EUROPÄISCHE
KOMMISSION

Brüssel, den 13.3.2019
C(2019) 1789 final

ANNEX 4

ANHANG

der

Delegierten Verordnung der Kommission

zur Ergänzung der Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates im Hinblick auf die Einführung und den Betrieb kooperativer intelligenter Verkehrssysteme

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

INHALTSVERZEICHNIS

ANHANG IV

1. C-ITS-SICHERHEITSSTRATEGIE

1.1. Begriffsbestimmungen und Abkürzungen

EU-CCMS	System für das Management von Sicherheitsberechtigungsnachweisen von C-ITS-Diensten in der EU (EU C-ITS security credential management system)
CAM	Cooperative Awareness Message [kooperative Aufklärungsmeldung]
CP	Certificate policy [Zertifizierungsrichtlinie]
DENM	Decentralised environmental notification message [dezentrale Umfeldbenachrichtigung]
ISMS	Information security management system [Informationssicherheits-Managementsystem]
IVIM	infrastructure-to-vehicle information message [Informationsmeldung Infrastruktur - Fahrzeug]
SPATEM	Signal phase and timing extended message [erweiterte Meldung Ampelphase und Timing]
SREM	Signal request extended message [erweiterte Meldung (Ampel)-Signalanforderungen]
SSEM	Signal request status extended message [erweiterte Meldung (Ampel)-Signalanforderung, Status]

1.2. BEGRIFFSBESTIMMUNGEN

Verfügbarkeit	Zugänglichkeit und Nutzbarkeit auf Anfrage einer berechtigten Stelle (ISO 27000) [2]
C-ITS-Infrastruktur	System aus Einrichtungen, Geräten und Anwendungen, die für den Betrieb einer Organisation erforderlich sind, die C-ITS-Dienste im Zusammenhang mit ortsfesten C-ITS-Stationen bereitstellt.
C-ITS-Beteiligte	Natürliche Person, Gruppe oder Organisation mit einer Funktion und Verantwortlichkeit im C-ITS-Netz
Vertrauliche Informationen	Informationen, die unbefugten natürlichen Personen, Stellen oder Prozessen nicht zugänglich gemacht oder offenbart werden dürfen (ISO 27000) [2]
Informations-sicherheit	Wahrung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen (ISO 27000) [2]
für die Informations-sicherheit relevanter	Ein(e) unerwünschte(s) oder unerwartete(s), die Informationssicherheit betreffende(s) Ereignis oder Reihe von Ereignissen, bei denen eine signifikante Wahrscheinlichkeit der Beeinträchtigung des Geschäftsbetriebs und Bedrohung

Vorfall	der Informationssicherheit besteht
Integrität	Eigenschaft der Richtigkeit und Vollständigkeit (ISO 27000) [2]
Lokale dynamische Landkarte (LDM)	Eine dynamisch aktualisierte Ablage für Daten mit Bezug zu örtlichen Fahrbedingungen einer fahrzeugseitigen C-ITS-Station; sie schließt Informationen ein, die von Bordsensoren und aus CAM- und DENM-Benachrichtigungen stammen (ETSI TR 102 893) [5]
Protokoll-steuerung	Die Protokollsteuerungsposten wählen für eine ausgehende Nachrichtenanforderung ein geeignetes Nachrichtenübertragungsprotokoll aus und senden die Nachricht in einem Format an die unteren Ebenen des Protokoll-Stacks, das von diesen Ebenen verarbeitet werden kann. Eingehende Nachrichten werden in ein Format umgewandelt, das innerhalb der C-ITS-Station gehandhabt und zur weiteren Verarbeitung an den maßgebliche Funktionsposten weitergeleitet werden kann (ETSI TR 102 893) [5]

1.3. Eine Strategie für die Informationssicherheit

1.3.1. Informationssicherheits-Managementsystem (ISMS)

(1) Jeder Betreiber einer C-ITS-Station betreibt ein ISMS im Einklang mit ISO/IEC 27001 und den in diesem Abschnitt festgelegten Einschränkungen und zusätzlichen Anforderungen.

