

AUTO-ISAC
AUTOMOTIVE CYBERSECURITY BEST PRACTICES

GOVERNANCE

Best Practice Guide
Version 1.3

Traffic Light Protocol: White.

This information may be shared in public forums.

GOVERNANCE

Traffic Light Protocol: White (May be shared in public forums)

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	17 August 2017	
v1.1	17 November 2017	Changed from TLP Amber to TLP Green for release to industry stakeholders via request on Auto-ISAC website
v1.2	19 July 2018	Changed from TLP Green to TLP White for release to the public via request on Auto-ISAC website
v1.3	01 July 2019	Performed periodic continuity and consistency refresh across all Best Practice documents

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.

Contents

Version History.....	i
1.0: Introduction	1
1.1 Best Practices Overview	1
1.2 Purpose	1
1.3 Scope	1
1.4 Audience	2
1.5 Authority and Guide Development	2
1.6 Governance and Maintenance	2
2.0 Best Practices	3
2.1 Framework for Governance in Vehicle Cybersecurity	3
2.2: Best Practices to Design a Vehicle Cybersecurity Program.....	4
2.2.1 Defining the Program's Scope	6
2.2.2 Articulating the Mission and Vision	7
2.2.3 Identifying Key Functions.....	7
2.3: Best Practices to Build a Vehicle Cybersecurity Program.....	8
2.3.1 Organizing "Within" – Activating Leadership and Decision Authority.....	9
2.3.2 Organizing "Within" – Creating a Staffing Model	10
2.3.3 Organizing "Within" – Staffing the Program	13
2.3.4 Organizing "Up and Across" – Integrating with the Business	14
2.3.5 Organizing "Up and Across" – Communicating with Executive Leadership.....	16
2.4: Best Practices to Operate a Vehicle Cybersecurity Program	16
2.4.1 Developing Policies and Processes.....	16
2.4.2 Managing Performance	17
2.4.3 Allocating Resources	18
Appendix A: Glossary of Terms	21
Appendix B: Additional References and Resources	22
Appendix C: Acronyms	23

1.0: Introduction

1.1 BEST PRACTICES OVERVIEW

This Best Practice Guide is one in a series 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 to the “Governance” function. Each company may use this Best Practices Guide as appropriate for their unique systems, processes, and risks.

1.2 PURPOSE

The purpose of this Guide is to assist auto industry stakeholders with developing governance functions for vehicle cybersecurity.

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 seeking guidance on how to govern their vehicle cybersecurity efforts. It contains best practices and implementation guidance for companies to design, build, and operate their vehicle cybersecurity programs. (Please note: this Guide uses the term “program” to denote the team, function, organization, business unit and/or set of related initiatives or activities, which is chartered with vehicle cybersecurity for a company.) These are voluntary, non-prescriptive, aspirational practices, which companies may use to determine an appropriate governance 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.



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, this Guide is most relevant for individuals who are tasked with leadership and management of vehicle cybersecurity efforts and senior executives who are working to determine how their business will address this emerging challenging area.

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	DENSO	Hyundai	Mobis
Auto Alliance	FCA	Infineon	Nissan
Bosch	Ford	Kia	NXP
BMW Group	General Motors	Lear Corporation	Subaru
Continental	Geotab	Magna	Toyota
Cooper Standard	Global Automakers	Mazda	Volkswagen
Cummins	Harman	Mercedes-Benz	Volvo
Daimler Trucks	Honda	Mitsubishi Motors	ZF
Delphi	Honeywell		

The Working Group also coordinated with several external stakeholders while developing this Guide, including NHTSA, NIST, CERT Coordination Center, and Aviation-ISAC.

1.6 GOVERNANCE AND MAINTENANCE

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

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

2.0 Best Practices

The purpose of this section is to define the primary elements of governance activities for vehicle cybersecurity and to provide implementation guidance and considerations for each area. Companies may augment these Best Practices with the References listed in Appendix B.

2.1 FRAMEWORK FOR GOVERNANCE IN VEHICLE CYBERSECURITY

The Governance framework for this Guide consists of three fundamental governance elements and associated activities: design, build, and operate, as depicted in Figure 2.

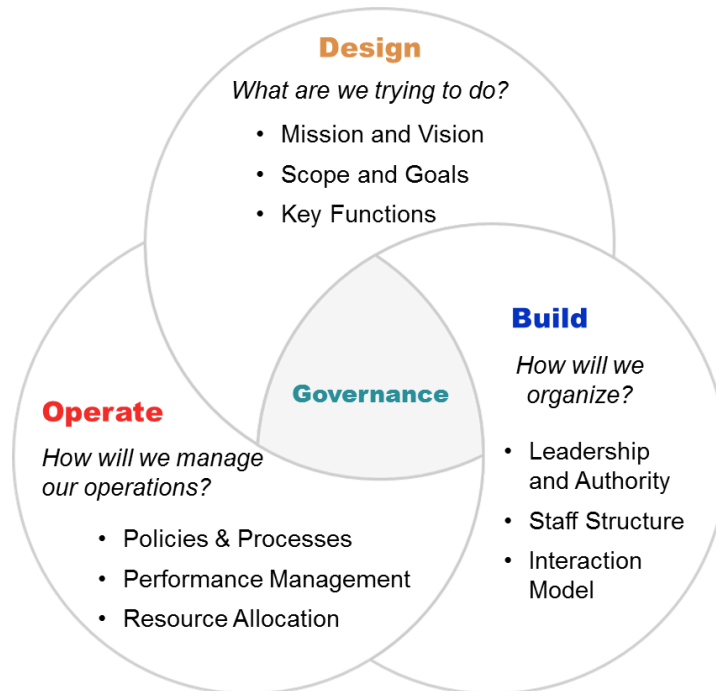


FIGURE 2: THREE CORE ELEMENTS OF GOVERNANCE

While these elements of governance are important for all programs, specific activities are most effective when they are customized to meet the unique needs of each company. Accordingly, this Guide does not prescribe requirements for program scope, organizational model, leadership structure or other governance factors. Instead, it describes decision factors that companies can use to determine what's appropriate for their unique risk landscape (Figure 3). Companies should evaluate all potential options while designing a vehicle cybersecurity program to identify the governance model that meets their needs.

