KOMISJA
EUROPEJSKA

Bruksela, dnia 13.3.2019 r.
C(2019) 1789 final

ANNEX 4

ZAŁĄCZNIK

do

rozporządzenia delegowanego Komisji

uzupełniającego dyrektywę Parlamentu Europejskiego i Rady 2010/40/UE w odniesieniu do wdrażania i eksploatacji współpracujących inteligentnych systemów transportowych

{SEC(2019) 100 final} - {SWD(2019) 95 final} - {SWD(2019) 96 final}

SPIS TREŚCI

ZAŁĄCZNIK IV

1. POLITYKA BEZPIECZEŃSTWA C-ITS

1.1. Definicje i skróty

EU CCMS	unijny system zarządzania danymi uwierzytelniającymi C-ITS
CAM	komunikat usługi świadomości współpracy
CP	polityka certyfikacji
DENM	komunikat powiadomienia w środowisku zdecentralizowanym
SZBI	system zarządzania bezpieczeństwem informacji
IVIM	komunikat przekazujący informacje infrastruktura–pojazd
SPATEM	rozszerzony komunikat dotyczący fazy i czasu sygnalizacji
SREM	rozszerzony komunikat dotyczący żądania priorytetu sygnalizacji
SSEM	rozszerzony komunikat dotyczący statusu żądania priorytetu sygnalizacji

1.2. Definicje

dostępność	dostępność i możliwość wykorzystania na żądanie uprawnionego podmiotu (ISO 27000) [2]
infrastruktura C-ITS	system obiektów, sprzętu i aplikacji potrzebnych do działania organizacji, która świadczy usługi C-ITS związane ze stałymi stacjami C-ITS.
zainteresowane strony C-ITS	osoba, grupa lub organizacja pełniąca rolę w sieci C-ITS oraz odpowiedzialna za nią
informacje poufne	informacje, których nie należy udostępniać ani ujawniać nieupoważnionym osobom, podmiotom lub procesom (ISO 27000) [2]
bezpieczeństwo informacji	zachowanie poufności, integralności i dostępności informacji (ISO 27000) [2]
incydent związany z bezpieczeństwem informacji	niepożądane lub nieoczekiwane zdarzenie związane z bezpieczeństwem informacji lub seria zdarzeń, w przypadku których prawdopodobieństwo zakłócenia działalności gospodarczej i zagrożenia bezpieczeństwa informacji jest wysokie
integralność	dokładność i kompletność (ISO 27000) [2]

lokalna mapa dynamiczna (LDM)	dynamicznie aktualizowane repozytorium danych dotyczących lokalnych warunków jazdy z pokładowej stacji C-ITS; obejmuje informacje otrzymane z czujników pokładowych oraz wiadomości CAM i DENM (ETSI TR 102 893) [5]
kontrola protokołu	Elementy zawiadujące kontrolą protokołu wybierają protokół przesyłania wiadomości odpowiedni do żądania dotyczącego wychodzącej wiadomości i przesyłają wiadomość do niższych warstw stosu protokolarnego w formacie, który może być przetwarzany w tych warstwach. Wiadomości przychodzące są przekształcane na format, który jest obsługiwany w danej stacji C-ITS, i przekazywane do odpowiedniego oprogramowania funkcjonalnego w celu dalszego przetworzenia (ETSI TR 102 893) [5]

1.3. Strategia na rzecz bezpieczeństwa informacji

1.3.1. System zarządzania bezpieczeństwem informacji (SZBI)

1) Każdy operator stacji C-ITS obsługuje SZBI zgodnie z normą ISO/IEC 27001, a także ograniczeniami i dodatkowymi wymogami określonymi w niniejszej sekcji.

2) Każdy operator stacji C-ITS określa zewnętrzne i wewnętrzne kwestie dotyczące C-ITS, w tym te opisane w:

   - COM(2016) 766 final [10]
   - ogólnym rozporządzeniu o ochronie danych [6].

3) Każdy operator stacji C-ITS określa strony, które mają znaczenie dla SZBI, i ich wymogi, w tym wszystkie zainteresowane strony C-ITS.

4) Zakres SZBI obejmuje wszystkie obsługiwane stacje C-ITS i wszystkie inne systemy przetwarzania informacji przetwarzające dane C-ITS w formie wiadomości C-ITS, które są zgodne z następującymi standardami:

   - CAM [7]
   - DENM [8]
   - IVIM [9]
   - SPATEM [9]
   - MAPEM [9]
   - SSEM [9]
   - SREM [9]

5) Każdy operator stacji C-ITS zapewnia zgodność swojej polityki bezpieczeństwa informacji z niniejszą polityką.

