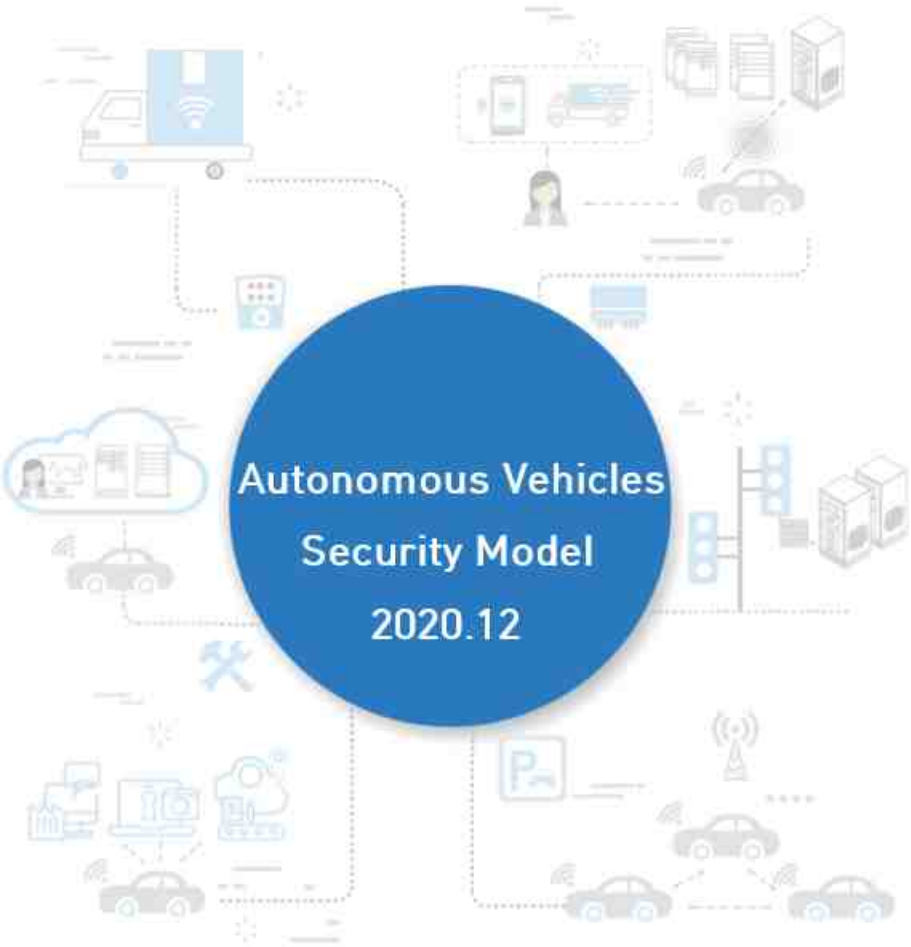
Autonomous Vehicles Security Model



KISA Korea Internet & Security Agency

Contents

Chapter 1 Summary

1.1 Purpose

Autonomous vehicles (or Self-driving Cars) are growing rapidly along with advances in connectivity technology and sensor technology. Global vehicle manufacturers such as Google, GM and Ford are actively developing self-driving cars, and Hyundai Motor Company is also showing self-driving cars at CES. Self-driving cars are no longer a story of the distant future, but a technology of reality in our hands.

Accordingly, service models using autonomous vehicles such as unmanned shuttles, parking, and delivery are being actively developed, and these services are showing synergy by convergence of automobiles, infrastructure, communication, electronics, and ICT. However, due to this convergence, cyber attacks that occurred in the existing ICT environment are being transferred to the automobile environment. Since the safety of automobiles is directly related to the safety of drivers and passengers as well as the safety of all objects on the road, it is necessary to prepare a defense posture against cyber attacks carried out on automobiles.

However, self-driving car services are not yet mature and are focusing on technology development, so they are not well prepared for cyber security. Therefore, this study intends to present an autonomous vehicle security model based on the results of the previously conducted self-driving service investigation and vehicle/infrastructure vulnerability analysis. This autonomous vehicle security model considers the following items.

.

• Schematic of security threats and attack paths according to the configuration of autonomous vehicles and related mobility services

• Based on the results of self-driving vehicle security vulnerability inspection and existing research cases, we present security technologies and solutions necessary for security enhancement.

1.2. Scope

A total of 7 types of services were identified through the self-driving service status survey, and the attack surface was confirmed through the Data Flow Diagram (DFD) for each service. However, it is not possible to know the detailed configuration of each service through the published data, and since each service provider takes a different configuration, there is no common data flow. Therefore, among the identified services, except for the following two cases where security consulting was performed, a general level of simple DFD and its threats were identified.

- self-driving shuttle
- Telematics service to provide autonomous driving service

The contents of investigation and analysis of autonomous driving service, countermeasures against security threats and security requirements, etc. are covered in the full version of 'Autonomous Vehicle Security Model'. This brief version deals with the configuration diagram of the security model, methods for checking security vulnerabilities, and a checklist for inspection.

Chapter 2 Self-driving car security model

2.1 Self-driving vehicle security model

To develop an autonomous vehicle security model, the target autonomous vehicle service was first investigated and the data flow for each service type was analyzed. Through this, common components of autonomous vehicle service were identified, and data flow for representative services of common components was analyzed.

As shown in Picture1, the vehicle performs cellular communication (C-V2X), WAVE communication, etc. between vehicles for V2X communication. At this time, signature and signature verification are performed for security. In order to obtain a certificate to be used for signature and signature verification, and to report abnormal behavior, the vehicle also communicates with the infrastructure through the RSU.

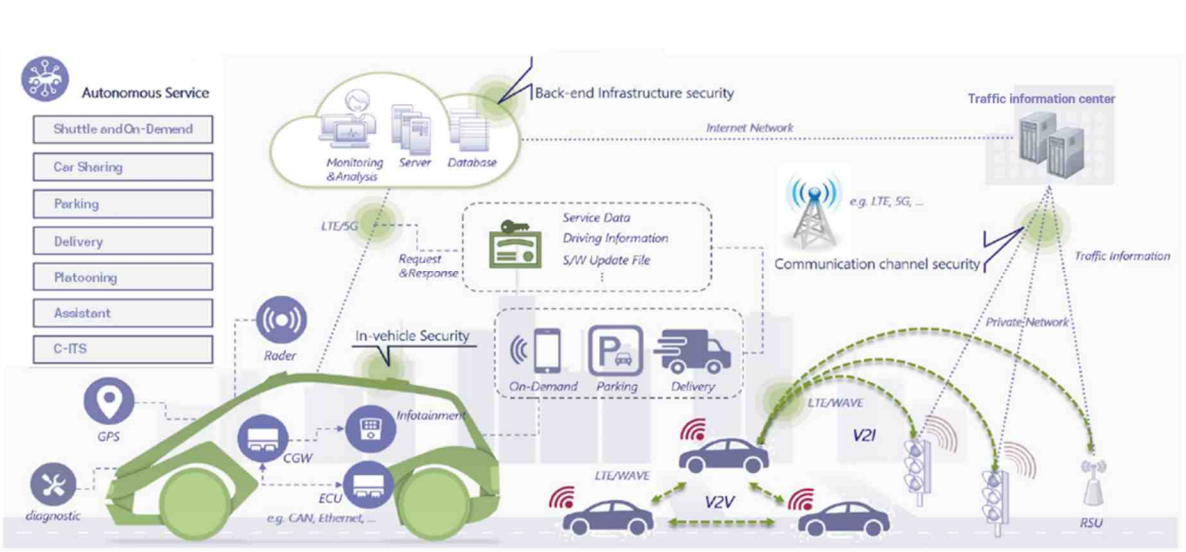
A shuttle service, an on-demand service, and a delivery service transmit various vehicle information to the backend infrastructure, receive necessary information, and provide related services. In addition, platoon driving and assistant service share information between vehicles, and provide remote control, safety, and convenience functions by checking vehicle status based on mobile communication technology.

The C-ITS service prevents accidents that may occur during autonomous driving by providing necessary traffic conditions and road information in real time while driving.

This self-driving car service delivers information such as traffic, safety, convenience, and vehicle management to the back-end infrastructure and traffic information center through various communication channels based on the vehicle, and Users can use the service by receiving the information through communication with the backend infrastructure or vehicle.

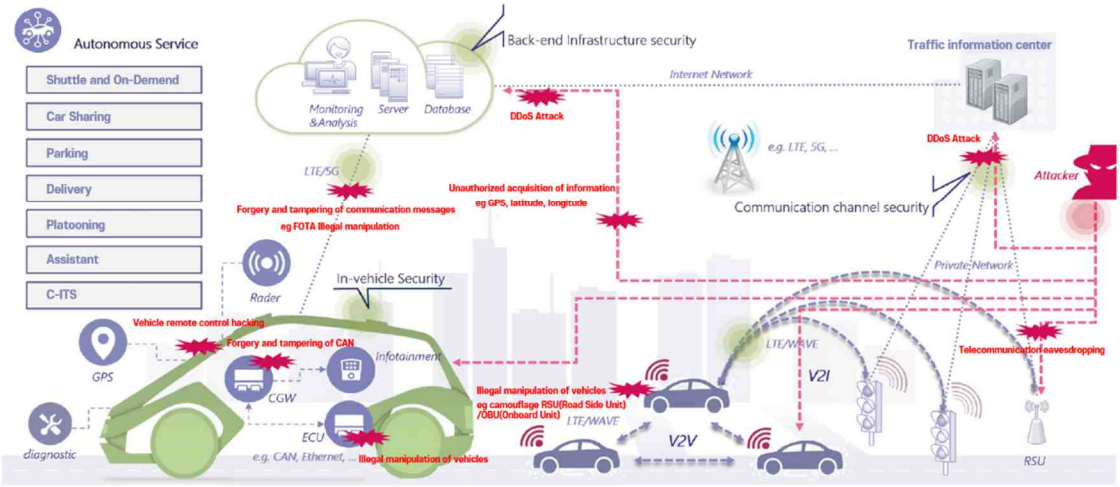
In Picture 1, 7 types of autonomous vehicle representative services were derived and the service composition diagram was briefly diagrammed with common components for each service and

with the development of autonomous vehicle technology and ICT application services, service types and composition may change.



Security threats by service type for this communication environment are deduced and described through the STRIDE threat modeling methodology. In addition, vulnerability inspection was performed based on the inspection checklist developed based on the UNECE and ISO/SAE 21434 standards, and the security threats derived through this process were described.

The following figure shows the threats that can occur in the types of autonomous vehicle service. When the vehicle and the backend infrastructure communicate, an attacker can conduct eavesdropping and data tampering, and can perform direct attacks such as DoS against the backend infrastructure. An attack may be performed by eavesdropping or modulating data transmitted/received or stored data through the interface of the vehicle controller or forgery an update package with respect to a vehicle.



