Vulnerability Assessment

Vulnerability Risk Value
This metric is based on the 'Risk Value' in accordance with ISO/SAE 21434 [-]. Accordingly, the value assigned to the 'Risk Value' is determined from the risk assessment defined in the company (e.g.: 'Risk Matrix'). This risk assessment takes into account the 'impact' and 'feasibility' assessments in a certain weighting. Impact and feasibility assessments are also defined in ISO/SAE 21434. If, in the context of a TARA, 'Risk Values' have already been defined in the product development phase for the 'Threat Scenario' that is now to be evaluated in real terms on the basis of the vulnerability, these values can be adopted here (the same applies to 'impact' or 'feasibility' evaluation). According to ISO/SAE 21434, a 'Risk Value' is determined for each SFOP impact category (Safety, Financial, Operational, Privacy) of a Threat Scenario. The relevant impact categories for this metric are Safety and Operational. If multiple threat scenarios (with associated attack paths) can be derived from the vulnerability to be assessed, then the threat scenario that has the highest risk value for the safety impact category is relevant. If this value is assigned to multiple threat scenarios, then the threat scenario that also has the highest risk value for the Operational impact category is relevant. The 'Risk Value' reflects the company-specific ('environmental') consideration of the impact. The 'Risk Value' should therefore not be equated with the CVSS Severity Base Score that is usually found in CVE and/or NVD entries.

Value	
Medium	Risk Value for Impact category 'Safety' is 1 and Risk Value for Impact category 'Operational' is smaller than 3
High	Risk Value for Impact category 'Safety' is higher than 1 and Risk Value for Impact category 'Operational' is higher than 2
Very High	Risk Value for Impact category 'Safety' higher than 2 and Risk Value for Impact category 'Operational' is higher than 3

Scope
This metric is adapted from the Common Vulnerability Scoring System v.3.1 (CVSS v3.1) The Scope metric captures whether a vulnerability in one vulnerable component impacts resources in components beyond its security scope. If a vulnerability in a vulnerable component can affect a component which is in a different security scope than the vulnerable component, a Scope change occurs. Intuitively, whenever the impact of a vulnerability breaches a security/trust boundary and impacts components outside the security scope in which vulnerable component resides, a Scope change occurs. Formally, a security authority is a mechanism (e.g., ECU, HSM, CGW) that defines and enforces access control in terms of how certain subjects/actors (e.g., drivers, processes) can access certain restricted objects/resources (e.g., data, car interior, functions) in a controlled manner. All the subjects and objects under the jurisdiction of a single security authority are considered to be under one security scope. The security scope of a component encompasses other components that provide functionality solely to that component, even if these other components have their own security authority. The Time Criticaliy Factor (TCF) is greater when a scope change occurs and the Grace Period Factor (GP´) is smaler accordingly. *A risk assessment within the scope of a TARA according to ISO/SAE 21434 does not consider the scope change criteria.* Examples: DoS attack on single component which then affects availability of the whole car leads to a changed scope. A vulnerability in ECU A leads to an attacker obtaining information that can be used to break the cryptography of ECU B. Since each ECU is a single security authority, a scope change occurs.

Value	
Changed	An exploited vulnerability can affect resources beyond the security scope managed by the security authority of the vulnerable component. In this case, the vulnerable component and the impacted component are different and managed by different security authorities.

Unchanged	An exploited vulnerability can only affect resources managed by the same security authority. In this case, the vulnerable component and the impacted component are either the same, or both are managed by the same security authority.

Incident Analysis

Exploit Code Maturity

This metric is adapted from the Common Vulnerability Scoring System v.3.1 (CVSS v3.1)
It measures the likelihood of the vulnerability being attacked, and is typically based on the current state of exploit techniques, exploit code availability, or active, “in-the-wild” exploitation. Public availability of easy-to-use exploit code increases the number of potential attackers by including those who are unskilled, thereby increasing the severity of the vulnerability. Initially, real-world exploitation may only be theoretical. Publication of proof-of-concept code, functional exploit code, or sufficient technical details necessary to exploit the vulnerability may follow. Furthermore, the exploit code available may progress from a proof-of-concept demonstration to exploit code that is successful in exploiting the vulnerability consistently. In severe cases, it may be delivered as the payload of a network-based worm or virus or other automated attack tools.
Since the maturity of an available exploit can affect attack complexity, privileges required, user interaction, as well as many other aspects, this metric bears much resemblance to exploitability assessment.
Further dependencies arise with the assessment of Attack Feasibility in the context of determining the Vulnerability Risk Value according to ISO/SAE 21434. The following further assessment criteria used for the assessment of Attack Feasibility in ISO/SAE 21434 may have overlaps with this metric (Furthermore, dependencies may also occur within these criterion):