Scope	Organizational Models	Leadership
<p>There is a very broad and diverse landscape a vehicle cybersecurity program may protect. For example, some may include services, manufacturing, supply chain, and back-office IT. Others may exclusively focus on the product.</p> <p>The goal is to ensure the full ecosystem is protected, regardless of where responsibility may fall.</p>	<p>Some programs may be matrixed, or geographically-, functionally- or domain-focused. Sometimes, vehicle cybersecurity may fit best in product engineering, but others may put it within a global cybersecurity organization, IT division, or compliance team.</p> <p>Overall, the organizational model works best when it fits the culture and risk landscape of the company.</p>	<p>Some companies may choose to elevate their vehicle cybersecurity leadership to the C-Suite. In other cases, vehicle cybersecurity leadership may fall under another organization.</p> <p>Clear authority, autonomy, and lines of communication across business leadership contribute to the success of a vehicle cybersecurity program.</p>

FIGURE 3: CONSIDERATIONS, NOT PRESCRIPTIVE REQUIREMENTS

2.2: BEST PRACTICES TO DESIGN A VEHICLE CYBERSECURITY PROGRAM

A vehicle cybersecurity program may be a team, function, business unit and/or set of related activities.

As companies design a program to protect vehicle cybersecurity, it can have broad responsibility within a company. Finding the best home for this key program within the company is a strategic decision that can have rippling effects on day to day operations and future strategic decisions.

In creating a vehicle cybersecurity program, companies may consider a current-state evaluation to consider critical functional, technical, and process interfaces with other teams when constructing the governance of this program. There will likely be overlap of responsibilities among vehicle cybersecurity and other teams within the company, such as IT Security, Corporate (enterprise or business) Physical Security, and Product Physical Security. Figure 4 below offers possible areas of responsibility for each of these functional work areas and possible areas of overlap between the different groups. Each company structure will be different, but identifying, understanding, and appropriately documenting these interfaces will facilitate robust vehicle cybersecurity within the corporation.

Companies may also consider existing cross-cutting functional team models like Safety and Quality, when determining how to design, build, and operate their vehicle cybersecurity programs. Vehicle cybersecurity may not need to reinvent the wheel and can learn from existing models within the company.

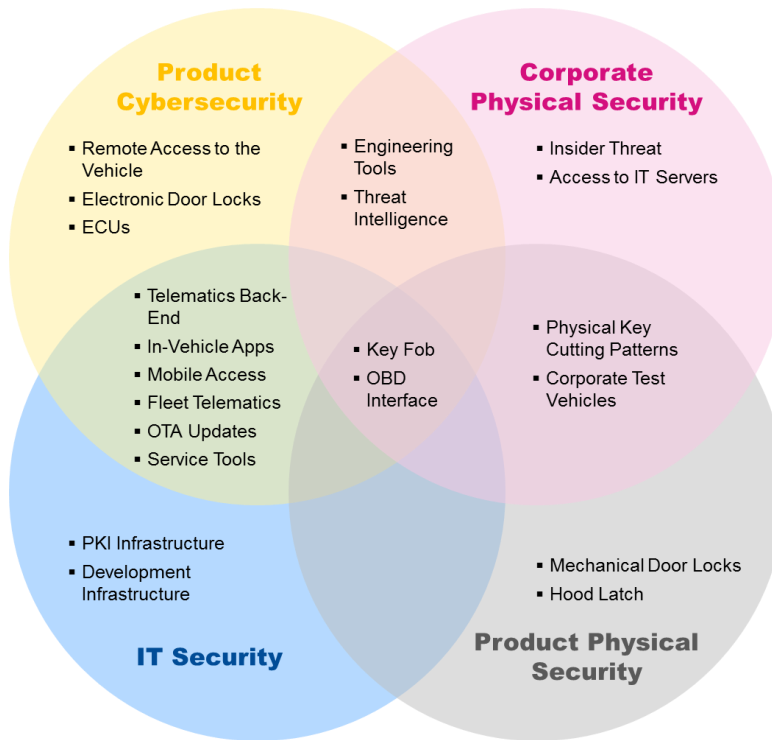


FIGURE 4: EXAMPLE INTERFACES WITH FUNCTIONAL WORK AREAS

This section addresses a core aspect of governing a vehicle cybersecurity program – determining what the program will be and what it will do. This includes best practices for determining the scope, mission, vision, and key functions of the program.

Specifics on where the program could sit and how to organize it (e.g. leadership, interaction model) are discussed further in section 2.3.

Best practices for designing a vehicle cybersecurity program include:

- Defining the program's scope
 - Program scope should be defined and communicated throughout the company
 - Responsibility for “out of scope” risk areas and activities that have potential to impact vehicle cybersecurity should be understood and defined
- Articulating the mission and vision
 - The program should have a mission and vision to guide operations
 - Specific goals (e.g. maturity or risk reduction targets) to achieve this mission and vision help define tactical plans and metrics for gauging program effectiveness
- Identifying key functions
 - The program should identify and prioritize core operational functions
 - These functions may fall entirely to the responsibility of the vehicle cybersecurity program. However, there are times where functions are operated better by different internal organizations; in these instances, the vehicle cybersecurity program determines how to coordinate and integrate with these operations

Detailed implementation guidance is below.

2.2.1 Defining the Program's Scope

When defining a vehicle cybersecurity program's scope, it is a best practice for companies to map out areas that make up the full potential scope of the program. Understanding the full vehicle ecosystem that needs to be protected helps companies determine responsibilities, while ensuring minimal gaps or confusion around accountability and authority. Once a company maps the full potential scope, companies may choose to narrow the program's scope to fit the company's needs and capabilities, sharing responsibilities with other stakeholders as appropriate.

