ISO 21434 Self Assessment Questionnaire

Authored by

AJ Khan, CISSP, CISA, PCIP, MBA

CEO, Vehiqilla Inc

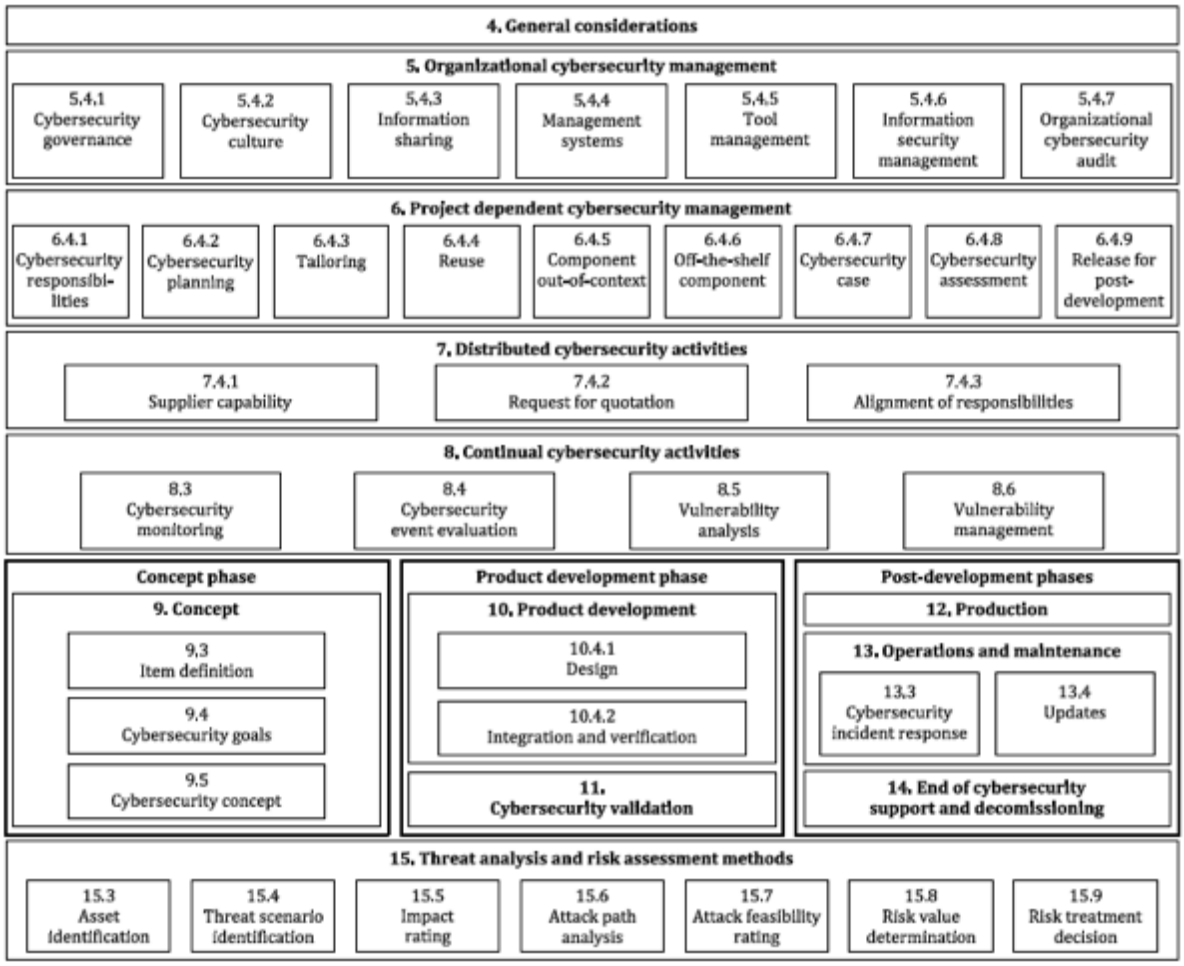
This Self Assessment Questionnaire (SAQ) has been developed to ensure understanding of your organization's preparation for compliance with the ISO 21434 Standard.

What is ISO 21434

ISO 21434 is formally called the Road Vehicles -- Cybersecurity Engineering Standard. It has been jointly developed by the International Organization for Standardization (ISO) and the Society for Automotive Engineers (SAE). The aim of this standard is to develop common terminology and criteria around key aspects of cybersecurity for the Automotive Sector. This standard helps identify the methodology which can be used to enable cyber controls in all aspects of vehicle development and operations. This means that by applying the controls available in the standard, companies will be able to demonstrate due care and due diligence related to cyber-threat prevention in vehicle development, operations, maintenance, and disposal.

