ nie ma potrzeby ponownego tworzenia spółki jako uczestnika TISAX. Można wykorzystać ponownie wszystkie osoby do kontaktu i lokalizacje zapisane w bazie danych TISAX.

Ważna uwaga:

PRZED kontaktem z dostawcą usług audytu proszę zarejestrować NOWY zakres. Państwa dostawca usług audytu może rozpocząć nowy proces oceny jedynie pod warunkiem, że podadzą mu Państwo nowy Identyfikator zakresu.

W większości przypadków rejestracja nowego zakresu jest łatwa. Trzeba po prostu przypisać nową nazwę zakresu, dodać osoby do kontaktu, wybrać cel(e) oceny i dodać lokalizacje. Można ponownie wykorzystać osoby do kontaktu oraz lokalizacje wprowadzone do systemu dla dowolnego wcześniej zarejestrowanego zakresu.

Ważna uwaga:

Prosimy o wykorzystanie istniejących rejestrów lokalizacji utworzonych i używanych podczas rejestracji poprzedniego zakresu. Nie należy tworzyć nowego rejestru lokalizacji o tym samym adresie.

Wynika to z faktu, że niektórzy uczestnicy TISAX automatycznie przetwarzają

wyniki oceny swoich partnerów. Synchronizują własny system z portalem ENX. Nawet niewielkie różnice mogą uniemożliwić pomyślną synchronizację. Co więcej, pozwala to uniknąć zaśmiecania danych uczestników zbędnymi powieleniami.

Ważna uwaga:

Jeśli w stosunkach z partnerem istnieje wymóg posiadania ważnych etykiet TISAX, gorąco zachęcamy do ustawienia w kalendarzu przypomnienia o konieczności rozpoczęcia niezbędnego procesu odnowienia.

Sugerujemy, by odnowienie rozpocząć na co najmniej rok przed wygaśnięciem etykiet TISAX.

Po otrzymaniu etykiet TISAX mogą Państwo przejść do ostatniego etapu i udostępnić je partnerowi.

6. Wymiana (Etap 3)

Szacowany czas czytania punktu poświęconego wymianie wynosi 7 minut.

Choć przeszli Państwo proces TISAX, Państwa partner nie widział jeszcze żadnego „dowodu”, że Państwa system zarządzania bezpieczeństwem informacji jest w stanie zapewnić ochronę danych poufnych partnera. w tym punkcie opisano sposób udostępniania partnerowi wyniku oceny oraz przedstawienia żądanego dowodu.

6.1. Założenie

Jedną z kluczowych cech TISAX jest fakt, że Państwa wynik oceny jest w pełni pod Państwa kontrolą. Bez uzyskania Państwa wyraźnej zgody nikomu nie udostępniamy informacji związanych z Państwa oceną.

6.2. Platforma wymiany

Platformę wymiany stanowi portal ENX.

Państwa dostawca usług audytu wczyta dwa pierwsze punkty (A i B) Państwa raportu z oceny TISAX. Na tym etapie, dostępu do tych informacji nie ma nikt poza Państwem.

Aby uzyskać dostęp do portalu i korzystać z platformy wymiany, mogą Państwo użyć konta utworzonego podczas rejestracji.

Dostęp do portalu mogą Państwo uzyskać pod tym adresem:
enx.com/en-US/SignIn

6.3. Ogólne warunki wstępne

Wynik oceny mogą Państwo udostępnić partnerowi pod warunkiem spełnienia tych dwóch warunków wstępnych:

1. Państwa dostawca usług audytu przesłał wynik oceny na platformę wymiany.
   Wynik oceny będzie dostępny na platformie wymiany zwykle po upływie 5–10 dni roboczych od wydania raportu z oceny TISAX.
2. Uiścili Państwo opłatę (jeżeli dotyczy).

Po spełnieniu obu warunków wstępnych Państwa zakres oceny ma status „Aktywny”.

Uwaga:

Każdy zakres oceny przechodzi pewien cykl. Na tym etapie Państwa zakres oceny musi mieć status „Aktywny”.

> Bardziej szczegółowe informacje na temat statusu zakresu oceny znajdują się w Punkt 7.5.5, “Assessment scope status „Awaiting your payment” (Status zakresu oceny „Oczekujący na Państwa płatność”)”.

Aby sprawdzić, czy wynik Państwa oceny jest gotowy do udostępniania (status zakresu oceny = Aktywny), należy wykonać następujące czynności:

1. Zalogować się na portalu ENX.
2. Przejść do głównego paska nawigacji i zaznaczyć „MY TISAX” („MÓJ TISAX”).
   . w rozwijanym menu zaznaczyć „SCOPES AND ASSESSMENTS” („ZAKRESY I OCENY”).
3. Przejść do tabeli i znaleźć wiersz zawierający Państwa zakres oceny.
4. Sprawdzić, czy zakres oceny posiada status „Active” („Aktywny”) (kolumna „Scope Status” („Status zakresu”)).

6.4. Trwałość wyników będących przedmiotem wymiany

Ważna uwaga:

Zgody na publikację lub udostępnianie nie można cofnąć.

Wynika to z faktu, że wszystkim biernym uczestnikom pragniemy zapewnić nieustanny dostęp do każdego otrzymanego przez nich wyniku oceny. w przeciwnym razie musieliby samodzielnie zarządzać wynikami oceny i je archiwizować.

Zgoda zachowuje ważność przez cały okres ważności Państwa oceny TISAX.

Prosimy o bezzwłoczny kontakt, jeśli pomyłkowo utworzyli Państwo zgodę na publikację lub udostępnianie.

6.5. Poziomy udostępniania

Poziomy udostępniania przekładają się na główne punkty A–E raportu z oceny TISAX w stosunku 1:1.

	Główne punkty raportu z oceny TISAX	Poziomy udostępniania na platformie wymiany
1	A. Informacje związane z oceną (Assessment Related Information)	
2	B. Wyniki zbiorcze (Summarized Results)	
3	C. Podsumowanie wyniku oceny (Assessment result summary)	

	Główne punkty raportu z oceny TISAX	Poziomy udostępniania na platformie wymiany
4	D. Poziomy dojrzałości ISA VDA (zakładka Wyniki) (🇬🇧 Maturity Levels of VDA ISA (Result Tab))	
5	E. Szczegółowe wyniki oceny (🇬🇧 Detailed Assessment Results)	

Tabela 12. Główne punkty raportu z oceny TISAX oraz poziomy udostępniania na platformie wymiany

Im wyższy poziom udostępniania, tym więcej szczegółów Państwa oceny TISAX będzie dostępnych dla uczestnika/uczestników.

Bardziej szczegółowe informacje na temat treści poszczególnych punktów raportu z oceny TISAX znajdują się w Punkt 5.4.7.4, “Raport z oceny TISAX”.

6.6. Publikacja Państwa wyniku oceny na platformie wymiany

Swój wynik oceny można udostępnić wszystkim innym uczestnikom TISAX w drodze publikacji na platformie wymiany. Dzięki temu wszyscy pozostali uczestnicy TISAX będą mieli dostęp do wyniku Państwa oceny do wskazanego poziomu udostępniania.

Wynik oceny można opublikować jedynie w przypadku, gdy całkowity wynik oceny to „spełnia”.

Poziomy udostępniania wyniku oceny na platformie wymiany ograniczają się do poniższych opcji:

- Do not publish (Default) (🇵🇱 Nie publikuj (Domyślnie))
- A. Assessment Related Information (🇵🇱 A. Informacje związane z oceną)
- A + Labels (🇵🇱 A + etykiety)
- A + Labels + B. Summarized Results (🇵🇱 A + etykiety + B. Wyniki zbiorcze)

Dla tego ogólnego rodzaju publikacji zalecamy poziom udostępniania „A + Labels” (🇵🇱 „A + etykiety”).

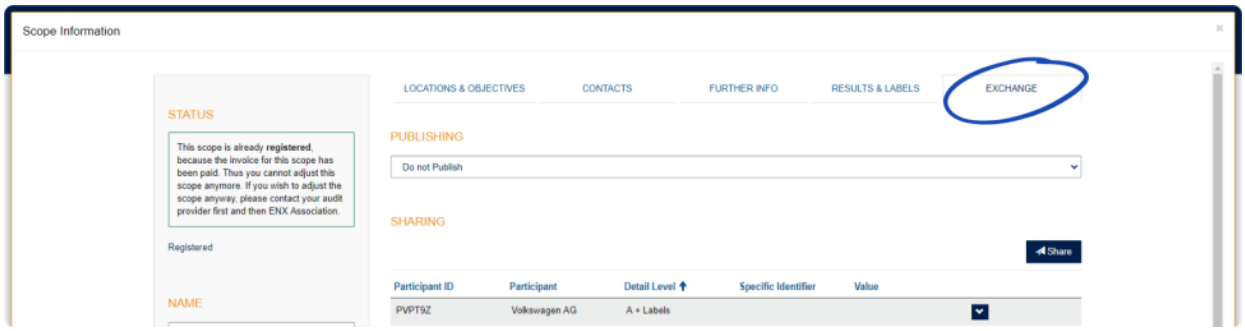
Ważna uwaga:

Wynik oceny można opublikować jedynie w przypadku spełnienia wymagań wstępnych opisanych w Punkt 6.3, “Ogólne warunki wstępne”.

Aby opublikować wynik oceny na platformie wymiany, należy wykonać poniższe czynności:

1. Zalogować się na portalu ENX.

2. Przejść do głównego paska nawigacji i zaznaczyć „MY TISAX” („MÓJ TISAX”).
   . w rozwijanym menu zaznaczyć „SCOPES AND ASSESSMENTS” („ZAKRESY I OCENY”).
3. Przejść do tabeli i znaleźć wiersz zawierający Państwa zakres oceny.
4. Sprawdzić, czy zakres oceny posiada status „Active” („Aktywny”) (kolumna „Scope Status” („Status zakresu”)).
5. Przejść na koniec wiersza tabeli dla zakresu oceny i kliknąć strzałkę w dół .
6. Zaznaczyć „Scope Information” („Informacje dotyczące zakresu”).
   . w nowym oknie („Scope Information” („Informacje dotyczące zakresu)) zaznaczyć kartę „EXCHANGE” („WYMIANA”).



7. Przejść do punktu „PUBLISHING” („PUBLIKACJA”), otworzyć rozwijane menu i zaznaczyć żądany poziom udostępniania (na podstawie powyższych sugestii).

Uwaga:

Wyniki oceny są publikowane wyłącznie na platformie wymiany. Dostęp do nich mogą mieć jedynie inni uczestnicy TISAX. Nie ma ogólnodostępnego wykazu wszystkich uczestników TISAX. Na ogólnodostępnej stronie internetowej TISAX może się znaleźć jedynie surowa liczba uczestników TISAX.

6.7. Udostępnianie własnego wyniku oceny konkretnemu uczestnikowi

Oprócz powyższej opcji publikacji wyniku oceny TISAX, na platformie wymiany mogą Państwo udostępnić go na wyższym poziomie udostępniania konkretnym uczestnikom TISAX.

W przeciwieństwie do wspomnianej wcześniej publikacji, wynik oceny można opublikować nawet w przypadku, gdy całkowity wynik oceny to (poważna/drobna) niezgodność.

Udostępnianie wyników oceny stanowi integralny element TISAX. Ocenę Państwa systemu zarządzania bezpieczeństwem informacji przeprowadzono jeden raz, ale teraz wynik oceny można udostępnić dowolnej liczbie partnerów.

Opcje udostępniania wyniku oceny na platformie wymiany są następujące:

1. A: Assessment Related Information (A: Informacje związane z oceną)
2. A + Labels (A + etykiety)
3. A + Labels + B: Assessment Summary (A + etykiety + B: Podsumowanie oceny)
4. A + Labels + B + C: Summarized Results (A + etykiety + B + C: Wyniki zbiorcze)
5. A + Labels + B + C + D: Detailed Assessment Results (A + etykiety + B + C + D: Szczegółowe wyniki oceny)
6. A + Labels + B + C + D + E: Maturity Levels according to ISA (A + etykiety + B + C + D + E: Poziomy dojrzałości wg ISA)

Zalecamy udostępnianie na poziomie „A + Labels” („A + etykiety”). w przypadku większości partnerów to wystarczy. w późniejszym terminie zawsze można wybrać wyższy poziom udostępniania.

Uwaga:

Niektórzy uczestnicy TISAX automatycznie przetwarzają wyniki oceny swoich partnerów. Synchronizują własny system z portalem ENX. Synchronizacja obejmuje jedynie wyniki oceny udostępnione konkretnie danemu uczestnikowi. Nie obejmuje samej publikacji, jak opisano w Punkt 6.6, “Publikacja Państwa wyniku oceny na platformie wymiany”.

Wśród producentów oryginalnego sprzętu korzystających z TISAX przykładem tego jest BMW. Jeśli są Państwo partnerem BMW, proszę udostępnić BMW (nie tylko opublikować) swój wynik oceny.

6.7.1. Warunki wstępne

Poniżej znajdują się warunki wstępne udostępniania wyniku własnej oceny partnerowi (lub innemu uczestnikowi TISAX):

- Wynik oceny TISAX można udostępnić jedynie innym uczestnikom TISAX.
- Państwa partner musi być uczestnikiem TISAX.
- Potrzebują Państwo Identyfikatora uczestnika swojego partnera.[30]
- Muszą Państwo uiścić opłatę (jeżeli dotyczy).