Elements of the vehicle ecosystem that may be considered in-scope for a comprehensive program:

- Product design
 - Vehicle design and development lifecycle, including connectivity and embedded systems
 - Engineering tools (in-house or external)
- Production and supply chain
 - Vehicle and parts manufacturing
 - Supply chain
 - Diagnostic tools
- Connected services
 - Interfaces to telematics services and backend infrastructure (e.g. GPS and cellular networks)
 - Interfaces to vehicle and telematics infrastructure, including vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication
 - Interfaces to cloud services
 - Interfaces to third party applications
 - Interfaces to mobile applications
- Aftermarket and servicing
 - Aftermarket products and services
 - Maintenance
 - Servicing
 - Interfaces to aftermarket products
 - End of life support
- External
 - Government regulations and policy
 - Interaction with external stakeholders (e.g. law enforcement, academia)
 - Interaction with standards development organizations (e.g. ISO, SAE)
 - Cross-industry partnerships (e.g. Auto-ISAC)

Companies may consider other stakeholders in the scope definition discussion, such as executive management, legal, engineering, regulatory, and quality teams to help ensure that key stakeholders understand the impact and potential risks associated with scoping decisions.

When finalizing program scope, companies may want to consider:

- Company size
- Cybersecurity risk tolerance
- Cybersecurity sophistication

- Corporate risk management efforts
- Available resources
- Geographic spread of company divisions
- Geopolitical situation of the company
- Insourcing/outourcing strategies
- Demand from customers
- Existing structures and processes
- Cybersecurity areas outside of the company's control
- Existing company-wide governance programs

When a scope is agreed upon, clearly documenting and communicating what is in and out of scope with key stakeholders (including program staff, leaders of other business units, and suppliers) helps ensure business-wide understanding.

2.2.2 Articulating the Mission and Vision

Creating clear and accurate mission and vision statements for a vehicle cybersecurity program helps the company determine the program's place within the broader business. A strong mission statement articulates the program's overall purpose, while the vision can be more forward-looking to show what the program hopes to accomplish in the future. Mission and vision statements can help companies facilitate dialogue with both internal and external vehicle cybersecurity stakeholders.

For a vehicle cybersecurity program, the mission and vision statements could include a variety of potential themes, including:

- Customer safety, privacy, and peace of mind
- Customer requirements
- Security build-in to the vehicle design
- Threat detection and prevention
- Vehicle-related incident response and recovery
- Risk management
- Continuous improvement
- Data protection
- Government engagement and regulatory compliance
- Brand protection

To bring this mission to life, companies may also consider setting appropriate goals to drive operations. These may include maturity or risk reduction targets.

2.2.3 Identifying Key Functions

Identification of the program's specific functions or capabilities allows stakeholders to define core activities to protect the identified ecosystem.

A program's functions do not have to be exclusively operated by program staff; responsibilities can be shared with other internal groups or outsourced to third party organizations with specific expertise.

A vehicle cybersecurity program may consider taking on the following functions:

- **Cybersecurity Risk Management** – understanding and assessing vehicle cybersecurity risk areas to prioritize resource allocation, determine appropriate investment, measure program success, and communicate outcomes
- **Policies and Requirements** – establishing security policies and requirements for designing, manufacturing, and deploying vehicles
- **Cybersecurity Compliance** – validating that internal policies, standards, federal/state legal, and regulatory compliance are being met
- **Cybersecurity Engineering** – designing, developing, and deploying cybersecurity solutions to protect the vehicle ecosystem
- **Cybersecurity Research** – identifying new cybersecurity methods, features, attacks, and control requirements, both through internal efforts and external engagements (e.g. working groups, information sharing organizations, collaborations with academia and start-ups)
- **Secure Development** – establishing secured vehicle development lifecycle activities, tasks, and standards (e.g. threat modeling, secure development)
- **Third-Party Collaboration** – engaging with external entities for voluntary information sharing activities, events, and programs to benefit from external expertise and partnerships to enhance vehicle cybersecurity
- **Vehicle Cybersecurity Monitoring** – continuous monitoring of products in the development cycle and in the field via intelligence gathering and other available methods and proactively detecting and identifying threats
- **Security Analytics** – developing and/or deploying tools and capabilities to more efficiently understand risk, security posture, and trends
- **Cybersecurity Testing** – functional security testing and penetration testing of products (may include activities like static analysis and code reviews) as part of pre- and post-launch secure development
- **Cybersecurity Incident Response** – identifying, triaging, containing, and remediating all vehicle cyber-related incidents throughout the product lifecycle
- **Security Training and Communications** – providing internal security training and awareness programs to help ensure that relevant staff are knowledgeable about security best practices and cultivate interest in cybersecurity
- **Performance Management and Reporting** – establishing performance tracking and reporting processes for senior leadership

Companies may choose to start with a small core set of functions and evolve over time to include more advanced functions to keep pace with the evolving risk landscape. The key is to help ensure that an appropriate set of functions is in place and that responsibilities and authorities are clear.

2.3: BEST PRACTICES TO BUILD A VEHICLE CYBERSECURITY PROGRAM

This section defines best practices for organizing a vehicle cybersecurity program. This includes shaping the internal program (organizing “within”) and determining the ways that the program will interact with the broader enterprise (organizing “up and across”).

Best practices for building a vehicle cybersecurity program include:

- Organizing “within”:

- There is identified leadership with appropriate authority, accountability, and budget to drive vehicle cybersecurity for the business
- Decision authorities are identified, understood, and clearly documented
- The organizational hierarchy, including roles and responsibilities, is clearly organized, documented, and articulated
- A core vehicle cybersecurity program—regardless of how it is structured and organized—exists to help ensure consistency, focus, and coverage across the company’s risk landscape
- Organizing “up and across”:
 - The program has identified critical collaborative relationships with other business units and assigned Points of Contacts (POCs) to manage each relationship
 - There is an integration plan to operationalize interaction points between vehicle cybersecurity and other business functions
 - There are defined decision authorities for situations that will involve input from outside the core vehicle cybersecurity program
 - There are established protocols for when and how to escalate information and decisions to company leadership

Detailed implementation guidance is below.

