Załącznik nr 2. Odniesienie wymagań TISAX (VDA ISA) do wymagań ISO 27001

ISO 27001	odniesienie do wymagań TISAX (VDA ISA)
1 Zakres normy	
2 Powołania normatywne	
3 Terminy i definicje	
4 Kontekst organizacji	
4.1 Zrozumienie organizacji i jej kontekstu	1.1 Ustanowienie systemu zarządzania bezpieczeństwem informacji
4.2 Zrozumienie potrzeb i oczekiwań stron zainteresowanych	1.1 Ustanowienie systemu zarządzania bezpieczeństwem informacji
4.3 Określenie zakresu systemu zarządzania bezpieczeństwem informacji	1.1 Ustanowienie systemu zarządzania bezpieczeństwem informacji
4.4 System zarządzania bezpieczeństwem informacji	1.1 Ustanowienie systemu zarządzania bezpieczeństwem informacji
5 Przywództwo	
5.1 Przywództwo i zaangażowanie	1.1 Ustanowienie systemu zarządzania bezpieczeństwem informacji
5.2 Polityka	
5.3 Role, odpowiedzialność i uprawnienia	
6 Planowanie	
6.1 Działania odnoszące się do ryzyk i szans	1.2 Zarządzanie ryzykiem bezpieczeństwa informacji
6.2 Cele bezpieczeństwa informacji i planowanie ich osiągnięcia	
7 Wsparcie	
7.1 Zasoby	
7.2 Kompetencje	
7.3 Uświadamianie	
7.4 Komunikacja	
7.5 Udokumentowane informacje	
8 Działania operacyjne	
8.1 Planowanie i nadzór nad działaniami operacyjnymi	1.3 Skuteczność SZBI
8.2 Szacowanie ryzyka w bezpieczeństwie informacji	1.2 Zarządzanie ryzykiem bezpieczeństwa informacji
8.3 Postępowanie z ryzykiem w bezpieczeństwie informacji	
9 Ocena wyników	
9.1 Monitorowanie, pomiary, analiza i ocena	1.3 Skuteczność SZBI
9.2 Audyt wewnętrzny	
9.3 Przegląd zarządzania	
10 Doskonalenie	
10.1 Niezgodność i działania korygujące	1.3 Skuteczność SZBI
10.2 Ciągłe doskonalenie	1.3 Skuteczność SZBI
A.5 Polityki bezpieczeństwa informacji	
A.5.1 Kierunki bezpieczeństwa informacji określane przez kierownictwo	5.1 Polityka bezpieczeństwa
A.6 Organizacja bezpieczeństwa informacji	
A.6.1 Organizacja wewnętrzna	6.1 Przypisanie odpowiedzialności za bezpieczeństwo informacji 6.2 Bezpieczeństwo informacji w projektach
A.6.2 Urządzenia mobilne i telepraca	6.3 Urządzenia mobilne
A.7 Bezpieczeństwo zasobów ludzkich	
A.7.1 Przed zatrudnieniem	7.1 Obowiązki pracowników w zakresie bezpieczeństwa informacji
A.7.2 Podczas zatrudnienia	7.2 Świadomość i szkolenia pracowników 23.7.2 Świadomość i szkolenie pracowników (połączenie z osobami trzecimi) 25.2.3 Świadomość (ochrona prototypów)
A.7.3 Zakończenie i zmiana zatrudnienia	7.1 Obowiązki pracowników w zakresie bezpieczeństwa informacji
A.8 Zarządzanie aktywami	
A.8.1 Odpowiedzialność za aktywa	8.1 Inwentaryzacja aktywów