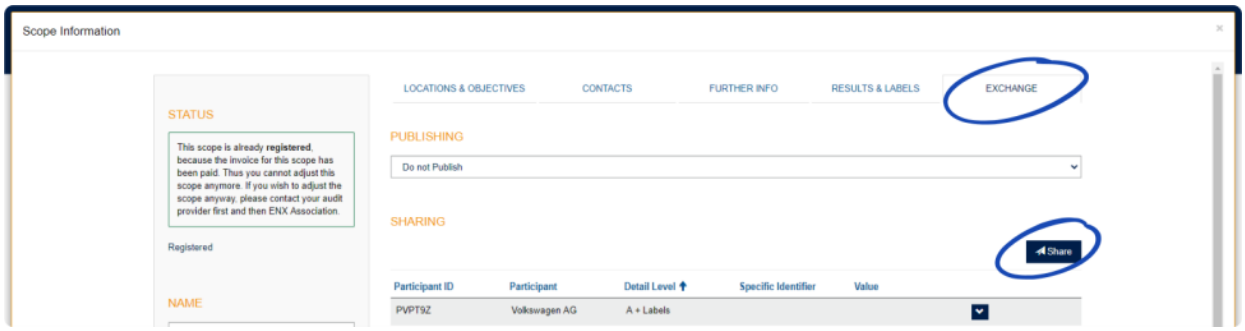
Ważna uwaga:

Wynik oceny można udostępnić jedynie w przypadku spełnienia ogólnych wymagań wstępnych opisanych w Punkt 6.3, “Ogólne warunki wstępne”.

6.7.2. Sposób tworzenia zgody na udostępnianie

Aby udostępnić wynik oceny innemu uczestnikowi TISAX, należy wykonać poniższe czynności:

1. Zalogować się na portalu ENX.
2. Przejść do głównego paska nawigacji i zaznaczyć „MY TISAX” („MÓJ TISAX”).
   . w rozwijanym menu zaznaczyć „SCOPES AND ASSESSMENTS” („ZAKRESY I OCENY”).
3. Przejść do tabeli i znaleźć wiersz zawierający Państwa zakres oceny.
4. Sprawdzić, czy zakres oceny posiada status „Active” („Aktywny”) (kolumna „Scope Status” („Status zakresu”)).
5. Przejść na koniec wiersza tabeli dla zakresu oceny i kliknąć strzałkę w dół .
6. Zaznaczyć „Scope Information” („Informacje dotyczące zakresu”).
   . w nowym oknie („Scope Information” („Informacje dotyczące zakresu)) zaznaczyć kartę „EXCHANGE” („WYMIANA”).



7. Przejść do punktu „SHARING” („UDOSTĘPNIANIE”) i kliknąć przycisk „Share” („Udostępnij”).
   . w nowym oknie („SHARE THIS SCOPE” („UDOSTĘPNIJ TEN ZAKRES”)) wprowadzić Identyfikator uczestnika partnera (lub zaznaczyć go na liście uczestników w sąsiednim polu wyszukiwania).
8. Zaznaczyć wymagany poziom udostępniania.
9. Kliknąć przycisk „Next” („Dalej”).
10. Zapoznać się z instrukcjami dotyczącymi braku możliwości cofnięcia zgody na udostępnianie i je zrozumieć.
11. Zaznaczyć dwa pola „confirm” („potwierdź”).
12. Kliknąć przycisk „Submit” („Prześlij”).

Wszystkim innym zajmie się platforma wymiany. Dla poziomu udostępniania A i B, informacje są dostępne na platformie wymiany. Państwa partner może się teraz zalogować na portalu ENX i sprawdzić udostępniony wynik oceny[31].

W przypadku wyższych poziomów udostępniania (C–E), platforma wymiany powiadamia dostawcę usług audytu. Wówczas dostawca usług audytu wysyła informacje (odpowiadające

wybranemu poziomowi udostępniania) głównej osobie do kontaktu ze strony uczestnika będącego Państwa partnerem.

6.8. Udostępnianie wyniku oceny poza TISAX

Zgodnie z zasadą[32] platformy wymiany TISAX można użyć jedynie w celu powiadomienia innych uczestników TISAX o własnym wyniku oceny.

6.8.1. Powody rygorystycznych regulacji mechanizmu wymiany

TISAX zapewnia standaryzowany mechanizm wymiany wyników oceny. Zapewnia to wartość dodaną w porównaniu z wymianą wyników innych procesów certyfikacji (np. ISO), gdzie dzieje się to na różne sposoby i nie zawsze zawiera wszystkie informacje niezbędne do uzyskania pełnego obrazu.

Tę standaryzację szczególnie cenią producenci oryginalnego sprzętu. z jasno określonych procedur korzystają jednak także inne spółki.

6.8.2. Poradnik dotyczący publicznych komunikatów na temat TISAX

Choć nie można publicznie informować o wyniku oceny, można wspomnieć o własnych staraniach w ramach TISAX. Na portalu ENX przekazujemy porady dotyczące sposobu podejścia do oświadczeń publicznych. Znajdą tam Państwo także logo TISAX, których można użyć.

Po zalogowaniu na portalu ENX można uzyskać dostęp do informacji w tym miejscu:
enx.com/en-US/myenxportal/marketing/
Bezpośrednie pobieranie archiwum w formie ZIP (dokument i logo):
enx.com/en-US/myenxportal/marketing/TISAX-Trademark-and-Logos-Terms-and-Conditions.zip

Gdyby się Państwo zastanawiali, czy istnieje certyfikat do powieszenia na ścianie:
Ze względu na opisany powyżej standaryzowany proces wymiany nie zapewniamy takiego certyfikatu.

6.8.3. Udostępnianie partnerowi, który nie jest jeszcze uczestnikiem TISAX

Jeśli chcą Państwo udostępnić swój wynik oceny TISAX partnerowi, który a) nie jest jeszcze uczestnikiem TISAX i b) nie otrzymał jeszcze etykiet TISAX (w drodze procesu oceny), mogą Państwo postąpić następująco:

1. Należy poprosić partnera o rejestrację w charakterze uczestnika TISAX.
   Państwa partner musi po prostu zarejestrować się jako uczestnik TISAX. Nie musi przejść do rejestracji zakresu oceny.
2. Należy poprosić partnera o kontakt z nami.
   Zwykle nową rejestrację przetwarzamy jedynie w przypadku, gdy spółka zarejestruje także

zakres oceny. Na żądanie Państwa partnera dokonamy przetwarzania jego rejestracji. w ten sposób zostanie uczestnikiem TISAX. Teraz może otrzymać Państwa wynik oceny TISAX w drodze standardowego procesu wymiany.

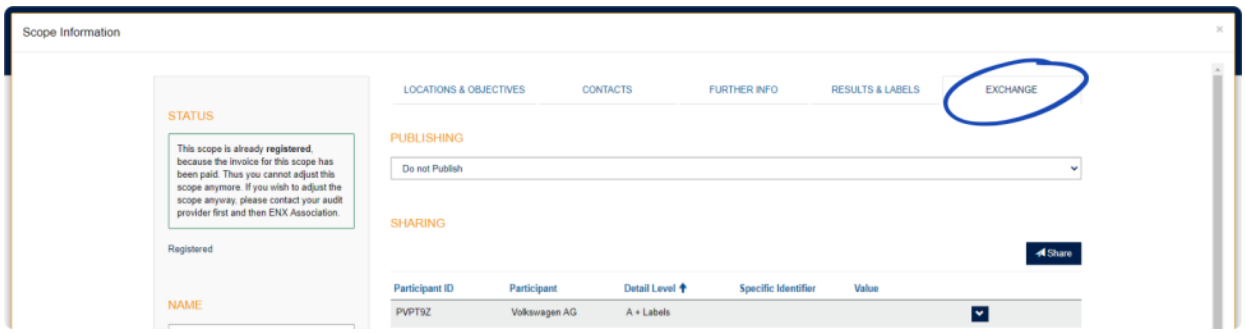
To podejście zapewnia, że Państwa partner zobowiązuje się przestrzegać „Warunków ogólnych uczestnictwa TISAX" regulujących wymianę wyników oceny TISAX.

Koszty generuje dopiero rejestracja zakresu oceny. Ponieważ rejestracja uczestnika TISAX jest darmowa, Państwa partner może nieodpłatnie otrzymać Państwa wynik oceny. Bez własnego wyniku oceny Państwa partner może otrzymać jedynie maksymalnie pięć wyników oceny i nie ma dostępu do publikacji.

6.8.4. Udostępnianie pracownikom Państwa partnera nieposiadającym bezpośredniego dostępu do portalu ENX

Państwa wynik mogą bezpośrednio wyświetlić jedynie pracownicy partnera posiadający konto na portalu ENX. Jeśli muszą Państwo udowodnić posiadane etykiety TISAX pracownikowi partnera bez dostępu do portalu, można użyć specjalnego dokumentu PDF. w celu uzyskania tego dokumentu należy postąpić następująco:

1. Udostępnić wynik oceny partnerowi w sposób opisany w Punkt 6.7, "Udostępnianie własnego wyniku oceny konkretnemu uczestnikowi".
2. Zalogować się na portalu ENX.
3. Przejść do głównego paska nawigacji i zaznaczyć „MY TISAX" („MÓJ TISAX").
   . w rozwijanym menu zaznaczyć „SCOPES AND ASSESSMENTS" („ZAKRESY I OCENY").
4. Przejść do tabeli i znaleźć wiersz zawierający Państwa zakres oceny.
5. Sprawdzić, czy zakres oceny posiada status „Active" („Aktywny") (kolumna „Scope Status" („Status zakresu")).
6. Przejść na koniec wiersza tabeli dla zakresu oceny i kliknąć strzałkę w dół .
7. Zaznaczyć „Scope Information" („Informacje dotyczące zakresu").
   . w nowym oknie („Scope Information" („Informacje dotyczące zakresu)) zaznaczyć kartę „EXCHANGE" („WYMIANA").



8. Przejść do sekcji „SHARING" („UDOSTĘPNIANIE") i znaleźć wiersz tabeli zawierający zgodę na udostępnianie (utworzoną na etapie 1).

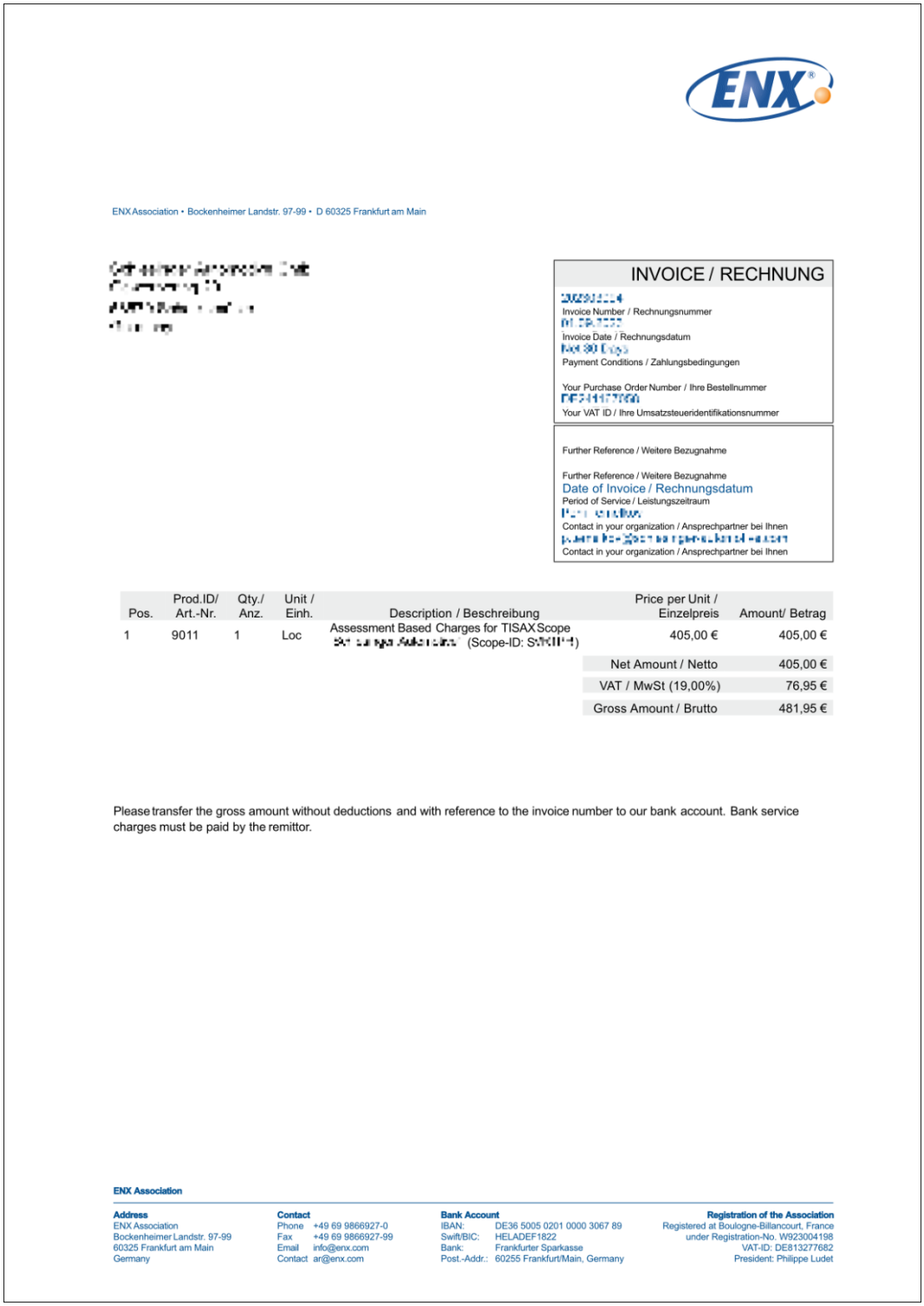
9. Przejść na koniec wiersza tabeli dla zgody na udostępnianie i kliknąć strzałkę w dół .
10. Zaznaczyć „Edit” („Edytuj”)
. w nowym oknie („SHARE THIS SCOPE” („UDOSTĘPNIJ TEN ZAKRES”)) przewinąć do dołu i zaznaczyć „Request Shared Information as PDF” („Wniosek o udostępniane informacje w postaci PDF”).
11. Należy chwilę poczekać na wygenerowanie dokumentu.
12. Pobrać dokument („Copy of information shared with ACME.pdf (66.84 KB)” („Kopia informacji udostępnionych ACME.pdf (66,84 kB)”))

7. Załączniki

7.1. Załącznik: Przykładowa faktura

Oto przykład wysyłanej przez nas faktury.