(2) Jeder Betreiber einer C-ITS-Station bestimmt externe und interne, für C-ITS maßgebliche Fragestellungen, etwa in Bezug auf:

- COM(2016) 766 final [10];
- die DSGVO [6].

(3) Jeder Betreiber einer C-ITS-Station bestimmt für das ISMS und die zugehörigen Anforderungen maßgebliche Parteien, einschließlich aller C-ITS-Interessenträger.

(4) Der Anwendungsbereich des ISMS umfasst sämtliche betriebenen C-ITS-Stationen und alle anderen Informationsverarbeitungssysteme, die C-ITS-Daten in Form von C-ITS-Nachrichten verarbeiten, die folgenden Normen entsprechen:

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

(5) Jeder Betreiber einer C-ITS-Station stellt sicher, dass seine Informationssicherheitsstrategie mit der vorliegenden Strategie kohärent ist.

(6) Jeder Betreiber einer C-ITS-Station stellt sicher, dass seine Ziele für die Informationssicherheit die Sicherheitsziele und übergeordneten Anforderungen der vorliegenden Strategie umfassen und mit ihnen kohärent sind.

(7) Die Betreiber von C-ITS-Stationen stufen die Informationen, auf die in Abschnitt 1.4 Bezug genommen wird, als vertraulich ein.

(8) Die Betreiber von C-ITS-Stationen wenden in geplanten Zeitabständen und dann, wenn erhebliche Änderungen vorgeschlagen werden oder eintreten, einen Prozess zur Bewertung von Informationssicherheitsrisiken gemäß Abschnitt 1.5 an.

(9) Die Betreiber und/oder Hersteller von C-ITS-Stationen legen gemäß Abschnitt 1.6 Anforderungen für die Minderung von Sicherheitsrisiken fest, die im Prozess zur Bewertung von Informationssicherheitsrisiken ermittelt wurden.

(10) Die Hersteller von C-ITS-Stationen entwerfen, entwickeln und bewerten C-ITS-Stationen und andere Informationsverarbeitungssysteme in einer Weise, die die Erfüllung der anwendbaren Anforderungen gewährleistet.

(11) Die Betreiber von C-ITS-Stationen betreiben C-ITS-Stationen und alle anderen Informationsverarbeitungssysteme, mit denen geeignete Steuerungen zur Behandlung von Risiken für die Informationssicherheit gemäß Abschnitt 1.6 umgesetzt werden.

1.4. Vertraulichkeitseinstufung von Informationen

In diesem Abschnitt werden die Mindestanforderungen an die Einstufung von Informationen als vertraulich festgelegt. Dies hindert keinen C-ITS-Beteiligten daran, strengere Anforderungen anzuwenden.

(12) Die Betreiber von C-ITS-Stationen stufen gehandhabte Informationen als vertraulich ein, wobei eine Sicherheitskategorie wie folgt dargestellt werden kann:

Information zur Sicherheitskategorie = {(Vertraulichkeit, Auswirkung), (Integrität, Auswirkung), (Verfügbarkeit, Auswirkung)};

(13) C-ITS-Beteiligte stufen verwaltete Informationen als vertraulich ein, wobei ein System von Sicherheitskategorien wie folgt dargestellt werden kann:

Informationssystem der Sicherheitskategorien = {(Vertraulichkeit, Auswirkung), (Integrität, Auswirkung), (Verfügbarkeit, Auswirkung)};

(14) die akzeptablen Werte für die potenziellen Auswirkungen sind gemäß der Zusammenfassung in Tabelle 1 „gering“, „mittel“ und „hoch“.