2.3.1 Organizing “Within” – Activating Leadership and Decision Authority

Establishing program leadership and bestowing it with an appropriate level of authority can help drive effective decision-making.

Features of effective program leadership may include:

- Authority to make decisions (budget and personnel), allocate resources, and resolve issues and conflicting priorities
- Processes for vehicle cybersecurity operations, including escalation and coordination across business units, as needed
- Visibility into different regional or functional groups
- Direct access to executive management

While a single vehicle cybersecurity organizational alignment may not work for every company, there are several options for leadership positioning, including:

- **At the executive level** – the leadership of the program reports directly to the company CEO
- **Directly under one executive** – the leadership of the program reports to an executive-level (i.e. C-suite) individual who runs a related business unit, such as the Chief Information, Product, Technology, Risk, or Security Officer
- **Directly under multiple executives** – the leadership of the program reports to multiple company leaders across functional or geographic domains

Companies may also consider a variety of options for the vehicle cybersecurity program’s leadership structure, including:

- **A single vehicle cybersecurity program leader** – in this model, one individual is implemented at the top of the program’s leadership hierarchy. Typically, this person is

accountable for the program's ultimate performance and serves as the primary interface with company leadership. Having one individual serve as the internal and external "face" of the program can help instill and communicate a singular vision for the program. However, it may be helpful to give others in the leadership chain authority over certain decisions to prevent a bottleneck.

- **A leadership team with multiple leads that each report "up and across"** – in this model, the vehicle cybersecurity program is split into functional or geographic domains, each led by an individual that reports up to domain or company leadership. This model allows each leader to focus on a specific area of expertise or familiar market without assuming responsibility for an expansive global program covering a wide variety of functions. In situations where program decisions affect multiple program domains, however, this model may require a greater engagement from company leadership "above" the program. It may require close coordination and proactive information sharing to minimize organizational barriers, gaps, and duplicate efforts.

2.3.2 Organizing "Within" – Creating a Staffing Model

Organizational models define lines of authority and clarify roles and responsibilities across the vehicle cybersecurity program.

There are several types of common organizational models from which companies can choose. Companies may adopt aspects of different models in designing a vehicle cybersecurity program that fit companies' specific needs. Common organizational models include:

Functional Model

The Functional Model (also known as a dispersed model) is a hierarchical structure wherein people are grouped by their area of specialization, based on common job functions. A functional manager with expertise in the same field supervises these personnel. This expertise allows the supervisor to effectively utilize the skills of the employees, which ultimately assists in achieving the company's business objectives. In an automotive company, this model would allow each team to focus on the product, technology, or service it is responsible for delivering, with cybersecurity as a "by-product." For example, in this model, an engineer responsible for the Body Control Module would also be responsible for handling security requirements associated with that product. Similarly, in this model, budgeting and resource allocation authority will often stay within the same functional unit.

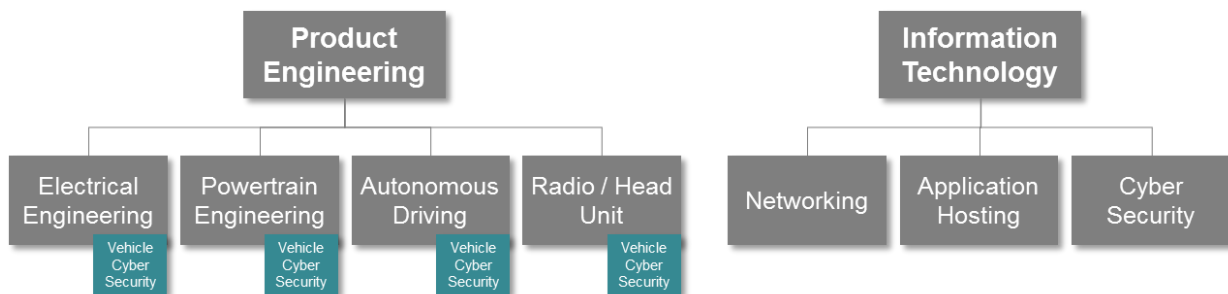


FIGURE 5: EXAMPLE OF FUNCTIONAL ORGANIZATIONAL MODEL

- **Benefits:**
 - Promotes high performance and efficiency in individual job functions
 - Enables a well-defined work scope, reducing the risk of duplicated efforts

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.

GOVERNANCE

Traffic Light Protocol: White (May be shared in public forums)

- Allows for a single authority and simple communications channels
- Ability to impact product design decisions at the appropriate times in the lifecycle
- **Challenges:**
 - May deter coordination between business units or departments
 - Decreases likelihood of knowledge transfer and sharing of best practices or lessons learned
 - Limits leadership visibility into broader security posture

To tackle these challenges, companies may consider establishing formal lines of communication between key organizations like Vehicle Cybersecurity and IT Security.

Geographic Model

The Geographic Model (also known as a regional or divisional model) is an option for companies that function in a large geographic area or have different types of products or market areas. Each division is structured and capable of operating like a small organization within the umbrella of the larger company, equipped with its own resources to function independently. This means that each region governs its own cybersecurity program, responsible for overseeing the products and services produced within that region.

To organize this work across the regions, companies may institute a Global Vehicle Cybersecurity Lead. The global office might be responsible for broad cybersecurity policies and priorities, resource allocation, best practices identification and management, and overall governance. The local regional office is specific to that market (or regional product), focused on key risk factors and priorities for local consumers. There are specific cybersecurity risks that are regional (e.g. telematics systems, cellular networks), and those may be addressed at the regional level. However, there is often interaction between regional cybersecurity activities and the global office to assist in addressing priorities.