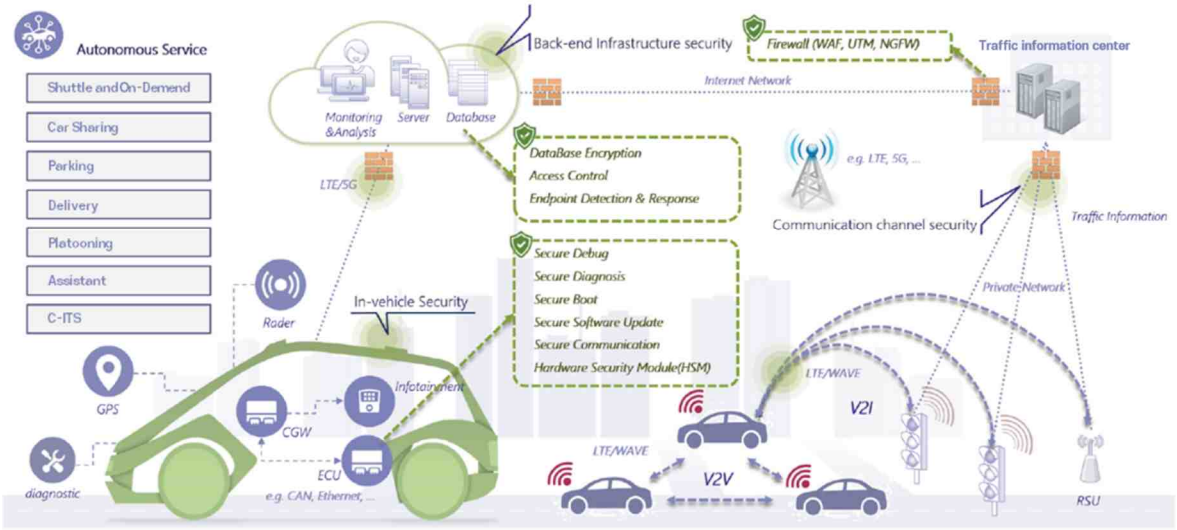
The following table summarizes the security threats that may occur in the vehicle, communication channel, and backend infrastructure areas. In the case of communication channels, various sections exist according to service types due to connectivity technology, and cyber attack vectors are increasing accordingly.

<Table 1> Security threats by service section for autonomous vehicles

Area	Section	Security Threat
Vehicle	N/A	Firmware modification, vehicle remote control hacking, CAN forgery, vehicle illegal operation, denial of service (DoS)
	Vehicle - Vehicle	

<table>
<tr><td rowspan="4">Communication Channel</td><td>Vehicle – Backend Infrastructure</td><td rowspan="4">Communication wiretapping, forgery of communication messages, unauthorized acquisition of information,
provision of false information, denial</td></tr>
<tr><td>Vehicle – Roadside Infrastructure</td></tr>
<tr><td>Backend Infrastructure – Roadside Infrastructure</td></tr>
<tr><td>Backend Infrastructure – Backend Infrastructure</td></tr>
<tr><td>Backend Infrastructure</td><td>N/A</td><td>Information Leakage, Elevation of Privilege, Denial of Service (DoS)</td></tr>
</table>

As a countermeasure against these security threats, in vehicles, security technologies such as 'HPSE(HSM)', 'Secure Boot', 'Secure Debug', 'Secure Diagnosis', 'Secure Flash', 'Secure Access', and 'Secure Software Update' can be applied to safely protect the vehicle. In addition, in the backend infrastructure, countermeasures according to security services ('confidentiality', 'integrity/availability', 'authority management', 'logging/audit trace', identification/authentication', , 'security management', 'access control' fields) present. It can be safely protected by applying security technologies and solutions such as Firewall, DataBase Encryption, Access Control, and Endpoint Detection & Response in data, system, and terminal areas.



The following table summarizes the security technologies that can be applied to security threats in each area.

Any cybersecurity can only be ensured through a holistic approach, as individual security functions are not sufficient to increase the difficulty of a successful attack.

<Table 2> Security response technology by security threat.

Area	Security threat	Security technology
Vehicle	Firmware Tampering	HPSE (HSM), Secure Boot, Secure Debug, Secure Diagnosis, Secure Flash, Secure Software Update
	Vehicle remote control hacking	Secure Access, Secure Diagnosis, IDS, SecOC
	CAN forgery	IDS, SecOC, Secure Software Update
	illegal vehicle operation	Secure Access, Secure Diagnosis
	Denial of Service (DoS)	IDS
Communication Channel	Communication eavesdropping	IPSec, TLS/DTLS, WAVE communication security technology
	Communication message forgery	
	Unauthorized acquisition of information	
	Giving false information	
	Denial	
Backend Infrastructure	Information leakage	Firewall (WAF, UTM, NGFW), DataBase Encryption, Access Control, Endpoint Detection & Response
	Elevation of privilege	Access Control
	Denial of Service (DoS)	Firewall (WAF, UTM, NGFW)

Chapter 3 Self-Driving Vehicle Service Security Vulnerability check method

3.1 Checking security vulnerabilities of self-driving car services.

As UNECE was adopted as a common regulation on cybersecurity approval in June 2020, the car
manufacturers must submit CSMS documents (cyber security management system) and VTA documents (type approval) to the certification authority.
In other words, manufacturers must comply with the provisions of the relevant laws to sell vehicles. Accordingly, this chapter introduces a checklist for checking security vulnerabilities in the vehicle, communication channel, and backend infrastructure areas by reflecting the security requirements required by the UNECE regulations and the ISO/SAE DIS 21434 standard.

3.2 Inspection scope.

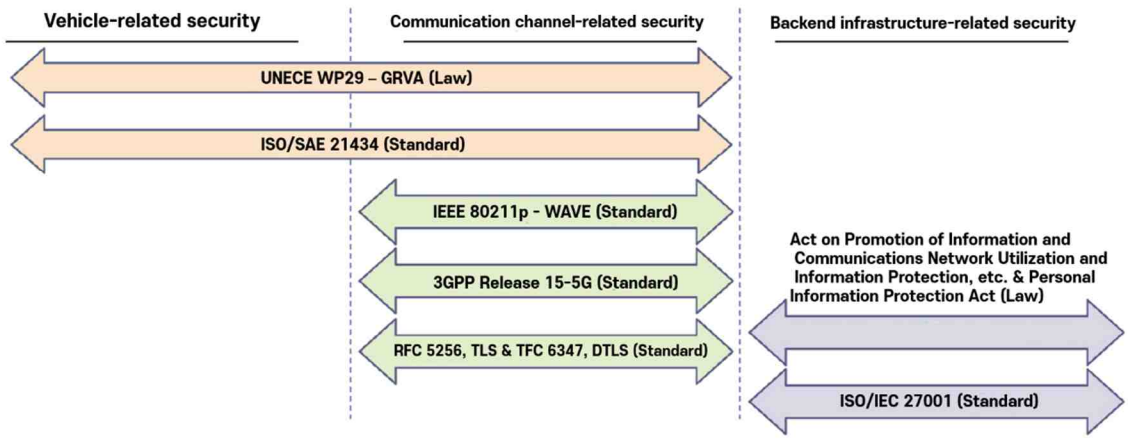
It analyzes the status of self-driving car services and identifies the scope of inspection accordingly.

• Scope from the perspective of the vehicle
It refers to devices applied for recognition, judgment, and control according to various situations in the vehicle.

• Scope of communication channels
A communication that transmits and receives data necessary for autonomous driving between vehicles or between vehicles and infrastructure.
• Scope in the backend infrastructure
It means a place that analyzes, processes, and manages data collected from vehicles, road facilities, roadside sensors, etc.

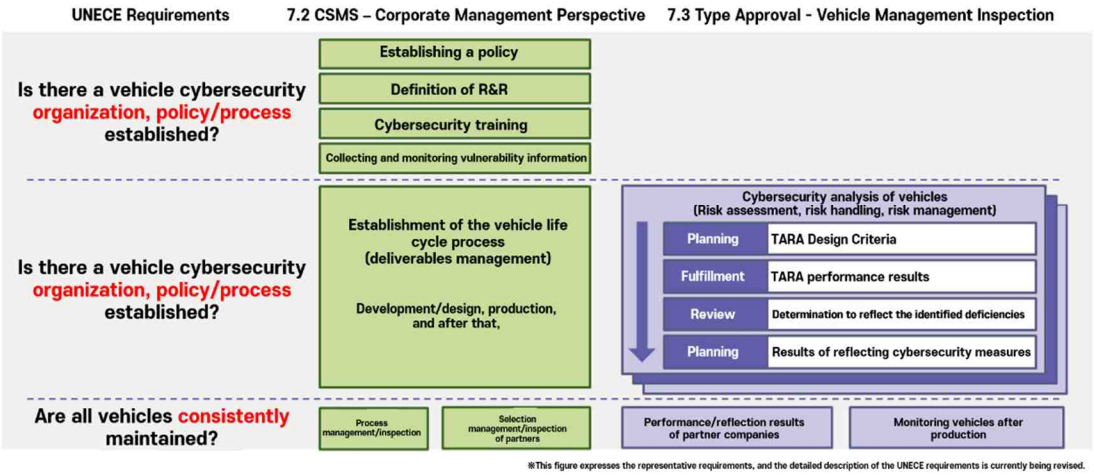
3.3 Inspection Criteria

Services related to autonomous vehicles must satisfy the following relevant laws and standards according to components.



UNECE WP.29 requires items for vehicle cyber security as follows, and includes policy, organization, concept, development/design, mass production, post-production operation,

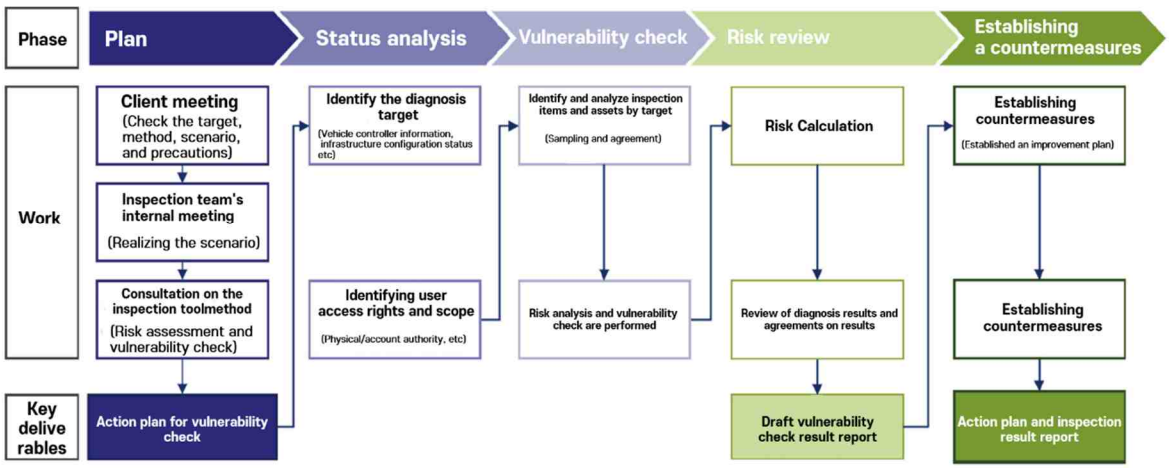
monitoring, and partner management.



