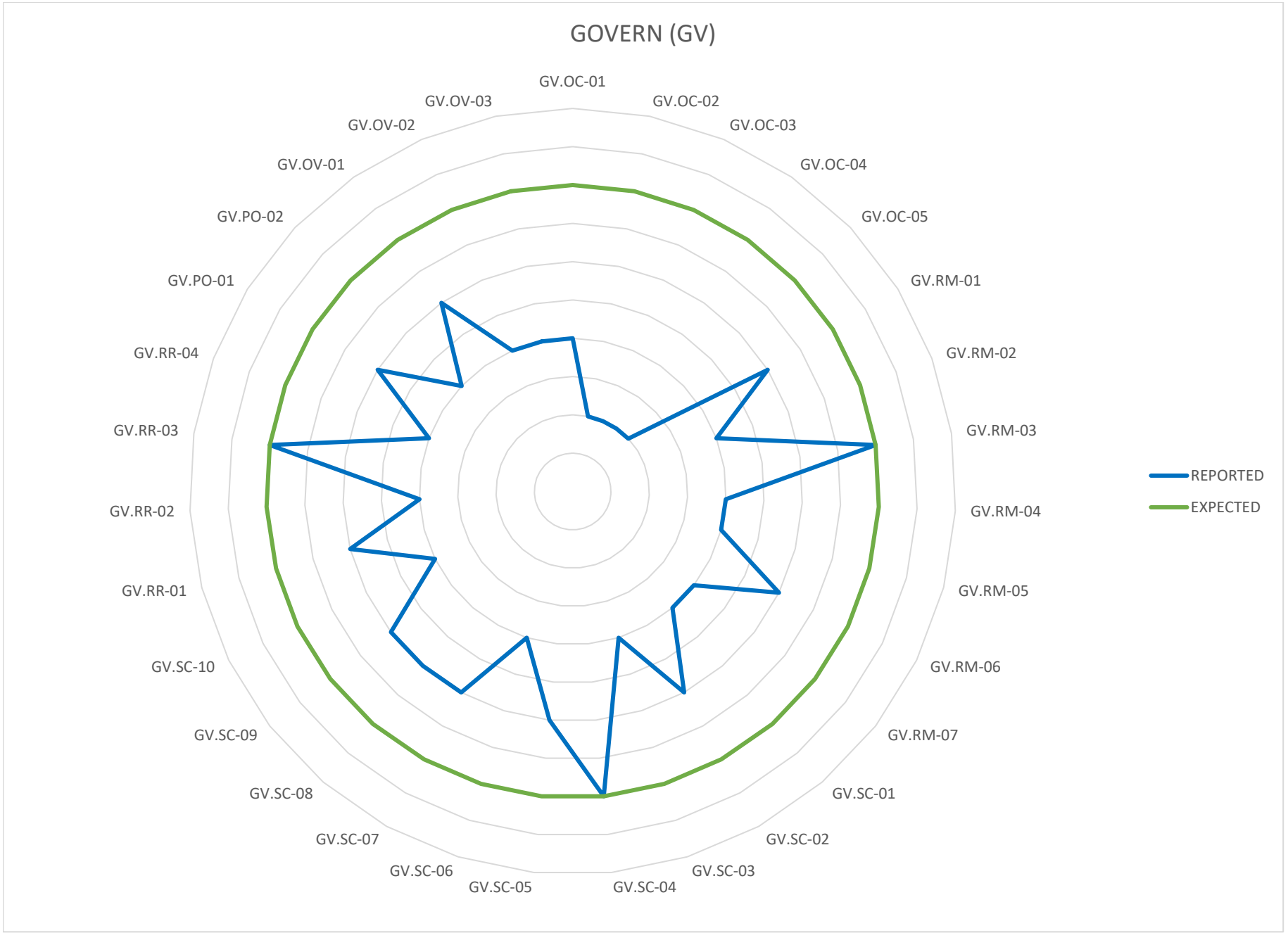
