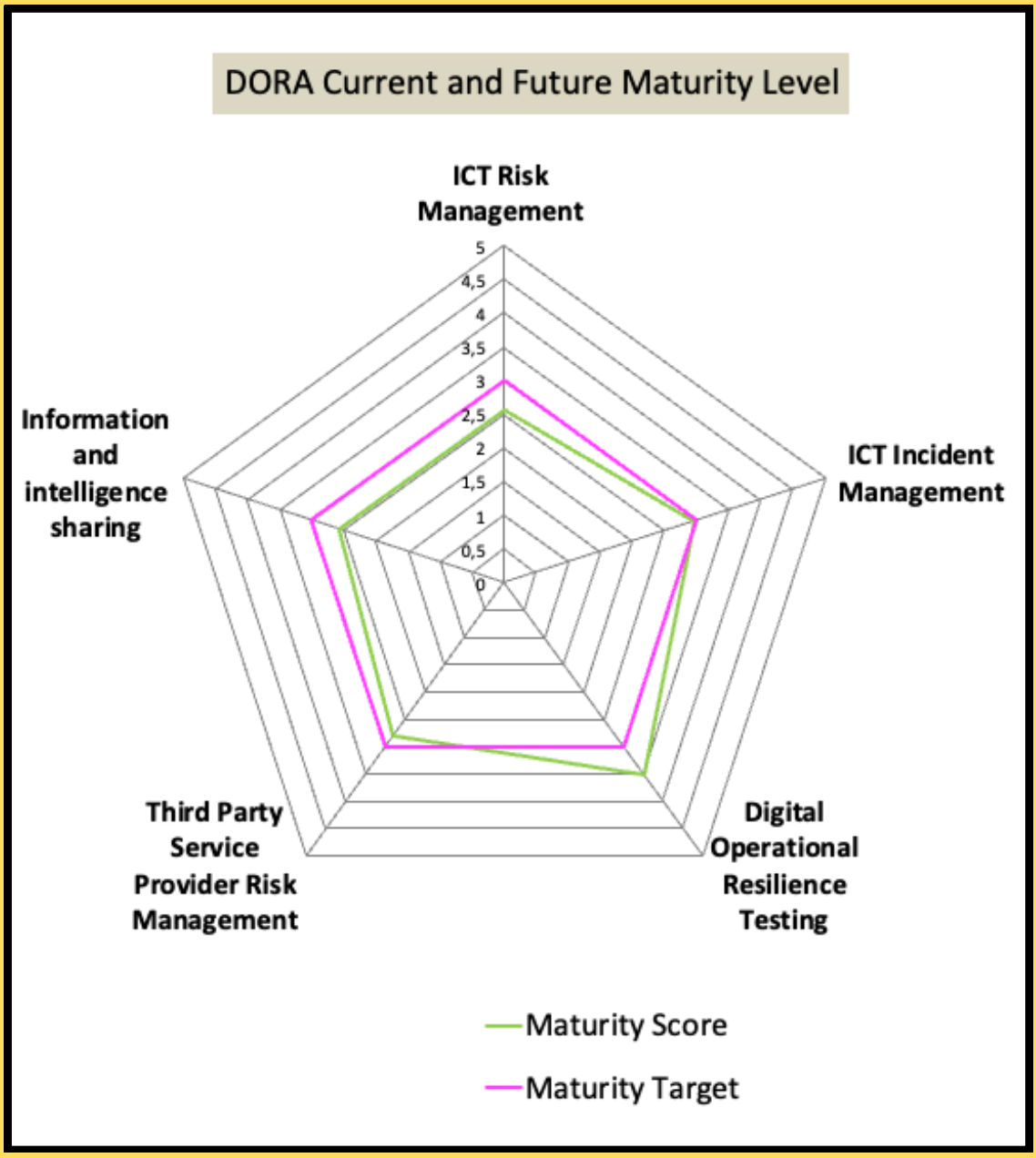
DORA “Quick” Gap Analysis and Maturity Assessment Against NIST CSF 2.0

A comprehensive and Automated Excel Spreadsheet

by Riadh Brinsi



Summary of the Document

This document presents a comprehensive framework for conducting a quick gap analysis and maturity assessment of an organization’s compliance with the Digital Operational Resilience Act (DORA) and NIST Cybersecurity Framework (CSF) 2.0. The assessment evaluates how well an organization has implemented various cybersecurity policies, processes, and risk management activities.