ISO/SAE 21434 requires risk assessment and vulnerability analysis and management for vehicle cyber security, and the Information and Communications Network Act and Personal Information Protection Act require administrative, technical, and physical protection measures. Standards for other communication channels require the use of protocols that have been proven safe so far.

3.4 Inspection procedure.

The security vulnerability inspection procedure for the autonomous vehicle service is divided into 5 stages, and necessary tasks are performed at each stage.



3.5 Inspection items.

There are a total of 315 inspection checklist items, and it is composed as follows.

<Table 3> Number of vehicle inspection items

Field	Vehicle inspection items	Backend Infrastructure Checklist
Administrative Security	140	51
Technical security	74	44
Physical security	-	7
Total by area	214	102
Total Sum	315	

3.6 Inspection item details

3.6.1 Vehicle inspection items

3.6.1.1 Administrative Security

Vehicle administrative security items are composed of 'Cyber Security Management', 'Cyber Security Risk Assessment', 'Concept/Development/Verification', 'Mass Production and Operation', and 'Supply Chain Cyber Security'.

3.6.1.1.1 Cyber Security Management

<Table 4> Vehicle cyber security management items

Classification	Control Name	Unified ID	Control Requirements
Enterprise Cyber Security Management	Cybersecurity audit	V-1-1-AUD-01	A cybersecurity audit should be performed to independently determine whether an enterprise's processes achieve the objectives of this checklist.
Enterprise Cyber Security Management	Culture	V-1-1-CUL-01	The enterprise should foster and maintain a cybersecurity culture.
Enterprise Cyber Security Management	Culture	V-1-1-CUL-02	Cybersecurity-related executives and employees must have the capacity and awareness to take responsibility for their work.
Enterprise Cyber Security Management	Culture	V-1-1-CUL-03	The enterprise shall establish and maintain continuous improvement activities.
Enterprise Cyber Security Management	Culture	V-1-1-CUL-04	The enterprise must define an environment in which sharing is necessary/allowed and prohibited both inside and outside the organization.
Enterprise Cyber Security Management	Governance	V-1-1-GOV-01	Must comply with vehicle cybersecurity-related policies and management's commitment (responsibility) to manage cybersecurity risks.

Enterprise Cyber Security Management	Governance	V-1-1-GOV-02	A process should be established to meet the requirements for the entire life cycle of vehicle cyber security, and a guide to the activities should be in place to fulfill the requirements.
Enterprise Cyber Security Management	Governance	V-1-1-GOV-03	For the entire life cycle of vehicle cyber security, it should be defined between the departments in charge of each organization and the departments that cooperate. (eg RASIC charts)
Enterprise Cyber Security Management	Governance	V-1-1-GOV-04	The enterprise must provide resources to combat cybersecurity.
Enterprise Cyber Security Management	Governance	V-1-1-GOV-05	The enterprise need to identify areas that relate to or interact with cybersecurity, and establish and maintain communication channels between those areas.
Enterprise Cyber Security Management	Governance	V-1-1-GOV-06	The enterprise should define risk classes based on risk decisions.
Enterprise Cyber Security Management	management system	V-1-1 - MGM-01	A company must establish and maintain an international standard or equivalent quality management system to support cyber security projects.
Enterprise Cyber Security Management	management system	V-1-1-MGM-02	Configuration information regarding the cybersecurity of products operating in the field must remain available until support ends.
Enterprise Cyber Security Management	cyber security risk management	V-1-1-RIS-01	Cybersecurity risk management shall comply with ISO 31000.
Enterprise Cyber Security Management	cyber security S/W Tool Management	V-1-1-SWT-01	Tools that can affect the cybersecurity of items, systems, and components must be managed.
continuous cyber security activity	cyber security event evaluation	V-1-2-ASS-01	Based on risk handling decisions, the cybersecurity incident response process should be applicable at the post- development stage.

Classification	Control Name	Unified ID	Control Requirements
continuous cyber security activity	cyber security event evaluation	V-1-2-ASS-02	Cybersecurity events should perform analysis activities to determine whether they affect vehicle components or items.
continuous cyber security activity	cyber security information collecting	V-1-2-COL-01	In order to collect cyber security information, internal and external data should be monitored.
continuous cyber security activity	cyber security event identification	V-1-2-IDE-01	Cyber security information screening has standards, and it should be able to be linked to a cyber security event according to the results of the screening criteria.
continuous cyber security activity	Vulnerability Analysis	V-1-2-VUL-01	Vulnerability identification should reflect cybersecurity events and known vehicle weaknesses.
continuous cyber security activity	Vulnerability Analysis	V-1-2-VUL-02	It is necessary to analyze the attack routes and map the discovered vulnerabilities to specific attack routes.
continuous cyber security activity	Vulnerability Analysis	V-1-2-VUL-03	An attack potential rating should be determined for the vulnerabilities found.
continuous cyber security activity	Vulnerability Management	V-1-2-VUM-01	The identified vulnerability should have a basis for taking action against the corresponding risk.
continuous cyber security activity	Vulnerability Management	V-1-2-VUM-02	Risk handling measures shall be carried out based on: -Vulnerability analysis results -Risk Determination Results
continuous cyber security activity	Vulnerability Management	V-1-2-VUM-03	Risk handling measures for vulnerabilities should be performed in both the 'risk handling decision' and 'design/development' procedures.

continuous cyber security activity	Vulnerability Management	V-1-2-VUM-04	If cyber security information that invalidates the existing vulnerability checklist is collected/provided, the vulnerability should be excluded from vulnerability management.
cyber security risk management	Information Security Management (ISMS)	V-1-4-ISM-01	WP information required by the cyber security plan should be managed by the management system.
cyber security risk management	cyber security management system	V-1-4-MGM-01	A cybersecurity system must be in place for the manufacturing lifecycle process.
cyber security risk management	cyber security risk management	V-1-4-RIS-01	Enterprises should maintain a link between vehicle cyber security risk management and corporate IT security risk management.
cyber security risk management	cyber security S/W Tool management	V-1-4-SWT-01	Until the support for the item ends, an appropriate environment should be in place to support the countermeasures against cyber security incidents.

3.6.1.1.2 Cybersecurity risk assessment

<Table 5> Vehicle cyber security risk assessment items

Classification	Control Name	Unified ID	Control Requirements
risk assessment methodology	attack path analysis	V-2--3-ANA-01	The attack routes description should include a reference to the threat scenarios that can be realized by the attack routes.
risk assessment methodology	attack path analysis	V-2--3-ANA-01	Threat scenarios should be analyzed to describe attack routes.
risk assessment methodology	attack path analysis	V-2--3-ANA-02	The attack routes analysis approach should be documented. - Top-down method: attack tree, attack graph -Bottom-up method: vulnerability analysis result
risk assessment methodology	attack potential evaluation	V-2-3-ASS-01	The attack potential evaluation method should be based on a specific security engineering technique.
risk assessment methodology	Asset identification	V-2-3-ASS-01	Damage scenarios should be identified.
risk assessment methodology	attack potential evaluation	V-2-3-ASS-01	The attack potential class of the attack path must be determined.
risk assessment methodology	attack potential evaluation	V-2-3-ASS-02	The decision to use an attackability-based approach should be based on key factors.
risk assessment methodology	Asset identification	V-2-3-ASS-02	Assets with cybersecurity attributes that result in compromise scenarios should be listed.
risk assessment methodology	attack potential evaluation	V-2-3-ASS-03	When using a CVSS-based approach, you must decide on a CVSS-based approach.

risk assessment methodology	attack potential evaluation	V-2-3-ASS-04	If an attack vector-based approach is used, the attack vector should be evaluated with reference to CVSS.
risk assessment methodology	Risk determination	V-2-3-DET-01	The risk class of a threat scenario should be determined according to the impact of the relevant damage scenario and the likelihood of an attack vector.
risk assessment methodology	Impact Assessment	V-2--3-IMP-01	An impact assessment SFOP (safety, financial, operational, privacy) should be performed for the damage scenario.
risk assessment methodology	Impact Assessment	V-2--3-IMP-02	The impact class of the damage scenario should be divided as follows. - Severe - Major - Moderate - Negligible
risk assessment methodology	Impact Assessment	V-2-3-IMP-03	Safety-related impact assessments shall use the HARA of functional safety (ISO 26262-3:2018, clause 6.4.3).

classification	control name	Unified ID	Control Requirements
risk assessment methodology	risk handling decision	V-2-3-RIS-01	In the case of a threat scenario corresponding to the risk level 1 determined in the risk determination analysis, the compliance requirements may be omitted.
risk assessment methodology	risk handling decision	V-2-3-RIS-02	The risk treatment decision should be derived by reflecting the impact assessment grade, attack path, and risk treatment decision result.
risk assessment methodology	SFOP	V-2-3-SFO-01	If additional impact categories beyond S, F, O and P (safety, financial, operational, personal) are considered, those categories should be documented.
risk assessment methodology	Threat Scenario Identification	V-2-3-THR-01	Threat scenarios should be established.

3.6.1.1.3 Concept/Development/Verification

<Table 6> Vehicle Concept/Development/Verification Items

Classification	Control Name	Unified ID	Control Requirements
project planning stage	cyber security evaluation	V-3-5-ASS-01	The cyber security assessment can also be judged based on this checklist as to whether the project-related objectives have been achieved.
project planning stage	cyber security evaluation	V-3-5-ASS-02	Recommendations for conditional acceptance should be included in the cybersecurity assessment results.
project planning stage	cyber security evaluation	V-3-5-ASS-03	The cyber security assessment should be based on the basis for determining whether or not to be performed for each item or component.
Project planning stage	cyber security evaluation	V-3-5-ASS-04	The rationale for [V-3-5-ASS-03] should be independently reviewed. * V-3-5-ASS-03: The cyber security assessment should be based on the basis for determining whether or not to be performed for each item or component
project planning stage	cyber security evaluation	V-3-5-ASS-05	A cybersecurity assessment should determine whether the available evidence provides sufficient assurance that the item or component has achieved cybersecurity.
project planning stage	cyber security evaluation	V-3-5-ASS-06	The cyber security assessment results should be prepared immediately prior to the post-production phase.
Project planning stage	cyber security evaluation	V-3-5-ASS-07	The person in charge/person in charge of planning and independently conducting cybersecurity evaluations appointed under [V-1-1-CUL-02] and [V-3-5-RES-01] shall be supported by [V-1-GOV-03] and [V-1-1-GOV-04).

Classification	Control Name	Unified ID	Control Requirements
project planning stage	cyber security evaluation	V-3-5-ASS-08	Persons conducting cybersecurity assessments should have access to relevant information, tools, and collaborations of persons performing cybersecurity activities.
project planning stage	cyber security evaluation	V-3-5-ASS-09	The scope of the cybersecurity assessment should be defined.
project planning stage	cyber security evaluation	V-3-5-ASS-10	The results of the cyber security assessment should include the results.
project planning stage	cyber security evaluation	V-3-5-ASS-11	When a conditional acceptance recommendation according to [V-3-5-ASS-02] is deduced, the acceptance condition shall be included in the cyber security evaluation result.
Project planning stage	cyber security evaluation	V-3-5-ASS-12	After development, the next WP should be prepared before publication. o Cyber Security Practices o Cybersecurity Assessment Results (if applicable) o Cybersecurity Requirements for Post-Production ([WP-10-02])
project planning stage	cyber security evaluation	V-3-5-ASS-13	For post-production of item or component, cyber security conditions must be met.
project planning stage	cyber security case	V-3-5-CAS-01	A cybersecurity case should be made to provide a WP-supported claim about the level of cybersecurity that the case has achieved.
project planning stage	Change/Modify cyber security activities	V-3-5-CHA-01	Cybersecurity activities must be custom designed.
project planning stage	Change/Modify cyber security activities	V-3-5-CHA-02	Where cybersecurity activities are tailored, justifications that are suitable and well-founded for the purpose of this document should be provided.

project planning stage	ready-made (off-the-shel - (component)	V-3-5-OFF-01	When integrating existing components, a decision should be made by collecting and analyzing cybersecurity-related information.
project planning stage	ready-made (off-the-shel - (component)	V-3-5-OFF-02	Where existing documentation is not sufficient to support the integration of off-the-shelf components, cybersecurity activities to comply with this document shall be identified and implemented.
project planning stage	independent development (out of context) (component)	V-3-5-OUT-01	Because the component was developed out of context, it must perform activities related to cybersecurity activities.
project planning stage	cyber security plan	V-3-5-PLA-01	An analysis should be performed to determine the cyber relevance of the Item/Component.

Classification	Control Name	Unified ID	Control Requirements
Project planning stage	cyber security plan	V-3-5-PLA-02	In accordance with [V-1-1-GOV-03] and [V-1-1-GOV-04], responsibility for maintaining cybersecurity plans and tracking the progress of cybersecurity activities shall be assigned. *V-1-1-GOV-03: The entire life cycle of vehicle cyber security should be defined between the departments responsible for each organization and the cooperating departments. (eg RASIC charts) *V-1-1-GOV-04: Businesses must provide resources to manage cybersecurity.
project planning stage	cyber security plan	V-3-5-PLA-03	The cyber security plan should mention and include the project development plan.
project planning stage	cyber security plan	V-3-5-PLA-04	The cybersecurity plan should specify the activities necessary to comply with cybersecurity requirements related to the design and development phases.
project planning stage	cyber security plan	V-3-5-PLA-05	The cyber security plan should include basic information such as the purpose of the activity, dependence on other activities, etc.
project planning stage	cyber security plan	V-3-5-PLA-06	The cybersecurity plan should be updated as changes or overhauls in the activities to be performed are identified.
project planning stage	cyber security plan	V-3-5-PLA-07	The results of the activities specified in the cyber security plan should be collected and managed during the design and development stages.
project planning stage	cyber security plan	V-3-5-PLA-08	Both OEMs and suppliers are required by the CIA to define a cybersecurity plan for each cybersecurity activity and interface.
project planning stage	cyber security plan	V-3-5-PLA-09	Cybersecurity plans and WPs resulting from cybersecurity activities as defined in the cybersecurity plan should be subject to management.

project planning stage	recycle	V-3-5-REC-01	If an existing Item or component is reused without modification or change, it should be reviewed.
project planning stage	recycle	V-3-5-REC-02	The reuse of an existing Item or component should be analyzed.
project planning stage	recycle	V-3-5-REC-03	Reuse analysis of existing components should confirm that cybersecurity requirements are met.
project planning stage	cyber security job roles and responsibility	V-3-5-RES-01	Responsibilities for cybersecurity activities of the project shall be assigned and communicated in accordance with [V-1-1-GOV-03].
concept stage	cyber security concept	V-3-6-CON-01	Cybersecurity requirements should state the cybersecurity objectives, including the rationale for achieving the cybersecurity objectives.

Classification	Control Name	Unified ID	Control Requirements
concept stage	cyber security concept	V-3-6-CON-02	Cybersecurity requirements must be assigned to one or more components or operating environments in an Item.
concept stage	cyber security concept	V-3-6-CON-03	Cybersecurity requirements and results should be verified.
concept stage	Item Definition	V-3-6-ITE-01	The following information about the Item should be identified. -Item boundary, - Function, -Primary architecture
concept stage	Item Definition	V-3-6-ITE-02	Operation environment information of cyber security related items should be described.
concept stage	Item Definition	V-3-6-ITE-03	Constraints and compliance (requirements) should be identified.
concept stage	Item Definition	V-3-6-ITE-04	Items and assumptions about the item's operating environment

			should be identified.
concept stage	Security Objectives	V-3-6-OBJ-01	Analysis should be performed to identify cybersecurity objectives.
concept stage	Security Objectives	V-3-6-OBJ-02	Risk treatment decision activities shall be performed for the identified threat scenarios and associated risks.
concept stage	Security Objectives	V-3-6-OBJ-03	If a risk handling decision reduces the risk for a threat scenario, the cybersecurity objectives associated with that scenario should also be reflected.
concept stage	Security Objectives	V-3-6-OBJ-04	The cyber security claim should be stated.
concept stage	Security Objectives	V-3-6-OBJ-05	Cybersecurity objectives and claims must be verified.
development stage	Integration and validation	V-3-7-INT-01	Component testing should be performed to detect unidentified vulnerabilities.
development stage	Integration and validation	V-3-7-INT-02	If testing is performed in the verification activity, the testing pass criteria and the contents of the test shall be specified.
development stage	Integration and validation	V-3-7-INT-03	The completeness of testing activities should be guaranteed by defining the test scope for each test case.
development stage	Integration and validation	V-3-7-INT-04	You should check whether undefined functions are included in the component.
development stage	Integration and validation	V-3-7-INT-05	If testing is used for verification activities, it shall be ensured that the test environment is suitable for achieving the test objectives.
development stage	Integration and validation	V-3-7-INT-06	If a vulnerability is identified in testing, the vulnerability should be managed.

development stage	Cyber Security Requirements and architecture design improvement	V-3-7-REQ-01	Cyber Security Controls items should be selected based on the cyber security requirements assigned at the higher level and the architecture design assigned at the higher level.

Classification	Control Name	Unified ID	Control Requirements
development stage	Cyber Security Requirements and architecture design improvement	V-3-7-REQ-02	The architectural design must be reorganized according to the level of development.
development stage	Cyber Security Requirements and architecture design improvement	V-3-7-REQ-03	Cybersecurity requirements should be improved to a higher level.
development stage	Cyber Security Requirements and architecture design improvement	V-3-7-REQ-04	The architectural design of the development stage should be improved in consideration of cyber security.
development stage	Cyber Security Requirements and architecture design improvement	V-3-7-REQ-05	Improved cybersecurity requirements should be assigned to the improved architecture component.
development stage	Cyber Security Requirements and architecture design improvement	V-3-7-REQ-06	Matters related to the implementation of improved architecture components and improved cybersecurity requirements should be described.

development stage	Cyber Security Requirements and architecture design improvement	V-3-7-REQ-07	In the process of improving cyber security requirements, the cyber security requirements of the post-development stage should be considered.
development stage	Cyber Security Requirements and architecture design improvement	V-3-7-REQ-08	If specific procedures are required to ensure cyber security in the post-development stage, the cyber security requirements and specific activities (operating environment) should be specified in detail.
development stage	Cyber Security Requirements and architecture design improvement	V-3-7-REQ-09	It shall be verified that improved cybersecurity requirements are ensured.
development stage	Cyber Security Requirements and architecture design improvement	V-3-7-REQ-10	The improved architecture should be validated.
development stage	Cyber Security Requirements and architecture design improvement	V-3-7-REQ-11	Vulnerability analysis should identify, including improved cybersecurity activities.

Classification	Control Name	Unified ID	Control Requirements
development stage	Cyber Security Requirements and architecture design improvement	V-3-7-REQ-12	Identified vulnerabilities must be managed.
development stage	Cyber Security Requirements and architecture design improvement	V-3-7-REQ-13	Vulnerability analysis should be verified.
development stage	Cyber Security Requirements and architecture design improvement	V-3-7-REQ-14	Verification activities should be verified through design implementation verification and component integration verification.
development stage	Cyber Security Requirements and architecture design improvement	V-3-7-REQ-15	Integration and verification activities should be defined.
development stage	software for development specific requirements	V-3-7-REQ-16	Design, modeling or programming language guides should be clear.
development stage	software for development specific requirements	V-3-7-REQ-17	For the security of the programming language itself, there should be a referenceable guide.
development stage	software for development specific requirements	V-3-7-REQ-18	Evidence of suboptimal use of the design, modeling or programming language should be verified.
Verification	cyber security	V-3-7-VER-	If the residual risk is unacceptable,

step	Verification	01	the concept and development phase activities must be re-performed.
Verification step	cyber security Verification	V-3-8-VER-02	As part of the validation activities of [V-3-8-VER-03], penetration testing to verify cybersecurity objectives shall be performed.
Verification step	cyber security Verification	V-3-8-VER-03	Verification activities shall be implemented.
Verification step	cyber security Verification	V-3-8-VER-04	Verification standards for verification activities should be defined in consideration of mass production.
Verification step	cyber security Verification	V-3-8-VER-05	Vulnerabilities revealed during verification activities should be managed through the vulnerability management procedure.
Verification step	cyber security Verification	V-3-8-VER-06	Item verification should be able to confirm that all risks identified in the concept and development stage have been accepted by theory or dealt with to be acceptable based on the rationale.

3.6.1.1.4 Mass production and operation

Table 7. Items for mass production and operation of vehicles.

Classification	Control Name	Unified ID	Control Requirements
mass production stage	vehicle service End of support	V-4-9-EOS-01	The cyber security impact of service support termination should be considered at the design/development stage.
mass production stage	cyber security Incident response	V-4-9-INF-01	A cyber security incident response plan should be prepared.
mass production stage	cyber security Incident response	V-4-9-INF-02	The status of improvement of cyber security incidents should be tracked.
mass production stage	cyber security Incident response	V-4-9-INF-03	Information related to cyber security incidents should be collected.
mass production stage	Mass Production	V-4-9-MAS-01	After development, cyber security requirements should be applied and mass production management plan should be established.
mass production stage	update	V-4-9-UPD-01	Updates and related functions should be developed in the design/ development stage.
mass production stage	update	V-4-9-UPD-02	Update and recovery functions should consider cybersecurity impact.
mass production stage	update	V-4-9-UPD-03	A procedure for terminating cyber security support must be prepared for an Item or Component.