Bardziej szczegółowe informacje znajdują się w Punkt 4.3.4, “Opłata”.



ENX Association • Bockenheimer Landstr. 97-99 • D 60325 Frankfurt am Main

[redacted]

INVOICE / RECHNUNG

[redacted]
Invoice Number / Rechnungsnummer
[redacted]
Invoice Date / Rechnungsdatum
[redacted]
Payment Conditions / Zahlungsbedingungen

Your Purchase Order Number / Ihre Bestellnummer
[redacted]
Your VAT ID / Ihre Umsatzsteueridentifikationsnummer

Further Reference / Weitere Bezugnahme

Further Reference / Weitere Bezugnahme
Date of Invoice / Rechnungsdatum
Period of Service / Leistungszeitraum
[redacted]
Contact in your organization / Ansprechpartner bei Ihnen
[redacted]
Contact in your organization / Ansprechpartner bei Ihnen

Pos.	Prod.ID/ Art.-Nr.	Qty./ Anz.	Unit / Einh.	Description / Beschreibung	Price per Unit / Einzelpreis	Amount/ Betrag
1	9011	1	Loc	Assessment Based Charges for TISAX Scope [redacted] (Scope-ID: [redacted])	405,00 €	405,00 €
					Net Amount / Netto	405,00 €
					VAT / MwSt (19,00%)	76,95 €
					Gross Amount / Brutto	481,95 €

Please transfer the gross amount without deductions and with reference to the invoice number to our bank account. Bank service charges must be paid by the remittor.

ENX Association

Address	Contact	Bank Account	Registration of the Association
ENX Association Bockenheimer Landstr. 97-99 60325 Frankfurt am Main Germany	Phone +49 69 9866927-0 Fax +49 69 9866927-99 Email info@enx.com Contact ar@enx.com	IBAN: DE36 5005 0201 0000 3067 89 Swift/BIC: HELADEF1822 Bank: Frankfurter Sparkasse Post.-Addr.: 60255 Frankfurt/Main, Germany	Registered at Boulogne-Billancourt, France under Registration-No. W923004198 VAT-ID: DE813277682 President: Philippe Ludet

7.2. Załącznik: Przykładowa wiadomość e-mail z potwierdzeniem

Wiadomość e-mail z potwierdzeniem wysyłamy Państwu z chwilą ukończenia wszystkich obowiązkowych etapów procesu rejestracji online.

Bardziej szczegółowe informacje na temat terminu wysyłania tej wiadomości e-mail z potwierdzeniem znajdują się w Punkt 4.5.8, “Wiadomość e-mail z potwierdzeniem”.

```
Temat: [TISAX] Zakres S3ZY5V Zatwierdzony

Szanowny Panie John Doe,

Dziękujemy za rejestrację zakresu oceny TISAX. Dokonałam rejestracji Państwa
zakresu{nbsp}i{nbsp}zatwierdziłam Państwa zakres.{nbsp}w{nbsp}załączeniu przesyłam
wyciąg{nbsp}z{nbsp}zakresu TISAX, zawierający wszystkie informacje na temat zakresu
oraz aktualny wykaz dostawców usług audytu TISAX.

Co dalej?

Przy pomocy załączonego wyciągu{nbsp}z{nbsp}zakresu TISAX mogą Państwo teraz
składać zapytania ofertowe wszystkim dostawcom usług audytu
TISAX{nbsp}w{nbsp}odniesieniu do własnego zakresu.

Potrzebna pomoc?

W przypadku dalszych pytań dotyczących TISAX zachęcamy do zapoznania
się{nbsp}z{nbsp}FAQ TISAX lub Podręcznikiem uczestnika TISAX. Jeśli potrzebują
Państwo dalszej pomocy dotyczącej TISAX, prosimy o kontakt{nbsp}z{nbsp}infolinią
TISAX pocztą elektroniczną (tisax@enx.com) lub telefonicznie (+49 69 986692-777).

Z poważaniem

Państwa zespół TISAX
```

7.3. Załącznik: Przykładowy wyciąg z zakresu TISAX

W załączeniu do wiadomości e-mail z potwierdzeniem otrzymują Państwo „Wyciąg z zakresu TISAX”.

Bardziej szczegółowe informacje znajdują się w Punkt 4.5.8, “Wiadomość e-mail z potwierdzeniem”.

TISAX Scope Excerpt [redacted]
Participant: [redacted]

Scope: [redacted]

Standard Scope 2.0

The TISAX Scope defines the scope of the assessment. The assessment includes all processes, procedures and resources under responsibility of the assessed organization that are relevant to the security of the protection objects and their protection goals as defined in the listed assessment objectives at the listed locations. The assessment is conducted at least in the highest Assessment Level listed in any of the listed Assessment Objectives. All assessment criteria listed in the listed assessment objectives are subject to the assessment.

Assessment Objectives	AL	Locations
Information with High Protection Needs	2	1

Maturity of ISMS	Certified on	Certified in
Established ISMS (already experienced, but not yet certified)		

Complexity of ISMS	Justification (only if simple ISMS)
Complex ISMS (very large number of methods/ processes)	

Use of Consulting Firm for ISMS	Name of Consulting Firm
No Support by consultancy provider	none

Earliest Kickoff-Meeting	Labels needed until	External Requirement
[redacted]	[redacted]	No

Location: [redacted]

Company Name and Address	Location-ID	DUNS
[redacted]	[redacted]	[redacted]
	Type	
	Campus owned and exclusively used by company	
	Passive Site Protection	**Employees**
	Yes	Overall: 1.001-5.000
	Industry	IT: 1-10
		IT-Security: 1-10
		Location Security: 4-10

2023[redacted]

Page **1** of **1**

7.4. Załącznik: Participant status (Status uczestnika)

7.4.1. Informacje ogólne: Participant status (Status uczestnika)

„Status uczestnika” określa, w jakim miejscu procesu TISAX się Państwo (jako spółka) znajdują.

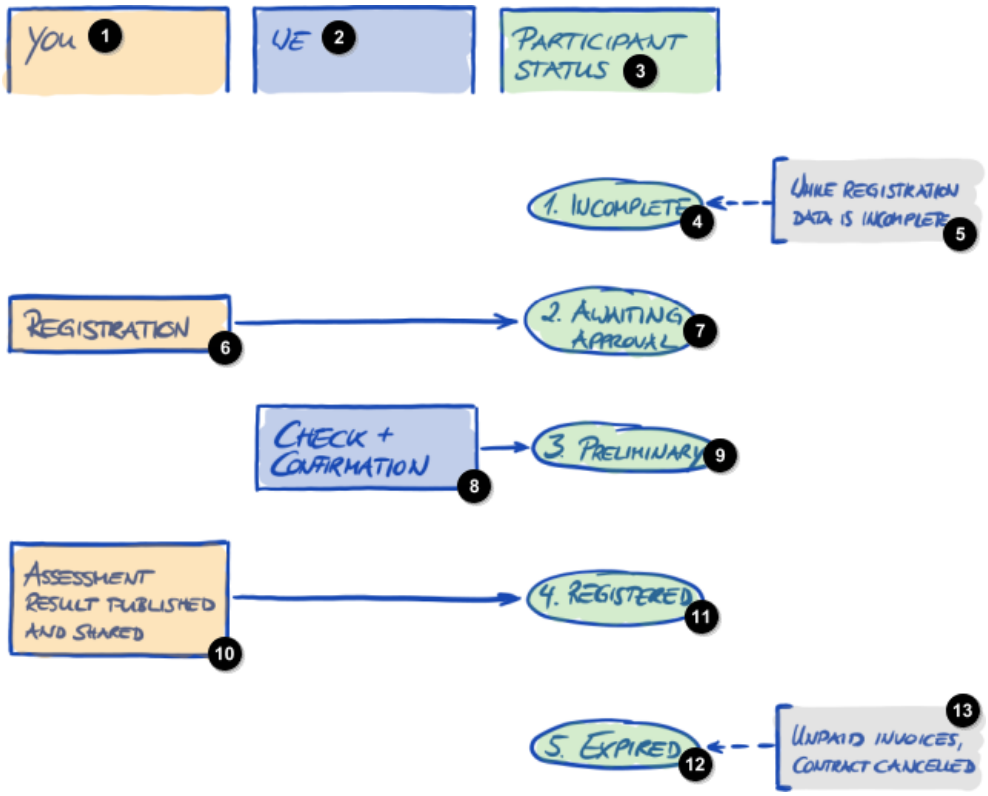
Państwa „status uczestnika” może być następujący:

1. Incomplete (Niekompletny)
2. Awaiting approval (Oczekujący na zatwierdzenie)
3. Preliminary (Wstępny)
4. Registered (Zarejestrowany)
5. Expired (Po terminie ważności)

Tabele w każdym punkcie dotyczącym statusu opisują teraz:

- Państwa sytuację
  (co jest prawdą w danej chwili, kiedy posiadają Państwo ten status)
- Państwa następną czynność
  (co trzeba zrobić w celu przejścia do kolejnego statusu, jeżeli dotyczy)
- naszą następną czynność
  (co musimy zrobić, by podnieść Państwa status, jeżeli dotyczy)
- następny status
  (jeżeli dotyczy)

Poniższa ilustracja przedstawia działania skutkujące przejściem do kolejnego statusu:



Rysunek 34. Informacje ogólne na temat statusu uczestnika

1. Państwo
2. My
3. Status uczestnika
4. 1. Niekompletny
5. Kiedy dane dotyczące rejestracji są niekompletne
6. Rejestracja
7. 2. Oczekujący na zatwierdzenie
8. Kontrola + potwierdzenie
9. 3. Wstępny
10. Wynik oceny opublikowano i udostępniono
11. 4. Zarejestrowany
12. 5. Po terminie ważności
13. Niezapłacone faktury, anulowana umowa

7.4.2. Participant status „Incomplete” (Status uczestnika „Niekompletny”)

Status	Sytuacja	Państwa następna czynność	Nasza następna czynność	Następny status
Niekompletny	Nie ukończyli Państwo rejestracji TISAX. Być może nie zaakceptowali Państwo warunków ogólnych. Być może nie określili Państwo głównej lokalizacji uczestnika. Być może nie przypisali Państwo głównej osoby do kontaktu ze strony uczestnika. Być może brakuje innych wymaganych przez nas informacji.	Ciąg dalszy pod adresem enx.com/en-US/SignIn	Przypomnienie przyślemy Państwu pocztą elektroniczną (zwykle w ciągu kilku dni).	Oczekujący na zatwierdzenie

7.4.3. Participant status „Awaiting approval” (Status uczestnika „Oczekujący na zatwierdzenie”)

Status	Sytuacja	Państwa następna czynność	Nasza następna czynność	Następny status
Oczekujący na zatwierdzenie	Państwa rejestracja TISAX jest kompletna. Być może nie zarejestrowali Państwo jeszcze zakresu oceny.	Proszę poczekać na naszą następną czynność.	Sprawdzimy i zwykle zatwierdzimy Państwa wniosek. Tę kontrolę zwykle inicjują Państwo, rejestrując także zakres oceny. Przypiszemy Państwu Identyfikator uczestnika i Identyfikator(y) zakresu. Wyślemy do Państwa wiadomość e-mail z potwierdzeniem. Załączony „Wyciąg z zakresu TISAX” (PDF) zawiera podsumowanie informacji w naszej bazie danych.	Wstępny

7.4.4. Participant status „Preliminary” (Status uczestnika „Wstępny”)

Status	Sytuacja	Państwa następna czynność	Nasza następna czynność	Następny status
Wstępny	Pomyślnie ukończyli Państwo proces rejestracji TISAX.	Proszę uiścić opłatę (jeżeli dotyczy). Proszę przejść proces oceny TISAX. Proszę opublikować i udostępnić wynik swojej oceny.	Brak	Zarejestrowany

7.4.5. Participant status „Registered” (Status uczestnika „Zarejestrowany”)

Status	Sytuacja	Państwa następna czynność	Nasza następna czynność	Następny status
Zarejestrowany	Pomyślnie ukończyli Państwo proces oceny TISAX i otrzymali etykiety TISAX. Opublikowali Państwo i udostępnili wynik swojej oceny. Etykiety TISAX otrzymują Państwo dopiero po pomyślnym ukończeniu procesu oceny TISAX. Na portalu ENX odzwierciedla to zakres oceny o statusie „Aktywny”.	Brak	Brak	(Po terminie ważności)

Uwaga:

Jeśli chcą Państwo uzyskać dostęp do wyników oceny swojego partnera/partnerów:

Warunkiem wstępnym umożliwiającym otrzymanie wyników oceny innych uczestników jest którykolwiek z poniższych:

- Udostępniają Państwo wynik własnej oceny (to „potwierdza”, że są Państwo poważnym uczestnikiem TISAX oraz członkiem społeczności branży motoryzacyjnej).
- Uznajemy Państwa na podstawie Państwa reputacji w branży motoryzacyjnej (jak producenci oryginalnego sprzętu, dostawcy 1. szczebla).

- Udowadniają Państwo uzasadniony interes związany z uzyskaniem wyników oceny od innych uczestników. Musimy to zweryfikować w trakcie skomplikowanego procesu, który może się wiązać ze znaczną kwotą opłaty. w celu uzyskania bardziej szczegółowych informacji prosimy o kontakt z nami.

7.4.6. Participant status „Expired” (Status uczestnika „Po terminie ważności”)

Status	Sytuacja	Państwa następna czynność	Nasza następna czynność	Następny status
Po terminie ważności	Nie uiścili Państwo opłaty. Nastąpiło anulowanie umowy przez Państwa lub przez nas (OWU).	Brak	Brak	nd.

7.5. Załącznik: Assessment scope status (Status zakresu oceny)

7.5.1. Informacje ogólne: Assessment scope status (Status zakresu oceny)

„Status zakresu oceny” określa miejsce zakresu oceny w jego cyklu życia.

Przypominamy, że „status zakresu oceny” jest czymś innym niż „status oceny”. Bardziej szczegółowe informacje na temat „statusu oceny” znajdują się w Punkt 7.6, “Załącznik: Assessment status (Status oceny)”.

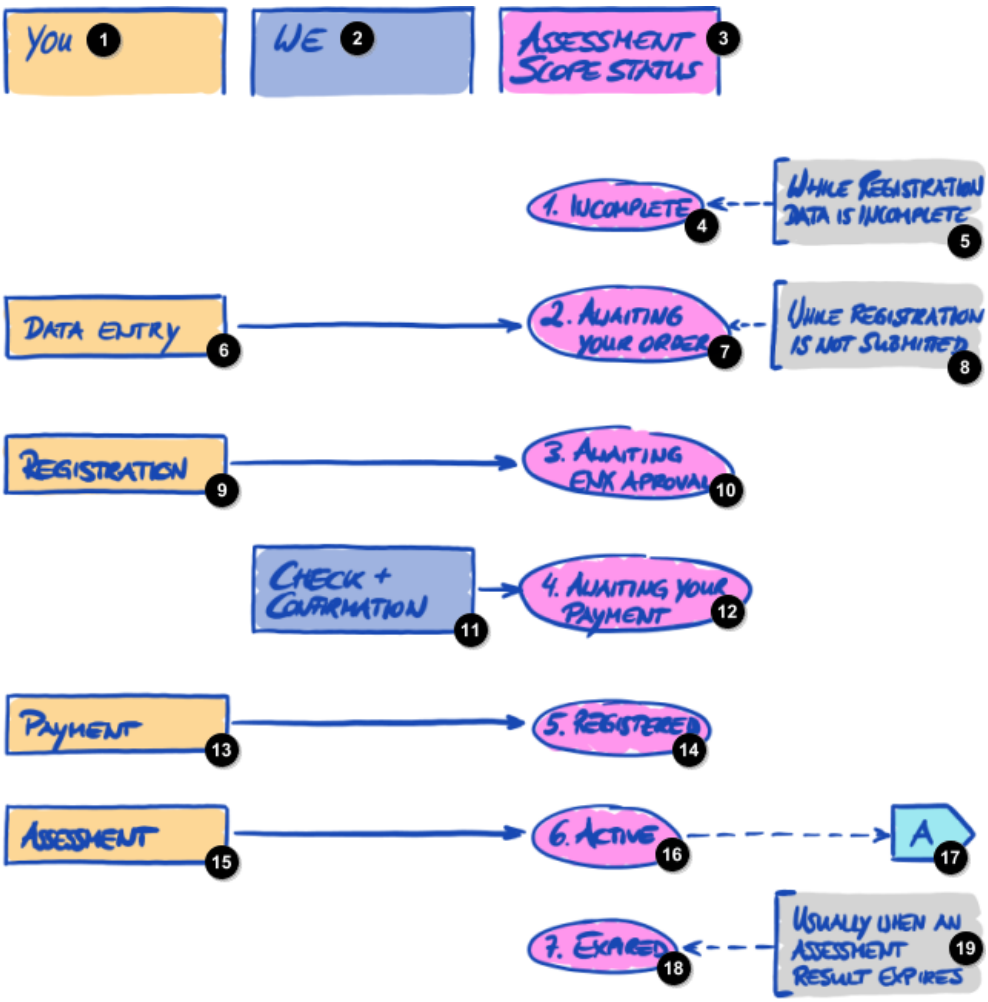
Państwa „status zakresu oceny” może być następujący:

1. Incomplete (Niekompletny)
2. Awaiting your order (Oczekujący na Państwa zlecenie)
3. Awaiting ENX approval (Oczekujący na zatwierdzenie ENX)
4. Awaiting your payment (Oczekujący na Państwa płatność)
5. Registered (Zarejestrowany)
6. Active (Aktywny)
7. Expired (Po terminie ważności)

Tabele w każdym punkcie dotyczącym statusu opisują teraz:

- Państwa sytuację
  (co jest prawdą w danej chwili, kiedy posiadają Państwo ten status)
- Państwa następną czynność
  (Co trzeba zrobić w celu przejścia do kolejnego statusu, jeżeli dotyczy)
- Naszą następną czynność
  (Co musimy zrobić, by podnieść Państwa status, jeżeli dotyczy)
- Następny status
  (jeżeli dotyczy)

Poniższa ilustracja przedstawia działania skutkujące przejściem do kolejnego statusu:



Rysunek 35. Informacje ogólne na temat statusu zakresu oceny

1. Państwo
2. My
3. Status zakresu oceny

4. 1. Niekompletny
5. Kiedy dane dotyczące rejestracji są niekompletne
6. Wprowadzanie danych
7. 2. Oczekujący na Państwa zlecenie
8. Kiedy nie przesłano rejestracji
9. Rejestracja
10. 3. Oczekujący na zatwierdzenie ENX
11. Kontrola + potwierdzenie
12. 4. Oczekujący na Państwa płatność
13. Płatność
14. 5. Zarejestrowany
15. Ocena
16. 6. Aktywny
17. A
18. 7. Po terminie ważności
19. Zwykle po wygaśnięciu wyniku oceny

Odnośnik „A” na powyższym rysunku wiąże status zakresu oceny „Aktywny” ze „statusem oceny”. Bardziej szczegółowe informacje na temat „statusu oceny” znajdują się w Punkt 7.6, “Załącznik: Assessment status (Status oceny)”.

7.5.2. Assessment scope status „Incomplete” (Status zakresu oceny „Niekompletny”)

Status	Sytuacja	Państwa następna czynność	Nasza następna czynność	Następny status
Niekompletny	Nie ukończyli Państwo rejestracji zakresu oceny. Lub nie podali Państwo wszystkich wymaganych informacji.	Ciąg dalszy pod adresem enx.com/en-US/SignIn	Przypomnienie przyślemy Państwu pocztą elektroniczną (zwykle w ciągu kilku dni).	Oczekujący na Państwa zlecenie

Bardziej szczegółowe informacje na temat miejsca, w którym odgrywa rolę ten status, znajdują się w Punkt 4.5.7, “Rejestracja zakresu oceny”.

7.5.3. Assessment scope status „Awaiting your order” (Status zakresu oceny „Oczekujący na Państwa zlecenie”)

Status	Sytuacja	Państwa następna czynność	Nasza następna czynność	Następny status
Oczekujący na Państwa zlecenie	Nie ukończyli Państwo rejestracji swojego zakresu.	Ciąg dalszy pod adresem enx.com/en-US/SignIn	Przypomnienie przyślemy Państwu pocztą elektroniczną (zwykle w ciągu kilku dni).	Oczekujący na zatwierdzenie ENX

Bardziej szczegółowe informacje na temat miejsca, w którym odgrywa rolę ten status, znajdują się w Punkt 4.5.7, “Rejestracja zakresu oceny”.

7.5.4. Assessment scope status „Awaiting ENX approval” (Status zakresu oceny „Oczekujący na zatwierdzenie ENX”)

Status	Sytuacja	Państwa następna czynność	Nasza następna czynność	Następny status
Oczekujący na zatwierdzenie ENX	Rejestracja Państwa zakresu oceny jest kompletna.	Proszę poczekać na naszą następną czynność.	Sprawdzimy i zwykle zatwierdzimy Państwa wniosek. Przypiszemy Identyfikator(y) zakresu. Wyślemy do Państwa wiadomość e-mail z potwierdzeniem. Załączony „Wyciąg z zakresu TISAX” (PDF) zawiera podsumowanie informacji w naszej bazie danych.	Oczekujący na Państwa płatność

Bardziej szczegółowe informacje na temat miejsca, w którym odgrywa rolę ten status, znajdują się w Punkt 4.5.7, “Rejestracja zakresu oceny”.

7.5.5. Assessment scope status „Awaiting your payment” (Status zakresu oceny „Oczekujący na Państwa płatność”)

Status	Sytuacja	Państwa następna czynność	Nasza następna czynność	Następny status
Oczekujący na Państwa płatność	Rejestracja Państwa zakresu oceny jest kompletna i zatwierdzona. Otrzymali Państwo od nas wiadomość e-mail z potwierdzeniem oraz „Wyciąg z zakresu TISAX”.	Proszę uiścić opłatę (jeżeli dotyczy). Proszę wysłać zapytania ofertowe do naszych dostawców usług audytu TISAX. Począwszy od statusu „Oczekujący na Państwa płatność”, Państwo: ▪ mogą zacząć udostępniać partnerowi wybrane informacje związane z oceną.[33] ▪ mogą wstępnie skonfigurować publikację Państwa wyniku oceny (wejdzie w życie dopiero, kiedy Państwa status zakresu oceny zmieni się na „Aktywny”.	Oczekiwanie na Państwa płatność.	Zarejestrowany

Bardziej szczegółowe informacje na temat miejsca, w którym odgrywa rolę ten status, znajdują się w Punkt 4.5.8, “Wiadomość e-mail z potwierdzeniem”.

7.5.6. Assessment scope status „Registered” (Status zakresu oceny „Zarejestrowany”)

Status	Sytuacja	Państwa następna czynność	Nasza następna czynność	Następny status
Zarejestrowany	Państwa zakres oceny jest zarejestrowany. Otrzymaliśmy od Państwa pełną kwotę płatności lub nasz status komercyjny to „zielony” ze względu na inne okoliczności.	Proszę przejść proces oceny TISAX.	Brak	Aktywny

7.5.7. Assessment scope status „Active” (Status zakresu oceny „Aktywny”)

Status	Sytuacja	Państwa następna czynność	Nasza następna czynność	Następny status
Aktywny	Pomyślnie ukończyli Państwo proces oceny TISAX i otrzymali etykiety TISAX.	Proszę opublikować i udostępnić wynik swojej oceny. Wchodzą w życie wszystkie zgody na publikowanie i udostępnianie wstępnie skonfigurowane przy niższym statusie.	Brak	Po terminie ważności

Bardziej szczegółowe informacje na temat publikacji i udostępniania znajdują się w Punkt 6, “Wymiana (Etap 3)”.

7.5.8. Assessment scope status „Expired” (Status zakresu oceny „Po terminie ważności”)

Status	Sytuacja	Państwa następna czynność	Nasza następna czynność	Następny status
Po terminie ważności	Albo: ▪ nie ukończyli Państwo rejestracji zakresu oceny w ciągu 90 dni,	Proszę rozpocząć nową rejestrację zakresu oceny.	Brak	Niekompletny lub Oczekujący na Państwa zlecenie lub Oczekujący na zatwierdzenie ENX
	• lub wystąpiło nadmierne opóźnienie w zapłacie przez Państwa opłaty,			
	• lub opuścili Państwo proces TISAX,			
	• lub wygasła ważność Państwa wyniku oceny (trzy lata),			
	• lub wystąpiły istotne zmiany zakresu oceny (przykład: żadna z lokalizacji wchodzących w zakres oceny nie należy już do Państwa spółki).			

7.6. Załącznik: Assessment status (Status oceny)

7.6.1. Informacje ogólne: Assessment status (Status oceny)

„Status oceny” określa Państwa miejsce w procesie oceny. Status ulega zmianie w ramach przejścia od jednego rodzaju oceny do drugiego (np. z „oceny wstępnej” do „oceny planu działań korygujących”).

Przypominamy, że „status oceny” jest czymś innym niż „status zakresu oceny”. Bardziej szczegółowe informacje na temat „statusu zakresu oceny” znajdują się w Punkt 7.5, “Załącznik: Assessment scope status (Status zakresu oceny)”.