- Elapsed Time
- Expertise
- Knowledge of system
- Equipment

The threat posed by the vulnerability to be assessed is considered over time. The 'risk value' that is taken from the documentation from the development phase (e.g. TARA) for the vulnerability assessment does not fully take into account the maturity of an actual real-world exploit at (or after) the time of the initial assessment of a real vulnerability.
Even if 0-days have to be evaluated differently compared to already publicly known vulnerabilities, it is true for both that the evaluation may differ from the one at the time of TARA.
The more easily a vulnerability can be exploited, the higher the score.

Value	
Not defined	Assigning this value indicates that there is not enough information to select one of the other values or the vulnerability is one that is completely unknown to the public ("0-day"). I.e., it has the same impact on the rating as assigning High.
High	Functional autonomously executable exploit/exploit kit exists (weaponized exploit) or no exploit is required (manual trigger) and details are widely available (e.g. black market, social media). Exploit code works in any situation or is actively provided. Systems connected to the vehicle component or network, reponsibly are likely to experience scanning or exploit attempts. Exploit development has reached the level of reliable, widely available and user-friendly automated tools (exploit packages).
Functional	Functional exploit code is available. The code works in most situations where the vulnerability is present.
Proof-of-Concept	Proof-of-concept exploit code is available, or an attack demonstration is not practical for most systems. Exploit code is actively provided (e.g., public exploit databases). The code or technique is not functional in all situations and may require significant modification by an experienced attacker.
Unproven	No exploit code is available, or an exploit is theoretical.

Remediation Level

The Remediation Level of a vulnerability is adapted from the Common Vulnerability Scoring System v.3.1 (CVSS v3.1). It assesses the reduction of the threat posed by the vulnerability to be assessed over time and is an important factor for vulnerability prioritization. Unlike in the IT area, the typical vulnerability in the autotive area is usually already patched when it becomes publicly known. Nevertheless, the remediation level influences the time criticaliy for measures like workarounds, hotfixes or final patches for the vulnerability to be assessed and for vulnerabilities related with it, since it reflects a decreasing urgency as remediation becomes final.
When a possible attack scenario is reported by a white hat, this report can contain several related vulnerabilities (attack vector). Since each vulnerability is assessed individually, these vulnerabilities can be assessed and thus prioritized differently. Mitigation or remediation can then simultaneously lead to mitigation or remediation of another related vulnerability. This metric captures such effects that lead to changes in exploitability over time. It must therefore be applied to the entirety of all threat scenarios (or attack paths) that include the vulnerability being assessed. If multiple threat scenarios (with associated attack paths) can be derived from the vulnerability to be assessed, then the effect of a measure on only the threat scenario that has the highest 'Risk Value' is relevant. Therefore, if an existing measure has no effect the threat scenario that has the highest 'Risk Value', then this measure is considered as 'Unavailable'.

The Time Criticaliy Factor (TCF) is greater as temporary and tentative a measure is and the Grace Period Factor (GP) is smaler accordingly. If no measure is in place this metric has no effect on the Grace Period Factor.

Value	
Not defined	Assigning this value indicates that there is not enough information to select one of the other values or the vulnerability is one that is completely unknown to the public ("0-day"). I.e. it has the same impact on the rating as assigning Unavailable.
Unavailable	Either there is no solution, or it is not applicable. Assigning this value does not lead to any changes in the assessment of attack feasibility/exploitability and thus the 'Risk Value'.
Workaround	There is an unofficial, vendor-neutral solution. In some cases, users of the affected technology create their own patch or provide steps to work around or otherwise mitigate the vulnerability.
Temporary Fix	There is an official, but temporary solution. This includes cases where the vendor issues a temporary hotfix, tool, or workaround.
Official Fix	A complete vendor solution is available. Either the vendor has released an official patch or an upgrade is available.