3.6.1.1.5 Supply chain cybersecurity

<Table 8> Supply Chain Cyber Security in Vehicles

Classification	Control Name	Unified ID	Control Requirements
supply chain cyber security	Request A Quote	V-5-10-QUO-01	When cyber security activities are divided, OEMs should request quotations from candidate partners.
supply chain cyber security	Supplier Demonstrate competence and evaluation	V-5-10-SUA-01	For the CIA division of labor, the supplier's ability to conduct development and post-development activities should be assessed in accordance with this checklist.
supply chain cyber security	Supplier Demonstrate competence and evaluation	V-5-10-SUA-02	To support the OEM's assessment of the supplier's capabilities, the supplier shall provide a record of its cybersecurity competency.
supply chain cyber security	with the supply chain Role/ Responsibilities	V-5-10-SUR-01	Supplier shall specify cyber security in the business agreement.
supply chain cyber security	with the supply chain Role/ Responsibilities	V-5-10-SUR-02	A Cybersecurity Interface Agreement (CIA) must be signed between the OEM and its suppliers at the beginning of the work

Classification	Control Name	Unified ID	Control Requirements
supply chain cyber security	with the supply chain Role/Responsibilities	V-5-10- SUR-03	The OEM and partner should discuss designating a person in charge and carrying out activities in case measures are required in the vulnerability report.
supply chain cyber security	with the supply chain Role/Responsi	V-5-10- SUR-04	There must be a bilateral agreement on when cybersecurity plans or cybersecurity-related risks should be accepted.

	bilities		
supply chain cyber security	with the supply chain Role/Responsibilities	V-5-10- SUR-05	In the event of a conflict regarding cybersecurity requirements between cybersecurity and related fields (see [V-1-1-GOV-05]), the parties shall notify the other party so that appropriate actions and decisions can be made. * V-1-1-GOV-05: Businesses should identify areas that are related to or interact with cybersecurity, and establish and maintain communication channels between those areas for the following purposes:
supply chain cyber security	with the supply chain Role/Responsibilities	V-5-10- SUR-16	If the OEM's cybersecurity requirements are unclear or not feasible, suppliers should consult with the OEM to seek mutual understanding.

3.6.1.2 Technical security.

The technical security item of the vehicle consists of the field of 'vehicle threat security'.

3.6.1.2.1 Vehicle Threat Security

Table 9. Vehicle Threat Security Items

Classification	Control Name	Unified ID	Control Requirements
backend server	related to field vehicles to the backend server Threat	V-6-1-BCK-01	It is necessary to ensure that vehicles are not attacked or data is leaked by insider attacks such as abuse of insider authority.
backend server	related to field vehicles to the backend server Threat	V-6-1-BCK-02	It must ensure that vehicles are not attacked or data leaked by unauthorized Internet access to the server.
backend server	related to field vehicles to the backend server Threat	V-6-1-BCK-03	It must ensure that vehicles are not attacked or data leaked by unauthorized physical access to the server.
backend server	related to field vehicles to the backend server Threat	V-6-1-BCK-04	It is necessary to ensure that the service of the backend system is not interrupted by an attack on the backend server, such as interfering with the interaction with the vehicle and the provision of services.

Classification	Control Name	Unified ID	Control Requirements
backend server	related to field vehicles to the backend server Threat	V-6-1-BCK-05	Vehicle data loss/damage/leakage due to abuse of insider authority should be blocked.
backend server	related to field vehicles to the backend server Threat	V-6-1-BCK-06	It is necessary to block the loss/damage/leakage of sensitive vehicle data due to the attack of the cloud service.
backend server	related to field vehicles to the backend server Threat	V-6-1-BCK-07	Vehicle data loss/damage/leakage by unauthorized Internet access to the server must be prevented.
backend server	related to field vehicles to the backend server Threat	V-6-1-BCK-08	Vehicle data loss/damage/leakage by unauthorized physical access to the server must be prevented.
backend server	related to field vehicles to the backend server Threat	V-6-1-BCK-09	Vehicle data loss/damage/leakage due to unintentional data sharing should be prevented.
unintentional user behavior	cyber attack facilitating, unintentional by an act that is not vehicle threat	V-6-2-VEH-61	Countermeasures must be taken to ensure that innocent victims (eg owners, operators, maintenance engineers) do not unintentionally load malicious programs or activate attacks.
unintentional user behavior	cyber attack facilitating, unintentional by an act that is not vehicle threat	V-6-2-VEH-62	Defined security procedures must be followed to ensure that unintended user actions do not create vehicle threats.
Physical loss of data loss	Vulnerabilities that can be exploited if not sufficiently	V-6-3-BCK-01	In case of damage by a third party, traffic accident, or theft, loss or damage of sensitive data due to physical damage should be prevented.

	protected or hardened		
Physical loss of data loss	Vulnerabilities that can be exploited if not sufficiently protected or hardened	V-6-3-BCK-02	User data loss due to DRM conflicts should be avoided.
Physical loss of data loss	Vulnerabilities that can be exploited if not sufficiently protected or hardened	V-6-3-BCK-03	It must counteract the loss of integrity of sensitive data due to long-term use and compromise of IT components (eg key change).
vehicle communicatio n channel	communication channel related vehicle threat	V-6-4-VEH-01	We must counteract message spoofing attacks through spoofing.
vehicle communicatio n channel	communication channel related vehicle threat	V-6-4-VEH-02	You have to counter Sybil attacks that spoof other vehicles by pretending there are many vehicles on the road.
vehicle communicatio n channel	communication channel related vehicle threat	V-6-4-VEH-03	The communication channel must not allow code injection.

Classification	Control Name	Unified ID	Control Requirements
vehicle communicatio n channel	communication channel related vehicle threat	V-6-4-VEH-04	The communication channel must not allow manipulation of the vehicle's data/code.
vehicle communicatio n channel	communication channel related vehicle threat	V-6-4-VEH-05	The communication channel shall not allow overwriting of the vehicle's data/code.
vehicle communicatio	communication channel related	V-6-4-VEH-06	The communication channel shall not allow the deletion of vehicle data/codes.

n channel	vehicle threat		
vehicle communicatio n channel	communication channel related vehicle threat	V-6-4-VEH-07	The communication channel shall not allow the addition of new data/codes to the vehicle.
vehicle communicatio n channel	communication channel related vehicle threat	V-6-4-VEH-08	Do not allow information from untrusted sources.
vehicle communicatio n channel	communication channel related vehicle threat	V-6-4-VEH-09	It must counter man-in-the-middle attacks or session hijacking attacks.
vehicle communicatio n channel	communication channel related vehicle threat	V-6-4-VEH-10	Attacks on communication gateways must be countered.
vehicle communicatio n channel	communication channel related vehicle threat	V-6-4-VEH-11	Detect and respond to information interception/signal interference/communication monitoring.
vehicle communicatio n channel	communication channel related vehicle threat	V-6-4-VEH-12	Control unauthorized access to files or data.
vehicle communicatio n channel	communication channel related vehicle threat	V-6-4-VEH-13	It must respond to denial-of-service attacks of vehicle information systems.
vehicle communicatio n channel	communication channel related vehicle threat	V-6-4-VEH-14	It must counter denial of service attacks on vehicle-to-vehicle communication.
vehicle communicatio n channel	communication channel related vehicle threat	V-6-4-VEH-15	It should be ensured that unauthorized users cannot gain access rights (eg root access).
vehicle communicatio n channel	communication channel related vehicle threat	V-6-4-VEH-16	It is necessary to respond to vehicle system infection caused by viruses embedded in communication media.
vehicle communicatio n channel	communication channel related vehicle threat	V-6-4-VEH-17	Malicious internal messages must be detected and blocked..
vehicle communicatio n channel	communication channel related vehicle threat	V-6-4-VEH-18	Malicious V2X messages must be detected and blocked.
vehicle communicatio	communication channel related	V-6-4-VEH-19	Malicious diagnostic messages should be blocked.

n channel	vehicle threat		
vehicle communicatio n channel	communication channel related vehicle threat	V-6-4-VEH-20	Malicious proprietary messages should be detected and blocked.
vehicle communicatio n channel	vehicle data/ Threats to your code	V-6-4-VEH-21	It is necessary to respond to unauthorized deletion or manipulation of the event log of the system.
update procedure	update process and Related vehicle threats	V-6-5-VEH-22	OTA software update procedure should avoid corruption.

Classification	Control Name	Unified ID	Control Requirements
update procedure	update process and Related vehicle threats	V-6-5-VEH-23	Damage to local/physical software update procedures should be avoided.
update procedure	update process and Related vehicle threats	V-6-5-VEH-24	Before the update process, make sure that the software is not tampered with or damaged.
update procedure	update process and Related vehicle threats	V-6-5-VEH-25	The encryption key of the software provider to allow invalid updates must be prevented from being compromised.
update procedure	update process and Related vehicle threats	V-6-5-VEH-26	You must respond to denial-of-service attacks on update servers or networks to limit essential software updates or leak customer identification information.
Cybersecurity attacks caused by unintentional	Vehicle threats by unintended	V-6-6-VEH-27	Countermeasures must be taken to ensure that innocent victims (eg owners, operators, maintenance engineers) do not

user actions	actions that facilitate cyberattacks		unintentionally load malicious programs or activate attacks.
Cybersecurity attacks caused by unintentional user actions	Vehicle threats by unintended actions that facilitate cyberattacks	V-6-6-VEH-28	Defined security procedures must be followed to avoid exposure to cybersecurity attacks due to unintended user actions.
External communications and connections	Vehicle threats related to external connectivity and connections	V-6-7-VEH-29	It must respond to manipulation of remote systems, such as remote keys, immobilizers, and charging files.
External communications and connections	Vehicle threats related to external connectivity and connections	V-6-7-VEH-30	It must respond to vehicle telematics manipulation.
External communications and connections	Vehicle threats related to external connectivity and connections	V-6-7-VEH-31	Interference with short-range wireless systems or sensors must be counteracted.
External communications and connections	Vehicle threats related to external connectivity and connections	V-6-7-VEH-32	A compromised application or an application with weak software security is used as a way to attack the vehicle system.
External communications and connections	Vehicle threats related to	V-6-7-VEH-33	External interfaces such as USB or other ports that are used as points of attack, for example from code injection, need to be

	external connectivity and connections		protected.
External communications and connections	Vehicle threats related to external connectivity and connections	V-6-7-VEH-34	It is necessary to prevent virus-infected transmission media from being connected to vehicle systems.
External communications and connections	Vehicle threats related to external connectivity and connections	V-6-7-VEH-35	Access to diagnostic access (eg, dongle for OBD port) used to facilitate an attack, such as direct/indirect manipulation of vehicle parameters, should be controlled.

