Annex 5

List of threats and corresponding mitigations

1. This annex consists of three parts. Part A of this annex describes the baseline for threats, vulnerabilities and attack methods. Part B of this annex describes mitigations to the threats which are intended for vehicle types. Part C describes mitigations to the threats which are intended for areas outside of vehicles, e.g. on IT backends.

2. Part A, Part B, and Part C shall be considered for risk assessment and mitigations to be implemented by vehicle manufacturers.

3. The high-level vulnerability and its corresponding examples have been indexed in Part A. The same indexing has been referenced in the tables in Parts B and C to link each of the attack/vulnerability with a list of corresponding mitigation measures.

4. The threat analysis shall also consider possible attack impacts. These may help ascertain the severity of a risk and identify additional risks. Possible attack impacts may include:

   (a) Safe operation of vehicle affected;

   (b) Vehicle functions stop working;

   (c) Software modified, performance altered;

   (d) Software altered but no operational effects;

   (e) Data integrity breach;

   (f) Data confidentiality breach;

   (g) Loss of data availability;

   (h) Other, including criminality.

Part A. Vulnerability or attack method related to the threats

1. High level descriptions of threats and relating vulnerability or attack method are listed in Table A1.

Table A1
List of vulnerability or attack method related to the threats

High level and sub-level descriptions of vulnerability/ threat			*Example of vulnerability or attack method*	
4.3.1 Threats regarding back-end servers related to vehicles in the field	1	Back-end servers used as a means to attack a vehicle or extract data	1.1	Abuse of privileges by staff (**insider attack**)
			1.2	**Unauthorized internet access** to the server (enabled for example by backdoors, unpatched system software vulnerabilities, SQL attacks or other means)
			1.3	**Unauthorized physical access** to the server (conducted by for example USB sticks or other media connecting to the server)
	2	Services from back-end server being disrupted, affecting the operation of a vehicle	2.1	**Attack on back-end server stops it functioning**, for example it prevents it from interacting with vehicles and providing services they rely on
	3	Vehicle related data held on back-end servers being lost or compromised ("data breach")	3.1	Abuse of privileges by staff (**insider attack)**
			3.2	**Loss of information in the cloud**. Sensitive data may be lost due to attacks or accidents when data is stored by third-party cloud service providers
			3.3	**Unauthorized internet access to the server** (enabled for example by backdoors, unpatched system software vulnerabilities, SQL attacks or other means)
			3.4	**Unauthorized physical access to the server** (conducted for example by USB sticks or other media connecting to the server)
			3.5	**Information breach** by unintended sharing of data (e.g. admin errors)
4.3.2 Threats to vehicles regarding their communication channels	4	Spoofing of messages or data received by the vehicle	4.1	**Spoofing of messages** by impersonation (e.g. 802.11p V2X during platooning, GNSS messages, etc.)
			4.2	**Sybil attack** (in order to spoof other vehicles as if there are many vehicles on the road)
	5	Communication channels used to conduct unauthorized manipulation, deletion or other amendments to vehicle held code/data	5.1	Communications channels permit **code injection**, for example tampered software binary might be injected into the communication stream
			5.2	Communications channels permit **manipulate** of vehicle held data/code
			5.3	Communications channels permit **overwrite** of vehicle held data/code
			5.4	Communications channels permit **erasure** of vehicle held data/code
			5.5	Communications channels permit introduction of data/code to the vehicle (write data code)
	6	Communication channels permit untrusted/unreliable messages to be accepted or are	6.1	Accepting information from an **unreliable or untrusted source**
			6.2	**Man in the middle** attack/ session hijacking