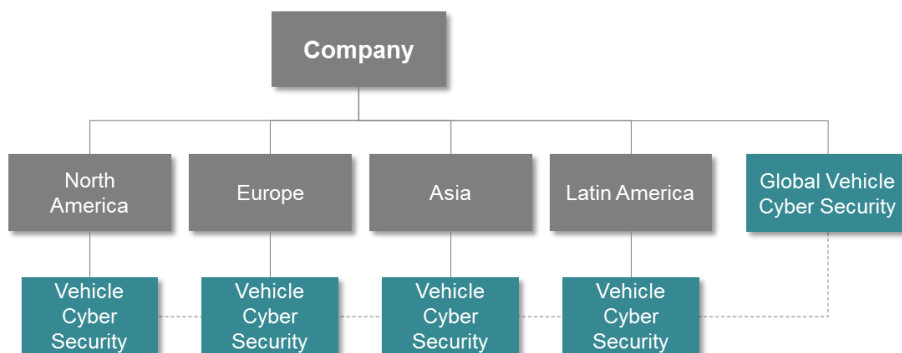


FIGURE 6: EXAMPLE OF GEOGRAPHIC ORGANIZATIONAL MODEL

- **Benefits:**
 - Allows cybersecurity managers to be near sources of supply or regional variations
 - Enables customization to unique market-based products and services
 - Promotes close coordination with other relevant business units in the region
 - Allows regional programs to focus on local consumer priorities
- **Challenges:**
 - Dispersed programs could lead to incompatible or inconsistent systems at the enterprise level

GOVERNANCE

Traffic Light Protocol: White (May be shared in public forums)

- May lead to inadvertent duplication of activities
- May cause challenges when security conflicts with functionality, timing, or cost

Matrix Model

The Matrix Model is a hybrid of multiple structures (e.g. functional and divisional). Typically used in global companies, this structure gives the employee both horizontal and vertical lines of communication where there is often part of a functional reporting line as well as a region-based reporting line. Employees function as shared resources amongst different projects and functional units thereby allowing their knowledge, skills, or talents to be shared between the functional department and regional team.

- **Benefits:**
 - Allows for improved communication across the broader team due to employees participating on both functional and geographic teams
 - Provides flexibility, allowing companies to create a hierarchy that accounts for geographic dispersion and product specificity
- **Challenges:**
 - Can create conflict when decisions involve two reporting hierarchies and competing projects and priorities
 - Requires effective communication between managers
 - May be difficult for larger companies to formulate policies or speak externally with a single voice