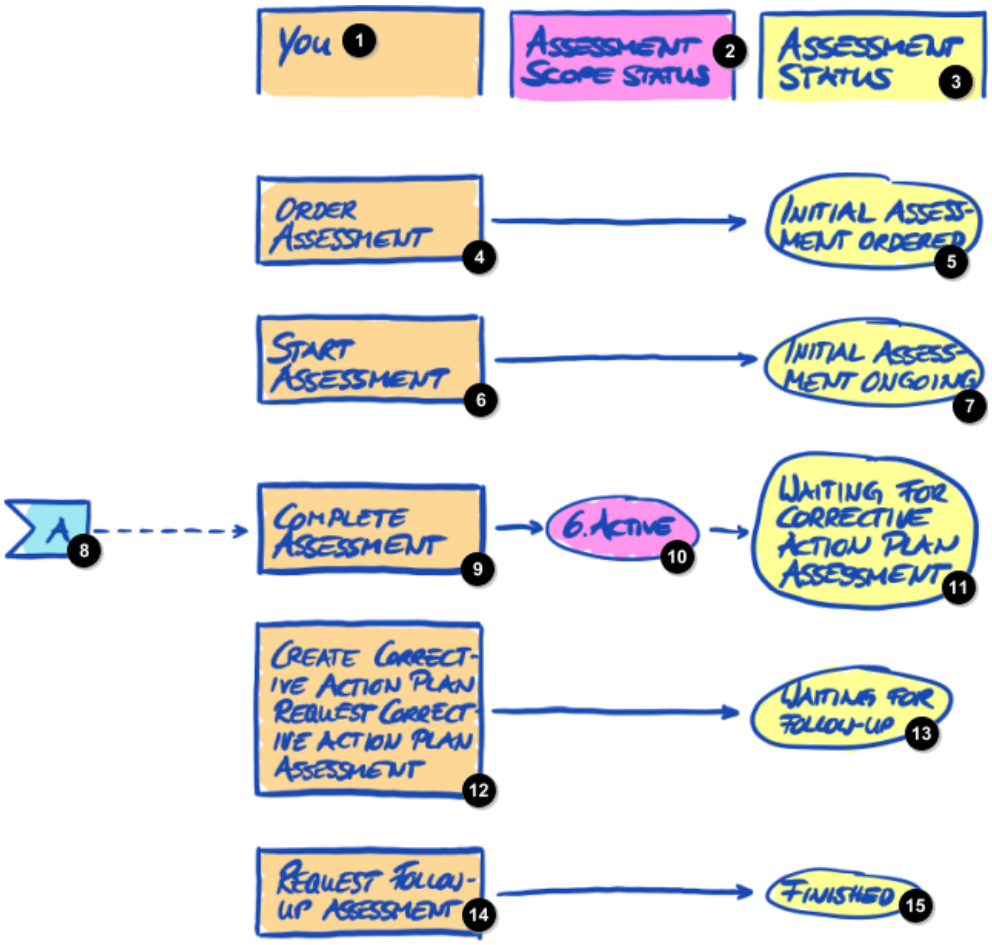
Państwa „status oceny” może być następujący:

1. Initial assessment ordered (Ocena wstępna zlecona)
2. Initial assessment ongoing (Ocena wstępna w toku)
3. Waiting for corrective action plan assessment (Oczekiwanie na ocenę planu działań korygujących)
4. Waiting for follow-up (Oczekiwanie na kontrolę)
5. Finished (Zakończony)

Tabele w każdym punkcie dotyczącym statusu opisują teraz:

- Państwa sytuację
  (co jest prawdą w danej chwili, kiedy posiadają Państwo ten status)
- Państwa następną czynność
  (Co trzeba zrobić w celu przejścia do kolejnego statusu, jeżeli dotyczy)
- Naszą następną czynność
  (Co musimy zrobić, by podnieść Państwa status, jeżeli dotyczy)
- Następny status
  (jeżeli dotyczy)

Poniższa ilustracja przedstawia działania skutkujące przejściem do kolejnego statusu:



Rysunek 36. Informacje ogólne na temat statusu oceny

1. Państwo
2. Status zakresu oceny
3. Status oceny
4. Zlecają ocenę
5. Ocena wstępna zlecona
6. Rozpoczynają ocenę
7. Ocena wstępna w toku
8. A
9. Kończą ocenę
10. 6. Aktywny
11. Oczekiwanie na ocenę planu działań korygujących
12. Opracowują plan działań korygujących
    Wnioskują o ocenę planu działań korygujących

13 Oczekiwanie na kontrolę

14 Wnioskują o ocenę kontrolną

15 Zakończony

Odnośnik „A” na powyższym rysunku wiąże status zakresu oceny „Aktywny” ze statusem oceny „Oczekiwanie na ocenę planu działań korygujących”. Bardziej szczegółowe informacje na temat „statusu zakresu oceny” znajdują się w Punkt 7.5, “Załącznik: Assessment scope status (Status zakresu oceny)”.

7.6.2. Assessment status „Initial assessment ordered” (Status oceny „Ocena wstępna zlecona”)

Status	Sytuacja	Państwa następna czynność	Nasza następna czynność	Następny status
Ocena wstępna zlecona	Wybrali Państwo jednego z naszych dostawców usług audytu TISAX i zlecili mu ocenę wstępną.	Proszę kontynuować proces oceny TISAX.	Brak	Ocena wstępna w toku

7.6.3. Assessment status „Initial assessment ongoing” (Status oceny „Ocena wstępna w toku”)

Status	Sytuacja	Państwa następna czynność	Nasza następna czynność	Następny status
Ocena wstępna w toku	Państwa ocena wstępna: ▪ rozpoczęła się ▪ lub została zakończona, lecz dostawca usług audytu nie przesłał jeszcze raportu z oceny TISAX	Brak	Brak	Oczekiwanie na ocenę planu działań korygujących (jeżeli dotyczy)

7.6.4. Assessment status „Waiting for corrective action plan assessment” (Status oceny „Oczekiwanie na ocenę planu działań korygujących”)

Status	Sytuacja	Państwa następna czynność	Nasza następna czynność	Następny status
Oczekiwanie na ocenę planu działań korygujących	Dostawca usług audytu przeprowadził ocenę wstępną. Dostawca usług audytu przekazał nam raport z oceny TISAX. Wynik oceny to (poważna/drobna) niezgodność.	Proszę opracować plan działań korygujących. Proszę rozpocząć działania korygujące. Proszę wystąpić o ocenę planu działań korygujących.	Brak	Oczekiwanie na kontrolę (jeżeli dotyczy)

Status oceny „Oczekiwanie na ocenę planu działań korygujących” ogranicza się do dziewięciu miesięcy. Bardziej szczegółowe informacje znajdują się w Punkt 5.4.9.3, “Wymagania dotyczące planu działań korygujących”.

7.6.5. Assessment status „Waiting for follow-up” (Status oceny „Oczekiwanie na kontrolę”)

Status	Sytuacja	Państwa następna czynność	Nasza następna czynność	Następny status
Oczekiwanie na kontrolę	Dostawca usług audytu zatwierdził Państwa plan działań korygujących. Wdrożyli Państwo działania korygujące.	Proszę wystąpić o ocenę kontrolną.	Brak	Zakończony

Status oceny „Oczekiwanie na kontrolę” ogranicza się do dziewięciu miesięcy. Bardziej szczegółowe informacje znajdują się w Punkt 5.4.9.3, “Wymagania dotyczące planu działań korygujących”.

7.6.6. Assessment status „Finished” (Status oceny „Zakończony”)

Status	Sytuacja	Państwa następna czynność	Nasza następna czynność	Następny status
Zakończony	Dostawca usług audytu przeprowadził ocenę kontrolną. Wynik oceny nie wykazał niezgodności. Dostawca usług audytu przekazał nam raport z oceny TISAX.	Proszę opublikować i udostępnić wynik swojej oceny.	Brak	nd.

7.7. Załącznik: Argumenty przeciwko „ocenom początkowym” i „analizom luk”

Zasadniczo odradzamy zlecenie dostawcy usług audytu przeprowadzenia „oceny wstępnej” lub „analizy luk”. Niemal zawsze rozsądniej jest od razu rozpocząć proces oceny TISAX.

W tym punkcie omówimy najczęstsze obawy.

Czy ocenę początkową rozważają Państwo z powodu:

1. Obaw, że Państwa klient może zobaczyć potencjalnie niekorzystny wynik oceny?

   Mają Państwo pełną kontrolę nad tym, kto zobaczy wyniki Państwa oceny. To Państwo decydują, czy dostawca usług audytu wczyta cokolwiek na portalu ENX. Jeśli nie chcą Państwo pokazać wyniku oceny, nikt go nie zobaczy (oczywiście z wyjątkiem audytora).

   Co więcej, dostawca usług audytu zawsze wczytuje jedynie pierwsze dwa punkty raportu z oceny TISAX, a tym samym *nigdy* nie wczytuje szczegółowych wyników oceny.

2. Myślą Państwo, że ocena początkowa może przynieść oszczędności?
   - W przypadku oceny początkowej, Państwo:
     - płacą za ocenę początkową
     - mogą ponieść koszty wewnętrzne usunięcia jakichkolwiek niezgodności
     - płacą Państwo pełny koszt oceny TISAX („oceny wstępnej”)

Nawet pod *nieobecność* ustaleń, zawsze płacą Państwo za *dwie* pełne oceny.

- Zaczynając od oceny TISAX, Państwo:
  - płacą za „ocenę wstępną”
  - mogą ponieść koszty wewnętrzne usunięcia jakichkolwiek ustaleń
  - mogą zapłacić znacznie mniej (w porównaniu z „oceną wstępną”) za tzw. „ocenę kontrolną”, gdzie audytor skupia się jedynie na usunięciu przez Państwa niezgodności stwierdzonych podczas oceny wstępnej

  Nawet w przypadku *stwierdzenia* ustaleń, płacą Państwo jedynie za pełną ocenę plus krótką ocenę kontrolną.

3. Myślą Państwo, że mogą Państwo nie przejść oceny, co będzie miało trwałe skutki?

   Nie można trwale nie przejść oceny, ponieważ można poddać się dowolnej liczbie ocen. Jeśli wynik oceny nie spełni Państwa oczekiwań lub jeśli przy pomocy działań korygujących nie uda się Państwu usunąć niezgodności w ciągu wymaganych dziewięciu miesięcy, po prostu uznają Państwo nieudaną próbę za ocenę początkową i zaczynają od nowa. Co więcej, nikt nie musi znać wyników pierwszej próby. Udostępniają Państwo jedynie wynik pomyślnej oceny.

Dalsze względy:

- Jeśli wynik oceny przekroczy oczekiwania, mogą Państwo otrzymać tymczasowe etykiety TISAX. Należy udostępnić je bezpośrednio partnerowi. Nie jest to możliwe w przypadku oceny początkowej.
- Jeśli dostawca usług audytu prowadzący ocenę początkową ma także prowadzić ocenę TISAX, nie może zapewniać Państwu konsultacji. w przeciwnym razie na potrzeby oceny TISAX należy wybrać innego dostawcę usług audytu.

Choć dla większości firm kontrolowanych ocena początkowa nie oznacza korzyści, pragniemy wspomnieć o jej następujących zaletach.

Audytor:

- może się skupić na krytycznych aspektach, gdy nie mają Państwo zaufania do własnego ISMS
- może poświęcić więcej czasu niż zwykle i rozszerzyć obserwacje
- może w odmienny sposób udokumentować ustalenia

Po zapoznaniu się z punktami dotyczącymi procesu oceny TISAX, łatwiej będzie Państwu zrozumieć nasze argumenty.

7.8. Załącznik: Zakresy niestandardowe

Niemal wszyscy uczestnicy TISAX wybierają zakres standardowy. Jednakże w pewnych, *rzadkich* okolicznościach, mogą Państwo być zmuszeni do wyboru zakresu niestandardowego.

Istnieją dwa rodzaje zakresów niestandardowych:

7.8.1. Zakres niestandardowy rozszerzony

Zakres można rozszerzyć. Zakres niestandardowy rozszerzony obejmuje WIĘCEJ niż zakres standardowy. Dostawca usług audytu przeprowadzi więcej kontroli.

Cel: zakres niestandardowy rozszerzony może być właściwy, jeśli chcą Państwo wykorzystać ocenę TISAX do celów wewnętrznych lub poza branżą motoryzacyjną.

Etykiety TISAX i udostępnianie wyników: zakres niestandardowy rozszerzony zawsze obejmuje zakres standardowy. Dlatego też zakres niestandardowy rozszerzony otrzyma etykiety TISAX[34]. Pozostali uczestnicy TISAX w dalszym ciągu zaakceptują wynik oceny.

Opis: choć zakres standardowy posiada określony opis, jeśli potrzebują Państwo zakresu niestandardowego rozszerzonego, muszą Państwo opracować własny opis zakresu.

7.8.2. Zakres niestandardowy pełny

Mogą Państwo w pełni zdefiniować własny zakres.

Cel: jeśli posiadają Państwo lokalizacje należące do różnych zakresów oceny i korzystają Państwo z usług w określonym zakładzie (np. centrum danych), w odniesieniu do takich usług mogą Państwo skorzystać z zakresu niestandardowego pełnego. Dzięki temu dostawca usług audytu TISAX może ponownie wykorzystać wynik oceny zakresu niestandardowego pełnego usługi.

Przykład: mają Państwo wiele lokalizacji (być może objętych różnymi zakresami) i w jednej z nich centralny dział IT. Określenie zakresu niestandardowego pełnego jedynie dla działu IT może ułatwić ponowne wykorzystanie danego wyniku oceny w ramach innych zakresów.

Etykiety TISAX i udostępnianie wyników: zakresy niestandardowe pełne nie otrzymują etykiet TISAX. Państwa wynik oceny jest rejestrowany na portalu ENX z datą, okresem oceny oraz wskazaniem, czy całkowity wynik oceny to „spełnia” czy też „niezgodność”. Taki wynik oceny mogą Państwo udostępnić. Jednak większości odbiorców udostępnienie wyniku oceny bez etykiet TISAX wyda się oceną „niepomyślną”. Pozostali uczestnicy TISAX zasadniczo nie akceptują wyników oceny zakresów niestandardowych pełnych.

Opis: podobnie jak w przypadku zakresu niestandardowego rozszerzonego, jeśli potrzebują Państwo zakresu niestandardowego pełnego, muszą Państwo opracować własny opis zakresu.

Ważna uwaga:

Aby podkreślić rzadkość korzystania z zakresu niestandardowego pełnego: istnieje 98% szansy, że dostawca usług audytu przywróci zakres niestandardowy pełny do zakresu standardowego. Żadnemu z uczestników *nigdy* nie udało się wybrać zakresu niestandardowego pełnego bez skorzystania z porady dostawcy usług audytu.