High level and sub-level descriptions of vulnerability/ threat			*Example of vulnerability or attack method*	
		vulnerable to session hijacking/replay attacks	6.3	**Replay attack**, for example an attack against a communication gateway allows the attacker to downgrade software of an ECU or firmware of the gateway
	7	Information can be readily disclosed. For example, through eavesdropping on communications or through allowing unauthorized access to sensitive files or folders	7.1	**Interception of information** / interfering radiations / monitoring communications
			7.2	Gaining **unauthorized access** to files or data
	8	Denial of service attacks via communication channels to disrupt vehicle functions	8.1	**Sending** a large number of garbage **data** to vehicle information system, **so that it is unable to provide services** in the normal manner
			8.2	**Black hole attack**, in order to disrupt communication between vehicles the attacker is able to block messages between the vehicles
	9	An unprivileged user is able to gain privileged access to vehicle systems	9.1	An unprivileged user is able to **gain privileged access**, for example root access
	10	Viruses embedded in communication media are able to infect vehicle systems	10.1	**Virus** embedded in communication media infects vehicle systems
	11	Messages received by the vehicle (for example X2V or diagnostic messages), or transmitted within it, contain malicious content	11.1	Malicious **internal** (e.g. CAN) **messages**
			11.2	Malicious **V2X messages,** e.g. infrastructure to vehicle or vehicle-vehicle messages (e.g. CAM, DENM)
			11.3	Malicious diagnostic messages
			11.4	Malicious **proprietary messages** (e.g. those normally sent from OEM or component/system/function supplier)
4.3.3. Threats to vehicles regarding their update procedures	12	Misuse or compromise of update procedures	12.1	Compromise of **over the air software update procedures**. This includes fabricating the system update program or firmware
			12.2	Compromise of **local/physical software update procedures**. This includes fabricating the system update program or firmware
			12.3	The **software** is **manipulated before the update process** (and is therefore corrupted), although the update process is intact
			12.4	**Compromise** of cryptographic keys of the software provider **to allow invalid update**
	13	It is possible to deny legitimate updates	13.1	Denial of Service attack against update server or network to **prevent rollout of critical software updates** and/or unlock of customer specific features
4.3.4 Threats to vehicles regarding unintended human actions facilitating a cyber attack	15	Legitimate actors are able to take actions that would unwittingly facilitate a cyber-attack	15.1	Innocent victim (e.g. owner, operator or maintenance engineer) being **tricked into taking an action** to unintentionally load malware or enable an attack
			15.2	**Defined security procedures** are not followed

High level and sub-level descriptions of vulnerability/ threat			*Example of vulnerability or attack method*	
4.3.5 Threats to vehicles regarding their external connectivity and connections	16	Manipulation of the connectivity of vehicle functions enables a cyber-attack, this can include telematics; systems that permit remote operations; and systems using short range wireless communications	16.1	Manipulation of **functions designed to remotely operate systems**, such as remote key, immobilizer, and charging pile
			16.2	**Manipulation of vehicle telematics** (e.g. manipulate temperature measurement of sensitive goods, remotely unlock cargo doors)
			16.3	Interference with **short range wireless systems** or sensors
	17	Hosted 3rd party software, e.g. entertainment applications, used as a means to attack vehicle systems	17.1	**Corrupted applications**, or those with poor software security, used as a method to attack vehicle systems
	18	Devices connected to external interfaces e.g. USB ports, OBD port, used as a means to attack vehicle systems	18.1	**External interfaces** such as USB or other ports used as a point of attack, for example through code injection
			18.2	Media infected with a **virus** connected to a vehicle system
			18.3	**Diagnostic access (e.g. dongles in OBD port)** used to facilitate an attack, e.g. manipulate vehicle parameters (directly or indirectly)
4.3.6 Threats to vehicle data/code	19	Extraction of vehicle data/code	19.1	Extraction of copyright or proprietary software from vehicle systems (product **piracy**)
			19.2	Unauthorized access to the **owner's privacy information** such as personal identity, payment account information, address book information, location information, vehicle's electronic ID, etc.
			19.3	Extraction of cryptographic keys
	20	Manipulation of vehicle data/code	20.1	Illegal/unauthorized changes to **vehicle's electronic ID**
			20.2	**Identity fraud.** For example, if a user wants to display another identity when communicating with toll systems, manufacturer backend
			20.3	Action to **circumvent monitoring systems** (e.g. hacking/ tampering/ blocking of messages such as ODR Tracker data, or number of runs)
			20.4	Data manipulation to **falsify vehicle's driving data** (e.g. mileage, driving speed, driving directions, etc.)
			20.5	Unauthorized changes to **system diagnostic data**
	21	Erasure of data/code	21.1	Unauthorized deletion/manipulation of **system event logs**
	22	Introduction of malware	22.2	Introduce **malicious software** or malicious software activity
	23	Introduction of new software or overwrite existing software	23.1	**Fabrication of software** of the vehicle control system or information system