The document categorizes the organization's maturity level across different cybersecurity domains into five stages.

Each section outlines the status of specific NIST CSF 2.0 subcategories, focusing on areas such as risk management, stakeholder communication, policy updates, incident response, and supply chain security.

Explanation of the Maturity Model with DORA Context :

- **Incomplete**: The organization has minimal or no processes in place.

Example: The organization has no formal incident response plan. In the event of a cybersecurity incident, there is no documented procedure, no designated response team, and no communication protocols for notifying stakeholders.

- **Partially complete**: Some processes exist, but they lack uniformity and standardization.

Example: The organization has begun implementing cybersecurity risk management policies, but these are not standardized. For example, some departments conduct risk assessments, but there is no consistent method or centralized oversight, leading to inconsistencies across the organization.

- **Averagely complete**: Many processes are in place and follow established standards.

Example: The organization has developed a supplier risk management process, but it is not fully integrated. They maintain an inventory of critical suppliers and assess their risks, but this practice is not enforced across all departments, leading to gaps in compliance.

- **Mostly complete:** Processes are implemented, measurable, and well-communicated.

Example: The organization has established incident recovery processes that are measurable and communicated throughout the organization. They regularly conduct incident simulations with relevant stakeholders, but there are still some gaps, such as incomplete documentation for all drills or delays in reviewing incident outcomes.

- **Fully complete**: Everything is optimized, fully implemented, documented, and continuously improved.

Example: The organization has a fully optimized cybersecurity risk management strategy. Policies are documented, communicated, and enforced across the entire organization, including suppliers. Continuous improvement mechanisms are in place, and regular audits ensure that the policies evolve to meet new cybersecurity threats. Lessons learned from incidents are promptly integrated into policy updates.

This maturity model helps organizations measure their current cybersecurity resilience and identify areas for improvement.