6) Każdy operator stacji C-ITS zapewnia, aby jego cele związane z bezpieczeństwem informacji obejmowały cele w zakresie bezpieczeństwa i były spójne z nimi, a także z ogólnymi wymaganiami niniejszej polityki.

7) Operatorzy stacji C-ITS dokonują klasyfikacji informacji, o których mowa w sekcji 1.4.

8) Operatorzy stacji C-ITS stosują proces oceny ryzyka związanego z bezpieczeństwem informacji określony w sekcji 1.5 w planowanych

odstępach czasu lub w przypadku gdy proponowane są lub zachodzą istotne zmiany.

9) Operatorzy lub producenci stacji C-ITS określają wymogi dotyczące ograniczania ryzyka związanego z bezpieczeństwem informacji zidentyfikowanego w procesie oceny takiego ryzyka zgodnie z sekcją 1.6.

10) Producenci stacji C-ITS projektują, opracowują i oceniają stacje C-ITS oraz inne systemy przetwarzania informacji w sposób zapewniający zgodność z obowiązującymi wymogami.

11) Operatorzy stacji C-ITS obsługują stacje C-ITS i wszystkie inne systemy przetwarzania informacji, które wdrażają odpowiednie środki kontroli w zakresie postępowania z ryzykiem związanego z bezpieczeństwem informacji zgodnie z sekcją 1.6.

1.4. Klasyfikacja informacji

W niniejszej sekcji określono minimalne wymogi w zakresie klasyfikacji informacji. Nie uniemożliwia to zainteresowanym stronom w dziedzinie C-ITS stosowania bardziej rygorystycznych wymogów.

12) Operatorzy stacji C-ITS klasyfikują obsługiwane informacje, przy czym kategorię bezpieczeństwa można przedstawić w następujący sposób:

Informacje w zakresie kategorii bezpieczeństwa = {(poufność, skutek), (integralność, skutek), (dostępność, skutek)};

13) Zainteresowane strony C-ITS klasyfikują informacje, którymi zarządzają, przy czym system kategorii bezpieczeństwa można przedstawić w następujący sposób:

System informacyjny w zakresie kategorii bezpieczeństwa = {(poufność, skutek), (integralność, skutek), (dostępność, skutek)};

14) Dopuszczalne wartości potencjalnego skutku to: niewielki, umiarkowany i poważny, jak przedstawiono w tabeli **1**.

Tabela 1 Definicje potencjalnych skutków w odniesieniu do każdego celu związanego z bezpieczeństwem: poufności, integralności i dostępności

	Potencjalny skutek		
Cel związany z bezpieczeństwem	**NIEWIELKI**	**UMIARKOWANY**	**POWAŻNY**
Poufność Zachowanie dozwolonych ograniczeń w zakresie dostępu do informacji i ich ujawniania, w tym środków ochrony prywatności i informacji zastrzeżonych	Nieuprawnione ujawnienie informacji może mieć ograniczone niekorzystne skutki dla funkcjonowania organizacji, aktywów organizacyjnych lub dla osób fizycznych.	Nieuprawnione ujawnienie informacji może mieć poważne niekorzystne skutki dla funkcjonowania organizacji, aktywów organizacyjnych lub dla osób fizycznych.	Nieuprawnione ujawnienie informacji może mieć poważne lub katastrofalne, niekorzystne skutki dla funkcjonowania organizacji, aktywów organizacyjnych lub dla osób fizycznych.

	Potencjalny skutek		
Integralność Ochrona przed niedozwolonymi zmianami informacji lub ich niszczeniem; obejmuje to zapewnienie niezaprzeczalności i autentyczności informacji	Nieuprawniona zmiana informacji lub ich nieuprawnione zniszczenie mogą mieć ograniczone niekorzystne skutki dla funkcjonowania organizacji, aktywów organizacyjnych lub dla osób fizycznych.	Nieuprawniona zmiana informacji lub ich nieuprawnione zniszczenie mogą mieć poważne niekorzystne skutki dla funkcjonowania organizacji, aktywów organizacyjnych lub dla osób fizycznych.	Nieuprawniona zmiana informacji lub ich nieuprawnione zniszczenie mogą mieć poważne lub katastrofalne niekorzystne skutki dla funkcjonowania organizacji, aktywów organizacyjnych lub dla osób fizycznych.
Dostępność Zapewnienie terminowego i niezawodnego dostępu do informacji oraz ich wykorzystania	Zakłócenia w dostępie do informacji lub systemu informacyjnego lub ich wykorzystania mogą mieć ograniczone niekorzystne skutki dla funkcjonowania organizacji, aktywów organizacyjnych lub dla osób fizycznych.	Zakłócenia w dostępie do informacji lub systemu informacyjnego lub ich wykorzystania mogą mieć poważne niekorzystne skutki dla funkcjonowania organizacji, aktywów organizacyjnych lub dla osób fizycznych.	Zakłócenia w dostępie do informacji lub systemu informacyjnego lub ich wykorzystania mogą mieć poważne lub katastrofalne niekorzystne skutki dla funkcjonowania organizacji, aktywów organizacyjnych lub dla osób fizycznych.

15) Pod względem skali szkód lub kosztów w odniesieniu do usługi C-ITS i zainteresowanych stron C-ITS spowodowanych incydentem związanym z bezpieczeństwem informacji pod uwagę bierze się następujące rodzaje skutków według klasyfikacji informacji:

- bezpieczeństwo ruchu drogowego – gdy skutki narażają użytkowników dróg na bezpośrednie ryzyko odniesienia obrażeń;
- bezpieczeństwo – gdy skutki narażają jakąkolwiek z zainteresowanych stron C-ITS na bezpośrednie ryzyko odniesienia obrażeń;
- skutki operacyjne – gdy skutki są zasadniczo negatywne dla efektywności ruchu drogowego lub występują inne skutki społeczne, takie jak ślad środowiskowy i przestępczość zorganizowana;
- skutki prawne – gdy skutki prowadzą do znaczących działań w zakresie zgodności prawnej lub regulacyjnej w odniesieniu do co najmniej jednej z zainteresowanych stron C-ITS;
- skutki finansowe – gdy skutki prowadzą do bezpośrednich lub pośrednich kosztów pieniężnych w odniesieniu do co najmniej jednej z zainteresowanych stron C-ITS;
- prywatność – ogólne rozporządzenie o ochronie danych ma skutki zarówno prawne, jak i finansowe;
- reputacja – gdy skutki prowadzą do uszczerbku na reputacji co najmniej jednej z zainteresowanych stron C-ITS lub sieci C-ITS, np. przedstawienie w prasie w niekorzystnym świetle lub poważne naciski polityczne na skalę krajową lub międzynarodową.

16) Zainteresowane strony C-ITS przestrzegają następujących minimalnych wartości skutków w odniesieniu do przetwarzanych informacji:

Tabela 2: Skutki

	Źródło informacji: stałe stacje C-ITS	**Źródło informacji: ruchome stacje C-ITS**
Poufność	CAM: niewielkie DENM: niewielkie IVIM: niewielkie MAPEM: niewielkie SPATEM: niewielkie SSEM: niewielkie	CAM: niewielkie DENM: niewielkie SREM: niewielkie dane osobowe zawarte w dowolnej z trzech wiadomości: umiarkowane
Integralność	CAM: umiarkowane DENM: umiarkowane IVIM: umiarkowane MAPEM: umiarkowane SPATEM: umiarkowane SSEM: umiarkowane	CAM: umiarkowane DENM: umiarkowane SREM: umiarkowane
Dostępność	CAM: niewielkie DENM: niewielkie IVIM: niewielkie MAPEM: niewielkie SPATEM: niewielkie SSEM: umiarkowane	CAM: niewielkie DENM: niewielkie SREM: umiarkowane

1.5. Ocena ryzyka

1.5.1. Informacje ogólne

17) Ocenę ryzyka przeprowadza się okresowo zgodnie z normą ISO/IEC 27005. Obejmuje ona odpowiednią dokumentację:

- zakresu oceny ryzyka, tj. ocenianego systemu oraz jego granic i celu systemowego, a także przetwarzanych informacji;
- kryteriów ryzyka związanego z bezpieczeństwem informacji;
- oceny ryzyka, w tym identyfikacji, analizy i ewaluacji.