Tabelle 1 Definitionen der möglichen Auswirkungen für die einzelnen Sicherheitsziele der Vertraulichkeit, Integrität und Verfügbarkeit

	Mögliche Auswirkungen		
Sicherheitsziel	**GERING**	**MITTEL**	**HOCH**

	Mögliche Auswirkungen		
Vertraulichkeit Wahrung autorisierter Beschränkungen des Zugangs zu Informationen und ihrer Offenlegung, einschließlich der Mittel zum Datenschutz und eigentumsrechtlich geschützter Informationen	Bei einer nicht genehmigten Offenlegung von Informationen sind **begrenzte** nachteilige Auswirkungen auf den Betrieb oder die Vermögenswerte der Organisation oder auf natürliche Personen zu erwarten.	Bei einer nicht genehmigten Offenlegung von Informationen sind **ernste** nachteilige Auswirkungen auf den Betrieb oder die Vermögenswerte der Organisation oder auf natürliche Personen zu erwarten.	Bei einer nicht genehmigten Offenlegung von Informationen sind **schwerwiegende oder katastrophale** nachteilige Auswirkungen auf den Betrieb oder die Vermögenswerte der Organisation oder auf natürliche Personen zu erwarten.
Integrität Schutz vor einer unzulässigen Veränderung oder Vernichtung von Informationen; dies schließt die Sicherstellung der Nichtabstreitbarkeit und Authentizität von Informationen ein	Bei einer nicht genehmigten Änderung oder Vernichtung von Informationen sind **begrenzte** nachteilige Auswirkungen auf den Betrieb oder die Vermögenswerte der Organisation oder auf natürliche Personen zu erwarten.	Bei einer nicht genehmigten Änderung oder Vernichtung von Informationen sind **ernste** nachteilige Auswirkungen auf den Betrieb oder die Vermögenswerte der Organisation oder auf natürliche Personen zu erwarten.	Bei einer nicht genehmigten Änderung oder Vernichtung von Informationen sind **schwerwiegende oder katastrophale** nachteilige Auswirkungen auf den Betrieb oder die Vermögenswerte der Organisation oder auf natürliche Personen zu erwarten.
Verfügbarkeit Sicherstellung des rechtzeitigen und verlässlichen Zugangs zu und der Nutzung von Informationen	Bei einer Unterbrechung des Zugangs zu Informationen oder einem Informationssystem und deren bzw. dessen Nutzung sind **begrenzte** nachteilige Auswirkungen auf den Betrieb oder die Vermögenswerte der Organisation oder auf natürliche Personen zu erwarten.	Bei einer Unterbrechung des Zugangs zu Informationen oder einem Informationssystem und deren bzw. dessen Nutzung sind **ernste** nachteilige Auswirkungen auf den Betrieb oder die Vermögenswerte der Organisation oder auf natürliche Personen zu erwarten.	Bei einer Unterbrechung des Zugangs zu Informationen oder einem Informationssystem oder deren bzw. dessen Nutzung sind **schwerwiegende oder katastrophale** nachteilige Auswirkungen auf den Betrieb oder die Vermögenswerte der Organisation oder auf natürliche Personen zu erwarten.

(15) Die folgenden Arten von Auswirkungen der Einstufung von Informationen als vertraulich sind unter dem Gesichtspunkt des Grades des Schadens oder der Kosten zu betrachten, die dem C-ITS-Dienst und den C-ITS-Beteiligten durch einen Informationssicherheitsvorfall entstehen.

- Verkehrssicherheit — wenn die Auswirkungen die Verkehrsteilnehmer einer unmittelbaren Verletzungsgefahr aussetzen;
- Sicherheit — wenn die Auswirkungen C-ITS-Beteiligten einer unmittelbaren Verletzungsgefahr aussetzen;
- betriebliche Auswirkungen — mit wesentlichen negativen Auswirkungen auf die Effizienz des Straßenverkehrs oder mit anderen gesellschaftlichen Auswirkungen wie dem ökologischen Fußabdruck und organisierter Kriminalität;

- rechtlich — wenn die Auswirkungen zu bedeutenden rechtlichen und/oder aufsichtsrechtlichen Schritten gegen einen oder mehrere der C-ITS-Beteiligte aufgrund eines Verstoßes gegen Vorschriften führen;
- finanziell — wenn die Auswirkungen für einen oder mehrere der C-ITS-Beteiligten zu mittel- oder unmittelbaren monetären Kosten führen;
- Datenschutz — wobei die DSGVO sowohl rechtliche als auch finanzielle Auswirkungen hat;
- Ruf — wenn die Auswirkungen für einen oder mehrere der C-ITS-Beteiligte und/oder das C-ITS-Netz zu einer Rufschädigung führen, z. B. nachteilige Berichterstattung in der Presse und/oder erheblicher politischer Druck auf nationaler oder internationaler Ebene.