Figure 1: ISO 21434 In Scope Activities

The below figure shows the overall structure of the standard



Source: ISO 21434 Road Vehicles Cybersecurity Engineering Standard

Threat Analysis & Risk Assessment (TARA)

An important aspect of the ISO / SAE 21434 Standard is the emphasis placed on Threat Analysis and Risk Assessment (TARA). The results of this assessment guide the activities in the product development stage of the vehicle and enable the adoption of Cyber Controls to safeguard the vehicle during its lifecycle. As is common with most cyber best practices, the standard emphasizes the need for a TARA, it does not describe a specific methodology for carrying out the TARA.

Cyber Security Management System

The standard also describes the overall in-vehicle cybersecurity architecture and mandates several processes that must be in place in the organization as well as in the supply chain. This means that any organization must develop a Cyber Security Management System (CSMS) to be compliant with the standard. Specific controls such as policies, procedures and technical controls must be designed to implement such an ISMS. However, the standard itself does not propose any specific technologies.

Cyber Assurance Levels

ISO21434 has utilized the concept of Cybersecurity Assurance levels (CALs) classification scheme that can be used to provide "Assurance" and "Trust" on the level of Cybersecurity embedded into the Vehicle components and the Vehicle itself.

Assurance is the measurement of correctness and a judgement of a system's effectiveness of security functionality. Basically, it is the Degree of Confidence in the Cybersecurity implementation of the system.

A *Trusted System* is designed and implemented in such a way that hardware, firmware, Operating System, and software together effectively support the security policy.

Demonstration and Evaluation of Supplier Capability

A critical component and far-reaching component of ISO 21434 is the focus on Supplier capability from an Automotive Cybersecurity perspective. Clause 7.4.1 specifically asks for the following

"evidence of the organization's capability concerning cybersecurity (e.g., cybersecurity best practices from the development, post-development, governance, quality, and information security);

This statement has two major implications. First, OEMs and Suppliers need to ensure that they have an adequate Supplier Cyber Assessment Program and second, Automotive Organization's have specific evidence of the organization's capabilities concerning cybersecurity.

Work Products

Several Work Products (WP) are required for each module of the Standard to enable cybersecurity activities in the organization as part the implementation of this standard. These Work Products (WP) are enumerated in the ISO 21434 Self-Assessment Questionnaire.

Section 5: Organizational Cybersecurity Management

This section outlines the steps needed to ensure overall Cybersecurity Governance in the Organization. It also enumerates the steps that are needed to change the overall Organization Culture to make it more Cyber aware.

Work Product	Questions to be asked	Compliant	Non-Compliant
[WP-05-01] Cybersecurity policy, rules, and processes	Does the Organization have a cybersecurity policy that acknowledges the road vehicles cyber risks and the Executive Management's commitment to protecting the Organization assets from these risks to the Organization?		
	Does the Organization have a formal Cyber Security Management System (CSMS) in place?		
	Does the Cyber Security Management System (CSMS) enumerate all relevant Cyber rules & processes, Cyber responsibilities & the resources needed to enable Cyber in the Organization?		
	Does the Cyber Security Management System (CSMS) assign roles and responsibilities for protecting data assets in the organization?		
	Does the Cyber Security Management System (CSMS) specify the stakeholders involved in protecting road vehicles data assets in the Organization? And has their Cyber responsibilities effectively communicated?		
	Have appropriate resources been assigned to ensure the Cybersecurity responsibilities are effectively carried out?		
	Has the Executive Management defined appropriate levels of Risks that are acceptable to the organization with respect to Cyber Risk?		
[WP-05-02] Evidence of competence management, awareness management and continuous improvement	Is there a formal program in place to change the Organization culture to have a more cyber-oriented mindset?		
	Is there a methodology in place to ensure continuous improvement of the CSMS?		
	Are competent and knowledgeable personnel responsible for Cyber Activities?		
[WP-05-03] Evidence of the organization's management systems	Does the Organization have clear guidelines on sharing of Data Assets?		

	Does the Organization have a change management program?		
	Does the Organization have a documentation management program?		
	Does the Organization have a Configuration Management Program?		
[WP-05-04] Evidence of tool management	Does the Organization have a list of Tools that may impact Cybersecurity?		
	Are these Tools managed to ensure mitigation of Cyber Risks?		
[WP-05-05] Organizational cybersecurity audit report	Is Risk Management in place in the Organization?		
	Is Compliance to the CSMS evaluated through periodic Cyber Audits?		