Classification	Control Name	Unified ID	Control Requirements
Targets or causes of potential attacks	Threats to vehicle data/code	V-6-8-VEH-36	Illegal extraction/copying of copyrighted or proprietary software in vehicle systems should be blocked.
Targets or causes of potential attacks	Threats to vehicle data/code	V-6-8-VEH-37	Unauthorized access to the owner's personal information, such as personally identifiable information, payment account information, address book information, location information, and vehicle electronic ID, should be blocked.
Targets or causes of potential attacks	Threats to vehicle data/code	V-6-8-VEH-38	Encryption key extraction must be blocked.
Targets or causes of potential attacks	Threats to vehicle data/code	V-6-8-VEH-39	Access control techniques and designs should be applied to protect system data/code.
Potential target of attack or cause	Threats to vehicle data/code	V-6-8-VEH-40	It is necessary to prevent forgery of identification information in the section communicating with the backend infrastructure.
Targets or causes of potential attacks	Threats to vehicle data/code	V-6-8-VEH-41	It must be ensured that the monitoring system is not bypassed. (e.g. number of hacking/falsification/blocking or execution of messages such as ODR Tracker data)
Targets or causes of potential attacks	Threats to vehicle data/code	V-6-8-VEH-42	Forgery of vehicle driving data should be prevented.
Targets or causes of potential attacks	Threats to vehicle data/code	V-6-8-VEH-43	Unauthorized changes to system diagnostic data must be prevented.
Targets or causes of potential attacks	Threats to vehicle data/code	V-6-8-VEH-44	It is necessary to respond to unauthorized deletion or manipulation of the event log of the system.
Targets or causes of potential attacks	Threats to vehicle data/code	V-6-8-VEH-45	Prevent the use of malicious software.
Targets or causes of potential attacks	Threats to vehicle data/code	V-6-8-VEH-46	Software counterfeiting of vehicle control systems or information systems must be prevented.

Targets or causes of potential attacks	Threats to vehicle data/code	V-6-8-VEH-47	The internal network must respond to CAN bus flooding attacks or denial of service attacks.
Targets or causes of potential attacks	Threats to vehicle data/code	V-6-8-VEH-48	Unauthorized access to falsify environmental variables for key vehicle functions, such as brake data and airbag activation thresholds, must be prevented.
Targets or causes of potential attacks	Threats to vehicle data/code	V-6-8-VEH-49	Unauthorized access to falsify charging parameters such as charging voltage, charging power, and battery temperature should be prevented.

Classification	Control Name	Unified ID	Control Requirements
Potential vulnerabilities that can be exploited if not fully protected or hardened	Vulnerabilities that can be exploited if not sufficiently protected or hardened	V-6-9-VEH-50	A secure encryption algorithm should be used in consideration of the encryption key length and validity period.
Potential vulnerabilities that can be exploited if not fully protected or hardened	Vulnerabilities that can be exploited if not sufficiently protected or hardened	V-6-9-VEH-51	Secure encryption algorithms should be used to protect sensitive systems.
Potential vulnerabilities that can be exploited if not fully protected or hardened	Vulnerabilities that can be exploited if not sufficiently protected or hardened	V-6-9-VEH-52	Eliminate the use of cryptographic algorithms that are already deprecated or will soon be deprecated.
Potential vulnerabilities that can be exploited if not	Vulnerabilities that can be exploited if not	V-6-9-VEH-53	It is necessary to develop hardware/software designed safely for attack detection and defense functions.

fully protected or hardened	sufficiently protected or hardened		
Potential vulnerabilities that can be exploited if not fully protected or hardened	Vulnerabilities that can be exploited if not sufficiently protected or hardened	V-6-9-VEH-54	You have to deal with potential vulnerabilities that can arise from software bugs.
Potential vulnerabilities that can be exploited if not fully protected or hardened	Vulnerabilities that can be exploited if not sufficiently protected or hardened	V-6-9-VEH-55	When using development-related resources, you must either allow access to the ECU or ensure that the attacker does not gain higher privileges.
Potential vulnerabilities that can be exploited if not fully protected or hardened	Vulnerabilities that can be exploited if not sufficiently protected or hardened	V-6-9-VEH-56	Unnecessary Internet ports should be disabled to block illegal access to network systems.
Potential vulnerabilities that can be exploited if not fully protected or hardened	Vulnerabilities that can be exploited if not sufficiently protected or hardened	V-6-9-VEH-57	You have to make sure you don't lose control by bypass network separation.

Classification	Control Name	Unified ID	Control Requirements
Data loss / vehicle data leakage	Vulnerabilities that can be exploited if not sufficiently protected or hardened	V-6-10-VEH-58	Personal information must be protected from leakage or infringement when changing vehicle users.
Physical manipulations that enable an attack	Vulnerabilities that can be exploited if not sufficiently protected or hardened	V-6-11-VEH-59	Personal information should not be infringed when changing vehicle users.
Physical manipulations that enable an attack	Vulnerabilities that can be exploited if not sufficiently protected or hardened	V-6-11-VEH-60	Unauthorized intrusion due to hardware manipulation should be prevented and detected. - Adding illegal electronic hardware to vehicles for man-in-the-middle attacks -Replace certified electronic hardware (sensor, etc.) with non-certified electronic hardware -Manipulation of information collected by sensors (e.g. using magnets to manipulate Hall-effect sensors connected to transmissions)

3.6.2 Backend Infrastructure Inspection Items

3.6.2.1 Management Security

The management security items of the backend infrastructure are composed with '1. Establishment and operation of a management system', '2. Requirements for Protection Measures - 2.1 In the fields of policy, organization, asset management, 2.2 human security, 2.3 external security', and '3. Requirements for each stage of personal information processing'.

Table 10. Administrative security items for backend infrastructure

Classification	Control Name	Unified ID	Control Requirements
Establishment of management system foundation	Executive Engagement	B-1-1-GOV-01	The top management shall establish and operate a reporting and decision-making system so that management can participate in the establishment of information protection and personal information protection
Establishment of management system foundation	Appointment of Chief Information Security Officer	B-1-1-GOV-02	The CEO shall designate the chief information security officer in charge of information protection work and the personal information protection officer in charge of personal information protection work at the executive level that can allocate resources such as budget and manpower.

Classification	Control Name	Unified ID	Control Requirements
Establishment of management system foundation	Organization	B-1-1-GOV-03	The CEO should form and operate a consultative body which are composed with a working organization for the effective implementation of information protection and personal information protection, a committee that can review and decide on major matters related to information protection and personal information protection across the organization. And also form and operate a consultative body with someone in charge of information protection and personal information protection by department for company-wide protection activities.
Establishment of management system foundation	range setting	B-1-1-GOV-04	The scope of the management system should be set in consideration of the organization's core services and the status of personal information processing, and related services, personal information processing tasks, organization, assets, and physical location should be documented.
Establishment of management system foundation	policy making	B-1-1-GOV-05	Establish and prepare information protection and personal information protection policies and enforcement documents, and at this time, the organization's information protection and personal information protection policies and directions should be clearly presented. In addition, policies and implementation documents must be approved by management and delivered in an easy-to-understand format to employees and related parties.

Establishment of management system foundation	resource allocation	B-1-1-GOV-06	The top management must secure human resources with expertise in each field of information protection and personal information protection, and allocate budget and resources for effective implementation and continuous operation of the management system.
Risk management	Identification of information assets	B-2-1-1GOV-07	The classification criteria for information assets should be established according to the business characteristics of the organization to identify and classify all information assets within the scope of the management system, calculate the importance, and then keep the list up-to-date.
Risk management	status and flow analysis	B-2-1-1GOV-08	Analyze the information service and personal information processing status for all areas of the management system, identify and document work procedures and flows, and periodically review them to maintain the latest status.
Risk management	risk assessment	B-2-1-1GOV-09	Risk information for each type is collected through internal and external environmental analysis of the organization, risk assessment methods suitable for the organization are selected, and risks are evaluated at least once a year in all areas of the management system. Acceptable risks must be managed with the approval of the management.
Risk management	Selection of protection measures	B-2-1-1GOV-10	In order to deal with the risks identified according to the risk assessment results, protection measures suitable for the organization should be selected, and an implementation plan including the

			priority of protection measures, schedule, person in charge, and budget should be established and approved by the management.
Management system operation	Implementation of protection measures	B-3-1-GOV-11	The selected protection measures are effectively implemented according to the implementation plan, and the management must check the accuracy and effectiveness of the implementation results.

Classification	Control Name	Unified ID	Control Requirements
Management system operation	Sharing protection measures	B-3-1-GOV-12	It is necessary to identify the departments and personnel responsible for the actual operation or implementation of the protection measures, share the relevant contents, and provide training to ensure continuous operation.
Management system operation	Operational status management	B-3-1-GOV-13	According to the management system established by the organization, operational activities and performance details that must be performed regularly or periodically are recorded and managed so that identification and tracking are possible, and the management must periodically check and manage the effectiveness of operational activities.
Management system check and improvement	Legal requirements Compliance review	B-4--1-GOV-14	Information protection and personal information protection-related legal requirements to be observed by the organization should be periodically identified and reflected in the regulations, and compliance should be continuously reviewed.

Management system check and improvement	Management system check	B-4--1-GOV-15	Ensure that the management system is effectively operated in accordance with internal policies and legal requirements by composing personnel with independence and expertise to check at least once a year and report any problems found to the management
Management system check and improvement	Management system improvement	B-4-1-GOV-16	Analyze the causes of problems in the management system identified through compliance review with legal requirements and inspection of the management system, establish and implement measures to prevent recurrence, and management must check the accuracy and effectiveness of improvement results..
policy, organization, asset management	maintenance of policies	B-5-1-COM-01	Information protection and personal information protection-related policies and enforcement documents should be reviewed periodically in accordance with laws and regulations, linkage with higher-level organizations and related institutional policies, and changes in the organization's internal and external environment, etc.
policy, organization, asset management	Organizational maintenance	B-5-1-COM-02	Each member of the organization shall be assigned roles and responsibilities related to information protection and personal information protection, and a system for evaluating their activities and a system for mutual communication between the organization and members of the organization shall be established and operated.
policy, organization, asset management	Information asset management	B-5-1-COM-03	Establish and implement handling procedures and protection measures according to the use and importance of information assets, and clearly define and manage responsibility for each asset

human security	Designation and management of key personnel	B-6-1-COM-04	Standards and management plans for major tasks such as handling of personal and important information or access to major systems should be established, and the list of major tasks should be kept up to date by designating the minimum number of major workers.
human security	separation of duties	B-6-1-COM-05	In order to prevent potential damage due to misuse or abuse of authority, standards for separation of duties should be established and applied. However, if separation of duties is unavoidable, separate supplementary measures should be prepared and implemented.