High level and sub-level descriptions of vulnerability/ threat			*Example of vulnerability or attack method*	
	24	Disruption of systems or operations	24.1	**Denial of service**, for example this may be triggered on the internal network by flooding a CAN bus, or by provoking faults on an ECU via a high rate of messaging
	25	Manipulation of vehicle parameters	25.1	Unauthorized access of **falsify the configuration parameters** of vehicle's key functions, such as brake data, airbag deployed threshold, etc.
			25.2	Unauthorized access of **falsify the charging parameters**, such as charging voltage, charging power, battery temperature, etc.
4.3.7 Potential vulnerabilities that could be exploited if not sufficiently protected or hardened	26	Cryptographic technologies can be compromised or are insufficiently applied	26.1	Combination of short **encryption keys** and long period of validity enables attacker to break encryption
			26.2	Insufficient use of cryptographic algorithms to protect sensitive systems
			26.3	Using already or soon to be deprecated **cryptographic algorithms**
	27	Parts or supplies could be compromised to permit vehicles to be attacked	27.1	**Hardware or software, engineered to enable an attack** or fails to meet design criteria to stop an attack
	28	Software or hardware development permits vulnerabilities	28.1	**Software bugs**. The presence of software bugs can be a basis for potential exploitable vulnerabilities. This is particularly true if software has not been tested to verify that known bad code/bugs is not present and reduce the risk of unknown bad code/bugs being present
			28.2	**Using remainders** from development (e.g. debug ports, JTAG ports, microprocessors, development certificates, developer passwords, …) can permit access to ECUs or permit attackers to gain higher privileges
	29	Network design introduces vulnerabilities	29.1	**Superfluous internet ports left open**, providing access to network systems
			29.2	Circumvent **network separation** to gain control. Specific example is the use of unprotected gateways, or access points (such as truck-trailer gateways), to circumvent protections and gain access to other network segments to perform malicious acts, such as sending arbitrary CAN bus messages
	31	Unintended transfer of data can occur	31.1	Information breach. Personal data may be leaked when the **car changes user** (e.g. is sold or is used as hire vehicle with new hirers)
	32	Physical manipulation of systems can enable an attack	32.1	**Manipulation of electronic hardware**, e.g. unauthorized electronic hardware added to a vehicle to enable "man-in-the-middle" attack **Replacement of authorized electronic hardware** (e.g., sensors) with unauthorized electronic hardware **Manipulation of the information** collected by a sensor (for example, using a magnet to tamper with the Hall effect sensor connected to the gearbox)

Part B. Mitigations to the threats intended for vehicles

1. Mitigations for "Vehicle communication channels"

Mitigations to the threats which are related to "Vehicle communication channels" are listed in Table B1.

Table B1
Mitigation to the threats which are related to "Vehicle communication channels"

Table A1 reference	*Threats to "Vehicle communication channels"*	*Ref*	*Mitigation*
4.1	Spoofing of messages (e.g. 802.11p V2X during platooning, GNSS messages, etc.) by impersonation	M10	The vehicle shall verify the authenticity and integrity of messages it receives
4.2	Sybil attack (in order to spoof other vehicles as if there are many vehicles on the road)	M11	Security controls shall be implemented for storing cryptographic keys (e.g., use of Hardware Security Modules)
5.1	Communication channels permit code injection into vehicle held data/code, for example tampered software binary might be injected into the communication stream	M10 M6	The vehicle shall verify the authenticity and integrity of messages it receives Systems shall implement security by design to minimize risks
5.2	Communication channels permit manipulation of vehicle held data/code	M7	Access control techniques and designs shall be applied to protect system data/code
5.3	Communication channels permit overwrite of vehicle held data/code		
5.4 21.1	Communication channels permit erasure of vehicle held data/code		
5.5	Communication channels permit introduction of data/code to vehicle systems (write data code)		
6.1	Accepting information from an unreliable or untrusted source	M10	The vehicle shall verify the authenticity and integrity of messages it receives
6.2	Man in the middle attack / session hijacking	M10	The vehicle shall verify the authenticity and integrity of messages it receives
6.3	Replay attack, for example an attack against a communication gateway allows the attacker to downgrade software of an ECU or firmware of the gateway		
7.1	Interception of information / interfering radiations / monitoring communications	M12	Confidential data transmitted to or from the vehicle shall be protected
7.2	Gaining unauthorized access to files or data	M8	Through system design and access control it should not be possible for unauthorized personnel to access personal or system critical data. Example of Security Controls can be found in OWASP
8.1	Sending a large number of garbage data to vehicle information system, so that it is unable to provide services in the normal manner	M13	Measures to detect and recover from a denial of service attack shall be employed