Section 6: Project dependent Cybersecurity Management

This section details the requirements to manage projects related to Cybersecurity in the Organization.

Work Product	Questions to be asked	Compliant	Non-Compliant
[WP-06-01] Cybersecurity plan	Does the Organization have a formal documented Organization Cybersecurity Plan in place?		
	Has there been a formal gap analysis carried out to define the activities detailed in the Organization Cybersecurity Plan?		
	Does the Organization Cybersecurity Plan specify the activities required, the roles & responsibilities, the dependencies, the desired outcomes, and the Work Products needed for relevant in scope assets?		
	Have the Cybersecurity responsibilities, as per the Organization Cybersecurity Plan, been effectively communicated to all stakeholders responsible for Cyber in the Organization?		
	Is the Organization Cybersecurity Plan continuously updated and validated?		
[WP-06-02] Cybersecurity case	Has a formal Cybersecurity Case been developed based on the Organization Cybersecurity Plan to ensure alignment with the Organization's Business Vision & Mission?		
[WP-06-03] Cybersecurity assessment report	Has a Cybersecurity assessment been carried out for the item or component under development?		
	Has the Cybersecurity assessment been carried out by an independent individual or entity?		
	Does the Cybersecurity assessment provide confidence that the achieved degree of cybersecurity of the item or component is sufficient?		
	Has the scope of the Cybersecurity assessment been adequately defined?		
[WP-06-04] Release for post-development report	Does the cybersecurity assessment report include a recommendation for the acceptance, conditional acceptance, or rejection of the achieved degree of cybersecurity of the item or component?		

	Are the conditions met for release of the report including the Cybersecurity case, the cybersecurity assessment report, and the cybersecurity requirement for post-development?		

Section 7: Distributed Cybersecurity Activities

This section outlines the Cybersecurity requirements for the supply chain.

Work Product	Questions to be asked	Compliant	Non-Compliant
[WP-07-01] Cybersecurity interface agreement	Has the Organization assessed the Cybersecurity capabilities of all its suppliers by analyzing the Supplier record of capability?		
	Do all Request for Quotations include the expectation of Cyber responsibilities from the suppliers?		
	Are Cybersecurity Interface Agreements executed with all suppliers of the Organization?		
	Does the Cybersecurity Interface Agreements include the roles and responsibilities of both the Customer and the Supplier?		
	Is there a clear communication plan between the Customer and the Supplier to ensure Cybersecurity roles & responsibilities are delivered upon?		

Continual Cybersecurity Activities

Section 8: Continual Cybersecurity Activities

Continual Cybersecurity activities are those activities which are required to be performed during all phases of the item or components lifespan and are not specific to a defined project.

Work Product	Questions to be asked	Compliant	Non-Compliant
[WP-08-01] Sources for cybersecurity information	Are all internal & external sources of Cybersecurity information monitored for Cybersecurity events?		
	Have all external sources of Cybersecurity been identified, including organization's customers & suppliers?		
	Have all internal sources been identified including information received from the field?		
[WP-08-02] Triggers resulting from the triage of cybersecurity information	Is there a formal methodology in place to define and maintain the triggers? (Added)		
	Is there a formal methodology defined to ensure triage of Cybersecurity Information?		
	Have criteria for triage been defined that can be used to distinguish trigger thresholds?		
	Are results from the triage of Cybersecurity information readily available for further action?		
[WP-08-03] Cybersecurity events	Is Cybersecurity event assessment carried out to analyze the impact of Cybersecurity events on a specific item or component?		
[WP-08-04] Weakness from cybersecurity events	Has the Cybersecurity event been evaluated to identify weakness in an item or/component?		
	Has a Risk Treatment decision been taken with respect to that specific item or component?		
	Are cybersecurity vulnerabilities identified using vulnerability analysis?		
[WP-08-05] Vulnerability analysis	Is a Vulnerability Management Program in place to mitigate & manage identified vulnerabilities?		
	Does the Vulnerability Management Program manage identified vulnerabilities based on identified risk associated with these vulnerabilities?		

Concept & Product Development Phases

Section 9: Concept Phase

This section defines the item, the need to carry out a TARA to develop a RTP, the definition of Cybersecurity Goals and Cybersecurity Claims for each specified item.