(16) Die C-ITS-Beteiligten beachten hinsichtlich der verwalteten Informationen die folgenden Mindestwerte für Auswirkungen:

Tabelle 2: Auswirkungen

	Informationen erzeugt von: ortsfesten C-ITS-Stationen	**Informationen erzeugt von: mobilen C-ITS-Stationen**
Vertraulichkeit	CAM: gering DENM: gering IVIM: gering MAPEM: gering SPATEM: gering SSEM: gering	CAM: gering DENM: gering SREM: gering in einer der drei Nachrichten enthaltene personenbezogene Daten: mittel
Integrität	CAM: mittel DENM: mittel IVIM: mittel MAPEM: mittel SPATEM: mittel SSEM: mittel	CAM: mittel DENM: mittel SREM: mittel
Verfügbarkeit	CAM: gering DENM: gering IVIM: gering MAPEM: gering SPATEM: gering SSEM: mittel	CAM: gering DENM: gering SREM: mittel

1.5. Risikobewertung

1.5.1. Allgemeines

(17) Risikobewertungen werden regelmäßig im Einklang mit ISO/IEC 27005 durchgeführt. Sie umfassen eine angemessene Dokumentation folgender Elemente:

- Umfang der Risikobewertung, d. h. das bewertete System, die Grenzen und der Zweck des Systems sowie die Informationen, die gehandhabt werden;
- die Kriterien für Sicherheitsrisiken;
- Risikobewertung einschließlich Ermittlung, Analyse und Evaluierung.

1.5.2. Kriterien für Sicherheitsrisiken

(18) Die Kriterien für Risikoevaluierungen werden unter Berücksichtigung der folgenden Aspekte bestimmt:

- des strategischen Werts des C-ITS-Dienstes und des C-ITS-Netzes für alle C-ITS-Beteiligten;
- des strategischen Werts des C-ITS-Dienstes und des C-ITS-Netzes für den C-ITS-Stationsbetreiber des Dienstes;
- der Folgen für den Ruf des C-ITS-Netzes;
- der gesetzlichen und aufsichtsrechtlichen Anforderungen sowie vertraglichen Verpflichtungen.

(19) Kriterien für die Auswirkungen von Risiken werden unter Berücksichtigung der Arten von Auswirkungen bestimmt, die sich aus der Einstufung von Informationen als vertraulich ergeben und auf die in Abschnitt 1.4 Bezug genommen wird.

(20) Kriterien für die Risikoakzeptanz schließen, nach Art der Auswirkung geordnet, die Ermittlung von Risikostufen ein, die für den C-ITS-Dienst und die C-ITS-Beteiligten nicht akzeptabel sind.

1.5.2.1. Risikoermittlung

(21) Risiken werden nach ISO/IEC 27005 ermittelt. Dabei gelten die folgenden Mindestanforderungen:

- die wichtigsten zu schützenden Wirtschaftsgüter sind gemäß Abschnitt 1.3.1 C-ITS-Nachrichten;
- unterstützende Wirtschaftsgüter sind zu ermitteln, einschließlich:
  - der für C-ITS-Nachrichten verwendeten Informationen (z. B. lokale dynamische Landkarte, Zeit, Protokollkontrolle usw.);
  - der C-ITS-Stationen und ihrer Software, Konfigurationsdaten und zugehörigen Kommunikationskanäle;
  - der zentralen Wirtschaftsgüter zur C-ITS-Steuerung;
  - jeder Stelle innerhalb des EU-CCMS;
- Bedrohungen dieser Güter und ihrer Quellen werden ermittelt;
- bestehende und geplante Kontrollen werden ermittelt;
- Schwachstellen, die dazu ausgenutzt werden können, den Gütern oder C-ITS-Beteiligten Schaden zuzufügen, werden ermittelt und als Szenarien für Vorfälle beschrieben;

- die möglichen Folgen von Sicherheitsvorfällen für die Wirtschaftsgüter werden auf der Grundlage der Vertraulichkeitseinstufung der Informationen ermittelt.