Report Confidence

This metric is adapted from the Common Vulnerability Scoring System v.3.1 (CVSS v3.1).
This metric measures the degree of confidence in the existence of the vulnerability and the credibility of the known technical details. Sometimes only the existence of vulnerabilities is published, but without specific details. For example, an impact may be identified as undesirable, but the root cause may not be known. The vulnerability may later be confirmed by research that suggests where the vulnerability may lie, although the research may not be certain. Finally, a vulnerability may be confirmed by confirmation from the author or vendor of the affected technology. Thus, the urgency of a vulnerability may vary over time as new discoveries lead to the assumption of a vulnerability's existence with altered certainty. This metric also indicates the level of technical knowledge and equipment available to potential attackers. Thus, overlaps may exist with the following criteria for determining the 'Risk Value' according to ISO/SAE 21434:

- Expertise
- Equipment

The more a vulnerability is validated by reputable sources, the higher the score.

Value	
Not defined	Assigning this value indicates that there is not enough information to select one of the other values and has no effect on the overall temporal score, i.e., it has the same effect on the score as assigning 'Confirmed'.
Confirmed	Detailed reports exist, or functional replication is possible (functional exploits can provide this). Source code is available to independently verify the research claims, or the author or vendor of the affected code has confirmed the presence of the vulnerability.
Reasonable	Important details are published, but there is a lack of either full confidence in the cause or access to the source code to fully confirm all interactions that may lead to the outcome. However, there is reasonable confidence that the bug is reproducible and at least one impact can be verified (proof-of-concept exploits can provide this). An example is a detailed description of the research on a vulnerability with an explanation (possibly obfuscated) that provides assurances about how the results will be reproduced.
Unknown	There are impact reports that indicate that a vulnerability exists. The reports indicate that the cause of the vulnerability is unknown, or the reports may differ on the cause or impact of the vulnerability. Reporters are unsure of the true nature of the vulnerability, and there is little confidence in the validity of the reports.

Exploit Code Dissemination

This metric measures the availability of exploit code that exploits the vulnerabilityto be assessed. The maturity of the exploit does not need to be evaluated (since this aspect is already evaluated by the metric 'Exploit Code Maturity'). Scoring is based on statistical significance from studies of historical data on vulnerabilities in the traditional IT environment and is driven by the following evidence-based assumptions:
- Considering the existence of exploit code for a given vulnerability in publicly accessible databases as a risk factor for actual exploitation in the wild can increase prediction rate up to 45 % better than only considering the CVSS Score.
- Considering the existence of exploit code for a given vulnerability on black market as a risk factor for actual exploitation in the wild can increase prediction rate up to 80 % better than only considering the CVSS Score.

As of 2021, only 232 CVE IDs existed for native automotive vulnerabilities. It must therefore be critically questioned to what extent historical data on vulnerabilities in public databases such as NVD, ExploitDB, etc. are suitable for making valid statements about the life cycle of automotive vulnerabilities.
Due to various control and monitoring services for the vehicle which require access by OEM backend servers (e.g., TCU), IT infrastructure is mixed with the pure vehicle system. This is also reflected in the potential threat posed by vulnerabilities. There are numerous attack vectors with an impact in the vehicle, but which exploit a vulnerable component in the IT infrastructure. When IT infrastructure is compromised, this can therefore pose a threat to data, but also to drivers and passengers. Almost 53% of vulnerabilities used in automotive exploits in 2021 are IT related (mobile apps, backend server).

The lower the prediction rate given by a risk factor, the lower the statistical exploitation probability on average. Thus, the time criticality factor (TCF) decreases. If there are no findings or if the prediction rate is as high as possible (external - black market), this metric has no (weakening) effect on TCF.

Value	
External - not public	Information was found (and reported) by external actors (e.g., researchers) and Exploit Code Maturity is known only to them. Neither vulnerability information, nor an exploit involving the vulnerability has been disclosed yet.
External - PoC	Vulnerability information is already disclosed and an corresponding exploit is already known to the broad public as a Proof-of-Concept (e.g., ExploitDB).
External - Black market	Vulnerability information is already disclosed but an corresponding exploit is not yet known to the broad public and is traded on the black market (e.g., RuMarket). The exploit is part of an exploit kit and/or readily applicable (weaponized). Since there are usually no countermeasures in place yet, there is an increased likelihood of exploitation.
Unclear	Assigning this value indicates there is insufficient information to choose one of the other values. It has no impact on the overall score, i.e., it has the same effect on scoring TCF as assigning 'External - Black market exploit'.