Table A1 reference	*Threats to "Vehicle communication channels"*	*Ref*	*Mitigation*
8.2	Black hole attack, disruption of communication between vehicles by blocking the transfer of messages to other vehicles	M13	Measures to detect and recover from a denial of service attack shall be employed
9.1	An unprivileged user is able to gain privileged access, for example root access	M9	Measures to prevent and detect unauthorized access shall be employed
10.1	Virus embedded in communication media infects vehicle systems	M14	Measures to protect systems against embedded viruses/malware should be considered
11.1	Malicious internal (e.g. CAN) messages	M15	Measures to detect malicious internal messages or activity should be considered
11.2	Malicious V2X messages, e.g. infrastructure to vehicle or vehicle-vehicle messages (e.g. CAM, DENM)	M10	The vehicle shall verify the authenticity and integrity of messages it receives
11.3	Malicious diagnostic messages		
11.4	Malicious proprietary messages (e.g. those normally sent from OEM or component/system/function supplier)		

2. Mitigations for "Update process"

Mitigations to the threats which are related to "Update process" are listed in Table B2.

Table B2
Mitigations to the threats which are related to "Update process"

Table A1 reference	*Threats to "Update process"*	*Ref*	*Mitigation*
12.1	Compromise of over the air software update procedures. This includes fabricating the system update program or firmware	M16	Secure software update procedures shall be employed
12.2	Compromise of local/physical software update procedures. This includes fabricating the system update program or firmware		
12.3	The software is manipulated before the update process (and is therefore corrupted), although the update process is intact		
12.4	Compromise of cryptographic keys of the software provider to allow invalid update	M11	Security controls shall be implemented for storing cryptographic keys
13.1	Denial of Service attack against update server or network to prevent rollout of critical software updates and/or unlock of customer specific features	M3	Security Controls shall be applied to back-end systems. Where back-end servers are critical to the provision of services there are recovery measures in case of system outage. Example Security Controls can be found in OWASP

3. Mitigations for "Unintended human actions facilitating a cyber attack"

Mitigations to the threats which are related to "Unintended human actions facilitating a cyber attack" are listed in Table B3.

Table B3
Mitigations to the threats which are related to "Unintended human actions facilitating a cyber attack"

Table A1 reference	*Threats relating to "Unintended human actions"*	*Ref*	*Mitigation*
15.1	Innocent victim (e.g. owner, operator or maintenance engineer) is tricked into taking an action to unintentionally load malware or enable an attack	M18	Measures shall be implemented for defining and controlling user roles and access privileges, based on the principle of least access privilege
15.2	Defined security procedures are not followed	M19	Organizations shall ensure security procedures are defined and followed including logging of actions and access related to the management of the security functions

4. Mitigations for "External connectivity and connections"

Mitigations to the threats which are related to "external connectivity and connections" are listed in Table B4.

Table B4
Mitigation to the threats which are related to "external connectivity and connections"

Table A1 reference	*Threats to "External connectivity and connections"*	*Ref*	*Mitigation*
16.1	Manipulation of functions designed to remotely operate vehicle systems, such as remote key, immobiliser, and charging pile	M20	Security controls shall be applied to systems that have remote access
16.2	Manipulation of vehicle telematics (e.g. manipulate temperature measurement of sensitive goods, remotely unlock cargo doors)		
16.3	Interference with short range wireless systems or sensors		
17.1	Corrupted applications, or those with poor software security, used as a method to attack vehicle systems	M21	Software shall be security assessed, authenticated and integrity protected. Security controls shall be applied to minimise the risk from third party software that is intended or foreseeable to be hosted on the vehicle
18.1	External interfaces such as USB or other ports used as a point of attack, for example through code injection	M22	Security controls shall be applied to external interfaces
18.2	Media infected with viruses connected to the vehicle		
18.3	Diagnostic access (e.g. dongles in OBD port) used to facilitate an attack, e.g. manipulate vehicle parameters (directly or indirectly)	M22	Security controls shall be applied to external interfaces

5. Mitigations for "Potential targets of, or motivations for, an attack "

Mitigations to the threats which are related to "Potential targets of, or motivations for, an attack " are listed in Table B5.