1.5.2.2. Risikoanalyse

(22) Für die Risikoanalyse gelten folgende Mindestanforderungen:

- die Auswirkungen der ermittelten Vorfälle im Zusammenhang mit der Informationssicherheit auf den C-ITS-Dienst und die C-ITS-Beteiligten werden auf der Grundlage der Informationen und der Sicherheitskategorie des Informationssystems bewertet; dabei werden mindestens die drei in Abschnitt 1.4 aufgeführten Stufen genutzt;
- die Auswirkungsstufen werden für Folgendes ermittelt:
  - das/die gesamte(n) bestehende(n) C-ITS-Netz/-Dienste;
  - einzelne C-ITS-Beteiligte/Organisationsstellen;
- die höchste Stufe wird der Gesamtauswirkung zugewiesen;
- die Wahrscheinlichkeit der ermittelten Vorfallszenarien wird mit Hilfe mindestens der folgenden drei Stufen beurteilt:
  - unwahrscheinlich (Wert 1) – das Vorfallszenario ist unwahrscheinlich/schwierig zu realisieren oder die Motivation für einen Angreifer ist sehr gering;
  - möglich (Wert 2) – das Vorfallszenario kann eintreten/seine Realisierung ist möglich oder die Motivation für einen Angreifer ist ausreichend hoch;
  - wahrscheinlich (Wert 3) – das Eintreten des Vorfallszenarios ist wahrscheinlich/leicht zu realisieren und die Motivation für einen Angreifer ist hoch;
- die Risikostufen werden für alle ermittelten Vorfallszenarien auf folgender Grundlage berechnet: Produkt aus Auswirkung und Wahrscheinlichkeit, aus dem sich mindestens die folgenden Risikostufen ergeben: gering (Werte 1,2), mittel (Werte 3,4) und hoch (Werte 6,9), die wie folgt definiert werden:

Tabelle 3: Risikostufen

Risikostufen als Produkt von Auswirkung und Wahrscheinlichkeit		**Wahrscheinlichkeit**		
		unwahrscheinlich (1)	**möglich (2)**	**wahrscheinlich (3)**
Auswirkung	**gering (1)**	gering (1)	gering (2)	mittel (3)
	mittel (2)	gering (2)	mittel (4)	hoch (6)
	hoch (3)	mittel (3)	hoch (6)	hoch (9)

1.5.2.3. Risikobewertung

(23) Um festzustellen, welche Risiken behandelt werden müssen, werden die Risikostufen mit Risikobewertungskriterien und Risikoakzeptanzkriterien

verglichen. Es müssen mindestens mäßig hohe oder hohe Risiken für den C-ITS-Dienst und das C-ITS-Netz gemäß Abschnitt 1.6 behandelt werden.

1.6. Risikobehandlung

1.6.1. Allgemeines

(24) Risiken werden nach einer der folgenden Methoden behandelt:

- Risikoänderung durch Kontrollen gemäß den Abschnitten 1.6.2 oder 1.6.3, sodass das Restrisiko als annehmbar eingestuft werden kann;
- Risikorückbehalt (wenn die Risikostufe den Risikoakzeptanzkriterien entspricht);
- Risikovermeidung.

(25) Bei Risiken für das C-ITS-Netz ist eine Teilung oder Übertragung von Risiken nicht zulässig.

(26) Die Risikobehandlung wird dokumentiert, was Folgendes umfasst:

- die Erklärung der Anwendbarkeit nach ISO 27001, in der die erforderlichen Kontrollen dargelegt und Folgendes bestimmt wird:
  - die verbleibende Eintrittswahrscheinlichkeit;
  - der verbleibende Schweregrad der Auswirkungen;
  - die Restrisikostufe;
- die Gründe für den Risikorückbehalt oder die Risikovermeidung.