Incident Scale

The evaluation of the scalability of damage is not fundamentally considered in the 'Risk Value' according to ISO/SAE 21434. This metric therefore does not represent an overlap. If the scalability of damage has already been taken into account in the development phase for a specific company, this assessment should nevertheless be reviewed and, if necessary, adjusted, since the assessment can change over time (e.g., if the expected delivery rate of the impacted/vulnerable component deviates significantly from the actual delivery rate).
The 'Incident Scale' does not necessarily reflect only the company-specific ('Environmental') view. The environment in which components could be exposed to a threat due to the given vulnerability must initially be defined. The environment under consideration is not necessarily only the environment of one or more companies, but potentially the entire world due to the highly instationary character and the connectivity of vehicles.
If a specification of the exact number of impacted/vulnerable components operated in the environment to be defined cannot be made with certainty, the maximum number to be assumed should be used. This can be the case, for example, if precise assembly documentation (e.g. via VIN) is available, but an exact assessment is not possible due to incomplete tracking of the software status of the impacted/vulnerable component. In this case, all components would have to be treated as if they had the impacted/vulnerable software version.
It should be noted that this metric does not evaluate possible significant scaling effects resulting from the vulnerability potentially enabling, for example, physical or functional bypass of an attacker to adjacent components/items/domains/functions along an attack path. Such effects are accounted for using the 'scope' metric. For example, this may refer to a vulnerability within a TCU that is located right at the interface to the backend server and could potentially allow the attacker to scale the attack to the backend.

Value	
Low	The total of all vehicles (potentially) affected by the vulnerability represents up to 1% of the manufacturer's total registered fleet.
Medium	The total of all vehicles (potentially) affected by the vulnerability represents between 1% and 5% of the manufacturer's total registered fleet.
High	The total of all vehicles (potentially) affected by the vulnerability represents more than 5% of the manufacturer's total registered fleet.
Unclear	Sometimes it could be difficult or impossible to assess the total of all vehicles (of different brands) which are potentially equipped with a vulnerabe or impacted component (e.g. for OEM). Assigning this value indicates there is insufficient information to choose one of the other values. It has no impact on the overall score.

Process Complexity

Supply chain scale

Multi-stakeholder processes for disclosing and remediating a vulnerability exhibit rising complexity as the number of vendors involved increases. Software from one supplier can be unique in each system implementation of the different customers, even if it maps the same function. A vulnerability can potentially affect multiple vendors in different ways. The assessment of risk and thus vulnerability prioritization may vary from vendor to vendor. Increased intra- as well as inter-cooperal communication needs, as well as increased potential for conflict, can delay the process. (It must be remembered that, in case of doubt, the process can only be as efficient as its weakest link). While the following factors have a significant impact on process duration, they are not considered for this metric because they are the responsibility of the manufacturer:

- Inadequate quality or quantity of human resources.
- Insufficient processes

This metric does not take into account whether pre-existing measures exist between participating vendors as part of contractual agreements or requirements documentation in the event that vulnerabilities occur in the field (e.g., within an Incident Response Plan or based on CAL-dependent requirements). These factors can greatly facilitate and specify the estimation of process criticality (PCF), but are not always present. Therefore, they are recorded separately.

The impact of the metric on process criticality (PCF) increases linearly with the number of stakeholders. The real given complexity is thus approximately modeled by assuming a only bilateral communication for both, intra- and inter-cooperal interactions. Each intra- and inter-interaction is assumed to have the same mean duration.

Value	
Low	The number of vendors involved in the disclosure process as well as patch development is 1
Medium	The number of vendors involved in the disclosure process as well as patch development is 2
High	The number of vendors involved in the disclosure process as well as patch development is 3
Very High	The number of vendors involved in the disclosure process as well as patch development is 4 or higher

Remediation Dissemination

This metric evaluates the appropriate grace period with respect to the impact of the responsible vendor's organizational-strategical patch or update management. Technical considerations that affect patch development or verification are specifically excluded from this metric. Such aspects, if they are part of agreements between manufacturers, can be included in the evaluation of the process criticality PCF with the Contractual Agreements (CA) metric. The assessment may change over time under certain circumstances. For example, if a temporary mitigation or hotfix is planned first and a more profound patch is planned for a later date. For clarity, the different definitions for a patch and an update are pointed out. An update is defined as a measure that is characterized by the intention to implement extended or optimized functionality. It is usually deployed on a cyclical basis. A patch, on the other hand, is defined as a measure characterized by being triggered by a specific incident. Deployment can be event-triggered or cyclic (synchronized with the update cycle), depending on given circumstances. Manufacturers usually pursue an efficient update management. Especially when no OTA functionality is available, the bundled release of patches (e.g., Microsoft's "Patchday") makes sense for many reasons. Key factors influencing patch and/or update management can be economic considerations, system availability and safety and liability risks (monetary or reputational). Keeping the system up-to-date with recently released patches results in higher operational costs, while patching the system infrequently for its vulnerabilities leads to higher damage costs associated with higher levels of exploitation. A basic distinction can be made between a time-driven approach and an event-driven approach.

In addition to the time at which a manufacturer provides patches, patch implementation management of the vehicle owner also plays a key role. The behavior of the vehicle owner lies outside the manufacturer's responsibility and is therefore not part of its incident response management. The patch implementation management on the part of the vehicle owner therefore has no influence on the evaluation of the appropriate grace period.

The evaluation is carried out either by a dimensionless score that is included in the PCF if no concrete time specification can be made, or by a concrete time specification in days. This then does not influence the PCF or GP, but is added to the calculated reasonable Grace Period.

Value	
None	For the existing vulnerability, no measures at all are developed (during vehicles operation time) regarding the given vulnerability, because e.g., the support has expired or a manufacturer involved in the development is no longer on the market. Assigning this value indicates that no time is needed for remediation dissemination.
No vehicle access required	For the existing vulnerability, no official patch is developed (during vehicles operation time) regarding the given vulnerability. However, measures are taken which do not require access to the vehicle (e.g., disabling a functionality via back end access or dissemination of user advise). Assigning this value indicates that no time is needed for remediation dissemination.

Immediately	For the existing vulnerability, a patch is developed and it is possible **and** appropriate (due to given circumstances) to disseminate remotly (event-driven release). This indicates there is the ability to update remotely without physical access (e.g., OTA) and the distribution of the remediation can be performed worldwide simultaneously and without loss of time directly after its completion. Assigning this value indicates that no time is needed for remediation dissemination.
Gradually - not determined	For the existing vulnerability, remediations are developed and their dissemination must be done with physical/local vehicle access (e.g., regular workshop service). A timeline can therefore **not be determined concretely**. Assigning this value indicates that 'Remediation Dissemination' increases the "PCF"- value by factoring in R. The dissemination circumstances for this measurs are decisive here. It should be assessed how long it takes until distribution has sufficiently advanced, to reduce the extent of an existing risk to an appropriate level (e.g., region, number of effected vehicles, number of service stations in case of workshop stop).
Gradually - determined	For the existing vulnerability, remediations are developed and there is no explicit need to disseminate immediatly/ within a prescribed period (e.g., internal requirements for recalls) or it is not appropriate to do so. Dissemination can therefore take place gradually via remote access (e.g., Patching Days) **at a pre determined date (given patch- or update release cycles)**. Assigning this value indicates that 'Remediation Dissemination' increases the overall GP´- value by Y working days.

Certification & approval	
This metric evaluates the appropriate grace period with respect to delays which may arise with necessary approval obligations. Regulations for type approval vary worldwide (e.g. UN 156 regulation). Depending on country-specific regulations, vehicle manufacturers may be required to provide processes as part of their internal software update management that can be used to verify whether and how a software update will modify (alter, remove, add, enable, disable) any parameters or functions of type approved systems to be updated/patched or parameters used to type approve those systems. Furthermore, this also applies to modifications of parameters or function that are defined within legislation or that will affect any other system required for the safe and continued operation of the vehicle. The responsibility for the correct assessment of the relevance of an update/patch for approval lies (also) with the vehicle manufacturer. Whether an extension or renewal of the approval is necessary must and can therefore be assessed by the manufacturer. The extent of the delay in patch dissemination due to approval processes should be specified on the basis of empirical values and/or in consultation with the Approval Authority or Technical Service.	
Value	
None	No relevance for approval
Extension	Extension of type approval is necessary. Assigning this value requires the specification of a concrete time value in working days for expected delay.
Renewal	Renewal of type approval is necessary. Assigning this value requires the specification of a concrete time value in working days for expected delay.

Contractual agreements

This metric can be used to include aspects into the evaluation of the reasonable grace period that may have been defined as part of agreements between the customer and supplier and can help to refine the assessment for the given specific vulnerability. These may be agreements between partners within a company or beyond. In particular, this metric reflects the RQ-07-04 and RQ-07-05 requirements of ISO/SAE 21434 and provides the ability to make the evaluation of the reasonable patching time more adaptable to given real circumstances. Since such agreements generally lack an objective judgment, this metric may be unsuitable for the 'Coordinated Vulnerability Disclosure' use case. However, it may be suitable for use in the internal patch or vulnerability prioritization process.

Example 1: Patch development and verification
Technical requirements of patch development and verification could serve as criteria. If qualitative or quantitative agreements on the organizational and/or technical management of patch development and verification are defined between costumer and supplier, these could be used to adapt the assessment. (e.g. required security testing activities)
Example 2: Incident Response Plan
Agreements defined in the context of an Incident Response Plan (ISO/SAE21434 requirement RQ-13-01) (criteria for closure of information, remedial actions).
Example 3: Cybersecurity Assurance Level - CAL
Given a CAL which is assigned to the vulnerable and/or affected component/item (resp. its security goals), special requirements has to be fullfilled by a supplier when it comes to the need to handle the vulnerability (e.g., patching, communication, providing information). The possible values to rate this metric could reflect the gap between the pre-defined assurance levels (e.g., 1-5) and the assigned 'Risk Value' or the assessment could be based on a pre-defined CAL classification scheme to detemine the level of rigour of necessary cybersecurity measures to provide the required assurance.
It may also be a combination of several such aspects.

NOTE on the calculation of the process criticality PCF resp. Grace Period Factor GP:
In principle, up to two CA aspects can be added to the calculation, which then increase the value of PCF resp. GP. However, the value of GP cannot be higher than 2. If two aspects are added, both are treated equally weighted, i.e. the average of both scores is used. (Since both the documentation and the source code for the calculation tool are open source, the score can be changed at any time to suit the needs of any entity that applies it).

Value	
None	Assigning this value indicates that no contractual agreements with impact on patchig time exist, or that existing agreements do not increase process criticality significantly enough for the standard grace period T_0 used to be found not reasonable. Both the process criticality PCF and the Grace Period T_GP are not affected.
Costumized	Dependent on internal and inter-corporate contractual conditions (e.g., defined CALs or Incident Response Plan for effected component)

Dimension	Criteria	Adaped from…	Abb.	Scoring				
Vulnerability Assessment	Vulnerability Risk Value	ISO/SAE 21434 -	RV	Medium	High	Very High		
				0,7272	0,8636	1		
	Scope	CVSSv3.1 Base Score	S	Unchanged	Changed			
				1	0			
Incident Analysis	Exploit Code Maturity	CVSSv3.1 Temporal Score	EM	Not Def.	High	Functional	Proof-of-Concept	Unproven
				1	1	0,97	0,94	0,91
	Remediation Level	CVSSv3.1 Temporal Score	RL	Not Def.	Unavailable	Workaround	Temporary Fix	Official Fix
				1	1	0,97	0,96	0,95
	Report Confidence	CVSSv3.1 Temporal Score	RC	Not Def.	Confirmed	Reasonable	Unknown	
				1	1	0,96	0,92	
	Exploit Code Dissemination	none	ED	Unclear	External - Black marke	External - PoC	External - not public	
				1	1	0,96	0,91	
	Incident Scale	none	ISC	Unclear	High	Medium	Low	
				1	1	0,97	0,95	
Process Complexity	Supply chain scale	none	SCS	Low	Medium	High	Very High	
				0	0,037057	0,074113	0,11117	
	Remediation Dissemination	none	R	None	No access req.	Immediately	not determined	determined
				0	0	0	0,11117	time value Y
	Certification & approval	UN R156	APP	None	Extension	Renewal		
				0	time value	time value		
	Contractual agreements - CAL	ISO/SAE 21434 - 15. Distributed CS Activities	*CA*	None	CAL1	CAL2	CAL3	CAL4
				0	0	0	0,0693	0,11117
	Contractual agreements - CS Incident Response Plan	*to be def.*	*to be def.*	None	….	…	…	…
				to be def.				
	Contractual agreements - …	*to be def.*	*to be def.*	None	….	…	…	…
				to be def.				