Załącznik nr 2. Odniesienie wymagań TISAX (VDA ISA) do wymagań ISO 27001

ISO 27001	odniesienie do wymagań TISAX (VDA ISA)
A.8.2 Klasyfikacja informacji	8.2 Klasyfikacja informacji 25.2.4 Klasyfikacja bezpieczeństwa (ochrona prototypów)
A.8.3 Postępowanie z nośnikami	8.3 Przechowywanie informacji na nośnikach mobilnych
A.9 Kontrola dostępu	
A.9.1 Wymagania biznesowe wobec kontroli dostępu	9.1 Dostęp do sieci i usług sieciowych
A.9.2 Zarządzenie dostępem użytkowników	9.2 Rejestrownie użytkowników 9.3 Uprzywilejowane konta użytkowników 23.9.2 Rejestracja użytkowników (połączenie z osobami trzecimi)
A.9.3 Odpowiedzialność użytkowników	9.4 Poufność danych uwierzytelniających
A.9.4 Kontrola dostępu do systemów i aplikacji	9.4 Poufność danych uwierzytelniających 9.5 Dostęp do informacji i aplikacji
A.10 Kryptografia	
A.10.1 Zabezpieczenia kryptograficzne	10.1 Kryptografia
A.11 Bezpieczeństwo fizyczne i środowiskowe	
A.11.1 Obszary bezpieczne	11.1 Strefy bezpieczeństwa 11.2 Ochrona przed zewnętrznymi wpływami i zagrożeniami 11.3 Środki ochrony w obszarze dostawy i wysyłki 23.11.1 Strefy bezpieczeństwa (połączenie z osobami trzecimi) 25.1.2 Bezpieczeństwo obszaru /otoczenia (ochrona prototypów) 25.1.5 Ochrona przed nieautoryzowanym wejściem i kontrola dostępu (ochrona prototypów) 25.1.6 Monitorowanie wtargnięcia (ochrona prototypów) 25.1.7 Udokumentowane zarządzanie gośćmi (ochrona prototypów) 25.2.5 Kontrola dostępu (ochrona prototypów) 25.2.6 Regulacje dotyczące filmów i zdjęć (ochrona prototypów) 25.2.7 Mobilne urządzenia wideo i fotograficzne (ochrona prototypów) 25.5.1 Prezentacje i wydarzenia (ochrona prototypów) 25.5.2 Sesje filmowe i fotograficzne (ochrona prototypów)
A.11.2 Sprzęt	11.4 Używanie wyposażenia
A.12 Bezpieczna eksploatacja	
A.12.1 Procedury eksploatacyjne i odpowiedzialność	12.1 Zarządzanie zmianami 12.2 Oddzielanie środowisk rozwojowych, testowych i produkcyjnych
A.12.2 Ochrona przed szkodliwym oprogramowaniem	12.3 Ochrona przed szkodliwym oprogramowaniem
A.12.3 Kopie zapasowe	
A.12.4 Rejestrowanie zdarzeń i monitorowanie	12.5 Rejestrowanie zdarzeń 12.6 Rejestrowanie działań administracyjnych
A.12.5 Nadzór nad oprogramowaniem produkcyjnym	
A.12.6 Zarządzanie podatnościami technicznymi	12.6 Rejestrowanie działań administracyjnych
A.12.7 Rozważania dotyczące audytu systemów informacyjnych	12.8 Przegląd systemów informatycznych
A.13 Bezpieczeństwo komunikacji	
A.13.1 Zarządzanie bezpieczeństwem sieci	13.1 Zarządzanie sieciami 13.2 Wymagania bezpieczeństwa dla sieci / usług 13.3 Separacja sieci (segmentacja sieci) 23.13.3 Separacja sieci (segmentacja sieci) (połączenie z osobami trzecimi)
A.13.2 Przesyłanie informacji	13.4 Elektroniczna wymiana informacji 13.5 Umowy o zachowaniu poufności dotyczące wymiany informacji ze stronami trzecimi 25.2.1 Obowiązki zachowania poufności (ochrona prototypów) 25.2.2 Podwykonawcy (ochrona prototypów)

Załącznik nr 2. Odniesienie wymagań TISAX (VDA ISA) do wymagań ISO 27001

ISO 27001	odniesienie do wymagań TISAX (VDA ISA)
A.14 Pozyskiwanie, rozwój i utrzymanie systemów	
A.14.1 Wymagania związane z bezpieczeństwem systemów informacyjnych	14.1 Wymagania dotyczące nabywania systemów informatycznych
A.14.2 Bezpieczeństwo w procesach rozwoju i wsparcia	14.2 Bezpieczeństwo podczas procesu tworzenia oprogramowania
A.14.3 Dane testowe	14.3 Zarządzanie danymi testowymi
A.15 Relacje z dostawcami	
A.15.1 Bezpieczeństwo informacji w relacjach z dostawcami	15.1 Zarządzanie ryzykiem we współpracy z dostawcami 25.2.2 Podwykonawcy (ochrona prototypów)
A.15.2 Zarządzanie usługami świadczonymi przez dostawców	15.2 Przegląd świadczenia usług przez dostawców
A.16 Zarządzanie incydentami związanymi z bezpieczeństwem informacji	
A.16.1 Zarządzanie incydentami związanymi z bezpieczeństwem informacji oraz udoskonaleniami	16.1 System raportowania incydentów związanych z bezpieczeństwem informacji (zarządzanie incydentami) 16.2 Procesowanie incydentów związanych z bezpieczeństwem informacji
A.17 Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania	
A.17.1 Ciągłość bezpieczeństwa informacji	17.1 Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania
A.17.2 Nadmiarowość	17.1 Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania
A.18 Zgodność	
A.18.1 Zgodność z wymaganiami prawnymi i umownymi	18.1 Przepisy prawne i umowne 18.2 Poufność i ochrona danych osobowych
A.18.2 Przeglądy bezpieczeństwa informacji	12.8 Przegląd systemów informatycznych 18.3 Audyt SZBI przez niezależne jednostki 18.4 Test skuteczności