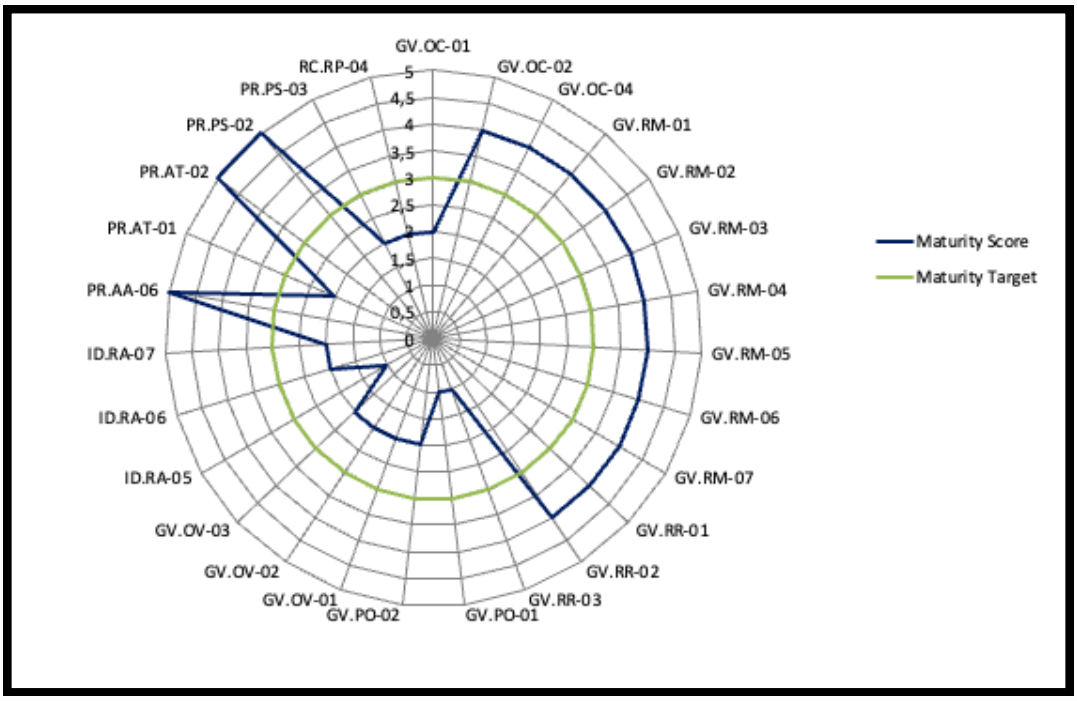
ICT Risk Management

NIST CSF 2.0 Subcategory	Status
GV.OC-01: The organizational mission is understood and informs cybersecurity risk management	Partially complete
GV.OC-02: Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered	Mostly complete
GV.OC-04: Critical objectives, capabilities, and services that stakeholders depend on or expect from the organization are understood and communicated	Mostly complete
GV.RM-01: Risk management objectives are established and agreed to by organizational stakeholders	Mostly complete
GV.RM-02: Risk appetite and risk tolerance statements are established, communicated, and maintained	Mostly complete
GV.RM-03: Cybersecurity risk management activities and outcomes are included in enterprise risk management processes	Mostly complete
GV.RM-04: Strategic direction that describes appropriate risk response options is established and communicated	Mostly complete
GV.RM-05: Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties	Mostly complete
GV.RM-06: A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated	Mostly complete
GV.RM-07: Strategic opportunities (i.e., positive risks) are characterized and are included in organizational cybersecurity risk discussions	Mostly complete
GV.RR-01: Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving	Mostly complete
GV.RR-02: Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced	Mostly complete
GV.RR-03: Adequate resources are allocated commensurate with the cybersecurity risk strategy, roles, responsibilities, and policies	Incomplete
GV.PO-01: Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced	Incomplete
GV.PO-02: Policy for managing cybersecurity risks is reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission	Partially complete
GV.OV-01: Cybersecurity risk management strategy outcomes are reviewed to inform and adjust strategy and direction	Partially complete
GV.OV-02: The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks	Partially complete

ICT Risk Management

NIST CSF 2.0 Subcategory	Status
GV.OV-03: Organizational cybersecurity risk management performance is evaluated and reviewed for adjustments needed	Partially complete
ID.RA-05: Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk and inform risk response prioritization	Incomplete
ID.RA-06: Risk responses are chosen, prioritized, planned, tracked, and communicated	Partially complete
ID.RA-07: Changes and exceptions are managed, assessed for risk impact, recorded, and tracked	Partially complete
PR.AA-06: Physical access to assets is managed, monitored, and enforced commensurate with risk	Fully complete
PR.AT-01: Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind	Partially complete
PR.AT-02: Individuals in specialized roles are provided with awareness and training so that they possess the knowledge and skills to perform relevant tasks with cybersecurity risks in mind	Fully complete
PR.PS-02: Software is maintained, replaced, and removed commensurate with risk	Fully complete
PR.PS-03: Hardware is maintained, replaced, and removed commensurate with risk	Partially complete
RC.RP-04: Critical mission functions and cybersecurity risk management are considered to establish post-incident operational norms	Partially complete

The result



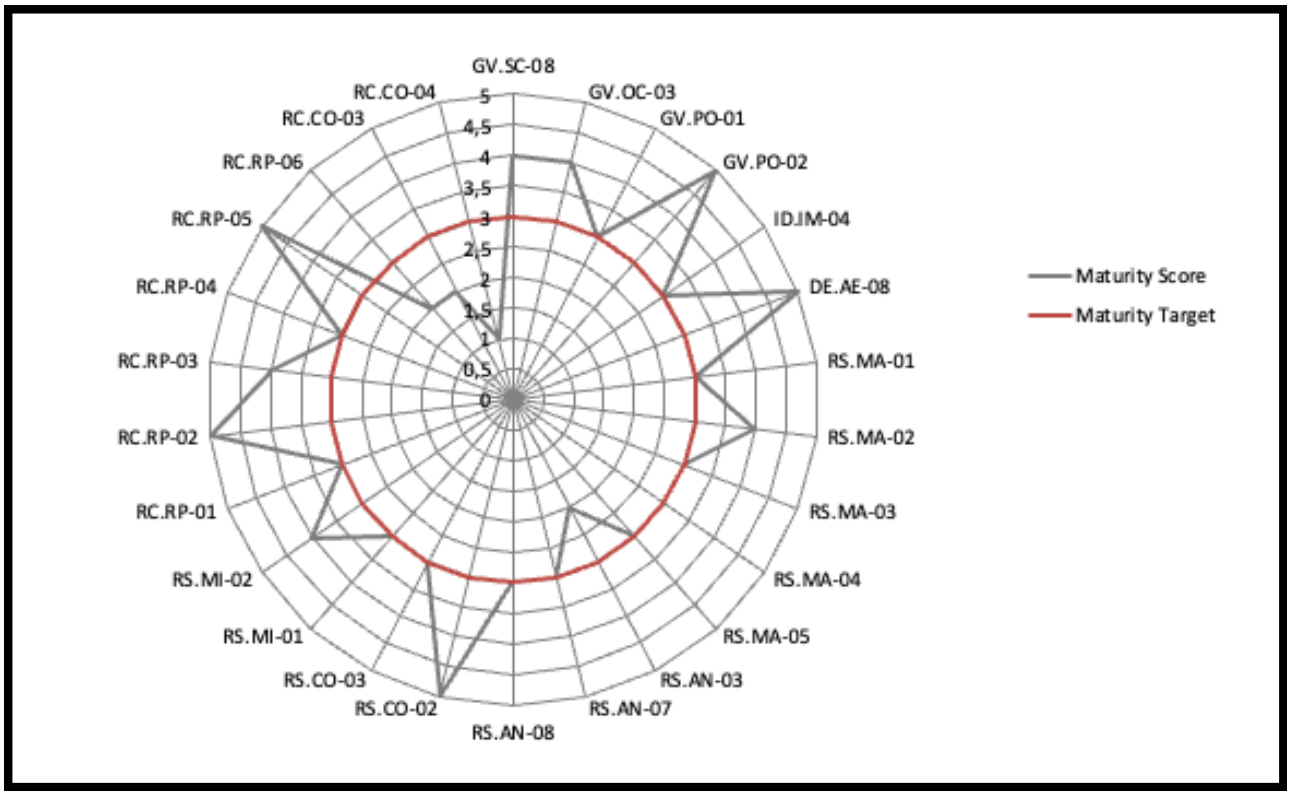
ICT related incident management

NIST CSF 2.0 Subcategory	Status
GV.SC-08: Relevant suppliers and other third parties are included in incident planning, response, and recovery activities	Mostly complete
GV.OC-03: Legal, regulatory, and contractual requirements regarding cybersecurity - including privacy and civil liberties obligations - are understood and managed	Mostly complete
GV.PO-01: Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced	Averagely complete
GV.PO-02: Policy for managing cybersecurity risks is reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission	Fully complete
ID.IM-04: Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved	Averagely complete
DE.AE-08: Incidents are declared when adverse events meet the defined incident criteria	Fully complete
RS.MA-01: The incident response plan is executed in coordination with relevant third parties once an incident is declared	Averagely complete
RS.MA-02: Incident reports are triaged and validated	Mostly complete
RS.MA-03: Incidents are categorized and prioritized	Averagely complete
RS.MA-04: Incidents are escalated or elevated as needed	Averagely complete
RS.MA-05: The criteria for initiating incident recovery are applied	Averagely complete
RS.AN-03: Analysis is performed to establish what has taken place during an incident and the root cause of the incident	Partially complete
RS.AN-07: Incident data and metadata are collected, and their integrity and provenance are preserved	Averagely complete
RS.AN-08: An incident's magnitude is estimated and validated	Averagely complete
RS.CO-02: Internal and external stakeholders are notified of incidents	Fully complete
RS.CO-03: Information is shared with designated internal and external stakeholders	Averagely complete
RS.MI-01: Incidents are contained	Averagely complete
RS.MI-02: Incidents are eradicated	Mostly complete

ICT related incident management

NIST CSF 2.0 Subcategory	Status
RC.RP-01: The recovery portion of the incident response plan is executed once initiated from the incident response process	Averagely complete
RC.RP-02: Recovery actions are selected, scoped, prioritized, and performed	Fully complete
RC.RP-03: The integrity of backups and other restoration assets is verified before using them for restoration	Mostly complete
RC.RP-04: Critical mission functions and cybersecurity risk management are considered to establish post-incident operational norms	Averagely complete
RC.RP-05: The integrity of restored assets is verified, systems and services are restored, and normal operating status is confirmed	Fully complete
RC.RP-06: The end of incident recovery is declared based on criteria, and incident-related documentation is completed	Partially complete
RC.CO-03: Recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders	Partially complete
RC.CO-04: Public updates on incident recovery are shared using approved methods and messaging	Incomplete

The result



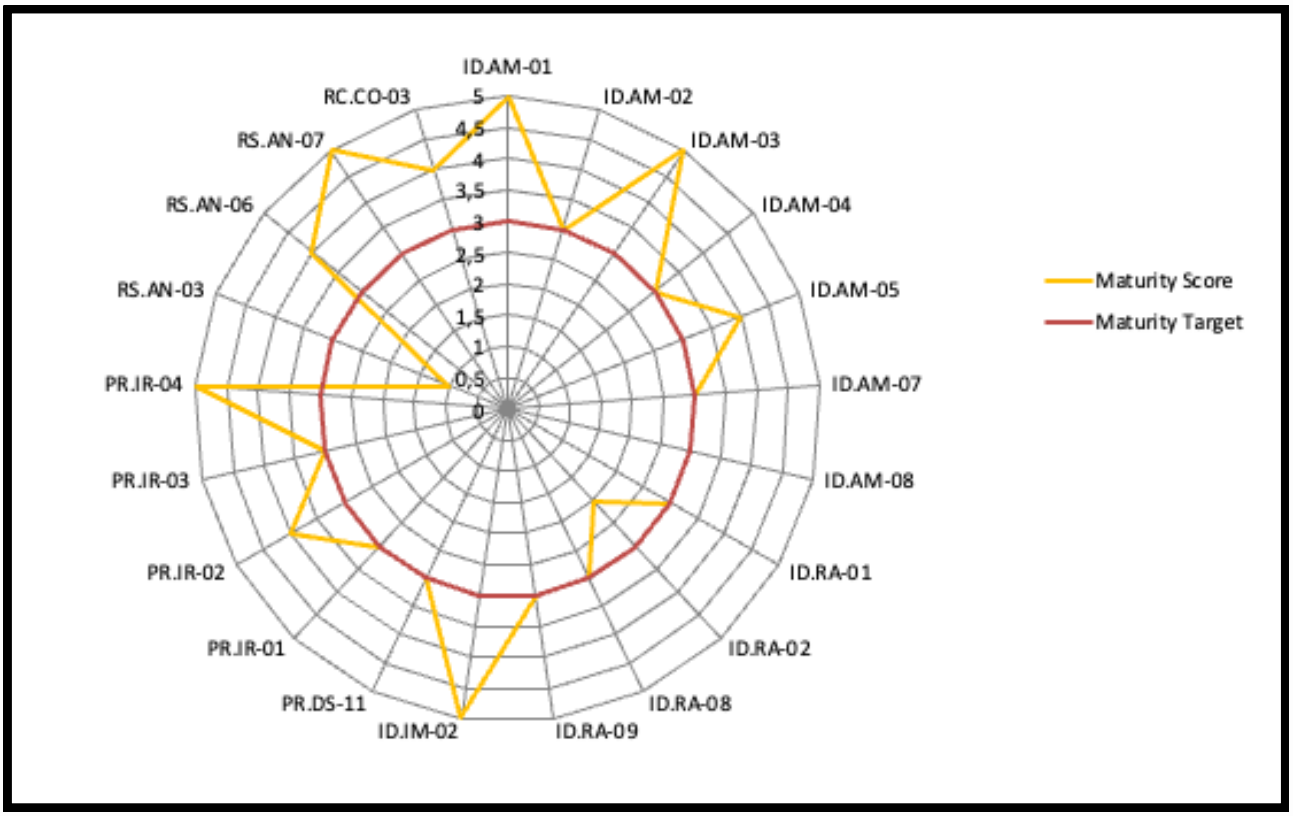
Digital operational resilience testing

NIST CSF 2.0 Subcategory	Status
GV.RM-05: Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties	Incomplete
GV.SC-01: A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders	Incomplete
GV.SC-02: Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally	Incomplete
GV.SC-03: Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes	Incomplete
GV.SC-04: Suppliers are known and prioritized by criticality	Incomplete
GV.SC-05: Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties	Partially complete
GV.SC-06: Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships	Partially complete
GV.SC-07: The risks posed by a supplier, their products and services, and other third parties are understood, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship	Partially complete
GV.SC-08: Relevant suppliers and other third parties are included in incident planning, response, and recovery activities	Partially complete
GV.SC-09: Supply chain security practices are integrated into cybersecurity and enterprise risk management programs, and their performance is monitored throughout the technology product and service life cycle	Partially complete
GV.SC-10: Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement	Partially complete
ID.AM-03: Representations of the organization's authorized network communication and internal and external network data flows are maintained	Partially complete
ID.AM-04: Inventories of services provided by suppliers are maintained	Averagely complete
ID.AM-05: Assets are prioritized based on classification, criticality, resources, and impact on the mission	Averagely complete
ID.RA-03: Internal and external threats to the organization are identified and recorded	Averagely complete
ID.RA-09: The authenticity and integrity of hardware and software are assessed prior to acquisition and use	Averagely complete
ID.RA-10: Critical suppliers are assessed prior to acquisition	Averagely complete

Digital operational resilience testing

NIST CSF 2.0 Subcategory	Status
ID.IM-02: Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties	Mostly complete
PR.AA-01: Identities and credentials for authorized users, services, and hardware are managed by the organization	Mostly complete
PR.AA-02: Identities are proofed and bound to credentials based on the context of interactions	Mostly complete
PR.AA-03: Users, services, and hardware are authenticated	Mostly complete
PR.AA-05: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties	Fully complete
PR.AA-06: Physical access to assets is managed, monitored, and enforced commensurate with risk	Fully complete
DE.CM-06: External service provider activities and services are monitored to find potentially adverse events	Fully complete
RS.MA-01: The incident response plan is executed in coordination with relevant third parties once an incident is declared	Fully complete

The result



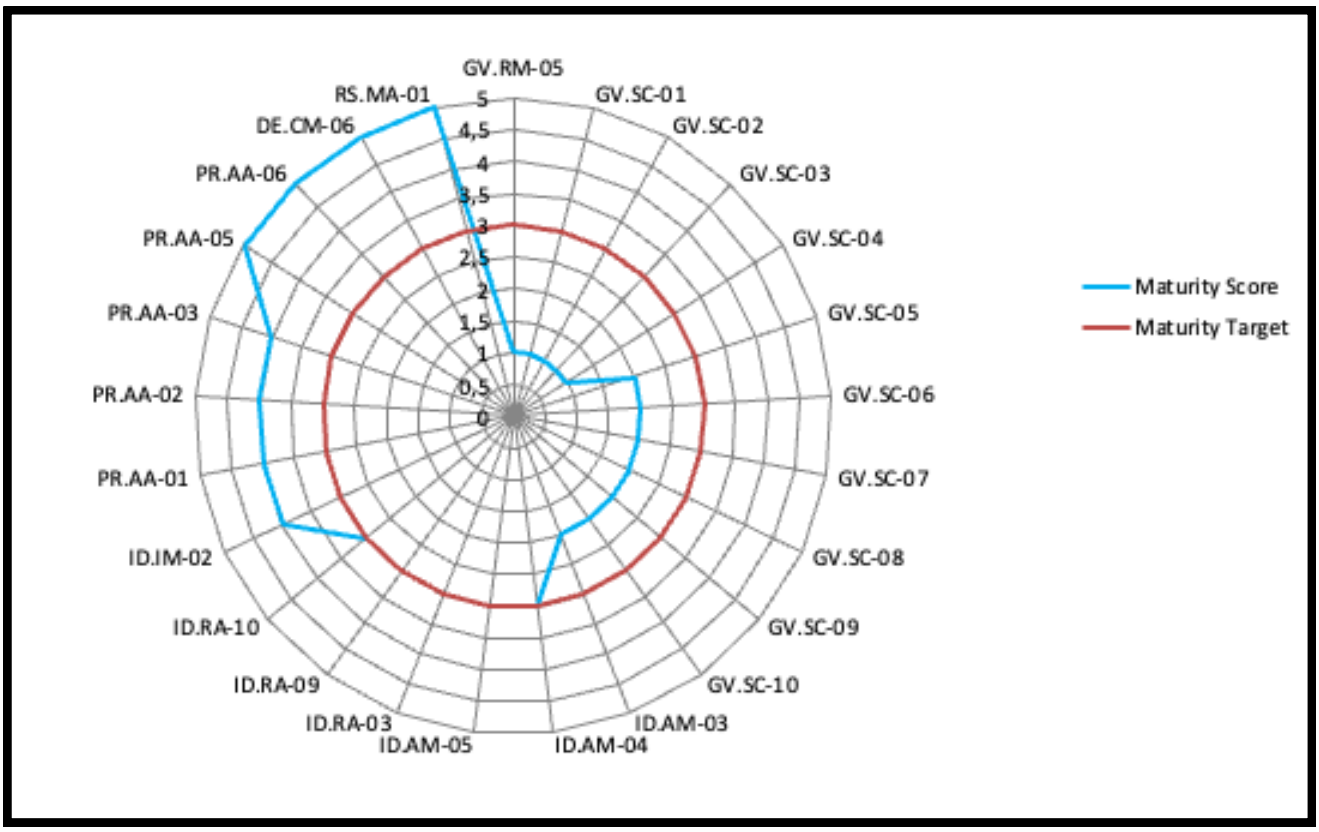
Third Party Service Provider Risk Management

NIST CSF 2.0 Subcategory	Status
GV.RM-05: Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties	Incomplete
GV.SC-01: A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders	Incomplete
GV.SC-02: Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally	Incomplete
GV.SC-03: Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes	Incomplete
GV.SC-04: Suppliers are known and prioritized by criticality	Incomplete
GV.SC-05: Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties	Partially complete
GV.SC-06: Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships	Partially complete
GV.SC-07: The risks posed by a supplier, their products and services, and other third parties are understood, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship	Partially complete
GV.SC-08: Relevant suppliers and other third parties are included in incident planning, response, and recovery activities	Partially complete
GV.SC-09: Supply chain security practices are integrated into cybersecurity and enterprise risk management programs, and their performance is monitored throughout the technology product and service life cycle	Partially complete
GV.SC-10: Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement	Partially complete
ID.AM-03: Representations of the organization's authorized network communication and internal and external network data flows are maintained	Partially complete
ID.AM-04: Inventories of services provided by suppliers are maintained	Averagely complete
ID.AM-05: Assets are prioritized based on classification, criticality, resources, and impact on the mission	Averagely complete
ID.RA-03: Internal and external threats to the organization are identified and recorded	Averagely complete
ID.RA-09: The authenticity and integrity of hardware and software are assessed prior to acquisition and use	Averagely complete
ID.RA-10: Critical suppliers are assessed prior to acquisition	Averagely complete

Third Party Service Provider Risk Management

NIST CSF 2.0 Subcategory	Status
ID.IM-02: Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties	Mostly complete
PR.AA-01: Identities and credentials for authorized users, services, and hardware are managed by the organization	Mostly complete
PR.AA-02: Identities are proofed and bound to credentials based on the context of interactions	Mostly complete
PR.AA-03: Users, services, and hardware are authenticated	Mostly complete
PR.AA-05: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties	Fully complete
PR.AA-06: Physical access to assets is managed, monitored, and enforced commensurate with risk	Fully complete
DE.CM-06: External service provider activities and services are monitored to find potentially adverse events	Fully complete
RS.MA-01: The incident response plan is executed in coordination with relevant third parties once an incident is declared	Fully complete

The result



Information and Intelligence Sharing

NIST CSF 2.0 Subcategory	Status
GV.RM-05: Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties	Mostly complete
ID.RA-02: Cyber threat intelligence is received from information sharing forums and sources	Mostly complete
DE.AE-03: Information is correlated from multiple sources	Mostly complete
DE.AE-06: Information on adverse events is provided to authorized staff and tools	Incomplete
DE.AE-07: Cyber threat intelligence and other contextual information are integrated into the analysis	Incomplete
RS.CO-02: Internal and external stakeholders are notified of incidents	Partially complete
RS.CO-03: Information is shared with designated internal and external stakeholders	Partially complete
RC.CO-03: Recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders	Partially complete
RC.CO-04: Public updates on incident recovery are shared using approved methods and messaging	Partially complete

The result