Classification	Control Name	Unified ID	Control Requirements
human security	security pledge	B-6-1-COM-06	Employees, temporary employees, outsiders, etc. who handle information assets or who are granted access rights must receive an information protection pledge according to the nature of their work so that they can clearly recognize the matters to be complied with, such as internal policies, related laws, and confidentiality obligations.
human security	Raising awareness and training	B-6-1-COM-07	Establish and operate annual awareness-raising activities and education and training plans so that executives and employees and related outsiders can understand the organization's management system and policies and secure professionalism for each job. As a

			result, the effectiveness should be evaluated and reflected in the next plan.
human security	retirement and Job change management	B-6-1-COM-08	In case of retirement or job change, procedures such as asset return, account and access rights recovery/adjustment, and result confirmation should be established and managed by departments related to personnel, information protection, personal information protection, IT, etc.
human security	Action in case of a security breach	B-6-1-COM-09	When executives and/or employees and related outsiders violate laws, regulations and internal policies, they shall establish and implement a corresponding action procedure.
outsider security	Outsiders Status management	B-7-1-COM-10	When outsourcing part of business (personal information handling, information protection, information system operation or development, etc.) or using external facilities or services (integrated information and communication facilities, cloud services, application services, etc.), Appropriate protection measures should be prepared by identifying the requirements and risks arising from external organizations and services.
outsider security	Security when contracting with an outsider	B-7-1-COM-11	When using an external service or entrusting work to an outside party, the requirements for information protection and personal information protection must be identified, and related contents must be specified in a contract or agreement.

outsider security	outsider security fulfillment management	B-7-1-COM-12	In accordance with the information protection and personal information protection requirements specified in the contract, agreement, and internal policy, the implementation of protection measures by outsiders shall be managed and supervised, such as periodic inspection or audit.
outsider security	Security on change and expiration of outsider contracts	B-7-1-COM-13	Protection measures such as return of provided information assets, deletion of information system access account, destruction of important information, and request for confidentiality of information acquired during business performance shall be implemented when contract expires, work is terminated, or the person in charge is changed.
Protection measures when collecting personal information	Consent to collection of personal information	B-17-1-PRI-01	Personal information must be collected with the consent of the information subject (user) or legally in accordance with related laws and regulations.

Classification	Control Name	Unified ID	Control Requirements
Protection measures when collecting personal information	Restrictions on processing of resident registration numbers	B-17-1-PRI-02	The resident registration number cannot be collected or used, except where there is a legal basis, and even if the processing of the resident registration number is permitted, alternative means must be provided on the Internet website, etc.
Protection measures when	Restrictions on processing	B-17-1-PRI-03	In order to process sensitive information and unique identification information (excluding resident

collecting personal information	of sensitive information and unique identification information		registration number), separate consent from the information subject (user) must be obtained, except when specifically required or permitted by laws and regulations.
Protection measures when collecting personal information	Indirect Collection Protection Measures	B-17-1-PRI-04	When personal information is collected or provided from other than the information subject (user), only the minimum amount of personal information necessary for work must be collected and used. And based on laws and regulations or if there is a request from the information subject (user), the source of personal information collection, purpose of processing, and right to request to suspend processing shall be informed.
Protection measures when collecting personal information	Installation and operation of image information processing equipment	B-17-1-PRI-05	When installing and operating an image information processing device in an open place, legal requirements (installation of information boards, etc.) must be complied with according to the purpose and location of the installation, and appropriate protection measures must be established and implemented.
Protection measures when collecting personal information	Measures when using for promotional and marketing purposes	B-17-1-PRI-06	In the case of collecting and using personal information for marketing purposes such as promotion of goods or services, sales solicitation, and transmission of advertising information, the purpose of collection and use shall be notified so that the information subject (user) can clearly recognize the purpose and obtain consent.
Protection measures when	Restrictions on collection	B-17-1-PRI-07	Personal information must legally and legitimately collect the minimum information necessary to provide

collecting personal information	of personal information		services. In the case of collecting personal information other than essential information, it shall not refuse to provide services on the grounds that the information is not provided by classifying it into optional items.
Protection of personal information and safeguards when using it	Personal information status management	B-18-1-PRI-08	The current status of personal information collected and held shall be regularly managed, such as the amount of personal information collected and held, the purpose and method of processing, and in the case of public institutions, it shall be registered with the head of the relevant institution prescribed by law.
Protection of personal information and safeguards when using it	Guarantee of personal information quality	B-18-1-PRI-09	For the collected personal information, management procedures shall be provided to the information subject (user) to ensure the accuracy, completeness and up-to-dateness of the personal information to the extent necessary for the purpose of processing.

Classification	Control Name	Unified ID	Control Requirements

Protection measures for retention and use of personal information	Restriction on display of personal information and protection measures when using it	B-18-1-PRI-10	When inquiring and outputting personal information (printing, screen display, file creation, etc.), the purpose shall be specified, and according to the purpose, the minimization of output items, restrictions on the display of personal information, and measures to protect the output shall be carried out. In addition, in order to prevent excessive use of personal information in the data processing process such as big data analysis and testing, personal information that is not essential for business must be deleted or taken measures to prevent identification.
Protection measures for retention and use of personal information	User terminal access protection	B-18-1-PRI-11	If it is necessary to access the information stored in the mobile communication terminal device of the information subject (user) and the functions installed in the mobile communication terminal device, it must be notified so that it can be recognized and the consent of the information subject (user) must be obtained.
Protection measures for retention and use of personal information	Use and provision of personal information for purposes other than the purpose	B-18-1-PRI-12	Personal information shall be used or provided only for the purpose of receiving notice and consent from the information subject (user) at the time of collection or within the scope based on laws and regulations. When using or providing in excess of this limit, obtain additional consent from the information subject (user) or check whether it is a legitimate case in accordance with relevant

			laws and regulations, and Protection measures shall be established and implemented.
Protection measures when providing personal information	Provision of personal information to third parties	B-19-1-PRI-13	When personal information is provided to a third party, it must be based on legal grounds or with the consent of the information subject (user), and protective measures must be established and implemented to safely protect personal information in the process of providing it.
Protection measures when providing personal information	Information subject notice according to business consignment	B-19-1-PRI-14	When entrusting personal information processing work to a third party, the information subject (user) shall be informed of the contents of the entrusted work and related matters such as the trustee, and if necessary, consent shall be obtained.
Protection measures when providing personal information	Transfer of personal information according to business transfer, etc.	B-19-1-PRI-15	When personal information is transferred or transferred due to the transfer or merger of business, appropriate protective measures such as notification of the information subject (user) shall be established and implemented.
Protection measures when providing personal information	Transfer of personal information abroad.	B-19-1-PRI-16	In the case of transferring personal information abroad, appropriate protection measures such as consent to overseas transfer and disclosure of related matters shall be established and implemented.

Protection measures when personal information is destroyed	Destruction of personal information .	B-20-1-PRI-17	Establish an internal policy related to the retention period and destruction of personal information, and when the time of destruction is reached, such as the expiration of the retention period of personal information and achievement of the purpose of processing, it shall be destroyed without delay in a way that can guarantee the safety and completeness of destruction.

Classification	Control Name	Unified ID	Control Requirements
Protective measures when destroying personal information.	Measures to be taken after the purpose of processing has been achieved	B-20-1-PRI-18	Even after the expiration of the retention period of personal information or the achievement of the purpose of processing, if it is preserved without being destroyed in accordance with relevant laws, etc., it shall be limited to the minimum items necessary for the purpose and stored and managed separately from other personal information.
Protective measures when destroying personal information.	Dormant User Management	B-20-1-PRI-19	In order to protect the personal information of dormant users who do not use the service for a certain period of time, appropriate protective measures such as notification of related matters and destruction or separate storage of personal information shall be implemented.
Protection of data subject rights	Disclosure of the personal information processing	B-21-1-PRI-20	Personal information processing policies should be established, including all necessary matters such as the purpose of processing personal information, and disclosed and

	policy.		continuously updated according to appropriate methods so that the data subject (user) can easily check them at any time.
Protection of data subject rights	Guarantee of data subject rights	B-21-1-PRI-21	Establish and implement methods and procedures for exercising rights so that information subjects (users) can access, correct/delete, suspend processing, raise objections, and request withdrawal of consent more easily than collection methods and procedures. And when receiving a request from information subjects (users), It should be handled without delay and related records should be left. In addition, standards such as request for deletion and temporary measures must be established and implemented so that information infringing on the rights of others, such as privacy infringement and defamation of the data subject (user), etc., is not distributed.
Protection of data subject rights	Notice of usage history	B-21-1-PRI-22	Matters to be notified to the information subject (user), such as details of use of personal information, shall be identified and notified periodically of the details thereof.

3.6.2.2 Technical security.

The technical security items of the backend infrastructure are consisted of '2. Requirements for Protection Measures-2.5 Authentication and Permission Management, 2.6 Access control, 2.7 encryption applied, 2.8 information system introduction and development security, 2.9 system and service operation management, 2.10 System and service security management, 2.11 accident prevention and response, and 2.12 disaster recovery'.

<Table 11> Technical security items for backend infrastructure

Classification	Control Name	Unified ID	Control Requirements
Authentication and Permission Management	user account management	B-9-1-COM-21	In order to control unauthorized access to information systems, personal information, and important information, and to minimize access rights according to the purpose of work, establish and implement procedures for user registration and authorization When registering and authorizing users, it is necessary to define and recognize that users have security responsibilities.
Authentication and Permission Management	User identification	B-9-1-COM-22	User accounts must be assigned identifiers so that they can be uniquely identified for each user, and the use of guessable identifiers must be limited. If the same identifier is shared and used, supplementary measures such as approval of the person in charge and securing of traceability shall be established and implemented by reviewing the reason and feasibility.
Authentication and Permission Management	User authentication	B-9-1-COM-23	Users' access to information systems and personal information and important information shall apply a secure authentication procedure and, if necessary, a strengthened authentication method. In addition, unauthorized access

			control measures such as limiting the number of logins and warning of illegal login attempts should be established and implemented.
Authentication and Permission Management	Password Management	B-9-1-COM-24	Establish and implement password management procedures used by information subjects (users) such as information system users, customers, and members in consideration of legal requirements and external threat factors
Authentication and Permission Management	Special account and Permission Management	B-9-1-COM-25	Accounts and privileges used for special purposes, such as information system management, personal information and important information management, should be given to a minimum and separately identified and controlled.
Authentication and Permission Management	Review access rights	B-9-1-COM-26	It is necessary to periodically review the history of registration, use, deletion, and granting, changing, and deleting access rights of the information system and user accounts accessing personal information and important information.
Access control	network access	B-10-1-COM-27	To control unauthorized access to the network, establish and implement management procedures such as IP management and terminal authentication, and apply network separation (DMZ, server farm, DB zone, development zone, etc.) and access control according to the business purpose and importance.