Table B5
Mitigations to the threats which are related to "Potential targets of, or motivations for, an attack"

Table A1 reference	*Threats to "Potential targets of, or motivations for, an attack"*	*Ref*	*Mitigation*
19.1	Extraction of copyright or proprietary software from vehicle systems (product piracy / stolen software)	M7	Access control techniques and designs shall be applied to protect system data/code. Example Security Controls can be found in OWASP
19.2	Unauthorized access to the owner's privacy information such as personal identity, payment account information, address book information, location information, vehicle's electronic ID, etc.	M8	Through system design and access control it should not be possible for unauthorized personnel to access personal or system critical data. Examples of Security Controls can be found in OWASP
19.3	Extraction of cryptographic keys	M11	Security controls shall be implemented for storing cryptographic keys e.g. Security Modules
20.1	Illegal/unauthorised changes to vehicle's electronic ID	M7	Access control techniques and designs shall be applied to protect system data/code. Example Security Controls can be found in OWASP
20.2	Identity fraud. For example, if a user wants to display another identity when communicating with toll systems, manufacturer backend		
20.3	Action to circumvent monitoring systems (e.g. hacking/ tampering/ blocking of messages such as ODR Tracker data, or number of runs)	M7	Access control techniques and designs shall be applied to protect system data/code. Example Security Controls can be found in OWASP. Data manipulation attacks on sensors or transmitted data could be mitigated by correlating the data from different sources of information
20.4	Data manipulation to falsify vehicle's driving data (e.g. mileage, driving speed, driving directions, etc.)		
20.5	Unauthorised changes to system diagnostic data		
21.1	Unauthorized deletion/manipulation of system event logs	M7	Access control techniques and designs shall be applied to protect system data/code. Example Security Controls can be found in OWASP.
22.2	Introduce malicious software or malicious software activity	M7	Access control techniques and designs shall be applied to protect system data/code. Example Security Controls can be found in OWASP.
23.1	Fabrication of software of the vehicle control system or information system		
24.1	Denial of service, for example this may be triggered on the internal network by flooding a CAN bus, or by provoking faults on an ECU via a high rate of messaging	M13	Measures to detect and recover from a denial of service attack shall be employed
25.1	Unauthorized access to falsify configuration parameters of vehicle's key functions, such as brake data, airbag deployed threshold, etc.	M7	Access control techniques and designs shall be applied to protect system data/code. Example Security Controls can be found in OWASP
25.2	Unauthorized access to falsify charging parameters, such as charging voltage, charging power, battery temperature, etc.		

6. Mitigations for "Potential vulnerabilities that could be exploited if not sufficiently protected or hardened"

Mitigations to the threats which are related to "Potential vulnerabilities that could be exploited if not sufficiently protected or hardened" are listed in Table B6.

Table B6
Mitigations to the threats which are related to "Potential vulnerabilities that could be exploited if not sufficiently protected or hardened"

Table A1 reference	*Threats to "Potential vulnerabilities that could be exploited if not sufficiently protected or hardened"*	*Ref*	*Mitigation*
26.1	Combination of short encryption keys and long period of validity enables attacker to break encryption	M23	Cybersecurity best practices for software and hardware development shall be followed
26.2	Insufficient use of cryptographic algorithms to protect sensitive systems		
26.3	Using deprecated cryptographic algorithms		
27.1	Hardware or software, engineered to enable an attack or fail to meet design criteria to stop an attack	M23	Cybersecurity best practices for software and hardware development shall be followed
28.1	The presence of software bugs can be a basis for potential exploitable vulnerabilities. This is particularly true if software has not been tested to verify that known bad code/bugs is not present and reduce the risk of unknown bad code/bugs being present	M23	Cybersecurity best practices for software and hardware development shall be followed. Cybersecurity testing with adequate coverage
28.2	Using remainders from development (e.g. debug ports, JTAG ports, microprocessors, development certificates, developer passwords, …) can permit an attacker to access ECUs or gain higher privileges		
29.1	Superfluous internet ports left open, providing access to network systems		
29.2	Circumvent network separation to gain control. Specific example is the use of unprotected gateways, or access points (such as truck-trailer gateways), to circumvent protections and gain access to other network segments to perform malicious acts, such as sending arbitrary CAN bus messages	M23	Cybersecurity best practices for software and hardware development shall be followed. Cybersecurity best practices for system design and system integration shall be followed

7. Mitigations for "Data loss / data breach from vehicle"

Mitigations to the threats which are related to "Data loss / data breach from vehicle" are listed in Table B7.