Ocena z zakresem niestandardowym pełnym nie otrzyma etykiet TISAX. Dlatego zasadniczo odradzamy wybór zakresu niestandardowego pełnego — przede wszystkim ze względu na fakt, że pozostali uczestnicy zasadniczo nie akceptują wyników oceny z zakresami niestandardowymi pełnymi.
Zakresu niestandardowego pełnego nie należy wybierać, jeśli nie posiadają Państwo wyraźnego potwierdzenia, że Państwa partner zaakceptuje wynik i jeśli nie ustalił z Państwem określonego opisu zakresu.

7.9. Załącznik: Zarządzanie cyklem życia danych uczestników

W poniższych punktach opisano, co należy zrobić w przypadku zmian Państwa danych uczestnika.

7.9.1. Utrata dostępu do danych uczestnika (portal ENX)

Prosimy o kontakt, jeśli w Państwa firmie nie została ani jedna osoba posiadająca dostęp do portalu ENX, a tym samym do Państwa danych uczestnika. Spróbujemy pomóc Państwu w odzyskaniu dostępu do danych uczestnika Państwa spółki.

7.9.2. Administrowanie osobami do kontaktu

Główne osoby w Państwa spółce do kontaktu ze strony uczestnika i inne „administracyjne osoby do kontaktu” posiadające konta na portalu mogą zawsze uzyskać dostęp do portalu ENX i:

- dodać nowe osoby do kontaktu
- usunąć istniejące osoby do kontaktu
- zmienić dane kontaktowe istniejących osób do kontaktu

7.9.2.1. Dodawanie nowej osoby do kontaktu

Aby dodać nową osobę do kontaktu, należy postąpić następująco:

1. Zalogować się na portalu ENX.
2. Przejść do głównego paska nawigacji i zaznaczyć „MY TISAX” (🇵🇱 „MÓJ TISAX”).

. w rozwijanym menu zaznaczyć „ADMINISTRATORS” („ADMINISTRATORZY”).

3. Kliknąć przycisk „Create new TISAX Administrator” („Utwórz nowego Administratora TISAX”).
4. Wprowadzić dane osoby do kontaktu.
5. Kliknąć przycisk „Save Contact” („Zapisz osobę do kontaktu”).
6. Przejść do tabeli i znaleźć wiersz zawierający osobę do kontaktu.
7. Przejść na koniec wiersza tabeli dla osoby do kontaktu i kliknąć strzałkę w dół .
8. Zaznaczyć „Edit TISAX Administrator” („Edytuj Administratora TISAX”).
   . w nowym oknie („Edit TISAX Contact” („Edytuj osobę do kontaktu TISAX”)) przewinąć do dołu do punktu „ENX PORTAL ACCESS” („DOSTĘP DO PORTALU ENX”).
9. Zaznaczyć „Yes” („Tak”).
   . w wyświetlonej sekcji „WEB ROLES” („ROLE SIECIOWE”) kliknąć przycisk „Add Role” („Dodaj rolę”).
10. Zaznaczyć rolę, którą chcą Państwo przypisać (np. „TISAX Administrator” („Administrator TISAX”)).
11. Kliknąć przycisk „Dodaj rolę”.
12. Kliknąć przycisk „Zapisz osobę do kontaktu”.

7.9.2.2. Usuwanie istniejącej osoby do kontaktu

Aby usunąć istniejącą osobę do kontaktu, należy postąpić następująco:

1. Zalogować się na portalu ENX.
2. Przejść do głównego paska nawigacji i zaznaczyć „MY TISAX” („MÓJ TISAX”).
   . w rozwijanym menu zaznaczyć „ADMINISTRATORS” („ADMINISTRATORZY”).
3. Przejść do tabeli i znaleźć wiersz zawierający osobę do kontaktu.
4. Przejść na koniec wiersza tabeli dla osoby do kontaktu i kliknąć strzałkę w dół .
5. Zaznaczyć „Delete TISAX Administrator” („Usuń Administratora TISAX”).
   . w wyświetlonej prośbie o potwierdzenie kliknąć przycisk „Delete” („Usuń”).

7.9.2.3. Aktualizacja danych istniejącej osoby do kontaktu

Aby zaktualizować dane istniejącej osoby do kontaktu, należy postąpić następująco:

1. Zalogować się na portalu ENX.
2. Przejść do głównego paska nawigacji i zaznaczyć „MY TISAX” („MÓJ TISAX”).
   . w rozwijanym menu zaznaczyć „ADMINISTRATORS” („ADMINISTRATORZY”).
3. Przejść do tabeli i znaleźć wiersz zawierający osobę do kontaktu.

4. Przejść na koniec wiersza tabeli dla osoby do kontaktu i kliknąć strzałkę w dół .
5. Zaznaczyć „Edit TISAX Administrator” („Edytuj Administratora TISAX”).
6. Zaktualizować dane.
7. Kliknąć przycisk „Save Contact” („Zapisz osobę do kontaktu”).

7.9.3. Administrowanie lokalizacjami

Główne osoby do kontaktu ze strony uczestnika w Państwa spółce i inne „administracyjne osoby do kontaktu” posiadające konta na portalu mogą zawsze uzyskać dostęp do portalu ENX i poprosić o:

- zmianę nazwy spółki
- zmianę lokalizacji (przeniesienie/relokacja)
- zmianę ulicy
- dodanie nowej lokalizacji

Niezbędne czynności opisujemy w kolejnych punktach.

Uwaga:

- W TISAX połączenie nazwy spółki i adresu określa „lokalizację”.
- Każda lokalizacja posiada „Identyfikator lokalizacji” (identyfikatory lokalizacji zawsze zaczynają się literą „L” i składają z sześciu znaków, na przykład L1L3XY).
- W przypadku przeniesienia spółki pod nowy adres, dawna lokalizacja nie jest lokalizacją prawidłową.

Ważna uwaga:

Kiedy na portalu ENX klikną Państwo przycisk „Zapisz lokalizację”, nie będą jej Państwo mogli już samodzielnie zmienić. w poniższych sytuacjach mogą Państwo wystąpić o wprowadzenie zmian.

7.9.3.1. Wniosek o zmianę nazwy spółki

Państwa sytuacja:	Państwa spółka zmieniła nazwę.
Przykład:	Dawna nazwa spółki brzmiała „ACME Tires Corporation”. Nowa nazwa spółki to „ACME Corporation”.

Jeśli chcą Państwo wystąpić o zmianę nazwy spółki, proszę postępować następująco:

1. Zalogować się na portalu ENX.
2. Przejść do głównego paska nawigacji i zaznaczyć „MY TISAX” („MÓJ TISAX”).
   . w rozwijanym menu zaznaczyć „LOCATIONS” („LOKALIZACJE”).
3. Przejść do tabeli i znaleźć wiersz zawierający Państwa lokalizację.
4. Przejść na koniec wiersza tabeli dla Państwa lokalizacji i kliknąć strzałkę w dół .
5. Zaznaczyć „Request Change” („Wniosek o zmianę”).
   . w nowym oknie („Request Change” („Wniosek o zmianę”)) przejść do pola formularza „Subject of the change” („Przedmiot zmiany”), otworzyć rozwijane menu i zaznaczyć „Company Name” („Nazwa spółki”).
6. Wypełnić pozostałe pola formularza
7. Przesłać formularz

Zapoznamy się z Państwa wnioskiem, być może zaakceptujemy prośbę o zmianę nazwy spółki, a po jej wprowadzeniu powiadomimy Państwa.

7.9.3.2. Wniosek o zmianę lokalizacji

Państwa sytuacja:	Państwa spółka przeniosła się do nowej lokalizacji.
Przykład:	Dawna lokalizacja to „ACME Corporation, Bockenheimer Landstraße 97–99, 60325 Frankfurt, Niemcy”. Nowa lokalizacja to „ACME Corporation, Behrenstraße 35, 10117 Berlin, Niemcy”.

Ważna uwaga:

W przypadku zmiany nazwy ulicy Państwa lokalizacji przez władze, bardziej szczegółowe informacje znajdą Państwo w Punkt 7.9.3.3, “Wniosek o zmianę nazwy ulicy”.

W przypadku przeniesienia jednej z Państwa lokalizacji pod nowy adres, proszę postępować następująco:

1. Utworzyć nową lokalizację:
   a. Zalogować się na portalu ENX.
   b. Przejść do głównego paska nawigacji i zaznaczyć „MY TISAX” („MÓJ TISAX”).
      .. w rozwijanym menu zaznaczyć „Locations” („Lokalizacje”).
   c. Kliknąć przycisk „Create TISAX Location” („Utwórz lokalizację TISAX”).
      .. w nowym oknie („CREATE TISAX LOCATION” („UTWÓRZ LOKALIZACJĘ TISAX”)) wypełnić formularz danymi nowej lokalizacji.

   d. Kliknąć przycisk „Save Location” (🇵🇱 „Zapisz lokalizację”).

2. Zapamiętać „Location ID” (🇵🇱 „Identyfikator lokalizacji”) dla nowo utworzonej lokalizacji. „Identyfikator lokalizacji” znajdą Państwo w pierwszej kolumnie tabeli „MY LOCATIONS” (🇵🇱 „MOJE LOKALIZACJE”). Dostawca usług audytu potrzebuje „Identyfikatora lokalizacji” w celu aktualizacji zakresu Państwa oceny na portalu ENX.

3. Powiadomić dostawcę usług audytu o relokacji (podać „Identyfikator lokalizacji” dawnej lokalizacji oraz nowej lokalizacji).
   Czy ukończyli już Państwo ocenę?

   a. Jeśli odpowiedź brzmi NIE, nie mogą Państwo zrobić nic więcej w odniesieniu do zmiany lokalizacji.

   b. Jeśli odpowiedź brzmi TAK, muszą Państwo wystąpić do dostawcy usług audytu z wnioskiem o „ocenę rozszerzenia zakresu” (🇬🇧 „scope extension assessment”). Bardziej szczegółowe informacje znajdują się w Punkt 7.10, “Załącznik: Ocena rozszerzenia zakresu”.

Dostawca usług audytu sprawdzi Państwa wniosek i zaktualizuje zakres Państwa oceny na portalu ENX.

Uwaga:

Dostawca usług audytu może zaktualizować zakres Państwa oceny jedynie w przypadku, gdy wcześniej zlecili mu Państwo ocenę.

7.9.3.3. Wniosek o zmianę nazwy ulicy

Państwa sytuacja:	Uległa zmianie nazwa ulicy Państwa lokalizacji. Państwa spółka w dalszym ciągu znajduje się fizycznie w tym samym miejscu.
Przykład:	Dawna lokalizacja to „ACME Corporation, Bockenheimer Landstraße 97–99, 60325 Frankfurt, Niemcy”. Nowa lokalizacja to „ACME Corporation, Behrenstraße 97–99, 60325 Frankfurt, Niemcy”.

W przypadku zmiany nazwy ulicy Państwa lokalizacji przez władze, proszę postępować następująco:

1. Zalogować się na portalu ENX.
2. Przejść do głównego paska nawigacji i zaznaczyć „MY TISAX” (🇵🇱 „MÓJ TISAX”).
   . w rozwijanym menu zaznaczyć „Locations” (🇵🇱 „Lokalizacje”).
3. Przejść do tabeli i znaleźć wiersz zawierający Państwa lokalizację.
4. Przejść na koniec wiersza tabeli dla Państwa lokalizacji i kliknąć strzałkę w dół ⏷.
5. Zaznaczyć „Request Change” (🇵🇱 „Wniosek o zmianę”).

. w nowym oknie („Request Change” („Wniosek o zmianę”)) przejść do pola formularza „Subject of the change” („Przedmiot zmiany”), otworzyć rozwijane menu i zaznaczyć „Address” („Adres”).

6. Wypełnić pozostałe pola formularza
7. Przesłać formularz

Zapoznamy się z Państwa wnioskiem, być może zaakceptujemy prośbę o zmianę nazwy ulicy, a po jej wprowadzeniu powiadomimy Państwa.

Ważna uwaga:

Te etapy obowiązują jedynie w przypadku, gdy Państwa spółka w dalszym ciągu znajduje się fizycznie w tym samym miejscu, choć władze zmieniły nazwę ulicy.
W przypadku przeniesienia spółki do nowej lokalizacji szczegółowe informacje znajdą Państwo w Punkt 7.9.3.2, “Wniosek o zmianę lokalizacji”.

7.9.3.4. Dodawanie kolejnej lokalizacji

W przypadku otwarcia dodatkowej lokalizacji w okresie ważności istniejących etykiet TISAX, mogą Państwo wystąpić do dostawcy usług audytu z wnioskiem o „ocenę rozszerzenia zakresu” („scope extension assessment”).

Bardziej szczegółowe informacje znajdują się w Punkt 7.10, “Załącznik: Ocena rozszerzenia zakresu”.

7.10. Załącznik: Ocena rozszerzenia zakresu

Oprócz standardowych rodzajów oceny opisanych w Punkt 5.4.3, “Rodzaje ocen TISAX” istnieje inny szczególny rodzaj oceny, tj. „ocena rozszerzenia zakresu” („scope extension assessment”).

Obecny zakres oceny TISAX można rozszerzyć, jeśli chcą Państwo dodać co najmniej jeden:

- cel oceny, lub
- lokalizację.

Nie można wybrać innego dostawcy usług audytu do przeprowadzenia „oceny rozszerzenia zakresu”. Ta ocena jest podobna do standardowych rodzajów oceny. Jednakże dostawca usług audytu najprawdopodobniej rozważy wykorzystanie odpowiednich wyników wcześniejszych ocen.

Po zakończeniu oceny rozszerzenia zakresu bez niezgodności dostawca usług audytu:

- zaktualizuje zakres Państwa oceny na portalu ENX.
- wyda raport z oceny rozszerzenia zakresu.

Ocena rozszerzenia zakresu nie przedłuża pierwotnego okresu ważności istniejących etykiet TISAX.