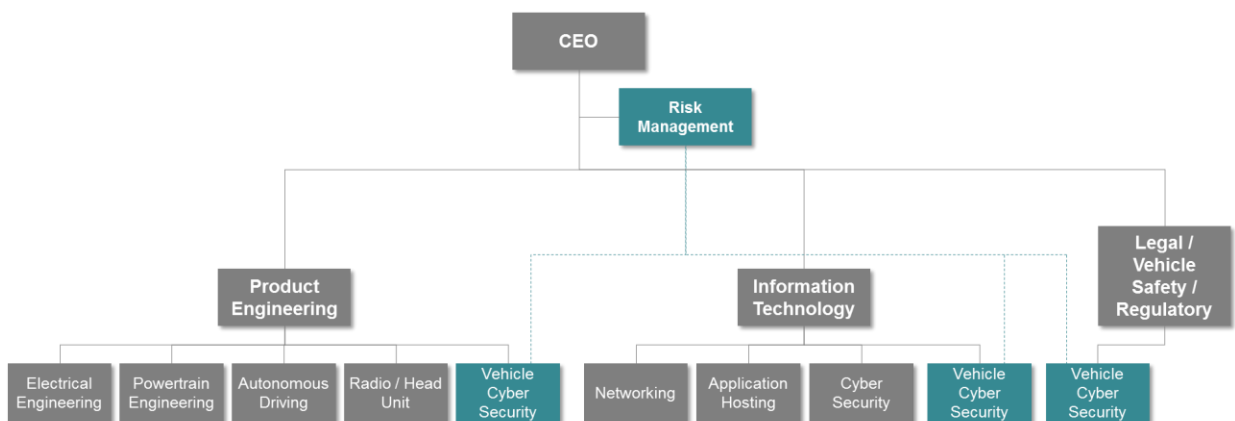


FIGURE 7: FIRST EXAMPLE OF MATRIX ORGANIZATIONAL MODEL

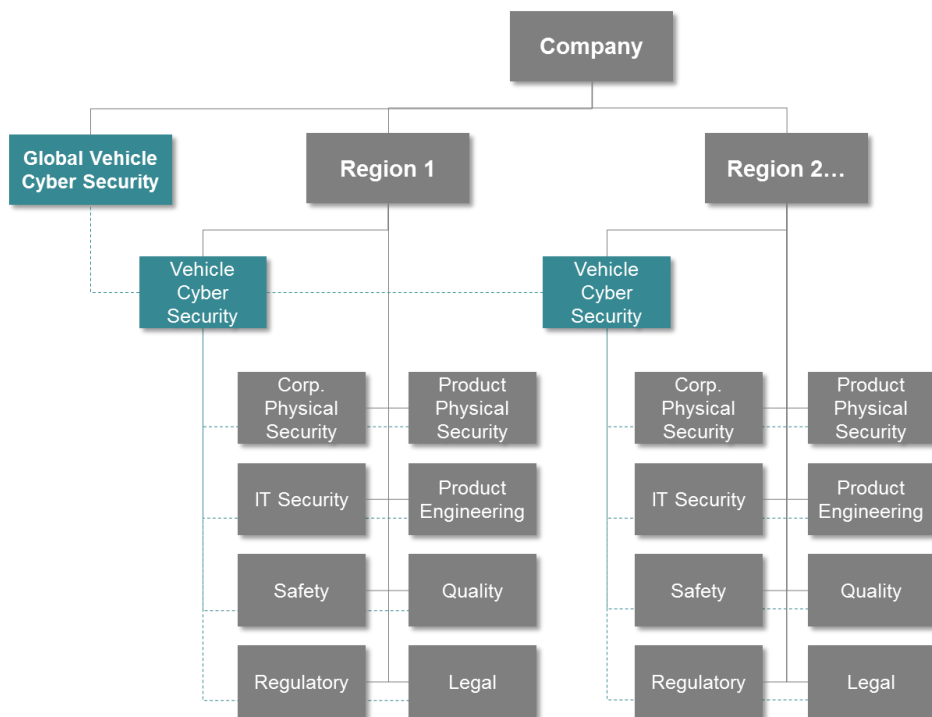


FIGURE 8: SECOND EXAMPLE OF MATRIX ORGANIZATIONAL MODEL

Regardless of which staffing model a company uses, a core dedicated security program can help ensure consistency and coverage across the company's full risk landscape.

2.3.3 Organizing “Within” – Staffing the Program

To help ensure recruitment efforts are efficient and targeted, program leaders may consider including these areas of expertise, as relevant, in job descriptions. Example areas of expertise to consider including in a vehicle cybersecurity program includes:

- Product design
 - Product development engineering
 - Systems engineering
 - Vehicle and IT networks
 - Mobile applications
 - Application development
 - Product development lifecycle
 - Systems development lifecycle (SDLC)
 - Connectivity
- Cybersecurity
 - Embedded systems security
 - Security policy development, enforcement, and management
 - Incident response
 - Network security

- Public Key Infrastructure (PKI)
- Cloud security
- Security development lifecycle
- Cybersecurity controls
- Cybersecurity strategy
- Red team and penetration testing
- Cybersecurity research
- Cryptography
- Hardware security
- Threat intelligence
- Data Forensics
- Threat modeling
- Validation engineering
- Identity management
- Governance and risk management
 - Corporate governance
 - Risk management
 - Lifecycle management
 - Program/project management
 - Document management
 - Compliance
 - Communications
- Other
 - Security education
 - Data science
 - Artificial intelligence
 - Computer engineering
 - Electrical engineering
 - Mathematics
 - Software engineering

Very few individuals are likely to join the program with a perfect combination of experiences and skills for their role. This makes it important for programs to consider how to cultivate the balance of technical and strategic skills across IT and product domains. They may consider informal mentorship programs, on-the-job training, onboarding training, lunch-and-learns, conferences, and other programs to foster staff growth.

2.3.4 Organizing “Up and Across” – Integrating with the Business

Securing the vehicle ecosystem involves developing, validating, communicating, implementing, and testing security that can come from many internal and external sources. Cybersecurity requires an “all hands on the deck” mindset—where everyone across the business understands its importance and their role in its enforcement.

Internal groups with which vehicle cybersecurity programs may collaborate include:

- C-Suite
- Board of Directors

- Safety
- Product Quality
- Product Development
- Research and Development
- Electrical, System, and Software Engineering
- Manufacturing
- Purchasing/Supply Chain
- Aftermarket/Vehicle Servicing
- IT
- IT Security
- Legal
- Corporate Communications
- External Communications
- Public Policy
- Government and Regulatory Affairs
- Privacy
- Audit
- Enterprise Risk Management
- Human Resources
- Customer Service
- Training
- Finance
- Marketing

The program's interactions with these groups will vary. Coordination with some groups (e.g. Legal, IT Security, Product Design, Engineering) may be important as part of the day-to-day functions of the program, while others may only be engaged for specific activities (e.g. incident response). In either case, preemptively establishing communication channels and interaction models enables vehicle cybersecurity programs to effectively and efficiently work with its stakeholders.

Best practices for communicating across internal business units include:

- Identifying one or several POCs within the cybersecurity program responsible for sharing information with appropriate team members in other units
- Creating and approving processes and mechanisms for propagating information
- Establishing and using common terms and processes (e.g. sourcing activities, incident response) with all business units
- Using enterprise change management tools when appropriate
- Creating a secure file management and versioning structure and location to share status updates and documents that must be shared outside the program
- Running tabletop exercises and wargames with key POCs in other business units to prepare for high-stakes situations and help non-security stakeholders understand their role in incident response processes

2.3.5 Organizing “Up and Across” – Communicating with Executive Leadership

Vehicle cybersecurity programs will communicate up to company leadership in several instances, such as during periodic risk, performance, and incident response reporting. Effective upward relationships benefit from clearly defined expectations and processes. This may include:

- Defining triggers, cadence, mechanisms, and content of leadership communications
- Identifying a POC for propagating incident information; the POC will be responsible for following organizational protocols in communications and elevating information to executive leadership
- Informing any other internal business units who may be affected by leadership decisions stemming from the communication before communicating up (unless information is sufficiently urgent to warrant immediate action)
- Periodically connecting with leadership face-to-face by holding in-person workshops and exercises to help manage geographic, cultural, and language barriers

2.4: BEST PRACTICES TO OPERATE A VEHICLE CYBERSECURITY PROGRAM

The purpose of this section is to define best practices for operating a vehicle cybersecurity program efficiently and effectively. These include:

- Developing consistent processes and policies
 - Policies and processes are clear, easy-to-follow, well-known, and available to those who must comply with them, both within and external to the vehicle cybersecurity program, and who are responsible for approving exceptions
 - Policies and processes are reviewed regularly and updated as needed
- Managing performance
 - Performance metrics and Key Performance Indicators (KPIs) are aligned to program goals and derived from available data
 - Key roles (e.g. performance reviewer, sources of input) are assigned in the performance management process, and individuals are aware of their responsibilities
- Allocating resources effectively
 - Resource allocations are carefully considered based on relevant organizational factors
 - Resource allocations are periodically reviewed and realigned based on consistent criteria (e.g. performance, risk reduction, ROI)

Detailed implementation guidance is below.