1.5.2. Kryteria ryzyka związanego z bezpieczeństwem informacji

18) Kryteria szacowania ryzyka określa się z uwzględnieniem następujących aspektów:

- strategicznej wartości usługi C-ITS i sieci C-ITS dla wszystkich zainteresowanych stron C-ITS;
- strategicznej wartości usługi C-ITS i sieci C-ITS dla operatora stacji C-ITS świadczącej usługi;

- konsekwencji dla reputacji sieci C-ITS;
- wymogów prawnych i regulacyjnych oraz zobowiązań umownych.

19) Kryteria skutków ryzyka określa się w świetle rodzajów skutków według klasyfikacji informacji, o których mowa w sekcji 1.4.

20) Kryteria akceptacji ryzyka obejmują określenie poziomów ryzyka, które są nie do przyjęcia dla usługi C-ITS i zainteresowanych stron C-ITS, według rodzaju wpływu.

1.5.2.1. Identyfikacja ryzyka

21) Ryzyko określa się zgodnie z normą ISO/IEC 27005. Zastosowanie mają następujące wymogi minimalne:

- główne aktywa, które należy chronić, to wiadomości C-ITS, o których mowa w sekcji 1.3.1;
- należy zidentyfikować aktywa wspierające, w tym:
  - informacje wykorzystywane na potrzeby wiadomości C-ITS (np. lokalna mapa dynamiczna, czas, kontrola protokołu itp.);
  - stacje C-ITS i ich oprogramowanie, dane konfiguracyjne i powiązane kanały komunikacyjne;
  - centralne aktywa kontrolne C-ITS;
  - każdy podmiot w ramach unijnego systemu zarządzania danymi uwierzytelniającymi C-ITS;
- określa się zagrożenia dla tych aktywów i ich źródeł;
- określa się przeprowadzane i planowane kontrole;
- określa się słabe punkty podatne na zagrożenia, szkodzące aktywom lub zainteresowanym stronom C-ITS, i opisuje się je jako scenariusze incydentów;
- na podstawie klasyfikacji informacji określa się ewentualne konsekwencje incydentów związanych z bezpieczeństwem w odniesieniu do aktywów.

1.5.2.2. Analiza ryzyka

22) Do analizy ryzyka stosuje się następujące wymogi minimalne:

- skutki zidentyfikowanych incydentów związanych z bezpieczeństwem informacji dla usług C-ITS i zainteresowanych stron C-ITS ocenia się na podstawie kategorii informacji oraz kategorii bezpieczeństwa systemu informacyjnego przy użyciu co najmniej trzech poziomów określonych w sekcji 1.4;
- poziomy skutków określa się dla:
  - całkowitej istniejącej sieci / całkowitych istniejących usług C-ITS; oraz
  - indywidualnej zainteresowanej strony / indywidualnego podmiotu organizacyjnego w dziedzinie C-ITS

- najwyższy poziom uznaje się za skutek całkowity;
- prawdopodobieństwo wystąpienia zidentyfikowanych scenariuszy incydentów ocenia się przy użyciu co najmniej trzech poziomów spośród następujących:
  - mało prawdopodobne (wartość 1) – scenariusz incydentu jest mało prawdopodobny / trudny do zrealizowania lub motywacja atakującego jest bardzo niska;
  - możliwe (wartość 2) – scenariusz incydentu może się wydarzyć / jest możliwy do zrealizowania lub motywacja atakującego jest racjonalna;
  - prawdopodobne (wartość 3) – scenariusz incydentu jest prawdopodobny / prosty do zrealizowania lub motywacja atakującego jest wysoka;
- poziomy ryzyka ustala się dla wszystkich zidentyfikowanych scenariuszy incydentów na podstawie iloczynu skutku i prawdopodobieństwa, który daje co najmniej następujące poziomy ryzyka: niewielki (wartości 1, 2), umiarkowany (wartości 3, 4) i poważny (wartości 6, 9), określane w następujący sposób:

Tabela 3: Poziomy ryzyka

Poziomy ryzyka jako iloczyn skutku i prawdopodobieństwa		**Prawdopodobieństwo**		
		mało prawdopodobne (1)	**możliwe (2)**	**prawdopodobne (3)**
Skutek	**niewielki (1)**	niewielki (1)	niewielki (2)	umiarkowany (3)
	umiarkowany (2)	niewielki (2)	umiarkowany (4)	poważny (6)
	poważny (3)	umiarkowany (3)	poważny (6)	poważny (9)

1.5.2.3. Szacowanie ryzyka

23) Poziomy ryzyka porównuje się z kryteriami szacowania ryzyka i kryteriami akceptacji ryzyka w celu określenia sposobu postępowania z ryzykiem. W odniesieniu do usługi C-ITS i sieci C-ITS z ryzykiem na poziomie co najmniej umiarkowanym lub poważnym postępuje się w sposób określony w sekcji 1.6.

1.6. Postępowanie z ryzykiem

1.6.1. Informacje ogólne

24) Ryzyko traktuje się w jeden z następujących sposobów:

- modyfikacja ryzyka za pomocą kontroli określonych w sekcji 1.6.2 lub 1.6.3, tak aby ryzyko rezydualne można było ponownie ocenić jako dopuszczalne;
- akceptacja ryzyka (w przypadku gdy poziom ryzyka spełnia kryteria akceptacji ryzyka);
- unikanie ryzyka.

25) Podział ryzyka ani przeniesienie ryzyka nie są dozwolone w odniesieniu do ryzyka dla sieci C-ITS.

26) Należy udokumentować sposób postępowania z ryzykiem, uwzględniając:

- oświadczenie o zastosowaniu zgodne z normą ISO 27001, w której podano niezbędne kontrole i określono:
  - rezydualne prawdopodobieństwo wystąpienia;
  - rezydualną dotkliwość skutków;
  - poziom ryzyka rezydualnego;
- powody akceptacji ryzyka lub jego uniknięcia.

1.6.2. Kontrole w odniesieniu do stacji C-ITS

1.6.2.1. Kontrole ogólne

27) Stacje C-ITS wdrażają odpowiednie środki zaradcze w celu modyfikacji ryzyka zgodnie z sekcją 1.6.1. Te środki zaradcze wdrażają kontrole ogólne zdefiniowane w normach ISO/IEC 27001 i ISO/IEC 27002.

1.6.2.2. Kontrole w odniesieniu do komunikacji między stacjami C-ITS

28) Następujące minimalne kontrole obowiązkowe przeprowadza się po stronie nadawcy:

Tabela 4: Kontrole po stronie nadawcy

	Źródło informacji: stałe stacje C-ITS	**Źródło informacji: ruchome stacje C-ITS**
Poufność	-	Dane osobowe zawarte w wiadomościach są zabezpieczane przy użyciu odpowiedniej procedury zmiany biletu autoryzacyjnego (AT) w celu zapewnienia poziomu bezpieczeństwa odpowiedniego do ryzyka ponownej identyfikacji kierowców w oparciu o przekazywane dane. W związku z tym stacje C-ITS odpowiednio zmieniają AT podczas wysyłania wiadomości i nie wykorzystują ponownie AT po zmianie, z wyjątkiem przypadków nieprzeciętnych[1] zachowań kierowców.
Integralność	Wszystkie wiadomości są podpisywane zgodnie z TS 103 097 [14].	Wszystkie wiadomości są podpisywane zgodnie z TS 103 097 [14].
Dostępność	-	-

29) Następujące minimalne kontrole obowiązkowe przeprowadza się po stronie odbiorcy:

[1] Definicja przeciętnego zachowania podczas jazdy opiera się na odpowiedniej analizie statystycznej zachowań kierowców w Unii Europejskiej, np. na danych Niemieckiej Agencji Kosmicznej (DLR).

Tabela 5: Kontrole po stronie odbiorcy

	Źródło informacji: stałe stacje C-ITS	**Źródło informacji: ruchome stacje C-ITS**
Poufność		Otrzymane dane osobowe należy przechowywać przez możliwie najkrótszy czas do celów prowadzenia działalności gospodarczej, maksymalnie przez pięć minut w przypadku surowych i możliwych do zidentyfikowania danych. Otrzymana wiadomość CAM lub SRM nie jest przekazywana/nadawana. Otrzymany komunikat DENM może być przekazywany/nadawany wyłącznie na ograniczonym obszarze geograficznym.
Integralność	Integralność wszystkich wiadomości wykorzystywanych przez aplikacje ITS zatwierdza się zgodnie z TS 103 097 [14].	Integralność wszystkich wiadomości wykorzystywanych przez aplikacje ITS zatwierdza się zgodnie z TS 103 097 [14].
Dostępność	-	Otrzymana wiadomość SRM zostaje przetworzona i powstaje SSM przekazywany do nadawcy SRM.

30) Aby spełnić wymogi w zakresie ochrony poufności, integralności i dostępności określone w powyższych tabelach, wszystkie stacje C-ITS (ruchome stacje C-ITS (w tym samochodowe stacje C-ITS) i stałe stacje C-ITS) ocenia się i certyfikuje, stosując kryteria oceny bezpieczeństwa określone we „wspólnych kryteriach" / ISO 15408[2]. Ze względu na różne cechy poszczególnych rodzajów stacji C-ITS oraz różne wymogi dotyczące prywatności lokalizacji można określić różne profile zabezpieczenia.

31) Wszystkie profile zabezpieczenia i powiązane dokumenty mające zastosowanie do certyfikacji bezpieczeństwa w przypadku stacji C-ITS podlegają ocenie, walidacji i certyfikacji zgodnie z ISO 15408, z zastosowaniem *umowy o wzajemnym uznawaniu dotyczącej certyfikatów oceny bezpieczeństwa technologii informacyjnych* zawartej przez grupę wyższych urzędników ds. bezpieczeństwa systemów informatycznych (SOG-IS)[3] lub równoważnego europejskiego systemu certyfikacji w odpowiednich europejskich ramach cyberbezpieczeństwa. Przy opracowywaniu takich profili zabezpieczenia producent może określić zakres certyfikacji bezpieczeństwa stacji C-ITS, z zastrzeżeniem oceny i zatwierdzenia CPA oraz organu oceny zgodności SOG-IS lub co najmniej równoważnego organu, jak opisano w następnym akapicie.

[2] Portal „Wspólne kryteria": http://www.commoncriteriaportal.org/cc/

[3] W sektorze transportu drogowego SOG-IS jest już na przykład zaangażowany w certyfikację bezpieczeństwa inteligentnych tachografów. Umowa SOG-IS stanowi obecnie jedyny program w Europie, który może przyczyniać się do harmonizacji certyfikacji bezpieczeństwa produktów elektronicznych. Na tym etapie SOG-IS wspiera jedynie proces „wspólnych kryteriów", dlatego stacje C-ITS muszą być oceniane i certyfikowane zgodnie ze „wspólnymi kryteriami"; zob. https://www.sogis.org/

32) Ze względu na znaczenie utrzymania możliwie najwyższego poziomu bezpieczeństwa certyfikaty bezpieczeństwa dla stacji C-ITS wydaje się w ramach systemu wspólnych kryteriów certyfikacji (ISO 15408) przez organ oceny zgodności uznany przez komitet zarządzający w ramach umowy SOG-IS lub przez organ oceny zgodności akredytowany przez krajowy organ certyfikacji cyberbezpieczeństwa państwa członkowskiego. Taki organ oceny zgodności zapewnia co najmniej warunki oceny bezpieczeństwa równoważne z warunkami przewidzianymi w umowie o wzajemnym uznawaniu SOG-IS.

1.6.2.3. Kontrole w odniesieniu do stacji C-ITS jako jednostki końcowej

33) Stacje C-ITS spełniają wymagania polityki certyfikacji [1] zgodnie z ich rolą jako jednostki końcowej unijnego systemu zarządzania danymi uwierzytelniającymi C-ITS.

1.6.3. Kontrole w odniesieniu do uczestników unijnego systemu zarządzania danymi uwierzytelniającymi C-ITS

34) Uczestnicy EU CCMS przestrzegają polityki certyfikacji [1] zgodnie z pełnioną przez nich rolą w unijnym systemie zarządzania danymi uwierzytelniającymi C-ITS.

1.7. Zgodność z niniejszą polityką bezpieczeństwa

35) Operatorzy stacji C-ITS okresowo zwracają się z wnioskiem o certyfikację zgodności z niniejszą polityką i otrzymują certyfikat zgodnie z wytycznymi dotyczącymi audytu ISO 27001 [12].

36) Organ kontrolny jest akredytowany i certyfikowany przez pracownika akredytacji europejskiej. Spełnia on wymogi [11].

37) Mając na celu uzyskanie certyfikacji operatorzy stacji C-ITS prowadzą i utrzymują dokumenty dotyczące wymogów w [3] zakresie udokumentowanych informacji, o których mowa w pkt 7.5. W szczególności operatorzy stacji C-ITS prowadzą i utrzymują następujące dokumenty dotyczące SZBI:

- zakres SZBI (sekcja 1.3.1 i [3], pkt 4.3);
- polityka i cele w zakresie bezpieczeństwa informacji (sekcja 1.3.1 i [3], pkt 5.2 i 6.2);
- szczegóły dotyczące oceny ryzyka i sposobu postępowania z ryzykiem (sekcja 1.5 i [3], pkt 6.1.2);
- sprawozdanie z oceny ryzyka (sekcja 1.5 i [3], pkt 8.2);
- oświadczenie o zastosowaniu (sekcja 1.6 i [3], pkt 6.1.3d);
- plan postępowania z ryzykiem (sekcja 1.6 i [3], pkt 6.1.3e i 8.3);
- dokumenty wymagane do wdrożenia wybranych kontroli (sekcja 1.6 i [3], załącznik A).

38) Ponadto operatorzy stacji C-ITS prowadzą i utrzymują następujące rejestry jako dowody uzyskanych wyników:

- rejestry szkoleń, umiejętności, doświadczenia i kwalifikacji ([3], pkt 7.2);
- wyniki monitorowania i pomiarów ([3], pkt 9.1);

- program audytu wewnętrznego ([3], pkt 9.2);
- wyniki audytów wewnętrznych ([3], pkt 9.2);
- wyniki przeglądu zarządzania ([3], pkt 9.3);
- wyniki działań naprawczych ([3], pkt 10.1).

2. DOKUMENTY ŹRÓDŁOWE

W niniejszym załączniku wykorzystano następujące dokumenty źródłowe:

[1] Załącznik III do niniejszego rozporządzenia

[2] ISO/IEC 27000 (2016): Information technology – security techniques – information security management systems – overview and vocabulary [Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Przegląd i terminologia]

[3] ISO/IEC 27001 (2015): Information technology — security techniques – information security management systems – requirements [Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania]

[4] ISO/IEC 27005 (2011): Information technology – security techniques – information security risk management [Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji]

[5] ETSI TR 102 893 V1.2.1, Intelligent transport systems (ITS) – security; threat, vulnerability and risk analysis (TVRA)

[6] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych);

[7] ETSI EN 302 637-2 V1.4.0, Intelligent transport systems (ITS) – Vehicular communications; Basic set of applications; Part 2: Specification of cooperative awareness basic service [Inteligentne systemy transportowe (ITS) – Komunikacja pojazdowa – Podstawowy zestaw aplikacji – Część 2: Specyfikacja podstawowej usługi świadomości współpracy]

[8] ETSI EN 302 637-3 V1.3.0, Intelligent transport systems (ITS) – Vehicular communications; Basic set of applications; Part 3: Specifications of decentralised environmental notification basic service [Inteligentne systemy transportowe (ITS) – Komunikacja pojazdowa – Podstawowy zestaw aplikacji – Część 3: Specyfikacje podstawowej usługi powiadamiania w środowisku zdecentralizowanym]

[9] ETSI TS 103 301 V1.2.1: Intelligent transport systems (ITS) – Vehicular communications; Basic set of applications; Facilities layer protocols and communication requirements for infrastructure services [Inteligentne systemy

transportowe (ITS) – Komunikacja pojazdowa; Podstawowy zestaw aplikacji; Protokoły warstwy obiektów i wymogi komunikacyjne dla usług infrastrukturalnych]

[10] Europejska strategia na rzecz współpracujących inteligentnych systemów transportowych – ważny krok w kierunku mobilności pojazdów współpracujących, połączonych i zautomatyzowanych (COM(2016) 766 z dnia 30 listopada 2016 r.);

[11] ISO/IEC 27006:2015 Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems [Technika informatyczna – Techniki bezpieczeństwa – Wymagania dla jednostek prowadzących audyt i certyfikację systemów zarządzania bezpieczeństwem informacji]

[12] ISO/IEC 27007:2011 Information technology — Security techniques — Guidelines for information security management systems auditing;

[13] ETSI EN 302 665 V1.1.1 Intelligent transport systems (ITS); Communications architecture [Systemy inteligentnego transportu (ITS) – Architektura komunikacji]

[14] ETSI TS 103 097 V1.3.1. Intelligent transport systems (ITS) security; security header and certificate formats [Inteligentne systemy transportowe (ITS) – Bezpieczeństwo; Formaty nagłówków bezpieczeństwa i certyfikatów]