Uwaga:

Jeśli powodem oceny rozszerzenia zakresu jest relokacja lub dodatkowa lokalizacja, na portalu ENX muszą Państwo utworzyć nową lokalizację. Dostawcy usług audytu należy przekazać „Wyciąg dotyczący lokalizacji” lub co najmniej „Identyfikator lokalizacji”.
Każda lokalizacja posiada „Identyfikator lokalizacji” (Identyfikatory lokalizacji zawsze zaczynają się literą „L” i składają z sześciu znaków, na przykład L1L3XY). Państwa dostawca usług audytu potrzebuje Identyfikatora lokalizacji w celu aktualizacji wyniku Państwa oceny na portalu ENX.

7.11. Załącznik: Zarządzanie cyklem życia ISA

Za utrzymanie ISA odpowiada grupa robocza ENX.

Być może zainteresują Państwa poniższe fakty:

- VDA oficjalnie publikuje nowe wersje.
- Dostawca usług audytu wykorzysta wersję ISA obowiązującą w chwili *zlecenia* przez Państwa oceny wstępnej
- Za obopólną zgodą mogą Państwo wykorzystać nowszą wersję ISA, opublikowaną w okresie od zlecenia do rozpoczęcia oceny wstępnej.
- Datę publikacji danej wersji ISA znajdą Państwo w arkuszu Excel „Okładka”.
  - Przykład:
    Wersja: 5.0 | Zmiana 4 | 16.04.2021 r.

7.12. Załącznik: Przydatne dokumenty

W tym punkcie wymieniono dokumenty uznane przez nas za przydatne.

- Biała księga „Harmonizacja poziomów klasyfikacji”

  „Niniejsza Biała księga opisuje propozycję grupy roboczej ds. bezpieczeństwa informacji związaną z opracowaniem planu skupionego na celu ochrony poufności. Oznacza to brak udostępniania informacji osobom, organizacjom lub procesom nieuprawnionym. Co więcej, niniejsza Biała księga nie obejmuje takich celów ochrony, jak dostępność, integralność i niezawodność”.

Wydawca: Verband der Automobilindustrie e.V. (niemieckie stowarzyszenie przemysłu motoryzacyjnego)

Dostępne języki: angielski, niemiecki

https://www.vda.de/en/news/publications/publication/harmonization-of-classification-levels
https://www.vda.de/de/aktuelles/publikationen/publication/whitepaper--harmonisierung-der-klassifizierungsstufen-

- Biała księga „Zarządzanie ryzykiem dla bezpieczeństwa informacji”

  „Niniejsza Biała księga zawiera informacje dla spółek branży motoryzacyjnej dotyczące zarządzania bezpieczeństwem informacji zorientowanym na ryzyko i umożliwiające tym spółkom ustanowienie skutecznego zarządzania ryzykiem dla bezpieczeństwa informacji. Jej celem jest wspieranie organizacji w procesie przygotowania lub prowadzenia oceny TISAX, aby spełnić wymagania pytania kontrolnego 1.4.1. ISA VDA. Jej treść należy traktować jak zalecenia na potrzeby wdrożenia, nie zaś jako obowiązkowe wymagania”.

  Wydawca: Verband der Automobilindustrie e.V. (niemieckie stowarzyszenie przemysłu motoryzacyjnego)

  Dostępne języki: angielski, niemiecki

  https://www.vda.de/en/news/publications/publication/white-paper--information-security-risk-management-
  https://www.vda.de/de/aktuelles/publikationen/publication/whitepaper--risikomanagement-in-der-informationssicherheit-

7.13. Załącznik: Zarządzanie reklamacjami

7.13.1. Powody reklamacji

Nasze zarządzanie reklamacjami rozróżnia następujące dwa obszary:

1. ENX Association — organizacja regulująca TISAX
2. Dostawcy usług audytu — organizacje prowadzące oceny TISAX

7.13.1.1. Reklamacje związane z ENX Association

W przypadku reklamacji związanej z ENX Association, prosimy o kontakt z naszym „dyżurnym menedżerem TISAX” (dane kontaktowe znajdą Państwo poniżej).

7.13.1.2. Reklamacje związane z dostawcami usług audytu

W pierwszej kolejności należy podjąć próbę rozwiązania problemu bezpośrednio z audytorem.

Kolejnym etapem powinna być osoba odpowiedzialna za TISAX po stronie dostawcy usług audytu.

Kolejną osobą do kontaktu będzie osoba odpowiedzialna za zarządzanie jakością po stronie dostawcy usług audytu.

Jeśli w dalszym ciągu nie uda się rozwiązać problemu, należy skontaktować się z naszym „dyżurnym menedżerem TISAX” (dane kontaktowe znajdą Państwo poniżej).

Istnieją także opcje na szczeblu wyższym niż „dyżurny menedżer TISAX”. w takich przypadkach będą Państwo rozmawiać z dyrektorem zarządzającym ENX Association.

VDA nie uczestniczy w zarządzaniu reklamacjami.

Uwaga:

Dostawca usług audytu ma obowiązek powiadomić Państwa o przysługującym Państwu prawie do wniesienia reklamacji podczas spotkania inauguracyjnego. Sam brak przekazania takiego powiadomienia stanowi powód do reklamacji.

7.13.1.3. Wymagania związane z reklamacjami

Jeśli chcą nas Państwo zaangażować, potrzebujemy następujących informacji:

- Kto wnosi reklamację?
  - Nazwa spółki
  - Identyfikator uczestnika TISAX
  - Osoba do kontaktu (nazwisko, adres e-mail, numer telefonu)
- O którą ocenę chodzi?
  - Identyfikator oceny
  - w przypadku oceny niezarejestrowanej jeszcze na portalu ENX: Identyfikator zakresu
- Kto jest dostawcą usług audytu?
  - Nazwa firmy dostawcy usług audytu
  - Nazwiska audytora/-ów
- Czego dotyczy reklamacja?
  1. Ogólna reklamacja dotycząca działań dostawcy usług audytu
  2. Reklamacja dotycząca podejścia audytora
  3. Reklamacja dotycząca treści oceny
- W przypadku reklamacji dotyczących treści oceny: Wobec którego ustalenia wnoszą Państwo sprzeciw?

- Środek kontrolny (np. 1.6.1 "W jakim zakresie przetwarzane są wydarzenia związane z bezpieczeństwem informacji?")
- Ustalenie (pełny tekst)
- Sprzeciw wobec:
  - Interpretacji środka kontrolnego
  - Ustalenie dotyczące treści (brak odpowiedniej oceny dostępnych dowodów)
  - Ocena ryzyka (nie uwzględniono odpowiedniości)
- Argumenty wskazujące, czemu Państwo inaczej oceniają dane kwestie

7.13.2. Osoba do kontaktu w odniesieniu do reklamacji

Prosimy o kontakt z „dyżurnym menedżerem TISAX”:

Pod adresem e-mail:	tisax-complaints@enx.com
Lub numerem telefonu:	+49 69 9866927-79

Można się z nim skontaktować w zwykłych godzinach pracy w Niemczech (UTC+01:00).

Posługuje się językiem angielskim oraz niemieckim.

8. Historia dokumentu

Wersja 2.7

- Dodano cztery kolejne języki (japoński, brazylijski portugalski, włoski, koreański)
- Dodano opcję zmiany języka w wersji HTML (w prawym górnym rogu)
- Poprawiono układ wersji PDF
- w różnych punktach dodano dwa nowe cele oceny poufności
- Zaktualizowano punkt „Lista celów oceny” (skorygowano treść celu oceny „Special data”, dodano uwagę dotyczącą przeniesienia etykiety)
- Skorygowano błędy literowe

Wersja 2.6

- W tej wersji dodano ogólną uwagę dotyczącą celów oceny i etykiet: w poprzednich wersjach cele oceny i etykiety miały długą „nazwę oficjalną” oraz „nazwę skróconą” (przykład: „Postępowanie z informacjami wymagającymi wysokiej ochrony” oraz „Info high”). Ponieważ większość ludzi używała jedynie nazwy skróconej, ta forma skrócona stała się teraz „nazwą oficjalną”. Wcześniejszą długą nazwę nazywa się teraz „Opisem”. Co więcej na portalu ENX oraz we wszystkich tłumaczeniach podręcznika uczestnika TISAX używamy *jedynie* oficjalnej nazwy w języku angielskim.
- Do punktu „Lista celów oceny” dodano dwa cele oceny „Wysoka dostępność” i „Bardzo wysoka dostępność” oraz usunięto „Rysunek 6. Cele oceny TISAX (przedstawienie tabeli, formy długie i skrócone)”
- Punkt „Cele oceny i ISA” zaktualizowano, by odzwierciedlić fakt, że do dwóch celów oceny „Wysoka dostępność” i „Bardzo wysoka dostępność” odnosi się jedynie podzbiór katalogu kryteriów Bezpieczeństwo informacji
- Usunięto punkt „Cele oceny i ich współzależności”
- Do punktu „Wybór celów oceny” dodano dwa cele oceny „Wysoka dostępność” i „Bardzo wysoka dostępność”
- Do punktu „Potrzeby ochrony i poziomy oceny” dodano dwa cele oceny „Wysoka dostępność” i „Bardzo wysoka dostępność” oraz usunięto „Tabelę 5. Powiązania katalogów kryteriów ISA i potrzeb ochrony na cele oceny TISAX”
- Do punktu „Katalogi kryteriów” dodano dwa cele oceny „Wysoka dostępność” i „Bardzo wysoka dostępność”
- Punkt „Wymagania” zaktualizowano, by odzwierciedlić fakt, że do dwóch celów oceny „Wysoka dostępność” i „Bardzo wysoka dostępność” odnosi się jedynie podzbiór katalogu kryteriów Bezpieczeństwo informacji

- Punkt „Hierarchia etykiet TISAX” zaktualizowano, by odzwierciedlić fakt, że obecnie hierarchia istnieje jedynie w zaledwie kilku przypadkach, oraz usunięto „Rysunek 36. Cele oceny TISAX i etykiety TISAX (współzależności i hierarchia)”
- Punkt „Załącznik: Przydatne dokumenty” zaktualizowano, by odzwierciedlić zmiany w hiperłączach
- Różne drobne wyjaśnienia i niewielkie korekty
- Skorygowano błędy literowe

Wersja 2.5.1

- Naprawiono uszkodzone hiperłącza

Wersja 2.5

- Dodano punkt „Administrowanie lokalizacjami”
- Punkt „Załącznik: Przydatne dokumenty” zaktualizowano, by odzwierciedlić zmiany w hiperłączach

Wersja 2.4

- Z Punkt 3.1, “Informacje ogólne” usunięto nieprecyzyjne stwierdzenie dotyczące maksymalnego czasu trwania procesu oceny TISAX
- Nazwę „raport TISAX” zmieniono na „raport z oceny TISAX”
- Zaktualizowano uwagę dotyczącą różnic między normą ISO 27001 a TISAX
- Zaktualizowano „Opis zakresu”, punkt dotyczący zakresu niestandardowego przeniesiono do załącznika
- „Opis zakresu standardowego” zaktualizowano do wersji 2.0
- Do punktu „Publikacja i udostępnianie” dodano uwagę dotyczącą udostępniania statusu oceny
- Do punktu „Potrzeby ochrony i poziomy oceny” dodano informację o „poziomie oceny 2,5”, „metodzie oceny zdalnej przy wsparciu wideo”, różnice między AL 2 a AL 3, kontrolę wiarygodności a weryfikację
- Zaktualizowano hiperłącze do rozpoczęcia procesu rejestracji
- Punkt „Konto na portalu” zaktualizowano, by odzwierciedlić zmiany procesu zaproszeń
- Zmieniono hiperłącza do pobrania dokumentu ISA (teraz dostępne także pod adresem enx.com)

- Do punktu „Wycena ofert” dodano podstawę obliczania szacunkowych kosztów
- Dodano punkt „Spotkanie inauguracyjne” (treść przeniesiono z punktu „Pierwsze formalne spotkanie otwierające”)
- Do punktu „Informacje o zgodności” dodano nową tabelą zawierającą cztery rodzaje ustaleń
- Do punktu „Ocena wstępna” dodano uwagę dotyczącą ograniczeń czasowych
- Do punktu „Raport z oceny TISAX” dodano uwagę dotyczącą planu aktywnych działań korygujących
- Do punktu „Opracowanie planu działań korygujących” dodano wymagania dotyczące „ustalenia” i „przyczyny źródłowej” oraz uwagę dotyczącą szablonów planu działań korygujących
- Do punktu „Ocena planu działań korygujących” dodano uwagę dotyczącą poczty elektronicznej jako wyłącznego kanału komunikacji
- Nazwę punktu „Wymagania wstępne oceny planu działań korygujących” zmieniono na „Powody oceny planu działań korygujących” i dodano dwa powody
- Do punktu „Tymczasowe etykiety TISAX” dodano przykłady i wyjaśnienia dotyczące okresu ważności
- Nazwę punktu „Raport TISAX” zmieniono na „Raport z oceny TISAX”
- Do punktu „Odnowienie etykiet TISAX” dodano uwagę dotyczącą ponownego użycia rejestrów lokalizacji na portalu ENX
- Dodano punkt „Załącznik: Argumenty przeciwko „ocenom początkowym” i „analizom luk””
- Dodano punkt „Załącznik: Zakresy niestandardowe” („Zakres rozszerzony” i „Zakres zawężony” zastąpiono „Zakresem rozszerzonym przez klienta” oraz „Zakresem niestandardowym pełnym”)
- Do punktu „Załącznik: Ocena rozszerzenia zakresu” dodano powody i uwagę dotyczącą dodania rejestrów lokalizacji do konta uczestnika na portalu ENX
- Punkt „Załącznik: Zarządzanie cyklem życia ISA” zaktualizowano, by odzwierciedlić aktualną sytuację
- Punkt „Załącznik: Przydatne dokumenty” zaktualizowano, by odzwierciedlić zmiany w hiperłączach
- Dodano punkt „Załącznik: Zarządzanie reklamacjami”
- Numery telefonów można teraz kliknąć
- Różne drobne wyjaśnienia i niewielkie korekty
- Skorygowano błędy literowe
- Uwaga dla dostawców usług audytu TISAX: tę aktualizację oparto na dokumencie ENX ID 612 w wersji 2.1