1.6.2. Kontrollen für C-ITS-Stationen

1.6.2.1. Generische Kontrollen

(27) C-ITS-Stationen müssen gemäß Abschnitt 1.6.1 geeignete Gegenmaßnahmen zur Risikoänderung umsetzen. Bei diesen Gegenmaßnahmen sind generische Kontrollen gemäß ISO/IEC 27001 und ISO/IEC 27002 anzuwenden.

1.6.2.2. Kontrollen für die Kommunikation zwischen C-ITS-Stationen

(28) Auf der Senderseite sind zumindest die folgenden vorgeschriebenen Kontrollen zu implementieren:

Tabelle 4: Kontrollen auf der Senderseite

	Informationen erzeugt von: ortsfesten C-ITS-Stationen	**Informationen erzeugt von: mobilen C-ITS-Stationen**
Vertraulichkeit	-	Die in Meldungen enthaltenen personenbezogenen Daten werden mit Hilfe eines adäquaten AT-Wechselverfahrens geschützt, damit ein Schutzniveau gewährleistet ist, das dem Risiko einer Wiedererkennung von Fahrern auf Basis ihrer übertragenen Daten angemessen entspricht. Aus diesem Grund wechseln C-ITS-Stationen die Berechtigungstickets (AT) beim Senden von Nachrichten in adäquater Weise und

		verwenden AT nach einem Wechsel nur dann erneut, wenn ein nicht dem Durchschnitt[1] entsprechendes Fahrerverhalten vorliegt.
Integrität	Alle Meldungen/Nachrichten müssen gemäß der TS 103 097 [14] unterzeichnet sein.	Alle Meldungen/Nachrichten müssen gemäß der TS 103 097 [14] unterzeichnet sein.
Verfügbarkeit	-	-

(29) Auf der Empfängerseite sind zumindest die folgenden vorgeschriebenen Kontrollen zu implementieren:

Tabelle 5: Kontrollen auf der Empfängerseite

	Informationen erzeugt von: ortsfesten C-ITS-Stationen	**Informationen erzeugt von: mobilen C-ITS-Stationen**
Vertraulichkeit		Empfangene personenbezogene Daten werden über einen möglichst kurzen Zeitraum zu geschäftlichen Zwecken gespeichert, wobei die **maximale Speicherungszeit** für Rohdatenelemente und identifizierbare Datenelemente **fünf Minuten** beträgt. Empfangene CAM oder SRM werden nicht weitergeleitet/ausgestrahlt. Empfangene DENM dürfen nur innerhalb eines begrenzten geografischen Gebiets weitergeleitet/übertragen werden.
Integrität	Die Integrität aller von ITS-Anwendungen genutzten Meldungen/Nachrichten ist gemäß der TS 103 097 [14] zu validieren.	Die Integrität aller von ITS-Anwendungen genutzten Meldungen/Nachrichten ist gemäß der TS 103 097 [14] zu validieren.
Verfügbarkeit	-	Eine empfangene SRM wird verarbeitet und erzeugt eine SSM-Übertragung an den Absender der SRM.

(30) Zur Förderung der in den vorstehenden Tabellen dargestellten Sicherheitsanforderungen hinsichtlich der Vertraulichkeit, Integrität und Verfügbarkeit werden alle C-ITS-Stationen (mobile C-ITS-Stationen (einschließlich fahrzeugseitiger C-ITS-Stationen) und ortsfeste C-ITS-Stationen) anhand von Sicherheitsbewertungskriterien gemäß der Spezifikation in den „gemeinsamen Kriterien“ / ISO 15408[2] bewertet und zertifiziert. Aufgrund der unterschiedlichen Merkmale der verschiedenen Typen von C-ITS-Stationen und aufgrund unterschiedlicher, standortbezogener datenschutzrechtlicher Anforderungen können verschiedene Schutzprofile definiert werden.

(31) Alle auf die Sicherheitszertifizierung der C-ITS-Station anwendbaren Schutzprofile und damit verbundenen Dokumente sind gemäß ISO 15408 zu

[1] Der Definition durchschnittlichen Fahrverhaltens liegen relevante statistische Analysen des Fahrverhaltens in der Europäischen Union, beispielsweise auf der Grundlage von Daten des Deutschen Zentrums für Luft- und Raumfahrt (DLR), zugrunde.