Work Product	Questions to be asked	Compliant	Non-Compliant
[WP-09-01] Item definition	Has item definition been carried out to ensure a formal implementation of Cyber best practices?		
	Does the item definition include item boundary, function, and architecture?		
	Does the item definition include operational environment of the item with respect to cybersecurity?		
	Does the item definition include constraints & compliance needs of the specific item?		
	Does the item definition enumerate any assumptions made during the item definition process?		
[WP-09-02] Threat analysis and risk assessment	Has a TARA been conducted for the defined item that includes all assets encompassed by the specified item?		
[WP-09-03] Cybersecurity goals	Is there a Risk Treatment Plan that enumerates Risk treatment decisions for identified Threat Scenarios and their associated risks?		
	Has Cybersecurity goals, such as CAL, been established based on the Risk Treatment Plan for each specified item?		
[WP-09-04] Cybersecurity claims	Have any Cybersecurity claims been stated for the operational environment that leads to reduction of risk for a Threat Scenario?		
	Have any Cybersecurity claims been stated for any risk treatment options that leads to sharing or transferring risk?		
[WP-09-05] Verification report for cybersecurity goals	Is the process to determine Cybersecurity Goals & Cybersecurity Claims verified through a well documented report?		
[WP-09-06] Cybersecurity concept	Has the Cybersecurity concept been documented that specifies the cybersecurity requirements needed to meet the Cybersecurity Goals of the specified item?		

[WP-09-07] Verification report of cybersecurity concept	Has the Cybersecurity concept been verified through a formal report?		

Concept & Product Development Phases

Section 10: Product Development

This section describes the cybersecurity requirements of the architecture design as well as the integration and verification activities need to ensure those cybersecurity requirements are met.

Work Product	Questions to be asked	Compliant	Non-Compliant
[WP-10-01] Cybersecurity specification	Have the Cybersecurity requirements been defined for Product development based on cybersecurity requirements allocated at a higher level?		
	Have the Cybersecurity requirements been defined for Product development based on architecture design from a higher level?		
	Do the Cybersecurity requirements include any applicable cybersecurity controls?		
	Has the architecture designed been refined to ensure applicability of various Cybersecurity requirements?		
	Have the interfaces between the components of the refined architecture design that are applicable to meet cybersecurity requirements been identified?		
[WP-10-02] Cybersecurity requirements for post-development	Have the cybersecurity implications for the post-development phase been considered while enumerating the cybersecurity requirements?		
	Have specific cybersecurity requirements been formally documented to ensure cybersecurity in the post-developmental phase?		
[WP-10-03] Documentation of the modelling design or programming languages and coding guidelines, if appliable	Has a Criteria for suitable design, modelling and programming languages for cybersecurity been established?		
[WP-10-04] Verification report for the cybersecurity specification	Have the refined cybersecurity requirements and the refined architecture design been verified through a formal documented report?		
[WP-10-05] Weaknesses found during product development	Has a Vulnerability analysis been carried out to identify weaknesses in the refined architecture design and the cybersecurity requirements?		
	Has the Vulnerability analysis been presented as a final documented report?		

[WP-10-06] Integration and verification specification	Have Integration & Verification specification been defined for the development phase?		
[WP-10-07] Integration and verification reports	Have Verification activities been performed to ensure compliance with the refined Cybersecurity requirements?		
	Are the Integration & Verification activities outlined in a formal documented report?		

Concept & Product Development Phases

Section 11: Cybersecurity Validation

This section outlines the Cybersecurity Validation of the Item at Vehicle Level

Work Product	Questions to be asked	Compliant	Non-Compliant
[WP-11-01] Validation report	Have Validation activities been carried out at the Vehicle level to ensure adequacy of cybersecurity goals?		
	Has a Validation specification been developed to define these Validation activities?		
	Has Penetration Testing been performed to validate the Cybersecurity Goals?		
	Has a Validation report been generated which details the risk identified and their acceptance rationale for a specific item during the Concept & Product Development phases?		

Post-Development Phases

Section 12: Production

This section ensures that the Cybersecurity requirements are applied during the production process and that no further vulnerabilities creep into the item or component during this process.

Work Product	Questions to be asked	Compliant	Non-Compliant
[WP-12-01] Production control plan	Has a Production Control Plan been created to apply the Cybersecurity requirements during the production process?		
	Does the Production Control Plan include the Cybersecurity requirements enumerated for Post-Development?		
	Does the Production Control Plan include details of how to achieve the Cybersecurity requirements during the production process?		
	Does the Production Control Plan include details on how to protect the item or component for unauthorized alteration?		
	Does the Production Control Plan include activities to validate that Cybersecurity requirements are met during the production process?		

Post-Development Phases

Section 13: Operations & Maintenance

This section describes the activities required for enabling relevant Cyber activities during the Operations & Maintenance of the Road Vehicle.

Work Product	Questions to be asked	Compliant	Non-Compliant
[WP-13-01] Cybersecurity incident response plan	Is there a Cybersecurity Incident Plan in place to handle Cybersecurity incidents?		
	Does the Cybersecurity Incident Plan define the remediation actions required to handle the Cybersecurity incident?		
	Does the Cybersecurity Incident Plan include an effective communication plan during the Cybersecurity incident?		
	Does the Cybersecurity Incident Plan define the roles & responsibilities to remediate the incident?		
	Does the Cybersecurity Incident Plan include a method for determining progress for remediating the Cybersecurity incident?		
	Does the Cybersecurity Incident Plan include criteria for closing the Cybersecurity Incident and actions to be undertaken at this stage?		
	Is all information relevant to a specific Cybersecurity incident gathered in a formal manner to ensure appropriate Cybersecurity incident response?		
	Are updates developed based on the Cybersecurity Goals of the item or components?		
	Are Cybersecurity implications of recovery options considered while carrying out updates?		
	Does a formal procedure exist to provide communication to clients on end of Cybersecurity support?		

Post-Development Phases

Section 14: End of cybersecurity support and decommissioning

This section outlines the Cybersecurity implications of Decommissioning activities.

Work Product	Questions to be asked	Compliant	Non-Compliant
[WP-14-01] Procedures to communicate the end of cybersecurity support	Are Cybersecurity implications of Decommissioning activities considered at the time of Decommissioning?		
	Is an item or component decommissioned in a secure manner?		

Section 15: Threat analysis & risk assessment methods

This section defines the Threat Analysis & Risk Assessment (TARA) to be used to ensure a formal Risk Treatment Plan is developed to address the risks associated with each Threat Scenario.

Work Product	Questions to be asked	Compliant	Non-Compliant
[WP-15-01] Damage scenarios	Is there a process in place to identify "Damage Scenarios" for assets involved in functioning of road vehicles?		
[WP-15-02] Assets with cybersecurity properties	Is there an asset inventory in place that identified all assets related to road vehicles in the Organization?		
	Is it ensured that assets with cybersecurity properties whose compromise leads to damage scenarios are detailed in the asset inventory?		
[WP-15-03] Threat scenarios	Are Threat scenarios applicable to the Organization assets identified?		
[WP-15-04] Impact rating, including the associated impact categories of the damage scenarios	Is impact to the Organization in terms of safety, financial, operational, and privacy (S,F,O,P) assessed for various Damage Scenarios?		
	Are Impact Ratings identified for the various Damage Scenarios for each independent category i.e. safety, financial, operational, and privacy (S,F,O,P)?		
[WP-15-05] Attack paths	Are Attack Paths analysed for each Threat Scenarios?		
[WP-15-06] Attack feasibility rating	For each Attack Path, has the Attack feasibility rating been determined?		
[WP-15-07] Risk values	Has the Risk Value for each Threat Scenario been determined?		
[WP-15-08] Risk treatment decision per threat scenario	Has Risk Treatment Options been analysed for each Threat Scenario based on its impact categories, attack paths and Risk Value?		
	Are these Risk Treatment Options formally documented in a Risk Treatment Plan?		

About the Author

AJ Khan, CISSP, CCSK, PCIP, MBA (Innovation & Entrepreneurship)

AJ Khan is the CEO of Vehiqilla Inc., the president Global Syndicate 4 Mobility Security and the Co-Chair of the Cyber Security Committee (CSC) of APMA. AJ has over 20 years of experience in Governance, Risk & Compliance, and 13 years of experience in Cybersecurity Innovation and Emerging Technologies. During this time, AJ has worked on Cybersecurity & GRC in Middle East and North America in multiple sectors including Financial Institutions, Oil & Gas, Telecom, Government, Retail & Manufacturing sectors. AJ's Cyber expertise includes building Cyber Governance strategies, policies & procedures, Payment Card security, Cloud security, Industry4.0 and Automotive Cybersecurity.

AJ is ardent advocate of Cyber Security and Governance, Risk and Compliance (GRC). In his view, there is a critical need to address Cyber Security in today's Connected and Cloud deployments and if considerable effort is not made to address this issue, corporations will incorporate considerable Security Debt that will manifest itself later in the form of major security breaches. This will not only lead to loss of critical data and disruptions in operations activity, it will also lead to a major loss in the brand equity and reputation. Hence, Governance, Risk & Compliance is imperative for today's technology and business strategies.