Wersja 2.3

- Przeformułowano tekst podpisu
- Zmiana podstawowego formatu podręcznika z Word/PDF na HTML
- Dostępne kolejne tłumaczenia (na chiński i francuski, patrz kolejny punktor)
- Dodano punkt „Podręcznik uczestnika TISAX w innych językach i formatach”
- Wszystkie hiperłącza do strony głównej ENX zmieniono z "https://portal.enx.com" na "https://enx.com" (poprzednie hiperłącza są nadal aktywne)
- „ISA VDA” staje się „ISA”
- Zmieniono punkt Punkt 5.2, “Samoocena na podstawie ISA”, by odzwierciedlić zmiany wprowadzone w wersji 5 dokumentu ISA
- Zmieniono kolejność wierszy wszystkich tabel zawierających cele oceny, dopasowując ją do zmienionej kolejności katalogów kryteriów w wersji 5 dokumentu ISA
- Zaktualizowano rysunki wymieniające cele oceny, dopasowując je do zmienionej kolejności katalogów kryteriów w wersji 5 dokumentu ISA
- Zaktualizowano punkt „Dostosowanie zakresu” (rysunek 6, skorygowano błąd literowy, zaktualizowano cele oceny)
- Do punktu „Opłata” dodano informacje na temat płatności kartą kredytową
- Zaktualizowano punkt „Schemat procesu oceny TISAX” (rysunek 34, usunięto odniesienie do dostawcy usług zarządzanych)
- Zaktualizowano punkt „Załącznik: Przydatne dokumenty” (dodano Białą księgę „Zarządzanie ryzykiem dla bezpieczeństwa informacji”)

Wersja 2.2.1

- Skorygowano błędy literowe

Wersja 2.2

- Usunięto problem drukarski na okładce
- Zmieniono wszystkie hiperłącza do naszej strony głównej i plików do pobrania
- Obecnie mówimy także po włosku
- Rozbudowano punkt „Zakres niestandardowy”
- Zaktualizowano punkt „Lokalizacje w ramach zakresu”
- Usunięto cele oceny „Powiązania z osobami trzecimi”; zaktualizowano rysunki 7, 9 i 38;

zaktualizowano tabele 4, 5, 6 i 8

- Tekst „*z* poziomem oceny” zastąpiono „*na* poziomie oceny”
- Usunięto odniesienie do „Listy aktywacji TISAX” w punkcie „Potrzeby ochrony i poziomy oceny”
  (nie dotyczy)
- Dodano punkt „Cele oceny a Państwa dostawcy”
- Do punktu „Osoba do kontaktu po stronie uczestnika” dodano informacje dotyczące adresów e-mail grupy oraz zapraszania osób do kontaktu, by umożliwić im zarządzanie danymi uczestnika na portalu ENX
- Do punktu „Rejestracja zakresu oceny” dodano uwagę dotyczącą zmian zakresu oceny
- Zaktualizowano punkt „Informacje dotyczące statusu” (rysunek 12)
- Do punktu „Działanie na podstawie wyniku samooceny” dodano informacje dotyczące pomocy zewnętrznej ze strony podmiotów zewnętrznych
- Do punktu „Zakres terytorialny” dodano hiperłącze do matrycy zakresu terytorialnego dostawcy usług audytu
- Zaktualizowano punkt „Zapytania ofertowe”
- Do punktu „Wycena ofert” dodano informacje dotyczące „ocen początkowych”
- Do punktu „Odnowienie etykiet TISAX” dodano informacje dotyczące potrzeby rejestracji nowego zakresu
- Różne podpunkty punktu „Wymiana (Etap 3)” zaktualizowano, by odzwierciedlić zmiany interfejsu portalu ENX
- Do punktu „Udostępnianie własnego wyniku oceny konkretnemu partnerowi” dodano zalecenie dotyczące poziomu udostępniania i uwagę na temat zautomatyzowanego przetwarzania udostępnionych wyników oceny
- Dodano punkt „Udostępnianie wyniku oceny poza TISAX”
- Dodano punkt „Zarządzanie cyklem życia ISA”
- Zaktualizowano punkt „Załącznik: Status zakresu oceny” (nowy status „Oczekujący na Państwa zlecenie”, nazwę statusu „Oczekujący na zatwierdzenie” zmieniono na „Oczekujący na zatwierdzenie ENX”, nazwę statusu „Zatwierdzony” zmieniono na „Oczekujący na Państwa płatność”, rysunek 40)
- Zaktualizowano punkt „Załącznik: Przykładowa wiadomość e-mail z potwierdzeniem”
- Zaktualizowano punkt „Załącznik: Przykładowy wyciąg z zakresu TISAX”
- Zaktualizowano punkt „Załącznik: Status oceny” (nowy status „Ocena wstępna w toku”, nazwę statusu „Oczekujący na ocenę kontrolną” zmieniono na „Oczekujący na kontrolę”, rysunek 41)
- Usunięto punkt „Załącznik: Wcześniejsze oceny Volkswagen” (wraz z odnośnikami do niego)

(nie obowiązują)

Wersja 2.1.2

- Formalny limit „odstępu” między „Państwa punktacją” a „maksymalną punktacją” skorygowano z 25% do 30%

Wersja 2.1.1

- Skorygowano błędy literowe

Wersja 2.1

- Usunięto punkt „Dostawcy usług zarządzanych”
- Nowe cele oceny TISAX / etykiety (etykiety ochrony danych na podstawie RODO; cztery zamiast dwóch etykiet prototypów; zmiana nazwy: potrzeby ochrony zamiast poziomów ochrony; zaktualizowano porady dotyczące wyboru)
- Aktualizacje wynikające ze zmian dokumentu ISA (wersja 4.0 na 4.1)
- Odwołanie do nowego dokumentu „Uproszczona ocena grupy TISAX” (dodatek do niniejszego podręcznika)
- Dodano sugestie przypisywania nazw lokalizacji oraz nazw zakresów
- Nazwę „opłaty za rejestrację” zmieniono na „opłatę”
- Dodano zalecenia dotyczące zastępców osób do kontaktu
- Usunięto Wybór modelu naliczania opłat

Powrót do góry.

[1] Aby zapobiec ewentualnemu pomyleniu cyfr i liter (np. 8 i B), w Identyfikatorach uczestnika nie można używać określonych liter. Niektóre starsze Identyfikatory uczestnika mogą jednak zawierać literę „G”.

[1] Mogą Państwo rozważyć proces TISAX jako etap wstępny. Niektóre firmy robią tak w celu zapewnienia sobie lepszego przygotowania. Posiadanie oceny zgodności z TISAX może oznaczać znacznie krótszy okres wdrożenia, a tym samym zapewniać przewagę nad konkurencją nieposiadającą jeszcze takiej oceny.

[2] „Etykiety TISAX” są koncepcją podsumowującą wynik Państwa oceny oraz rezultatem procesu TISAX. Bardziej szczegółowe informacje znajdują się w Punkt 5.4.14, “Etykiety TISAX”.

[3] Etapy rejestracji trzeba przejść tylko raz, na początku uczestnictwa w TISAX. Podczas odnawiania wyniku oceny trzeba

jedynie zaktualizować i potwierdzić dane podane na etapie rejestracji.

[4] Zmiany OWU opublikujemy na portalu ENX i powiadomimy o nich zarejestrowane osoby do kontaktu.

[5] Dotyczy to również wszelkich innych dodatkowych umów (np. kodeksów postępowania).

[6] Przypominamy, że obecnie Państwa partner nie otrzymuje automatycznie informacji na temat nowych zgód. Kiedy wynik oceny będzie dostępny dla partnera, prawdopodobnie zechcą go Państwo powiadomić.

[7] Jeśli chcą się Państwo znaleźć na tej liście, prosimy o kontakt.

[8] Dowody to wszystko, co potwierdza Państwa oświadczenie o spełnieniu określonego wymogu. Dowody to przede wszystkim dokumenty. w charakterze dowodów z pewnością wykorzystają Państwo dokumenty wewnątrzfirmowe.

[9] Rozmowy w ramach oceny na poziomie oceny 2 zwykle prowadzi się w formie konferencji internetowej. Na Państwa żądanie rozmowy można prowadzić na miejscu

[10] Teoretycznym minimum na potrzeby uproszczonych ocen grupy są trzy lokalizacje.

[11] Jeśli już Państwo wiedzą, że będzie trzeba poprawić system zarządzania bezpieczeństwem informacji, zalecanym minimum jest zawsze co najmniej dwanaście lokalizacji.

[12] ISA odwołuje się do katalogów kryteriów także jako do „modułów”.

[13] Odpowiednią funkcję programu Excel znajdą Państwo na pasku „Dane”, sekcja „Informacje ogólne”.

[14] Czy posiadają Państwo dostawców usług audytu na potrzeby podobnych ocen (np. ISO 27001) zainteresowanych także prowadzeniem oceny TISAX? w takim przypadku prosimy o udostępnienie im niniejszego podręcznika i poproszenie ich o kontakt z nami, dzięki czemu będą mogli ustalić, jak zostać dostawcą usług audytu TISAX

[15] Dostawcy usług audytu niewymienieni na naszej liście nie mogą prowadzić ocen TISAX.

[16] W przypadku zakończenia procesu oceny nie otrzymają Państwo etykiet TISAX.

[17] Tak naprawdę istnieje też czwarty rodzaj: „ocena rozszerzenia zakresu”. Ponieważ jest to szczególny przypadek, szczegółowo opisano go w załączniku w Punkt 7.10, “Załącznik: Ocena rozszerzenia zakresu”.

[18] Formalne spotkanie *otwierające* opiszemy szczegółowo jedynie na potrzeby oceny wstępnej. w odniesieniu do innych ocen TISAX, harmonogram i kształt tych spotkań przekaże Państwu dostawca usług audytu.

[19] Niektórzy dostawcy usług audytu mogą używać terminu „spotkanie inauguracyjne” jako synonimu „formalnego spotkania otwierającego”.

[20] Formalne spotkanie *kończące* opiszemy szczegółowo jedynie na potrzeby oceny wstępnej. w odniesieniu do innych ocen TISAX, harmonogram i kształt tych spotkań przekaże Państwu dostawca usług audytu.

[21] Jeśli nie uda się rozstrzygnąć sporu, tę kwestię można eskalować. Bardziej szczegółowe informacje znajdują się w Punkt 7.13, “Załącznik: Zarządzanie reklamacjami”.

[22] Bardziej szczegółowe informacje na temat metod i intensywności audytu znajdują się w Punkt 4.3.3.5, “Potrzeby ochrony i poziomy oceny”.

[23] Jeśli nie uda się rozstrzygnąć sporu, tę kwestię można eskalować. w celu uzyskania bardziej szczegółowych informacji prosimy o kontakt.

[24] Przypominamy, że pomimo określenia odpowiednich działań korygujących mogą Państwo uzyskać całkowity wynik oceny „poważna niezgodność”. Będzie tak w przypadku braku/niemożności zapewnienia natychmiastowej skuteczności Państwa środków.

[25] Oczywiście dotyczy to oceny wstępnej, która wykazała niezgodności. w przypadku oceny wstępnej o wyniku „spełnia”, ocena kontrolna nie jest potrzebna.

[26] W teorii może to być dziewięć miesięcy po zakończeniu oceny wstępnej.

[27] Tak naprawdę istnieje też czwarty rodzaj: „raport z oceny rozszerzenia zakresu”. Ponieważ jest to szczególny przypadek, szczegółowo opisano go w Punkt 7.10, “Załącznik: Ocena rozszerzenia zakresu”.

[28] „Raport z oceny TISAX” jest oparty na szablonie, którego mają obowiązek używać wszyscy dostawcy usług audytu TISAX.

[29] Termin „odnowienie” może być mylący. Aby zachować etykietę TISAX na ponad trzy lata, trzeba ponownie przejść proces TISAX. Zaczyna się on od rejestracji nowego zakresu oceny.

[30] Nie prowadzimy wykazu identyfikatorów uczestników „ogólnodostępnych w TISAX”. Wynika to z faktu, że pragniemy uniknąć publicznego udostępniania firmom o podobnych nazwach oraz innych „błędów ludzkich”. w związku z tym Identyfikator uczestnika partnera należy zawsze uzyskać bezpośrednio od niego.

[31] Państwa partner musi się zalogować i wyszukać udostępniony wynik Państwa oceny. Państwa partner nie otrzyma automatycznego powiadomienia o nowo udostępnionych wynikach oceny.

[32] Zasadę określono w „Warunkach ogólnych uczestnictwa TISAX” (https://enx.com/tisaxgtcen.pdf).

[33] Dla statusu zakresu oceny „Oczekujący na Państwa płatność” lub „Zarejestrowany” „Informacje związane z oceną” obejmują lokalizację/lokalizacje zakresu oceny, status zakresu oceny oraz cel(e) oceny. Nie obejmują one wyników oceny ani etykiet TISAX.

[34] „Etykiety TISAX” są koncepcją podsumowującą wynik Państwa oceny oraz rezultatem procesu TISAX. Bardziej szczegółowe informacje znajdują się w Punkt 5.4.14, “Etykiety TISAX”.