Table B7
Mitigations to the threats which are related to "Data loss / data breach from vehicle"

Table A1 reference	*Threats of "Data loss / data breach from vehicle"*	*Ref*	*Mitigation*
31.1	Information breach. Personal data may be breached when the car changes user (e.g. is sold or is used as hire vehicle with new hirers)	M24	Best practices for the protection of data integrity and confidentiality shall be followed for storing personal data.

8. Mitigations for "Physical manipulation of systems to enable an attack"

Mitigation to the threats which are related to "Physical manipulation of systems to enable an attack" are listed in Table B8.

Table B8
Mitigations to the threats which are related to "Physical manipulation of systems to enable an attack"

Table A1 reference	*Threats to "Physical manipulation of systems to enable an attack"*	*Ref*	*Mitigation*
32.1	Manipulation of OEM hardware, e.g. unauthorised hardware added to a vehicle to enable "man-in-the-middle" attack	M9	Measures to prevent and detect unauthorized access shall be employed

Part C. Mitigations to the threats outside of vehicles

1. Mitigations for "Back-end servers"

Mitigations to the threats which are related to "Back-end servers" are listed in Table C1.

Table C1
Mitigations to the threats which are related to "Back-end servers"

Table A1 reference	*Threats to "Back-end servers"*	*Ref*	*Mitigation*
1.1 & 3.1	Abuse of privileges by staff (insider attack)	M1	Security Controls are applied to back-end systems to minimise the risk of insider attack
1.2 & 3.3	Unauthorised internet access to the server (enabled for example by backdoors, unpatched system software vulnerabilities, SQL attacks or other means)	M2	Security Controls are applied to back-end systems to minimise unauthorised access. Example Security Controls can be found in OWASP
1.3 & 3.4	Unauthorised physical access to the server (conducted by for example USB sticks or other media connecting to the server)	M8	Through system design and access control it should not be possible for unauthorised personnel to access personal or system critical data
2.1	Attack on back-end server stops it functioning, for example it prevents it from interacting with vehicles and providing services they rely on	M3	Security Controls are applied to back-end systems. Where back-end servers are critical to the provision of services there are recovery measures in case of system outage. Example Security Controls can be found in OWASP
3.2	Loss of information in the cloud. Sensitive data may be lost due to attacks or accidents when data is stored by third-party cloud service providers	M4	Security Controls are applied to minimise risks associated with cloud computing. Example Security Controls can be found in OWASP and NCSC cloud computing guidance
3.5	Information breach by unintended sharing of data (e.g. admin errors, storing data in servers in garages)	M5	Security Controls are applied to back-end systems to prevent data breaches. Example Security Controls can be found in OWASP

2. Mitigations for "Unintended human actions"
Mitigations to the threats which are related to "Unintended human actions" are listed in Table C2.

Table C2
Mitigations to the threats which are related to "Unintended human actions"

Table A1 reference	*Threats relating to "Unintended human actions"*	*Ref*	*Mitigation*
15.1	Innocent victim (e.g. owner, operator or maintenance engineer) is tricked into taking an action to unintentionally load malware or enable an attack	M18	Measures shall be implemented for defining and controlling user roles and access privileges, based on the principle of least access privilege
15.2	Defined security procedures are not followed	M19	Organizations shall ensure security procedures are defined and followed including logging of actions and access related to the management of the security functions

3. Mitigations for "Physical loss of data"
Mitigations to the threats which are related to "Physical loss of data" are listed in Table C3.

Table C3
Mitigations to the threats which are related to "Physical loss of data loss"

Table A1 reference	*Threats of "Physical loss of data"*	*Ref*	*Mitigation*
30.1	Damage caused by a third party. Sensitive data may be lost or compromised due to physical damages in cases of traffic accident or theft	M24	Best practices for the protection of data integrity and confidentiality shall be followed for storing personal data. Example Security Controls can be found in ISO/SC27/WG5
30.2	Loss from DRM (digital right management) conflicts. User data may be deleted due to DRM issues		
30.3	The (integrity of) sensitive data may be lost due to IT components wear and tear, causing potential cascading issues (in case of key alteration, for example)		