Classification	Control Name	Unified ID	Control Requirements
access control	information system Access	B-10-1-COM-28	Users who allow access to information systems such as servers and network systems, access restriction methods, and safe access methods should be defined and controlled.
access control	Application Access	B-10-1-COM-29	Criteria should be established and applied to limit the right to access applications according to the importance of each user's work and access information, and to minimize the exposure of unnecessary or important information.
access control	database Access	B-10-1-COM-30	Information stored and managed in the database, such as table lists, should be identified, and access control policies should be established and implemented according to the importance of information, application programs and user types.
access control	wireless network Access	B-10-1-COM-31	When using a wireless network, wireless network protection measures such as user authentication, transmission and reception data encryption, and AP control must be applied. In addition, protection measures against unauthorized wireless network access such as AD Hoc access and unauthorized AP use should be established and implemented.
access control	remote access control	B-10-1-COM-32	In principle, information system management and processing of personal information in places other than the protected area are prohibited, and when remote access is permitted for unavoidable reasons such as telecommuting, disability response, remote collaboration, etc. , protection measures such as enhanced authentication, section encryption, and

			access terminal security (Vaccine, patch, etc.) should be established and implemented.
access control	Internet access control	B-10-1-COM-33	Internet access control policies should be established and implemented, such as restricting Internet access or services (P2P, Webhard, Messenger, etc.) to major information systems, major job performance, and personal information handling terminals to prevent information leakage, malicious code infection, and penetration.
Encryption applied	Apply password policy	B-11-1-COM-34	In order to protect personal information and key information, policies for encryption target, password strength, and password use reflecting legal requirements should be established, and encryption should be applied when storing, transmitting, and delivering personal information and key information.
Encryption applied	encryption key management	B-11-1-COM-35	Management procedures for safe creation, use, storage, distribution, and destruction of encryption keys shall be established and implemented, and recovery measures shall be prepared if necessary.
information system introduction and development security	Defining security requirements	B-12-1-COM-36	When the information system is introduced/developed/changed, security requirements such as legal requirements related to information protection and personal information protection, latest security vulnerabilities, and safe coding methods shall be defined and applied.

Classification	Control Name	Unified ID	Control Requirements
Introduction and development security of information systems	Security Requirements review and test	B-12-1-COM-37	To review whether an information system has been introduced or implemented in accordance with predefined security requirements, review standards and procedures such as compliance with legal requirements, checking the latest security vulnerabilities, implementing safe coding, and evaluating personal information impact should be established and improved for discovered problems.
Introduction and development security of information systems	Separation of test and operating environment.	B-12-1-COM-38	Development and testing systems should, in principle, be separated in order to reduce the risk of unauthorized access and modification to the operating system.
Introduction and development security of information systems	Test data security	B-12-1-COM-39	In order to prevent leakage of operational data in the process of system testing, procedures for creation, use, management, destruction, and technical protection measures of test data shall be established and implemented.
Introduction and development security of information systems	source program management	B-12-1-COM-40	The source program should be managed so that only authorized users can access it, and in principle, it should not be stored in the operating environment.
Introduction and development security of information systems	Operational environment transfer	B-12-1-COM-41	Controlled procedures should be followed when newly introduced/ developed or changed systems are transferred to the operating environment, and executable codes should be executed according to the test and user acceptance procedures.

system and service security management	security system operation	B-13-1-COM-42	For each type of security system, it is necessary to establish and implement operational procedures such as designation of managers, update of the latest policy, change of rulesets, and event monitoring, and manage the status of policy application by security system.
system and service operation management	change management	B-13-1-COM-43	Procedures should be established and implemented to manage all changes to information system-related assets, and the impact on system performance and security should be analyzed before changes.
system and service operation management	performance and disability management	B-13-1-COM-44	To ensure the availability of information systems, performance and capacity requirements should be defined and the status quo should be continuously monitored, and procedures such as detection, recording, analysis, recovery, and reporting should be established and managed to effectively respond to failures.
system and service operation management	backup and recovery management	B-13-1-COM-45	In order to maintain the availability and data integrity of the information system, procedures such as backup target, period, method, storage location, storage period, and dissipation shall be established and implemented. In addition, in the event of an accident, it must be managed so that it can be restored in a timely manner.
system and service operation management	log and Access record management	B-13-1-COM-46	Set the log type, retention period, and preservation method of user access records, system logs, and authorization details for information systems such as servers, application programs, security systems, and

			network systems, and keep them safely managed to prevent forgery, falsification, theft, or loss.

Classification	Control Name	Unified ID	Control Requirements
system and service operation management	Check log and access history	B-13-1-COM-47	In order to ensure the normal use of the information system and to prevent user misuse and abuse (unauthorized access, excessive inquiry, etc.), log review standards for access and use should be established and periodically checked, and follow-up measures should be taken in a timely manner.
system and service operation management	time synchronization	B-13-1-COM-48	In order to ensure the accuracy of logs and access records and to analyze the logs reliably, the time of the related information system shall be synchronized with the standard time and periodically managed.
system and service operation management	Reuse and disposal of information assets	B-13-1-COM-49	In the process of reuse and disposal of information assets, safe reuse and disposal procedures shall be established and implemented so that personal information and important information are not recovered or reproduced.
system and service security management	cloud security	B-14-1-COM-50	When using cloud services, protection measures for administrator access and security settings must be established and implemented so that important and personal information are not leaked or exposed due to unauthorized access or setting errors according to the service type (SaaS, PaaS, IaaS, etc.).

system and service security management	public server security	B-14-1-COM-51	In the case of a server that is open to the external network, it must be separated from the internal network and reinforced protection measures such as vulnerability check, access control, authentication, information collection, storage, and disclosure procedures must be established and implemented.
system and service security management	e-commerce and Fintech Security	B-14-1-COM-52	When providing electronic transactions and Fintech services, protection measures such as authentication and encryption should be established to prevent infringement accidents such as information leakage or data manipulation and fraud, and safety should be checked when linking with external systems such as payment systems.
system and service security management	Information transmission security	B-14-1-COM-53	When transmitting personal information and important information to other organizations, a safe transmission policy should be established, and management responsibilities, transmission methods, and technical protection measures for protecting personal and important information shall be agreed upon and implemented through agreement between organizations.
system and service security management	Business terminal device security	B-14-1-COM-54	When terminal devices such as PCs and mobile devices are connected to the network for business purposes, access control measures such as device authentication and approval, access range, and device security settings should be established and periodically checked.

system and service security management	Auxiliary storage device management	B-14-1-COM-55	Management procedures should be established and implemented to prevent leakage of personal or important information or infection of malicious code through auxiliary storage devices, and auxiliary storage devices containing personal or important information should be stored in a safe place.

Classification	Control Name	Unified ID	Control Requirements
system and service security management	patch management	B-14-1-COM-56	The latest patches should be applied to prevent infringements caused by vulnerabilities in software, operating systems, and security systems. However, if it is difficult to apply the latest patch after reviewing the impact of the service, a separate supplementary measure should be prepared and implemented.
system and service security management	Malicious code Control	B-14-1-COM-57	In order to protect personal information, important information, information systems and business terminals from malicious codes such as viruses, worms, Trojan horses, and ransomware, protection measures should be established and implemented such as prevention, detection and response of malicious codes.
Accident Prevention and Response	Establishment of accident prevention and response system	B-15-1-COM-58	Establish systems and procedures for the detection, response, analysis, and sharing of internal and external intrusion attempts to prevent intrusion accidents and personal information leakage, and to respond quickly and effectively in the event of an accident, and establish a

			cooperative system with related external organizations and experts.
Accident Prevention and Response	Vulnerability check and action	B-15-1-COM-59	In order to check whether the vulnerabilities of the information system are exposed, a vulnerability check should be performed regularly, and any vulnerabilities found should be promptly taken action. In addition, it is necessary to continuously identify the occurrence of the latest security vulnerabilities, analyze the impact on the information system, and take measures.
Accident Prevention and Response	Abnormal behavior analysis and monitoring	B-15-1-COM-60	Network and data flows are collected and analyzed to quickly detect and respond to internal and external intrusion attempts, personal information leakage attempts, and fraudulent acts, and follow-up actions according to monitoring and inspection results should be taken in a timely manner.
Accident Prevention and Response	Incident response training and improvement	B-15-1-COM-61	Simulation training according to the scenario should be conducted at least once a year to ensure that employees and stakeholders are familiar with the procedures for responding to infringement incidents and personal information leakage, and the response system should be improved by reflecting the training results.
Accident Prevention and Response	incident response and restore	B-15-1-COM-62	Upon recognizing signs or occurrences of intrusion accidents and personal information leakage, legal notice and reporting obligations shall be complied with, and shall be promptly responded to and restored according to the procedure, and

			measures to prevent recurrence should be established and reflected in the response system after accident analysis.
Disaster recovery	Safety measures against disasters.	B-16-1-COM-63	Types of disasters that may threaten the operational continuity of the organization's core services and systems, such as natural disasters, communication/power failures, and hacking, should be identified, and the expected damage and impact of each type should be analyzed. In addition, it is necessary to define the recovery target time and recovery target point, and establish a disaster recovery system such as recovery strategies and countermeasures, emergency recovery organization, emergency contact system, and recovery procedures.
Disaster recovery	Disaster recovery testing and improvement	B-16-1-COM-64	The appropriateness of the disaster recovery strategy and countermeasures should be tested regularly, and the recovery strategy and countermeasures should be supplemented by reflecting the test results, changes in the information system environment, and changes according to laws and regulations.

3.6.2.3 Physical Security

The physical security item of the backend infrastructure consists of the '2. Requirements for protective measures - 2.4 Physical Security' field.

<Table 12> Physical security of backend infrastructure

Classification	Control Name	Unified ID	Control Requirements
Physical Security	Designation of a protected area	B-8-1-COM-14	To protect personal information, important information, documents, storage media, major facilities and systems, etc. from physical and environmental threats, physical protection areas such as controlled areas, restricted areas, and reception areas must be designated, and protection measures for each area must be established and implemented.
Physical Security	Access Control	B-8-1-COM-15	Access and access history should be reviewed periodically to ensure that only authorized persons enter the protected area and ensure accountability.
Physical Security	Information System Protection	B-8-1-COM-16	Information systems should be placed in consideration of their importance and characteristics to reduce environmental threats, harmful factors, and the possibility of unauthorized access, and should protect communications and power cables from damage.
Physical Security	Protection equipment operation	B-8-1-COM-17	Depending on the importance and characteristics of the information system located in the protected area, protective equipment such as temperature and humidity control, fire detection, fire extinguishing equipment, leak detection, UPS, emergency generator, and dual power lines shall be installed, and operation

			procedures shall be established and operated.
Physical Security	work in the protected area	B-8-1-COM-18	Work procedures should be established and implemented to prevent unauthorized acts and abuse of authority within the protected area, and work records should be reviewed periodically.
Physical Security	Control of the moving-in and out equipment.	B-8-1-COM-19	Establishment and implementation of import/export control procedures for information systems, mobile devices, storage media, etc. within the protected area, and periodically review them.
Physical Security	Work environment security	B-8-1-COM-20	Work environment protection measures such as clean desks and regular inspections shall be established and implemented to prevent personal information and important information from being exposed or leaked to unauthorized persons through shared office devices (document storage, public PC, multifunction devices, file server, etc.) and personal work environment (work PC, desk, etc.).

Self-driving car security model (summary)

The self-driving car security model (summary) separately includes some items among all the contents of the self-driving car security model.

Please refer to the overall security model as it is a compilation of the service analysis, security threats, and countermeasures mentioned in this summary.

Contact : Korea Internet & Security Agency Convergence Security Policy Team 061-820-1287,

Email : cslivinglab@kisa.or.kr