2.4.1 Developing Policies and Processes

Cybersecurity is a broad and multi-faceted area that benefits from a holistic governing perspective. It benefits from attention at every phase of operation, including quoting, planning, requirements, design/definition, implementation, and validation phases. It is beneficial for everyone responsible for vehicle cybersecurity to have a common understanding of what to do in certain cybersecurity-related situations (e.g. responding to an incident, managing a vulnerability, reacting to public disclosures). A strong vehicle cybersecurity program benefits from a culture of stability, transparency, traceability, and accountability.

For all these reasons, establishing, executing, and monitoring policies and processes is important to a vehicle cybersecurity program's success. Some example types of policies and processes are:

- Incident Response
- Vulnerability Management
- Security Testing (e.g. penetration testing)
- Supply Chain or Design Requirements
- Requirements and Compliance Verification and Validation
- Information Management
- Ongoing Operation
- Threat and Risk Analysis
- Secure Development Standards
- Key Management Systems
- Performance Management (see section 2.4.2)
- Coordinated Vulnerability Disclosure
- Information Sharing Policies
- Other Public-Facing Policies

When establishing these policies and processes, program leadership may want to consider:

- Consistently documenting processes for distribution to relevant stakeholders
- Involving dedicated experts in the process, with support and input from relevant groups within the company (e.g. Legal, Product Quality, Public Relations, Safety), especially where there may be functional overlap or synergy
- Periodically reviewing and updating policies and processes to help ensure they are up to date with security best practices, requirements, standards, and changes to the business
- Aligning policies and processes to commonly used frameworks (e.g. NIST Cybersecurity Framework, SAE J3061) and, when appropriate, relevant industry standards (e.g. ISO 27000)
- Ensuring traceability of detailed processes and procedures to higher-level policies
- Embedding policies and processes into project management, systems development life cycle, corporate policy manuals, or service management processes
- Attempting to incorporate policies into supplier contracts and requirements that impact vehicle cybersecurity
- Establishing process adherence (or compliance) mechanisms to ensure cybersecurity policies and processes are followed

2.4.2 Managing Performance

Cybersecurity is a constantly evolving field, so a successful vehicle cybersecurity program may regularly evaluate and improve its operations to meet dynamic requirements. This typically involves a well-defined performance management system that allows leaders to assess the program's effectiveness.

Though the output of the program – the ultimate security of the product or system it's designed to protect – is an important metric, leaders will benefit from assessing other aspects of the program to identify inefficiencies and areas with potential to improve. It may help to align performance management with the holistic security method the program has identified, such as the

Cybersecurity Engineering Process (CEP) or Cybersecurity Design Lifecycle (CDL). Companies may want to consider:

- Creating a method that is agnostic to how the program establishes security roles, so it can continue to be used if/when the structure of the program shifts
- Assigning key performance management responsibilities, including the “metrics producer” (the individual(s) that compute key metrics based on performance management tools), the “process responsible” (the individual(s) that are responsible for elements of CEP/CDL that impact metrics), and the “metrics consumer” (the individual(s) that judges the program’s performance based on metrics reviews)
- Creating transparent and consistent KPIs that are distributed across all elements of the program and comply with the defined CEP/CDL, if applicable
- Acquiring performance management tools that align with program KPIs and organizational goals
- Ensuring that data collection is occurring in all areas and levels of the program, including the lowest levels of the staffing hierarchy
- Including formal goal setting and evaluation procedures that include a wide variety of stakeholders, particularly the “metrics producers” and “process responsible”

Some example metrics that a vehicle cybersecurity program may measure against include:

- Progress against key milestones and timelines at the functional level
- Risk assessments (e.g. potential impact of threats, vulnerabilities)
- Net risk and reduction method metrics
- Automotive Software Process Improvement and Capability Evaluation (ASPICE) levels
- Levels of compliance against internal requirements
- Penetration testing results (see the Auto-ISAC’s *Risk Assessment and Management Best Practice Guide* for more information)
- Incident response and vulnerability remediation
- Supplier performance against requirements
- A software security model (e.g. BSIMM)
- Sharing of vehicle cybersecurity information with the industry

2.4.3 Allocating Resources

Based on the mission, key functions, and structure of the program, leaders determine what resources the program needs and how to allocate them. Performance management processes help leaders to adjust those resources over time to address gaps and maintain success.

Resources can be broken out into three categories: monetary, personnel, and material. The **monetary** category is straightforward – it is the capital that the program has at its disposal to hire personnel, purchase equipment, invest in initiatives or activities that can help mature the program, reserve for use for urgent/emergency activities, and cover administrative costs, such as travel, lodging, employee welfare activities, communications, and office supplies.

Examples of **personnel resources** include:

- **Leadership** – senior management who are ultimately responsible for answering to executive leadership regarding the program’s performance

- **Security Experts** – individuals with security expertise in key functional areas, including systems engineering (hardware, software), penetration testing, SDLC evaluation, security architecture, in-vehicle networks, manufacturing, vehicle, or product design, etc.
- **Process Architects** – individuals who will design and document the relevant cybersecurity policies for each functional area
- **Project Managers** – individuals who will oversee process users on a day-to-day basis and be responsible for delivering quality results on time
- **Change Agents/Instructors** – individuals responsible for managing change within the program, including overseeing training
- **Process Users** – individuals who will implement the program's processes in their daily jobs
- **Third-Party Resources** – external testing, audit, and consulting firms who can augment expertise and provide independent performance reviews

Examples of **material resources** include:

- Labs and testing facilities
- Security operating centers (SOCs) and relevant equipment and subscriptions
- Test vehicles
- Production vehicles
- Vehicle components (hardware and software)
- Work benches
- Threat modeling tools
- Supply chain management programs
- Risk management tools
- Contingency planning tools

How and when to allocate these resources will depend on many factors. Factors and questions that leaders may want to consider when allocating resources include:

- **Organizational Structure/Culture** – is the program structured to centralize cybersecurity functions or is it distributed so individual groups/departments own specific aspects? Is there a parent organization that would define overarching/product related policies around cybersecurity or does the program have authority to define internal processes?
- **Organizational Maturity** – is the program just starting to organize around vehicle cybersecurity? Is there a mature cybersecurity organization (e.g. Enterprise IT) that it can leverage?
- **Fit with Existing Processes** – can the company leverage existing processes to encompass cybersecurity or will there be a separate set of processes that will need dedicated resources?
- **Existing Skill Sets** – does the company have the right skill sets to meet the cybersecurity needs or is new personnel needed?
- **Training** – does the company already have a cybersecurity skill set that can be leveraged or is additional training needed?
- **Supplier Relationships** – is the company tied to a specific supplier or can they select from different suppliers to support their cybersecurity needs?



GOVERNANCE

Traffic Light Protocol: White (May be shared in public forums)

- **Funding/Budget** – is there a specific budget for cybersecurity or does it come out of each department when funding is available?
- **Past Performance** – how has the function/program performed to date? Are there significant gaps that need to be addressed? Does the existing level of resources match the output of a function or program?
- **Executive Vision** – what is the target maturity of the program compared to the industry? what are the top-line goals that the leadership has set for the vehicle cybersecurity program?
- **Time for Non-Security Personnel** – what additional overhead costs are added when non-security engineers must support security work as part of their role?
- **Lessons Learned** – has the program already been impacted by a cybersecurity incident? Is there a culture of learning from other organizations?
- **Regional Considerations/Market-Based Priorities** – is the consumer concerned with cybersecurity aspects of the vehicle? Does this vary in different international markets?
- **Function/Program Impact** – how critical and/or impactful is a certain area to the overall program's mission and objectives? How critical is it to customer satisfaction and safety?
- **Organizational Changes** – have major changes taken place in the broader company or in the program's geographic or functional domain that could affect the program's resource allocation or needs?
- **Public Relations Potential** – how likely is a function or program to impact the company's brand and relationship with the public?

Revisiting the factors and questions above on a regular basis helps programs evaluate effectiveness of resource allocation decisions to adjust for efficiency.

Appendix A: Glossary of Terms

Relevant terms used in this Guide are defined below.

TERM	DEFINITION
Performance Metrics	Quantifiable measures that are used to track and assess the status of a program's behavior, activities, and processes against defined objectives; it should support a range of stakeholder needs from leadership, customers, shareholders to employees
Secure Development	Use of assurance processes, controls, and tools in the development lifecycle of technical systems to ensure systems (hardware and software) are designed, built, operated, and disposed of in accordance with security policies and address security compliance requirements
Tabletop Exercises	Tactical training tools that focus on particular issues and known threats and test a particular portion of a company's ability to coordinate response procedures
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).
Vehicle Cybersecurity	The activities, processes, and capabilities that protect, detect, and respond to cybersecurity occurrences (e.g. remote control, unauthorized access, disruption, manipulation) that actually or potentially result in adverse consequences to a vehicle, connected infrastructure, or information that the vehicle processes, stores, or transmits
Vehicle Cybersecurity Program	This non-prescriptive term is used in this Best Practice Guide to denote the team, function, business unit and/or set of related initiatives or activities, which is chartered with vehicle cybersecurity for a company
Wargames	Enterprise-wide training and testing tools aimed at analyzing broad incident response capabilities and quantifying strategic impacts of key decision-makers across a company

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
NHTSA – Cybersecurity Best Practices for Modern Vehicles < link >
NIST – 800 Series < link >
NIST – Cybersecurity Framework < link >
NIST – NICE Cybersecurity Workforce Framework < link >
NIST – National Initiative for Cyber Security Education: Best Practices for Planning a Cybersecurity Workforce < link >
US-CERT National Initiative for Cybersecurity Careers and Studies < link >
SEI / Carnegie Mellon University – Structuring the Chief Information Security Office Organization < link >
Harvard Business Review – The New Path to the C-Suite < link >
SAE J3061 – Cybersecurity Guidebook for Cyber-Physical Vehicle Systems < link >
RESOURCES – ORGANIZATIONS THAT MAY OFFER ADDITIONAL INSIGHTS
Auto-ISAC < link > (For sharing potential vulnerabilities, threats and other information. You are not required to be a Member to share information with Auto-ISAC. Membership eligibility information is also available on the link provided.)
Institute of Electrical and Electronics Engineers (IEEE) < link >
International Organization for Standardization (ISO) < link >
SAE International < link >
US-CERT < link >
Software Engineering Institute (SEI) CERT Division < link >
National Institute of Standards and Technology (NIST) < link >
NIST National Initiative for Cybersecurity Education (NICE) < link >

Appendix C: Acronyms

ASPICE	Automotive Software Process Improvement and Capability Evaluation
Auto-ISAC	Automotive Information Sharing and Analysis Center
Aviation-ISAC	Aviation Information Sharing and Analysis Center
BSIMM	Building Security in Maturity Model
CDL	Cybersecurity Design Lifecycle
CEO	Chief Executive Officer
CEP	Cybersecurity Engineering Process
C-Suite	Chief Executives Suite
GPS	Global Positioning System
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Organization for Standardization
IT	Information Technology
KPI	Key Performance Indicators
NHTSA	National Highway Traffic Safety Administration
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
OEM	Original Equipment Manufacturer
OTA	Over-The-Air
PKI	Public Key Infrastructure
POC	Point of Contact
ROI	Return on Investment
SAE	Society of Automotive Engineers
SDLC	System Development Lifecycle
SEI	Software Engineering Institute
SOC	Security Operations Center
TLP	Traffic Light Protocol
US-CERT	United States Computer Emergency Readiness Team



GOVERNANCE

Traffic Light Protocol: White (May be shared in public forums)

V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle