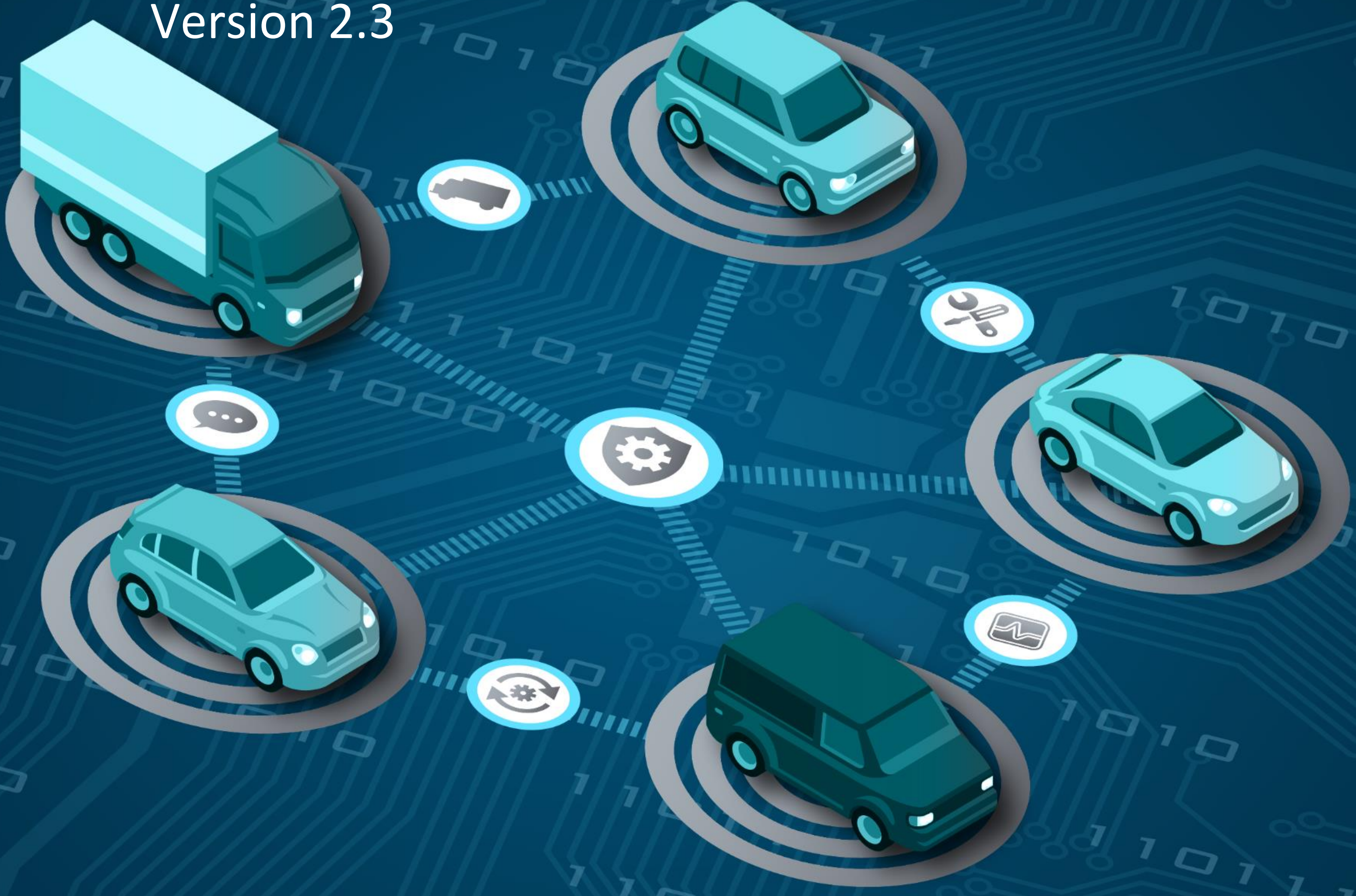
AUTO-ISAC
AUTOMOTIVE CYBERSECURITY BEST PRACTICES

RISK ASSESSMENT AND MANAGEMENT

Best Practice Guide
Version 2.3



Traffic Light Protocol: WHITE.

This information may be shared in public forums.

AUTO-ISAC
Automotive Information Sharing and Analysis Center

Version History

This is a living document, which will be periodically updated under the direction of the Auto-ISAC Best Practices Working Group. We will track any updates in the table below.

Version Notes:

Version	Revision Date	Notes
v1.0	18 January 2018	
v2.0	19 July 2018	Updated by the Best Practice Working Group Task Force
v2.1	30 November 2018	Changed from TLP **Amber** to TLP **Green** for release to industry stakeholders via request on Auto-ISAC website
v2.2	01 July 2019	Performed periodic continuity and consistency refresh across all Best Practice documents
v2.3	19 August 2019	Changed from TLP **Green** to TLP **White** for release to the public via request on Auto-ISAC website

Contents

This Guide does not prescribe or require specific technical or organizational practices.
These are voluntary and aspirational practices, which may evolve over time.
Please see Section 1.2 for more information.

1.0 Introduction

1.1 Best Practices Overview

This Best Practice Guide is one in a series of seven Guides intended to provide the automotive industry with guidance on the Key Cybersecurity Functions defined in the Automotive Cybersecurity Best Practices Executive Summary:

1. Incident Response
2. Collaboration and Engagement with Appropriate Third Parties
3. Governance
4. **Risk Assessment and Management**
5. Awareness and Training
6. Threat Detection, Monitoring and Analysis
7. Security Development Lifecycle

Guides offer greater detail to complement the high-level Executive Summary. This Guide aligns with the "Risk Assessment and Management" function and is made available for use by companies, as appropriate for their unique systems, processes, and risks.

1.2 Purpose

The purpose of this Guide is to assist automotive industry stakeholders in integrating vehicle cybersecurity risk management into their overall corporate risk management structure (e.g. based on ISO 31000:2009 family or COSO 2017 Enterprise Risk Management Framework). This Guide assumes that organizations already have a risk management strategy in place.

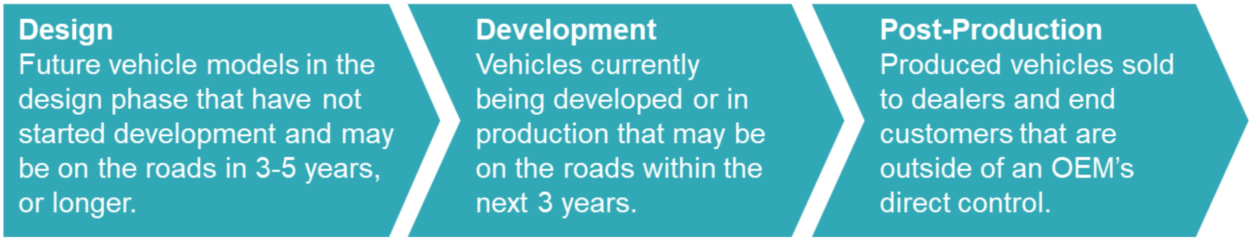
This Guide provides forward-looking guidance without being prescriptive or restrictive. These best practices are:

- **Not Required**. Companies have autonomy and can decide which of these practices to select and can adopt these practices based on their respective risk landscapes and organizational structures.
- **Aspirational**. These practices are forward-looking and voluntarily implemented over time, as appropriate.
- **Living**. Auto-ISAC plans to periodically update this Guide to adapt to the evolving automotive cybersecurity landscape.

1.3 Scope

This Guide describes key considerations for companies around vehicle cybersecurity risk management efforts. It contains best practices and implementation guidance for companies to integrate, evaluate and remediate cyber risk assessments throughout the product development lifecycle. These are voluntary, non-prescriptive, aspirational practices, which companies may use to determine an appropriate approach for their unique risk landscape.

The scope of the guide covers all phases of the vehicle lifecycle, including design, development, and post-production. These phases are described in Figure 1 below.



Design
Future vehicle models in the design phase that have not started development and may be on the roads in 3-5 years, or longer.

Development
Vehicles currently being developed or in production that may be on the roads within the next 3 years.

Post-Production
Produced vehicles sold to dealers and end customers that are outside of an OEM's direct control.

FIGURE 1: VEHICLE LIFECYCLE PHASES

1.4 AUDIENCE

This Guide was written for use by light-duty and heavy-duty vehicle OEMs, light-duty and heavy-duty vehicle suppliers, and commercial vehicle companies (e.g. fleets, carriers). It may also provide insights for other stakeholders across the connected vehicle ecosystem.

Within these organizations, the primary audience is vehicle cybersecurity managers, leaders, and senior executives who are responsible for managing vehicle cybersecurity risk.

1.5 AUTHORITY AND GUIDE DEVELOPMENT

The Auto-ISAC Best Practices Working Group wrote this Guide, with support from Booz Allen Hamilton vehicle cybersecurity SMEs who facilitated the Guide's development. The Working Group is comprised of over 130 representatives from Auto-ISAC Members, including:

AT&T
Bosch
BMW
Continental
Cooper Standard
Cummins
Delphi
DENSO
EHI
FCA
Ford
General Motors
Geotab
Harman
Honda
Honeywell
Hyundai
Infineon
Kia
Lear Corporation
Magna
Mazda
Mercedes-Benz
Mitsubishi Motors
Mobis
Nissan
NXP
Panasonic
Subaru
Toyota
Volkswagen
Volvo
ZF

The Working Group also coordinated with several external stakeholders while developing this Guide, including Auto Alliance, Global Automakers, National Highway Traffic Safety Administration (NHTSA), National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO), and SAE International (SAE).

1.6 GOVERNANCE AND MAINTENANCE

The Auto-ISAC Best Practices Standing Committee is responsible for the maintenance of the Guide, which will undergo periodic refresh to incorporate, as appropriate, lessons learned, new policies, updated or new engineering standards, and the like.

This Guide does not prescribe or require specific technical or organizational practices.
These are voluntary and aspirational practices, which may evolve over time.
Please see Section 1.2 for more information.

This Guide will be rolled out in phases and marked accordingly with the appropriate Traffic Light Protocol (TLP) classification:

- **First 3 months after publication: TLP Amber** - available exclusively to Auto-ISAC Members
- **3 to 9 months after publication: TLP Green** - released by request to industry stakeholders
- **9 months after publication: TLP White** - released to the public via the Auto-ISAC website (www.automotiveisac.com), subject to Board of Directors confirmation

This Guide was developed while the ISO and SAE were in the process of jointly developing the ISO/SAE 21434 Road Vehicles – Cybersecurity Engineering Standard. After ISO/SAE 21434 is published, the Standing Committee plans to review and update this Guide, if required.

2.0 Best Practices

The objective of this document is to provide guidance for handling cyber risk management associated with the vehicle ecosystem. This document assumes that a risk methodology is already in place for the organization and addresses the application of that methodology throughout the product lifecycle, and the possible actions associated with an objective risk score. Furthermore, it discusses how corporate risk management practices, for instance risk treatment, can be adapted by a company to the vehicle product cybersecurity domain.

Many risk management methodologies exist, and each is likely to be individually tailored to each organization to accommodate for application-specific details or unique organizational attributes, which may consider culture, process or experience. Possible risk methodologies to consider for implementation are available in Appendix B: Additional References and Resources of this document.

2.1 Scope and Requirements

It is important to define the overall scope and requirements associated with implementing a cyber risk assessment methodology. Defining the boundaries of the program will allow for better control and governance of the activities and manage the potential cost impact.

The same cyber risk assessment methodology typically is used throughout the organization, and through the product or vehicle lifecycle, including the following organizational departments or phases of development:

- Product Development Engineering
- Service
- Operations
- Procurement
- Aftermarket

The cyber risk management process may be tailored throughout the development cycle (see Section 2.2 Coverage), and the levels of acceptable risk may change throughout the lifecycle as well (see Section

2.4 Risk **LIFECYCLE**).

Products, components or systems that may be considered for a cyber risk assessment include all products that may impact vehicle cybersecurity, which may include the following:

- Electrical or electronic parts or systems installed in road vehicles
- Connected components or access to the outside world (e.g. USB, OBD II)
- Storage of personal data
- Fully connected ecosystem

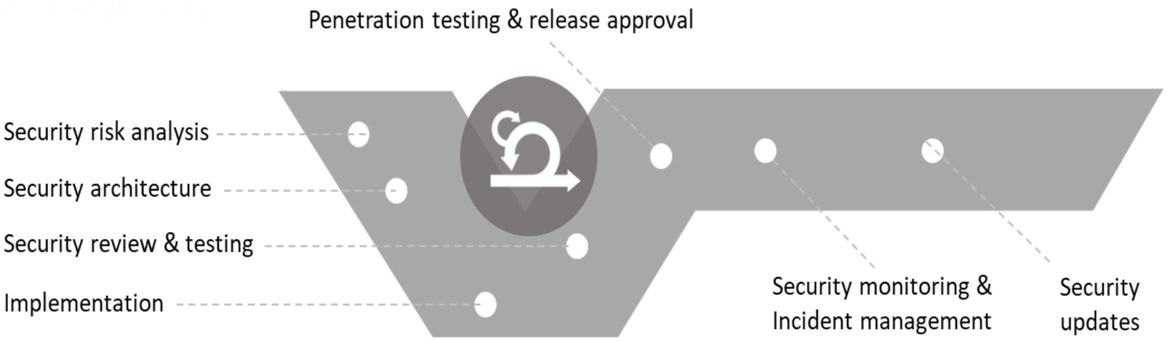
The complete vehicle ecosystem may include networked systems and connected electronic components that control or otherwise interact with the connected vehicle ecosystem. These systems and components enable the collection, processing, storage, and transportation of data, as well as taking action based on data.

2.2 COVERAGE

An effective cyber risk management process can be based on various types of assessments performed during certain states of a vehicle or product's entire lifecycle and will support the identification of cybersecurity risks.

The vehicle or product lifecycle may consist of several milestones and phases involving different stakeholders within an automotive company. If the company uses the well-known waterfall or V model for its development lifecycles, significant milestones may include the follow phases:

- Design
- Implementation and Integration
- Testing
- Production
- Aftersales


Penetration testing & release approval
Security risk analysis
Security architecture
Security review & testing
Implementation
Security monitoring & Incident management
Security updates

During these different phases, different types of security assessments can be performed along the waterfall model, as well as after product deployment, as shown in the following figure:

FIGURE 2. SAMPLE SECURITY ASSESSMENTS DURING PRODUCT DEVELOPMENT CYCLE

2.2.1 Design

In an early stage, it will be useful to perform a security risk analysis (paper analysis) of a vehicle or product's overall functional concept to consider assets, threat vectors and actors, as well as the resulting protection goals. Based on the outcome of a paper analysis, new risks for cyber risk management can be identified, and design decisions about new requirements for the overall architecture can be made and agreed upon. In addition, a company may consider performing further paper analysis on planned products, which might be derived in the future and which might consist of both new technology as well as legacy technology (e.g. to reuse existing component designs in new products).

A risk analysis in the design phase should consider:

- The relevant threats, threat actors and threat vectors identified during the Threat Detection phase (see *the Auto-ISAC's Threat Detection, Monitoring and Analysis Best Practice Guide* for more information)
- Anticipated risks in the subsequent phases of the vehicle lifecycle (Implementation, Testing, Production, Aftersales)
- Risks associated with the entire vehicle ecosystem: vehicle electronics, connectivity interfaces (e.g. OBD II, cellular, WiFi) manufacturing facilities and their IT systems, supply chain and logistics risks, risks with vendor software, connectivity infrastructure services (e.g. software update management), security services (e.g. Public Key Infrastructure, certificate or credential management)
- Risks related to supplier and vendor products (hardware and software)

2.2.2 Implementation and Integration

After the design phase but before implementation, all requirements can be measured against their effectiveness in reaching company-specific protection goals. Furthermore, it may be useful to update the vehicle's overall security posture after all paper analyses have been conducted.

Some products use different development methodologies. Consider the following example: Mobile applications are often developed in shorter lifecycles (i.e. in an agile style and thus do not necessarily follow the V model). In this case, it is generally important to define synchronous security milestones reflecting that the vehicle or product's functionality has reached its necessary maturity and that connected functions can be tested together with mobile applications. During the final stages of development, unanticipated vulnerabilities are likely to be identified. It is therefore helpful to have budgeted sufficient time in the planning stages for the remediation of identified risks.

2.2.3 Testing

During the planning phase and before implementation, it is important to introduce several milestones which ensure that the product's maturity is in a state where security is testable. Penetration tests, security code scanning, and other functional security tests can be planned according to these milestones. The planning of the security testing milestones in the testing phase typically considers the time to remediate identified vulnerabilities and the remaining length of the development phase. It might prove useful to rate identified vulnerabilities with a risk rating methodology and prioritize remediation based on that. Vulnerabilities which might not be quickly fixed, as well as newly identified weaknesses, could then be treated by the aftersales vehicle cyber risk management process.

2.2.4 Production

A company may consider performing a security approval at the end of the testing phase to check product security, and if possible, audit the implementation of security requirements. This security approval may have the added benefit of raising security awareness within the company, as well as leading to a natural understanding of security-related tests by involved development departments. The outcome of this approval may be reflected to the design process to lead to long-term security improvements and a security-minded culture.

It is important that production cybersecurity risk management not end with the production security approval. Maintaining a focus on security throughout production helps to manage the risk landscape. Cybersecurity quality checks often are performed to ensure that the security measures are being implemented correctly and no unauthorized changes are applied. Production approved changes can go through a similar, if not the same, risk assessments as were done during development. Additionally, supply chain risk can be assessed and managed throughout the production life of the product.

2.2.5 Aftersales

After a product's market launch, it is useful to have threat monitoring in place, which helps to identify new trends in the threat landscape (e.g. in the hacker scene, potential emerging attack vectors, newly discovered vulnerabilities, cybersecurity incidents). To achieve long-term cybersecurity product improvements, the cyber risk assessment team can be informed about newly identified attack vectors and the organization's cyber risk protection goals may be continuously updated. Over-the-air updates may introduce new features or be helpful in remediating vulnerabilities or neutralizing potential threats of already deployed vehicles. An over-the-air update also typically is subject to appropriate assessments (e.g. through paper analysis and/or penetration tests and code audits).

In addition to threat monitoring and vulnerability management activities a manufacturer can manage risks in the portion of the aftersales environment where they may have influence, such as their associated dealership network, connected applications, and accessory parts. During the development process, each of these areas typically has been considered and ongoing attention to these areas needs to be sustained throughout the product lifecycle. In the dealer network, items such as service tools need to be designed, produced, and maintained to have proper security controls in place. Connected applications should be monitored and the risk assessment should be updated as the environment changes. Accessory and aftermarket parts also need to be properly assessed for cybersecurity risk and proper controls put in place.

2.3 Roles and Responsibilities

This section offers a basic understanding of the different roles and responsibilities that are possible within a vehicle or product cyber risk management process. The first part of this section describes the different stakeholders and their roles, while the second part explains the associated responsibilities regarding their tasks and timing. This section does not refer explicitly to the product development cycle phases, since most of the tasks are recurring (e.g. assessments after new cyber incidents or after a product change). This section also discusses how a "second set of eyes policy" is beneficial. At the end, the interaction of the roles and responsibilities is shown in an example RASIC (Responsible, Approve, Support, Inform, Consult) chart.

The structure and membership of product cybersecurity teams can vary significantly across companies based on factors including the cultures, organizational structures, and personnel within each company. There is no single correct way to allocate roles and responsibilities. Instead, each company properly can allocate roles and responsibilities in the way that makes most sense in the contexts of their own businesses. Here we offer one example of how a company might allocate responsibilities for risk management within one example cybersecurity product team structure. The use of this example is not intended to suggest that it is preferable to other approaches. For example, a company may choose to include different members or teams within its risk management process or allocate responsibilities differently among the team members.

In the example provided here, the parties involved in the cyber risk management process are:

1. Cyber Leader
2. Product Cybersecurity Team, including Cyber Risk Managers and Cybersecurity Analysts
3. Penetration Testing Team (Pen Testing Team)
4. Incident Response Team
5. Design Team including its Program Manager
6. Developers
7. An appropriate executive manager; (e.g. Director)

Organizations may consider the following roles and associated core responsibilities described below.

1. In this example, the Cyber Leader is defined as the individual who is responsible for leading efforts and managing the Product Cybersecurity Team, Penetration Testing Team, and Vehicle Incident Response Team. The Cyber Leader is the facilitator of all assessment results and has the job of communicating results to the interested stakeholders.

   Responsibilities may include:

   - Overseeing the Product Cybersecurity Team to help ensure that cybersecurity tests and risk assessments are conducted throughout the vehicle lifecycle, and to direct interaction with appropriate teams to help ensure that standards are being met.
   - Helping to ensure the completed tests and risk assessments are logged and reported as appropriate to leadership and the Product Team.
   - Collaboration with the Design Team Management to help ensure that there is firm milestone planning known and followed by all parties.
   - Reporting to upper management about the product’s cybersecurity state and threat landscape.
   - First-line approval on the acceptability (risk tolerance) of identified cybersecurity risk assessments and escalation to upper management of high-risk topics, as needed.
   - Reporting vehicle cyber risks to corporate risk management based on predefined thresholds.

2. The Product Cybersecurity Team is often referred to in the security domain as the “Blue Team.” It typically consists of the individuals who perform the day-to-day cybersecurity processes, including cyber risk assessments on concepts, as well as defining new protection goals to counter the changing threat landscape. This team is typically removed (organizationally) from the Design Teams to enable impartiality during all assessments.

   Responsibilities may include:
   - Ownership of the product cyber risk assessment process.
   - Help ensure that all relevant components and functions of a vehicle are assessed regarding cyber risks throughout the vehicle lifecycle.
   - Monitoring and regularly updating the risk landscape.
   - Defining protection goals for vehicle cybersecurity and the security posture together with the Design Team that is responsible for a vehicle overall architecture.
   - Defining and updating product security policies (e.g. basic security requirements set).
   - Review and approval or consulting of specific ECU and functional cybersecurity concepts delivered by the Design Team.
   - Interaction and discussions with the Design Team regarding technical requirements and if these are sufficient to meet the defined protection goals.
   - Driving the remediation of identified vulnerabilities together with the Design Team and developers.

3. The Pen Testing Team is in the security domain referred to as the “Red Team” and is defined as those individuals who perform penetration testing on vehicles, ECUs, or functions. This team may be internal or external. Separation of the Pen Testing Team from the Design Team supports impartiality. It can narrow down the practicability of possible vehicle cyber-attacks and thus can rate the robustness of a product against cyberattacks. The Pen Testing Team is also able to support the Incident Response team in certain technical assessments.

   Responsibilities may include:
   - Creation of a test plan on cybersecurity tests and perform related penetration tests.
   - Performance of periodic source code audits to identify vulnerabilities and raise awareness for insecure coding styles.
   - Identification and rating of vulnerabilities regarding practicability of attacks and impact according to the risk rating methodology mentioned in chapter 7.
   - Reporting on all performed tests as well as audits.
   - Definition of new test-cases derived from publicly-known cyber-attacks and delivery to Design Team and Developers as appropriate.

   The Pen Test leader may create test policies, statements of work, or other related documentation to ensure the completeness of penetration testing. The leader also may oversee related tests, review reports, and escalate as appropriate.

4. The Incident Response Team is defined as the group who is responsible for technical analysis of vehicle-related cyber incidents, rating discovered risks and handling incidents by generating a corporate response.

   Responsibilities may include:

   - Technical analysis of vehicle cyber incidents or potential incidents (e.g. unauthorized access related to a discovered vulnerability, rating resulting risks and managing incidents by responding and communicating accordingly).
   - Facilitate conclusion of incidents on a technical and a business level, according to company risk tolerance, and remediation options described in Section 2.6 Evaluation of Results and Risk Treatment.
   - Delivery of new attack patterns or concept weaknesses to the Product Cybersecurity Team to enhance security for future products.

Note that some companies may not task their Incident Response Team with evaluating risks identified in an incident but might hand off that task to other entities such as a vulnerability management team. Such a team also may handle vulnerabilities more broadly and have responsibility for the integration of vulnerability management into risk management.

5. The Design Team are those that work in engineering and who develop or support development of the hardware and software that is being created and tested. The Design Team is typically responsible for ensuring that the owners (Cyber Leader and Product Cybersecurity Team) are provided with the evaluation evidence for accurate risk assessments, typically program managers.

   Responsibilities may include:

   - Design of functionalities and definition of requirements for products.
   - Planning of milestones for product maturity and its testability.
   - Break-down of the security posture, which was created at the beginning of the development lifecycle by the Product Cybersecurity Team into specific product requirements.
   - Meeting security performance requirements and specifications as determined by the product Cyber Leader and Product Cyber Team.
   - Evaluation of cybersecurity specific test-cases provided by the Product Cybersecurity Team and Pen Test Team.
6. Developers implement the product requirements defined by the Design Team. The difference between the Design Team and the developers is that software and hardware are often developed by different suppliers, while functionality and specification are often designed within a company. Depending on a company's structure, it can be easier or harder for the Product Cybersecurity Team to communicate directly with developers, discuss vulnerabilities or source code audit findings and educate them on cybersecurity best practices.

   Responsibilities may include:

   - Implementation of requirements delivered by Design Team.
   - Implementation of changes based on the results of risk assessments delivered by the Product Cybersecurity Team during certain milestones.

- Report any identified implementation risks (e.g. vulnerable third-party software libraries) to Design Team and Product Cybersecurity Team.

7. The company's Director makes business decisions that affect the product's cybersecurity. The Director receives briefs by the Cyber Leader to make best interest decisions for the company.

   Responsibilities may include:

   - Approves the risk tolerance policy and thresholds for risk escalation.
   - Take briefings by the Cyber Leader into account when making business decisions.

However, they decide to allocate roles and responsibilities in the context of their own businesses, organizations may consider the following advice:

The risk evaluation evidence required for performing these assessments should not have any obvious internal inconsistencies or inconsistencies with other risk evaluation evidence. This indicates that all results are initially inconclusive and remain so until a final risk score is assigned to the system/component.

One person acting as Cyber Leader controls the reporting and helps to remove bias and errors. Stakeholders are defined as leadership of the design team, cybersecurity, senior leadership, or other internal stakeholders. The results of risk assessments being accurate and independent of bias is crucial.

The review of cyber risk assessments may go to leadership in cybersecurity, design, and executive management. The safety concerns and importance of considering risk in the design process and throughout product life requires appropriate involvement of these key stakeholders.

Control gate reviews happen initially in two stages. The initial paper-based assessment and the last penetration test before start of production are leadership's way of controlling production and development of new systems/components while understanding the present risk. Penetration tests and source code audits are often not just performed at the end of the development cycle, but also during it to identify risks and remediate these depending on their criticality before the product is deployed in the field. Continuous reassessments of products after deployment can be done on a periodic basis to help the Product Cybersecurity Team and the Cyber Leader recognize changes to the risk landscape. Based on product alterations post-production, it might be useful to repeat the different types of assessments to ensure that safety and risk standards are still being followed.

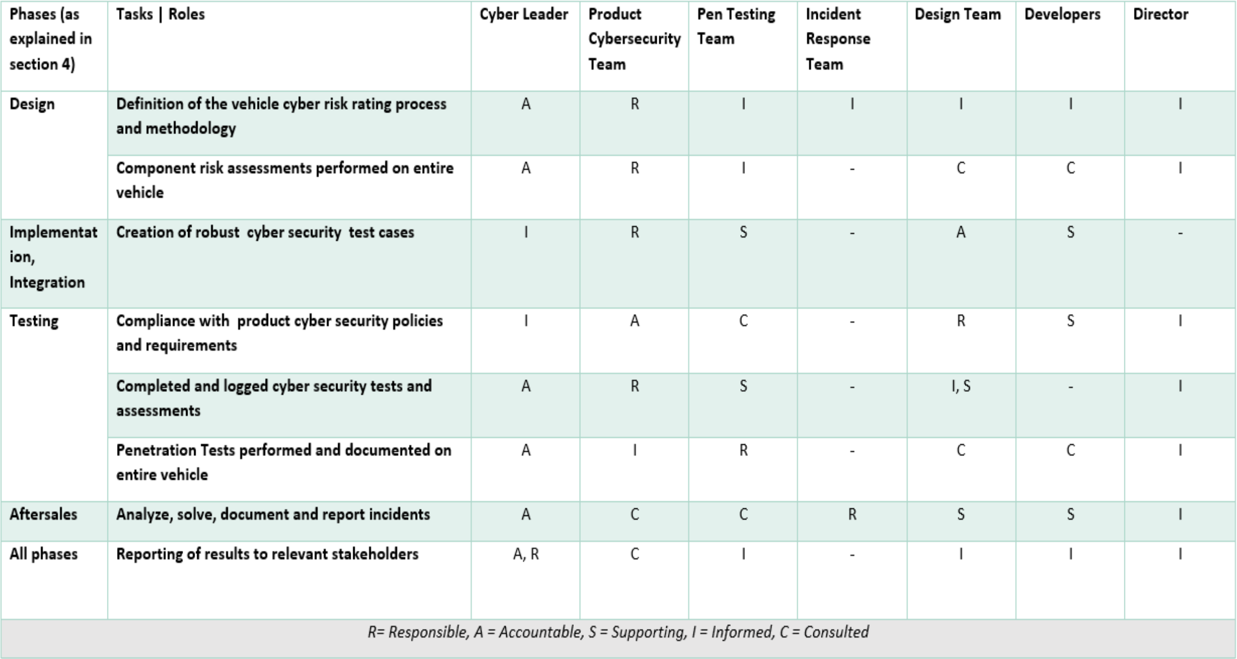
It may be useful to establish a 2nd pair of eyes principle (i.e. another authority can approve all performed assessments regarding their scopes and results during each step in the development phase). The 2nd pair of eyes principle can be achieved by introducing certain quality gates or milestones which need to be approved by another individual or group not directly involved with the working product. However, it might be hard to find this independent 2nd pair of eyes within a company, since approving cybersecurity relevant concepts or implementations extensive knowledge in cybersecurity by the approving authority is required. Instead it might be a useful alternative to establish periodic third party authority process audits on all cyber risk assessment processes to check if these processes are complete, performed properly, and their results fulfill the work quality standards as defined by the Cyber Leader.

Below are two examples in which the 2nd pair of eyes principle may be applied:

1. The Cyber Leader approves the last penetration test report regarding its scope and identified vulnerabilities before vehicle deployment.
2. The Product Cybersecurity team approves compliance with cybersecurity policies of a design concept for a new component.

Depending on the size, organization, and maturity of the cybersecurity team, it may be more appropriate for the Design Team to take responsibility for the execution of the risk assessment, while the Product Cybersecurity Team provides consulting oversight and responsibility for the overall management. This scenario may be a more appropriate implementation for an OEM, where the core technical expertise in understanding the details of the component design are held by the Design Team. The Product Cybersecurity Team can provide counseling and cyber-specific expertise, but the Design Team is typically responsible for compliance to the Product Cybersecurity team's policies or guidelines.

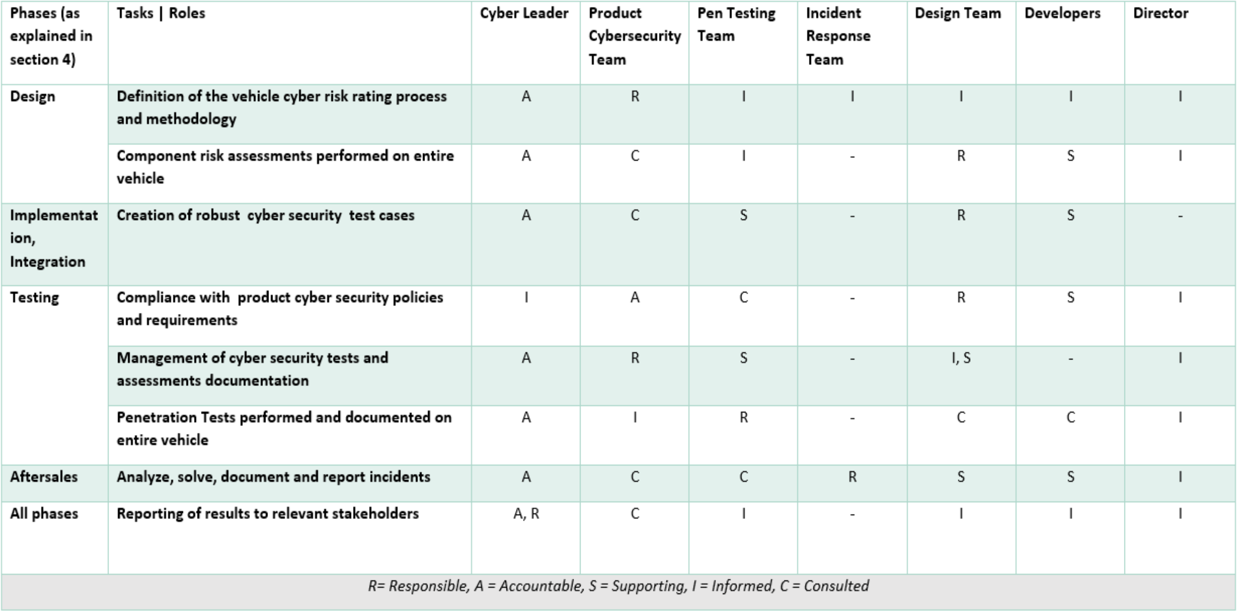
The RASIC tables below show examples of how an interaction between the roles described above may be defined within a company with more responsibilities assigned to the Product Cybersecurity Team as in Table 1 or more responsibilities assigned to the Design Team as in Table 2:



Phases (as explained in section 4)	Tasks | Roles	Cyber Leader	Product Cybersecurity Team	Pen Testing Team	Incident Response Team	Design Team	Developers	Director
Design	Definition of the vehicle cyber risk rating process and methodology	A	R	I	I	I	I	I
	Component risk assessments performed on entire vehicle	A	R	I	-	C	C	I
Implementation, Integration	Creation of robust cyber security test cases	I	R	S	-	A	S	-
Testing	Compliance with product cyber security policies and requirements	I	A	C	-	R	S	I
	Completed and logged cyber security tests and assessments	A	R	S	-	I, S	-	I
	Penetration Tests performed and documented on entire vehicle	A	I	R	-	C	C	I
Aftersales	Analyze, solve, document and report incidents	A	C	C	R	S	S	I
All phases	Reporting of results to relevant stakeholders	A, R	C	I	-	I	I	I

R= Responsible, A = Accountable, S = Supporting, I = Informed, C = Consulted

TABLE 1. AN EXAMPLE OF A RASIC CHART TO SHOW INTERACTION BETWEEN VEHICLE CYBER RISK MANAGEMENT STAKEHOLDERS



Phases (as explained in section 4)	Tasks | Roles	Cyber Leader	Product Cybersecurity Team	Pen Testing Team	Incident Response Team	Design Team	Developers	Director
Design	Definition of the vehicle cyber risk rating process and methodology	A	R	I	I	I	I	I
	Component risk assessments performed on entire vehicle	A	C	I	-	R	S	I
Implementation, Integration	Creation of robust cyber security test cases	A	C	S	-	R	S	-
Testing	Compliance with product cyber security policies and requirements	I	A	C	-	R	S	I
	Management of cyber security tests and assessments documentation	A	R	S	-	I, S	-	I
	Penetration Tests performed and documented on entire vehicle	A	I	R	-	C	C	I
Aftersales	Analyze, solve, document and report incidents	A	C	C	R	S	S	I
All phases	Reporting of results to relevant stakeholders	A, R	C	I	-	I	I	I

R= Responsible, A = Accountable, S = Supporting, I = Informed, C = Consulted

TABLE 2. AN EXAMPLE RASIC CHART WITH DESIGN TEAM RESPONSIBLE

2.4 RISK LIFECYCLE

Throughout the vehicle or product lifecycle, the assessed risk category may change as new information is available. This may include updates due to design maturity, updated and added product functionality, or changes in technology. It's vital to ensure that the cyber risk management process can accommodate these changes over time, and the risk profile is current. It is useful to update the risk assessment logically, not simply based on milestones or changes in lifecycle. For example, further design details may reveal additional interfaces, attack paths or technologies that were undetermined previously.

Depending on the risk assessment method used, it is often helpful to determine the right frequency, schedule, and scope (e.g. function, single ECU, system, full vehicle, and specified triggers for residual risk assessments or updates). These methods only require an updated risk assessment if there is a change to the item that could affect the initial risk assessment (e.g. changes in functionality). Having a reasonable and practical risk assessment process helps control costs and enables the company to focus on risk reduction efforts in the areas that require the most attention.

Integrity Level, as defined by ISO 26262, determines the level of rigor in designing the component, system or product. Cyber risk management may consider this Integrity level and other factors, such as privacy, as a guideline for rigor in completing and updating cyber risk assessments. A higher Integrity level or other such factors may drive greater diligence and attention in maintaining a current cyber assessment.

Frequency of review and updates is also subject to organizational security culture. A company or product with a lower risk tolerance may be more sensitive to changes. For example, areas of higher risk may continue to receive greater attention and updates than known lower risk areas.

It is important to tailor requirements for your organization and risk tolerance and identify areas for higher frequency in updating risk assessments. Possible triggers to consider may include:

- Changes in system architecture
- New functionality in the design
- Accumulation of residual risk
- New developments that could impact aged or previous projects
- Changes in perceived value of cybersecurity target
- Age of deployed technology
- Discovery of a new vulnerability or disclosure of an exploit
- New vulnerabilities, new threat actors, etc.

Changes in components, part number changes or physical hardware changes may lead to a decision to undertake a new or updated cyber risk assessment. A change analysis may be conducted to determine if a new risk assessment is required only on the changes, or an update can be completed on the original assessment. It may be possible to create cascading risk assessments, as needed. The following events can be evaluated for consideration of a new (versus updated) risk assessment:

- Small component design change
- Major component change
- Architecture change
- New functionality
- New attack paths
- New threats or incidents

2.5 Risk Tolerance

Risk Tolerance is an organization's maximum level of risk deemed to be acceptable. Risk Tolerances for different circumstances can be determined by evaluating risk acceptance criteria, such as the scale of consequences, potential brand damage, and regulatory compliance requirements. Organizations may benefit from defining their Risk Tolerance throughout the phases of the product lifecycle (e.g. concept, development, production, and for different risk categories (e.g. safety, privacy, non-safety, non-privacy)). For example, having a higher Risk Tolerance in the concept phase allows progress in cases where risk mitigation capable of meeting lower downstream Risk Tolerance levels may be possible (see Figure 3). However, such a narrowing Risk Tolerance approach may be disruptive in cases where risks tolerated in earlier phases cannot be mitigated to meet the Risk Tolerance levels in later phases. Therefore, some organizations may prefer a consistent or broadening Risk Tolerance to minimize such disruptions (see Figure 2). Organizations may choose a higher Risk Tolerance for non-safety / non-privacy risks as compared with safety / privacy risks, while complying with regulatory requirements. As vehicles approach their End-of-Life (EOL) date, organizations may choose to raise their Risk

Tolerance for non-safety / non-privacy risks and communicate such EOL timing and potential consequences to customers as many software and IoT manufacturers do.

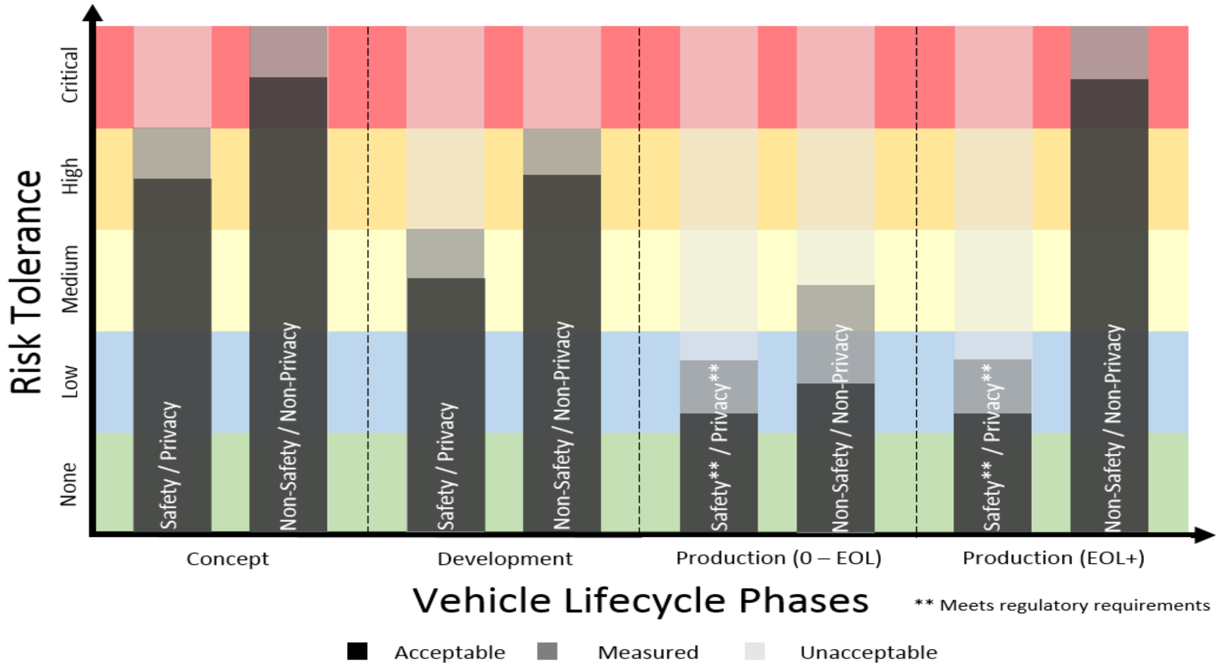


FIGURE 3. EXAMPLE OF NARROWING RISK TOLERANCES

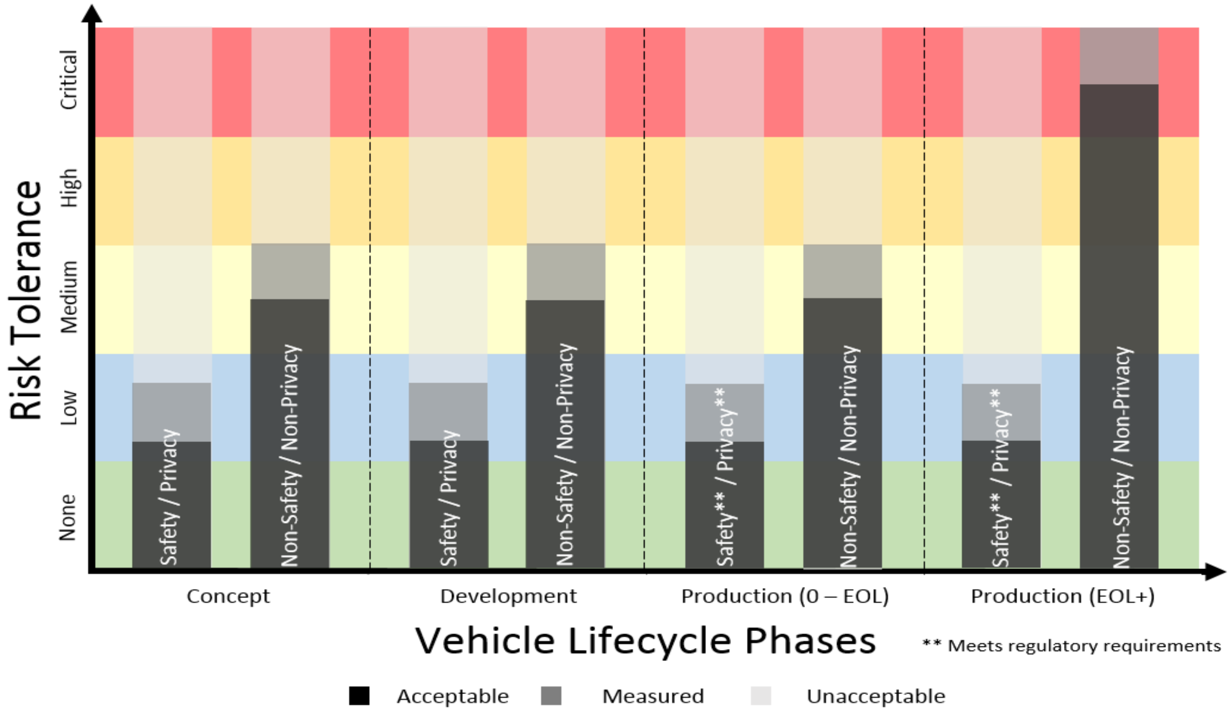


FIGURE 4. EXAMPLE OF CONSISTENT RISK TOLERANCES

2.6 Evaluation of Results and Risk Treatment

Outlining a company's acceptable levels for risk tolerance helps ensure that risk-based decisions can be addressed objectively. It is also valuable to use a scoring system, such as the Common Vulnerability Scoring System (CVSS), to rate the potential level of impact for each risk in a reproducible way. Since not all product cybersecurity risks are the same, separating risks into different categories can be useful.

Automotive companies may consider the following examples for risk categories concerning a vehicle driver or other road users such as passengers, pedestrians, etc.:

- Safety Critical – Items that can directly affect the steering, braking or motion function of a vehicle, or produce other imminent safety hazards or driver distractions.
- Privacy – Items that directly compromise the Personally Identifiable Information (PII) and other personally sensitive automotive data on-board the vehicle affecting users or the vehicle.
- Functional – Items that would impair or interfere with the functional operation of non-safety critical components.
- Nuisance – Items that could interfere with a user's experience but does not impede the function or safe operation of the product.

Some examples of product cybersecurity risk categories that affect automotive companies but not directly affect vehicle drivers may include:

- Financial – Items that could lead to financial losses of the user or commercial entities.
- Brand – Items related to the cybersecurity of a specific product that might affect the reputation of a product, brand, or corporation.
- Compliance – Items that would render the product non-compliant with applicable laws. Compliance risks may also be treated by corporate risk management and avoided in the product development process. However, there might be cybersecurity events, which may have effect on already deployed vehicles and threaten their compliance with regulations.

Each category of risk can have a risk tolerance range based on a scoring system that ranges from acceptable to unacceptable. Risks that fall within the tolerance range can be judged on how factors such as effectiveness, cost and complexity of treatment measure up against the potential severity and likelihood of an incident. An example risk tolerance chart is shown below:

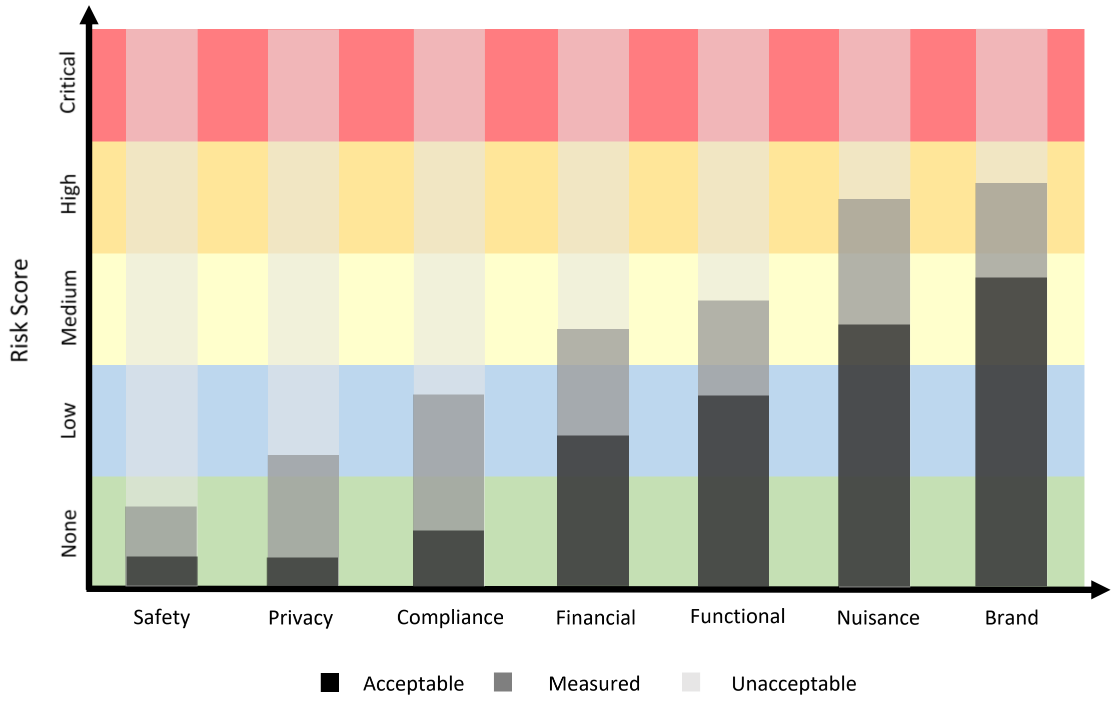


FIGURE 5. EXAMPLE RISK TOLERANCE CHART

Having categorized, scored, and assessed a risk against the company's risk tolerance scale it is then possible to make informed, risk-based decisions on possible treatment options. Treatments can be classified into different action vectors depending if they target a cyber incident, a design risk in early stage, or an identified vulnerability during development:

- Contain (imminent threat)
    - Taking actions to reduce the immediate impact of a threat or vulnerability caused by a cyber incident (e.g. disable cellular connectivity, "do not drive" instruction)
    - Likely a short-term reaction to an imminent attack, possibly followed up by a longer-term solution (remediation / mitigation)
- Remediate / Mitigate
    - Risk is sufficiently high, and action is needed to remedy
        - A high-risk vulnerability that is publicly disclosed may rise to the level of an imminent threat for containment
    - Countermeasures will be taken to eliminate the risk
        - If the risk cannot be eliminated, efforts will be towards minimizing the potential impact
        - Countermeasures may be applied just to new products or to post-production products in the market
        - Under certain circumstances countering the threat actor may mitigate the risk. This may require the involvement of external resources (e.g. law enforcement)
    - Implement actions to prevent future recurrence (e.g. feed upcoming design phase with the risk report for long-term mitigation)

- Avoid
  - Actions are taken to eliminate the risk before countermeasure actions need to be considered
  - Avoid the activity or condition that introduces the risk by choosing an alternative, less risky activity or approach that meets business objectives
  - Avoidance can be a technical as well as non-technical treatment (e.g. update operation manual, disclaimers, or Terms and Conditions (T&C's))
- Transfer
  - Certain risks may be transferred to other entities (e.g. when a company is insuring against loss in the case of an event)

- Accept and Monitor (also called "measure", see graphics)
  - Risk is sufficiently low; no immediate action is required to remedy.
  - Effective treatment options may not be feasible
  - Continued monitoring and re-evaluation of technology, vulnerabilities, etc.

2.7 Communicating Risk to Leadership and Stakeholders

An important part of a risk management program is communicating risks to business leaders and stakeholders. Internal stakeholders to consider for communicating vehicle cybersecurity risks include:

- Board of Directors
- Drivers (e.g. Customer Relations)
- Dealers and affiliates
- Information technology
- Legal
- Product development
- Product security
- Public relations
- Quality assurance
- Research and engineering
- Risk management
- Regulatory affairs
- Senior executives (e.g. CEO, CIO, CRO, CISO)

When communicating vehicle cybersecurity risks across the organization, key points of emphasis include:

- **Impact –** What is the impact to customers? What is the potential or actual consequence to the business?
- **Likelihood –** What is the probability of exploitation? Is the threat event realistic? What special expertise or equipment is required? How close do adversaries need to be to vehicles? What are the attack vectors?
- **Treatment –** What are the costs, and implementation timelines of risk treatment options? Is the risk acceptable without mitigation?

- **Risk management –** What is the risk management policy? What are the roles and responsibilities that fall under risk management?

When communicating risks outside of the company (e.g. to city infrastructure planners, consumers, operators, other manufacturers/ suppliers), it's often helpful to clarify the risk definition upfront to avoid miscommunication or misunderstanding. It is also helpful to clearly communicate with non-technical business stakeholders using non-technical terminology to help them compare vehicle cybersecurity risks to other more traditional enterprise risks with which they are more familiar. Proper risk communication mechanisms can avoid unnecessary or uncontrolled external communications, which can impact company reputation.

2.8 Governance and Compliance

Prioritization of cybersecurity across the enterprise can help successfully conduct cyber risk management throughout the product lifecycle. To that end, normal business processes and procedures can be reviewed for incorporation of cybersecurity risk reviews, including process documents, control gate reviews, checklists, etc. Full integration into normal business conduct supports integration into the full product lifecycle, with opportunities for consideration of cyber risk assessments as part of the advanced development reviews, purchasing agreements, quality and service activities, as well as other pre- and post-production scope. (See the Auto-ISAC's *Governance Best Practice Guide* for more information)..

Basing cyber risk assessments on internally published standards can ensure that each individual business entity is calculating risk the same way, and with established tolerance levels.

Further integration into the development cycle would leverage the published standards for risk evaluation onto the supply base. Cybersecurity thus can be a consideration in the purchasing documentation, reviews, audits, etc.

To ensure internal compliance with the published standard, and complete integration into the lifecycle, auditing is an option to evaluate the progress and success of integration. Auditing could be conducting internally or externally by a third party, depending on readiness or sophistication of the program anticipated.

To ensure the risk methodology is being applied consistently throughout the organization by all users, consider establishing a periodic audit cycle. Audits may be conducted internally or externally and represent an independent viewpoint.

Consider conducting independent risk assessments on a random sampling of the risks reported in the previous period. Risks within a reasonable tolerance range of the originally reported risks are considered acceptable.

If any of the sampled reports are deemed unacceptable, consider taking the following actions:

1. Notification of deviation from the Risk Assessment process
2. Specific and directed training on assessment deviation from expectations
3. Peer review or provide support during the completion of the next Risk Assessment completed by the risk owner

The audit results may be reviewed for any opportunities for improvement to the Risk Assessment process. This includes reviewing reported risks and updating risk ranges identified in this document to accurately reflect the current corporate risk tolerance, if needed. This may also feed back into the Risk Assessment methodology or management documents, including opportunities for clarity or refinement.

Staying current with industry standards and published best practices can help keep the Risk Methodology relevant. For example, a company may stay aware of internal and external changes that may impact a risk assessment, which may include changes to the product, systems or interfaces within the vehicle ecosystem, or industry evolution. It may sometimes be appropriate to deep-dive into the current processes and documentation to conduct a periodic review of the published content for relevancy to the current business or technology. Willingness to adjust to changes is important to remain relevant – internal changes in the organization, changes to the product, systems, interfaces, or external industry evolution may all have significant impact on the cyber risk assessment and evaluation process.

Appendix A: Glossary of Terms

Relevant terms used in this Guide are defined below.

TERM	DEFINITION
Attack Vector	A path or means by which a threat actor can gain access to the networks or assets to deliver a malicious outcome.
Enterprise Risk Management (ERM)	The process of planning, organizing, leading, and influencing the activities of an organization to minimize the effects of risk on an organization's capital and earnings. ERM covers financial, strategic, operational, cyber and other risks.
Impact	Estimate of magnitude of harm to stakeholders originating from a threat and/or attack
Incident	An occurrence that actually or potentially results in adverse consequences to a vehicle, connected infrastructure, or information that the vehicle processes, stores, or transmits and that may require a response action to mitigate the consequences.
Inherent Risk	The risk that an event would pose if no controls or other mitigating factors were in place (the gross risk or risk before controls).
Penetration Testing	The practice of testing a system, network or application to find vulnerabilities that a threat actor could exploit.
Post-Production Product	Vehicles that have been produced and sold to a dealer or end customer and are outside the OEM's ownership.
Risk Scoring	A quantitative and qualitative measuring process of risk based on a framework, which assigns a score to the risk according to a hierarchical grading system.
Residual Risk	The risk that remains after security controls are taken into account (the net risk or risk after controls).
Risk Profile	An evaluation of a company's risks, including the number of risks, type of risk, and potential effects of risks.
Risk Tolerance	The threshold of risk that an organization or individual is willing to accept without some form of response.
Threat Actor	A person or entity posing a threat to the vehicle ecosystem.
Threat Event	An event or circumstance, perpetrated by a threat actor, that has the potential to cause a negative impact to the vehicle ecosystem.
Vehicle Cybersecurity Risk	The likelihood of and potential impact from the exploitation of a vehicle ecosystem cybersecurity vulnerability in a threat event.
Vehicle Ecosystem	The components and infrastructure on or connected to the vehicle (e.g. hardware and software, intellectual property, mobile applications, customer data, vehicle data, supplier/manufacturing networks, applications, processes and organizations that directly or indirectly touch the vehicle and may play a role in vehicle cybersecurity).

Vulnerability	Weakness of an asset or control that can be exploited by one or more threats.

Appendix B: Additional References and Resources

The following References and Resources provide additional content and expertise for companies to consider in conjunction with the Best Practices discussed in this Guide.

REFERENCES – DOCUMENTS THAT MAY OFFER ADDITIONAL IMPLEMENTATION GUIDANCE
ISO/SAE 21434 - Road Vehicle Cybersecurity Engineering Standard (under development) <link>
Unified Compliance Framework (UCF), SANS Critical Security Controls <link>
NIST SP 800-30 - Guide for Conducting Risk Assessments <link>
SAE J3061 - Cybersecurity Guidebook for Cyber-Physical Vehicle Systems <link>
NIST Cybersecurity Framework <link>
EVITA - E-safety Vehicle Intrusion Protected Applications <link>
JSAE-JASO TP-15002 - (in Japanese currently) – Guideline for Automobile Information Security Analysis <link>
ISO/IEC 15408 – Information Technology - Security Techniques <link>
ISO/IEC 17799 – Code of Practice for Information Security Management <link>
ISO/IEC 27001 – Information Security Management Systems - Requirements <link>
ETSI Cyber Security Technical Committee (TC CYBER) ETSI TR 103 456 – Implementation of the Network and Information Security (NIS) Directive <link>
DOT HS 812 073 – NIST Cybersecurity Risk Framework Applied to Modern Vehicles <link>
ISO 31000:2009 – Principles and Guidelines on Implementation
ISO/IEC 31010:2009 – Risk Management – Risk Assessment Techniques
COSO (Committee of Sponsoring Organizations of the Treadway Commission) - Enterprise Risk Management Integrated Framework 2004

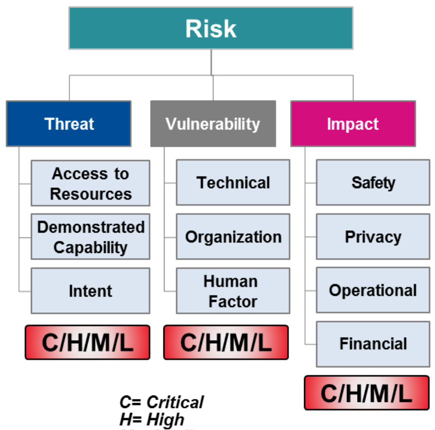
RESOURCES – ORGANIZATIONS THAT MAY OFFER ADDITIONAL INSIGHTS
European Telecommunications Standards Institute (ETSI) <link>
Common Vulnerability Scoring System (CVSS) <link>
International Organization for Standardization (ISO) <link>
Institute of Risk Management (IRM) <link>
ISA/IEC 62443 Cybersecurity Certificate Programs <link>
National Institute of Standards and Technology (NIST) <link>
National Highway Traffic Safety Administration (NHTSA) <link>
PMI PMBOK Guide <link>
Public Risk Management Association <link>
Risk Management Society (RIMS) <link>
SAE International <link>

Appendix C: Sample Risk Scoring Frameworks

This Appendix includes sample risk scoring frameworks. Note that companies may choose to use a wide range of frameworks, including those that differ substantially from the examples provided here.

Sample Vehicle Cybersecurity Risk Scoring Framework #1

Sample Risk Scoring Framework (Illustrative)



C= Critical
H= High
M = Medium
L = Low

Total Gross Risk Score

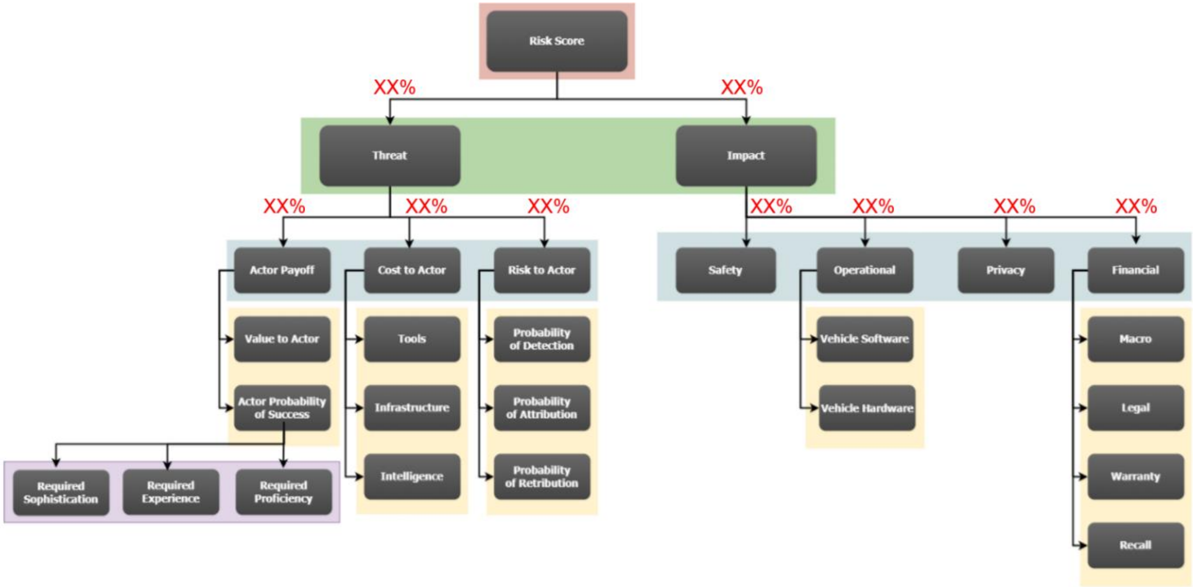
Threat (X*Y) + Impact (X*Y) + Vulnerability (X*Y) = Gross Risk Scoring = Y = C/H/M/L

Threat			
Factor	**Question**	**Weighting**	**Scoring**
Access	Do threat actors have access to the required resources?	X	Y
Capability	Has this event been successfully executed in the past?	X	Y
	Is it possible for this event to occur unintentionally?	X	Y
Intent	Has a threat actor publicly stated or demonstrated interest?	X	Y

Vulnerability		
Factor	**Weighting**	**Scoring**
Technical	X	Y per relevant vulnerability
Organizational	X	Y per relevant vulnerability
Human	X	Y per relevant vulnerability

Impact			
Factor	**Question**	**Weighting**	**Scoring**
Safety	Are the driver's and/or passenger's safety or wellbeing impacted?	X	Y
Privacy	Is the customer's privacy impacted?	X	Y
Operations	Are vehicle operations and vehicle features / services impacted?	X	Y
Financial	Is the company financially impacted?	X	Y

Sample Vehicle Cybersecurity Risk Scoring Framework #2



This Guide does not prescribe or require specific technical or organizational practices.
These are voluntary and aspirational practices, which may evolve over time.
Please see Section 1.2 for more information.

Appendix D: Acronyms

Auto-ISAC	Automotive Information Sharing and Analysis Center
CEO	Chief Executive Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CRO	Chief Risk Officer
CAN	Controller Area Network
CERT	Computer Emergency Readiness Team
COSO	Committee of Sponsoring Organizations
CVSS	Common Vulnerability Scoring System
ECU	Electronic Control Unit
EOL	End of Life
ERM	Enterprise Risk Management
ETSI	European Telecommunications Standards Institute
EVITA	E-safety Vehicle Intrusion Protected Applications
IEC	International Electrotechnical Commission
IRM	Institute of Risk Management
ISA	International Society of Automation
ISO	International Organization for Standardization
IT	Information Technology
JASO	Japanese Automotive Standards Organization
JSAE	Society of Automotive Engineers of Japan
NHTSA	National Highway Traffic Safety Administration
NIST	National Institute of Standards and Technology
NIS	Network and Information Security
OBD II	On-Board Diagnostics
OEM	Original Equipment Manufacturer
OTA	Over-the-Air

PII	Personally Identifiable Information
PMBOK	Project Management Body of Knowledge
PMI	Project Management Institute
RASIC	Responsible, Approve, Support, Inform, Consult
RMI	Risk Management Society
SAE	Society of Automotive Engineers
SME	Subject Matter Expert
TLP	Traffic Light Protocol
UCF	Unified Compliance Framework
USB	Universal Serial Bus