[2] Portal für „Gemeinsame Kriterien“: http://www.commoncriteriaportal.org/cc/.

bewerten, zu validieren und zu zertifizieren, wobei das „Mutual Recognition Agreement of Information Technology Security Evaluation Certificates“ (Vereinbarung über die gegenseitige Anerkennung von IT-Sicherheitszertifikaten) der Gruppe Hoher Beamter für Informationssicherheit (SOG-IS)[3] oder ein gleichwertiges europäisches Zertifizierungsprogramm gemäß dem einschlägigen europäischen Cybersicherheitsrahmen anzuwenden ist. Bei der Entwicklung solcher Schutzprofile kann der Anwendungsbereich der Sicherheitszertifizierung der C-ITS-Station vom Hersteller festgelegt werden, vorbehaltlich der Bewertung und Genehmigung durch die für die C-ITS Certificate Policy zuständige Stelle (CPA) und ein SOG-IS-Konformitätsbewertungsgremium oder zumindest eine gleichwertigen Gremiums gemäß dem folgenden Absatz.

(32) Angesichts der Bedeutung der Aufrechterhaltung eines höchstmöglichen Sicherheitsniveaus sind die Sicherheitszertifikate für C-ITS-Stationen im Rahmen des Zertifizierungssystems anhand gemeinsamer Kriterien (ISO 15408) von einem Konformitätsbewertungsgremium zu erteilen, das vom Managementausschuss im Rahmen der SOG-IS-Vereinbarung oder von einer nationalen Cybersicherheits-Zertifizierungsbehörde eines Mitgliedstaates akkreditiert wurde. Ein solches Konformitätsbewertungsgremium muss bei der Sicherheitsbeurteilung Bedingungen anwenden, die den in der SOG-IS-Vereinbarung zur gegenseitigen Anerkennung vorgesehenen Bedingungen mindestens gleichwertig sind.

1.6.2.3. Kontrollen für C-ITS-Stationen als Endteilnehmer

(33) Die C-ITS-Stationen müssen die Certificate Policy [1] im Einklang mit ihrer Funktion als EU-CCMS-Endteilnehmer einhalten.

1.6.3. Kontrollen für EU-CCMS-Teilnehmer

(34) Die EU-CCMS-Teilnehmer müssen die Certificate Policy [1] im Einklang mit ihrer Funktion im EU-CCMS einhalten.

1.7. Konformität mit der vorliegenden Sicherheitsstrategie

(35) Die Betreiber von C-ITS-Stationen müssen regelmäßig im Einklang mit den Leitlinien für einen ISO-27001-Audit in [12] eine Zertifizierung der Einhaltung der vorliegenden Strategie beantragen und erhalten.

(36) Das Audit-Gremium muss von einem Mitglied des europäischen Akkreditierungssystems akkreditiert und zertifiziert sein. Es muss die Anforderungen von [11] erfüllen.

(37) Im Hinblick auf die Einholung der Zertifizierung müssen die Betreiber von C-ITS-Stationen Dokumente erstellen und pflegen, die den Anforderungen an zu dokumentierende Informationen in [3], Klausel 7.5 entsprechen. Im Einzelnen erzeugen und pflegen die Betreiber von C-ITS-Stationen folgende, auf das ISMS bezogene Dokumente:

[3] Im Straßenverkehrssektor hat sich die SOG-IS beispielsweise bereits an der Sicherheitszertifizierung des intelligenten Fahrtenschreibers beteiligt. Derzeit ist die SOG-IS-Vereinbarung in Europa das einzige Programm, das die Harmonisierung der Sicherheitszertifizierung elektronischer Produkte unterstützen kann. Im derzeitigen Stadium unterstützt die SOG-IS nur den Prozess der „gemeinsamen Kriterien“, sodass die C-ITS-Stationen nach den „gemeinsamen Kriterien“ bewertet und zertifiziert werden müssen; siehe https://www.sogis.org/.

