Załącznik nr 1. Odniesienie wymagań ISO 27001 oraz innych standardów do wymagań TISAX (VDA ISA)

System Zarządzania bezpieczeństwem informacji

wymagany poziom dojrzałości	Obszar TISAX (VDA ISA)	odniesienie do wymagań ISO 27001 i innych standardów
	1 Aspekty ogólne	
3	1.1 Ustanowienie systemu zarządzania bezpieczeństwem informacji	ISO 27001: 4 i 5.1
3	1.2 Zarządzanie ryzykiem bezpieczeństwa informacji	ISO 27001: 8.2 i 6.1.2
3	1.3 Skuteczność SZBI	ISO 27001: 8.1, 9.1, 10.1 i 10.2
	5 Polityka bezpieczeństwa	
3	5.1 Polityka bezpieczeństwa	ISO 27001: Zabezpieczenie A.5.1.1 i A.5.1.2
	6 Organizacja bezpieczeństwa informacji	
3	6.1 Przypisanie odpowiedzialności za bezpieczeństwo informacji	ISO 27001: Zabezpieczenie A.6.1.1
3	6.2 Bezpieczeństwo informacji w projektach	ISO 27001: Zabezpieczenie A.6.1.5
3	6.3 Urządzenia mobilne	ISO 27001: Zabezpieczenie A.6.2.1 i A.6.2.2
3	6.4 Role i odpowiedzialności zewnętrznych dostawców usług IT	ISO 27017: Zabezpieczenie CLD.6.3.1
	7 Bezpieczeństwo zasobów ludzkich	
3	7.1 Obowiązki pracowników w zakresie bezpieczeństwa informacji	ISO 27001: Zabezpieczenie A.7.1.2 i A.7.3.1
4	7.2 Świadomość i szkolenia pracowników	ISO 27002: Zabezpieczenie 7.2.1 i 7.2.2
	8 Zarządzanie aktywami	
3	8.1 Inwentaryzacja aktywów	ISO 27001: Zabezpieczenie A.8.1.1, A.8.1.2, A.8.1.3 i A.8.1.4
2	8.2 Klasyfikacja informacji	ISO 27001: Zabezpieczenie A.8.2.1, A.8.2.2 i A.8.2.3
3	8.3 Przechowywanie informacji na nośnikach mobilnych	ISO 27001: Zabezpieczenie A.8.3.1, A.8.3.2 i A.8.3.3
3	8.4 Usuwanie aktywów informacyjnych przechowywanych na zewnątrz (np. w chmurze)	ISO 27017: Zabezpieczenie CLD.8.1.5
	9. Kontrola dostępu	
3	9.1 Dostęp do sieci i usług sieciowych	ISO 27001: Zabezpieczenie A.9.1.2
4	9.2 Rejestrownie użytkowników	ISO 27001: Zabezpieczenie A.9.2.1, A.9.2.2, A.9.2.4 i A.9.2.5
3	9.3 Uprzywilejowane konta użytkowników	ISO 27001: Zabezpieczenie A.9.2.3
3	9.4 Poufnośc danych uwierzytelniających	ISO 27001: Zabezpieczenie A.9.3.1 i A.9.4.3
3	9.5 Dostęp do informacji i aplikacji	ISO 27001: Zabezpieczenie A.9.4.1
3	9.6 Rozdzielanie informacji we współdzielonych środowiskach	ISO 27017: Zabezpieczenie CLD.9.5.1 i CLD.9.5.2
	10 Kryptografia	
3	10.1 Kryptografia	ISO 27001: Zabezpieczenie A.10.1.1
	11 Bezpieczeństwo fizyczne i środowiskowe	
3	11.1 Strefy bezpieczeństwa	ISO 27001: Zabezpieczenie A.11.1.1 i A.11.1.2
3	11.2 Ochrona przed zewnętrznymi wpływami i zagrożeniami	ISO 27001: Zabezpieczenie A.11.1.4
2	11.3 Środki ochrony w obszarze dostawy i wysyłki	ISO 27001: Zabezpieczenie A.11.1.6
2	11.4 Używanie wyposażenia	ISO 27001: Zabezpieczenie A.11.2.5, A.11.2.6 i A.11.2.7
	12 Bezpieczna ekslpoatacja	
4	12.1 Zarządzanie zmianami	ISO 27001: Zabezpieczenie A.12.1.2
2	12.2 Oddzielanie środowisk rozwojowych, testowych i produkcyjnych	ISO 27001: Zabezpieczenie A.12.1.4
4	12.3 Ochrona przed szkodliwym oprogramowaniem	ISO 27001: Zabezpieczenie A.12.2.1
4	12.4 Procedury kopii zapasowej	ISO 27001: Zabezpieczenie A.12.3.1
3	12.5 Rejestrowanie zdarzeń	ISO 27001: Zabezpieczenie A.12.4.1 i A.12.4.2
2	12.6 Rejestrowanie działań administracyjnych	ISO 27001: Zabezpieczenie A.12.4.3

Załącznik nr 1. Odniesienie wymagań ISO 27001 oraz innych standardów do wymagań TISAX (VDA ISA)

4	12.7 Śledzenie podatności na zagrożenia (zarządzanie łatkami)	ISO 27001: Zabezpieczenie A.12.6.1 i A.12.6.2
2	12.8 Przegląd systemów informatycznych	ISO 27001: Zabezpieczenie A.12.7.1, A.18.2.3
3	12.9 Uwzględnienie kluczowych funkcji administracyjnych usług w chmurze	ISO 27017: Zabezpieczenie CLD.12.1.5
	13 Bezpieczeństwo komunikacji	
3	13.1 Zarządzanie sieciami	ISO 27001: Zabezpieczenie A.13.1.1
3	13.2 Wymagania bezpieczeństwa dla sieci / usług	ISO 27001: Zabezpieczenie A.13.1.2
3	13.3 Separacja sieci (segmentacja sieci)	ISO 27001: Zabezpieczenie A.13.1.3
3	13.4 Elektroniczna wymiana informacji	ISO 27001: Zabezpieczenie A.13.2.1 i A.13.2.3
3	13.5 Umowy o zachowaniu poufności dotyczące wymiany informacji ze stronami trzecimi	ISO 27001: Zabezpieczenie A.13.2.4
	14 Pozyskiwanie, rozwój i utrzymanie systemów	
3	14.1 Wymagania dotyczące nabywania systemów informatycznych	ISO 27001: Zabezpieczenie A.14.1.1, A.14.1.2 i A.14.1.3
3	14.2 Bezpieczeństwo podczas procesu tworzenia oprogramowania	ISO 27001: Zabezpieczenie A.14.2.1 - A.14.2.9
2	14.3 Zarządzanie danymi testowymi	ISO 27001: Zabezpieczenie A.14.3.1
3	14.4 Zatwierdzanie zewnętrznych usług IT	ISO 27017: CLD.14.1.1
	15 Relacje z dostawcami	
3	15.1 Zarządzanie ryzykiem we współpracy z dostawcami	ISO 27001: Zabezpieczenie A.15.1.1 - A.15.1.3
3	15.2 Przegląd świadczenia usług przez dostawców	ISO 27001: Zabezpieczenie A.15.2.1
	16 Zarządzanie incydentami związanymi z bezpieczeństwem informacji	
3	16.1 System raportowania incydentów związanych z bezpieczeństwem informacji (zarządzanie incydentami)	ISO 27001: Zabezpieczenie A.16.1.1 - A.16.1.3
4	16.2 Procesowanie incydentów związanych z bezpieczeństwem informacji	ISO 27001: Zabezpieczenie A.16.1.4 - A.16.1.7
	17 Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania	
3	17.1 Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania	ISO 27001: Zabezpieczenie A.17.1.1 - A.17.1.3 i A.17.2.1
	18 Zgodność	
3	18.1 Przepisy prawne i umowne	ISO 27001: Zabezpieczenie A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.5
3	18.2 Poufność i ochrona danych osobowych	ISO 27001: Zabezpieczenie A.18.1.4 + moduł: ochrona danych
3	18.3 Audyt SZBI przez niezależne jednostki	ISO 27001: Zabezpieczenie A.18.2.1
3	18.4 Test skuteczności	ISO 27001: Zabezpieczenie A.18.2.2, A.18.2.3

Połączenie z osobami trzecimi

wymagany poziom dojrzałości	Obszar TISAX (VDA ISA)	odniesienie do wymagań ISO 27001 i innych standardów
	23 Dodatkowe wymagania dotyczące połączenia z osobami trzecimi	
	23.7 Bezpieczeństwo zasobów ludzkich	
3	23.7.2 Świadomość i szkolenie pracowników	ISO 27001: Zabezpieczenie A.7.2.1 i A.7.2.2
	23.9 Kontrola dostępu	
3	23.9.2 Rejestracja użytkowników	ISO 27001: Zabezpieczenie A.9.2.1, A.9.2.2, A.9.2.4 i A.9.2.5
	23.11 Bezpieczeństwo fizyczne i środowiskowe	
3	23.11.1 Strefy bezpieczeństwa	ISO 27001: Zabezpieczenie A.11.1.1 i A.11.1.2
	23.13 Bezpieczeństwo komunikacji	
3	23.13.3 Separacja sieci (segmentacja sieci)	ISO 27001: Zabezpieczenie A.13.1.3

Załącznik nr 1. Odniesienie wymagań ISO 27001 oraz innych standardów do wymagań TISAX (VDA ISA)

Ochrona prototypów

wymagany poziom dojrzałości	Obszar TISAX (VDA ISA)	odniesienie do wymagań ISO 27001 i innych standardów
	25 Ochrona prototypów	
	25.1 Bezpieczeństwo fizyczne i środowiskowe	
3	25.1.1 Koncepcja bezpieczeństwa	no reference to ISO 27001
3	25.1.2 Bezpieczeństwo obszaru /otoczenia	ISO 27001: Zabezpieczenie A.11.1.1
3	25.1.3 Trwałość powłoki zewnętrznej	no reference to ISO 27001
3	25.1.4 Ochrona przed wzrokiem osób nieuprawnionych	no reference to ISO 27001
3	25.1.5 Ochrona przed nieautoryzowanym wejściem i kontrola dostępu	ISO 27001: Zabezpieczenie A.11.1.1, A.11.1.2 i A.11.1.3
3	25.1.6 Monitorowanie wtargnięcia	ISO 27001: Zabezpieczenie A.11.1.2
3	25.1.7 Udokumentowane zarządzanie gośćmi	ISO 27001: Zabezpieczenie A.11.1.1
3	25.1.8 Separacja Klienta	no reference to ISO 27001
	25.2 Wymagania organizacyjne	
3	25.2.1 Obowiązki zachowania poufności	ISO 27001: Zabezpieczenie A.13.2.4
3	25.2.2 Podwykonawcy	ISO 27001: Zabezpieczenie A.13.2.4, A.15.1.1, A.15.1.2 i A.15.1.3
3	25.2.3 Świadomość	ISO 27001: Zabezpieczenie A.7.2.1 i A.7.2.2
3	25.2.4 Klasyfikacja bezpieczeństwa	ISO 27001: Zabezpieczenie A.8.2.2
3	25.2.5 Kontrola dostępu	ISO 27001: Zabezpieczenie A.11.1.2
3	25.2.6 Regulacje dotyczące filmów i zdjęć	ISO 27001: Zabezpieczenie A.11.1.5
3	25.2.7 Mobilne urządzenia wideo i fotograficzne	ISO 27001: Zabezpieczenie A.11.1.5
	25.3 Obsługa pojazdów, komponentów i części	
3	25.3.1 Transport	no reference to ISO 27001
3	25.3.2 Parking i przechowywanie	no reference to ISO 27001
	25.4 Wymagania dotyczące pojazdów testowych	
3	25.4.1 Kamuflaż	no reference to ISO 27001
3	25.4.2 Obszar prób i testów	no reference to ISO 27001
3	25.4.3 Próby i testy na drogach publicznych	no reference to ISO 27001
	25.5 Wymagania dotyczące wydarzeń	
3	25.5.1 Prezentacje i wydarzenia	ISO 27001: Zabezpieczenie A.11.1.5
3	25.5.2 Sesje filmowe i fotograficzne	ISO 27001: Zabezpieczenie A.11.1.5