- Umfang des ISMS (Abschnitt 1.3.1 und [3], Klausel 4.3);
- Informationssicherheitsstrategie und -ziele (Abschnitt 1.3.1 und [3], Klauseln 5.2 und 6.2);
- Einzelheiten der Risikobewertungs- und -behandlungsmethode (Abschnitt 1.5 und [3], Klausel 6.1.2);
- Risikobewertungsbericht (Abschnitt 1.5 und [3], Klausel 8.2);
- Anwendbarkeitserklärung (Abschnitt 1.6 und [3], Klausel 6.1.3d);
- Risikobehandlungsplan (Abschnitt 1.6 und [3], Klauseln 6.1.3e und 8.3);
- für die Durchführung ausgewählter Kontrollen erforderliche Dokumente (Abschnitt 1.6 und [3], Anhang A).

(38) Darüber hinaus erstellen und pflegen die Betreiber von C-ITS-Stationen folgende Aufzeichnungen als Nachweis für die erzielten Ergebnisse:

- Aufzeichnungen über Schulungen, Kompetenzen, Erfahrungen und Qualifikationen ([3], Klausel 7.2);
- Überwachungs- und Messergebnisse ([3], Klausel 9.1);
- internes Audit-Programm ([3], Klausel 9.2);
- Ergebnisse interner Audits ([3], Klausel 9.2);
- Ergebnisse der Managementprüfung ([3], Klausel 9.3);
- Ergebnisse von Korrekturmaßnahmen ([3], Klausel 10.1).

2. REFERENZDOKUMENTE

In diesem Anhang wurden folgende Referenzdokumente herangezogen:

[1] Anhang III dieser Verordnung

[2] ISO/IEC 27000 (2016): Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Überblick und Terminologie

[3] ISO/IEC 27001 (2015): Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen

[4] ISO/IEC 27005 (2011): Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits-Risikomanagement

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

[6] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).

[7] ETSI EN 302 637-2 V1.4.0, Intelligent transport systems (ITS) – Vehicular

communications; Basic set of applications; [intelligente Verkehrssysteme – Fahrzeugkommunikation; Basissatz an Anwendungen]; Teil 2: Specification of cooperative awareness basic service [Spezifikation des Basisdienstes „kooperative Aufklärung“]

[8] ETSI EN 302 637-3 V1.3.0, Intelligent transport systems (ITS) – Vehicular communications; Basic set of applications; [intelligente Verkehrssysteme – Fahrzeugkommunikation; Basissatz an Anwendungen]; Teil 3: Specifications of decentralised environmental notification basic service [Spezifikation des Basisdienstes für dezentrale Umfeldbenachrichtigungen]

[9] ETSI TS 103 301 V1.2.1: Intelligent transport systems (ITS) – Vehicular communications; Basic set of applications; [intelligente Verkehrssysteme – Fahrzeugkommunikation; Basissatz an Anwendungen]; Facilities layer protocols and communication requirements for infrastructure services [Protokolle der Anlagenebene und Kommunikationsanforderungen an Infrastrukturdienste]

[10] Eine europäische Strategie für Kooperative Intelligente Verkehrssysteme –- ein Meilenstein auf dem Weg zu einer kooperativen, vernetzten und automatisierten Mobilität (COM(2016) 766, 30. November 2016)

[11] ISO/IEC 27006:2015 Informationstechnik – IT-Sicherheitsverfahren – Anforderungen an Institutionen, die Audits und Zertifizierungen von Informationssicherheits-Managementsystemen anbieten

[12] ISO/IEC 27007:2011 Informationstechnik – Sicherheitstechniken – Richtlinien für Informationssicherheits- und Managementsystemaudits

[13] ETSI EN 302 665 V1.1.1 Intelligent transport systems (ITS); Kommunikationsarchitektur

[14] ETSI TS 103 097 V1.3.1. Intelligent transport systems (ITS) security; security header and certificate formats [Intelligente Verkehrssysteme Sicherheit; Sicherheitskopfsatz und Zertifikatformate]