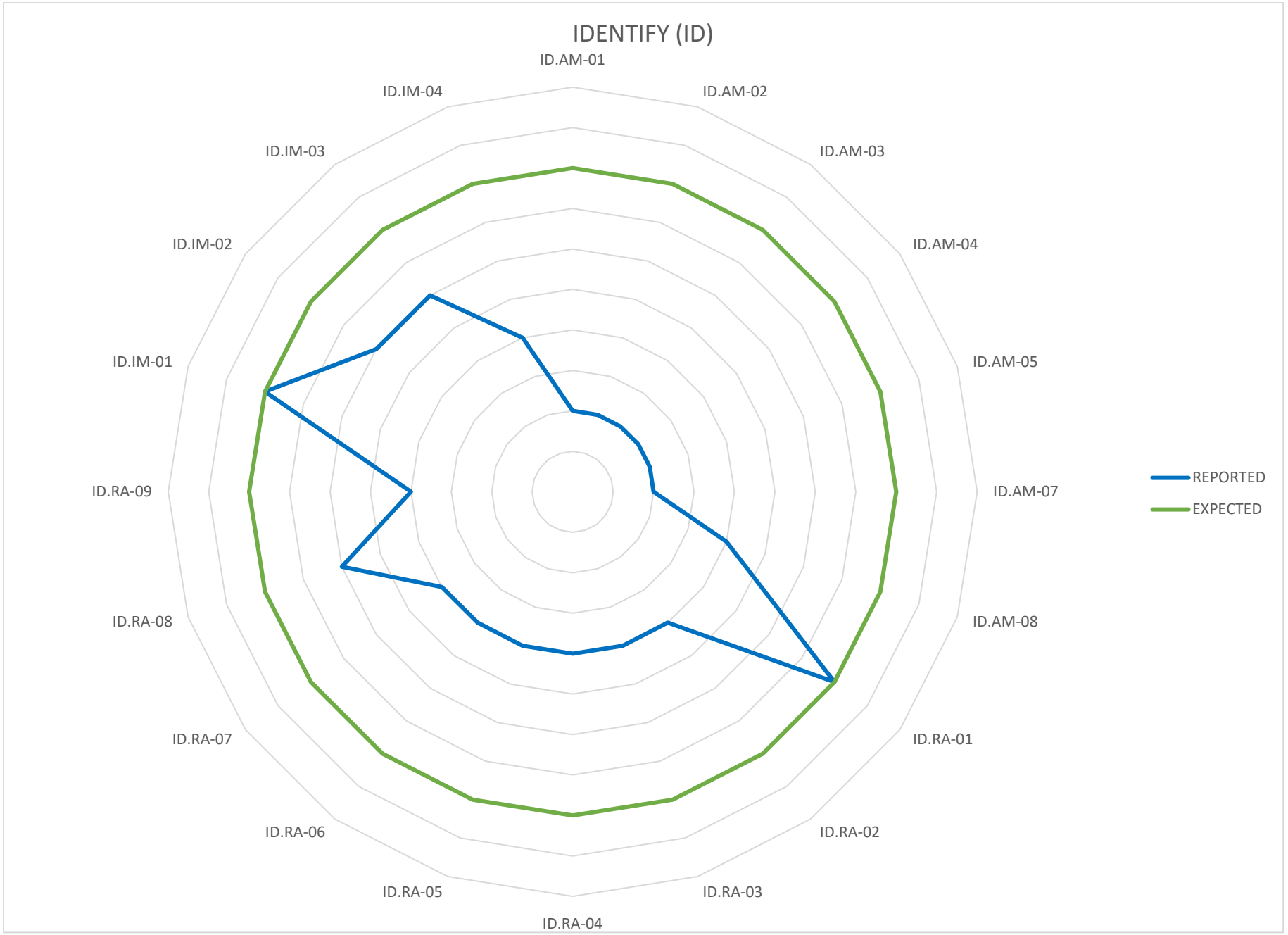
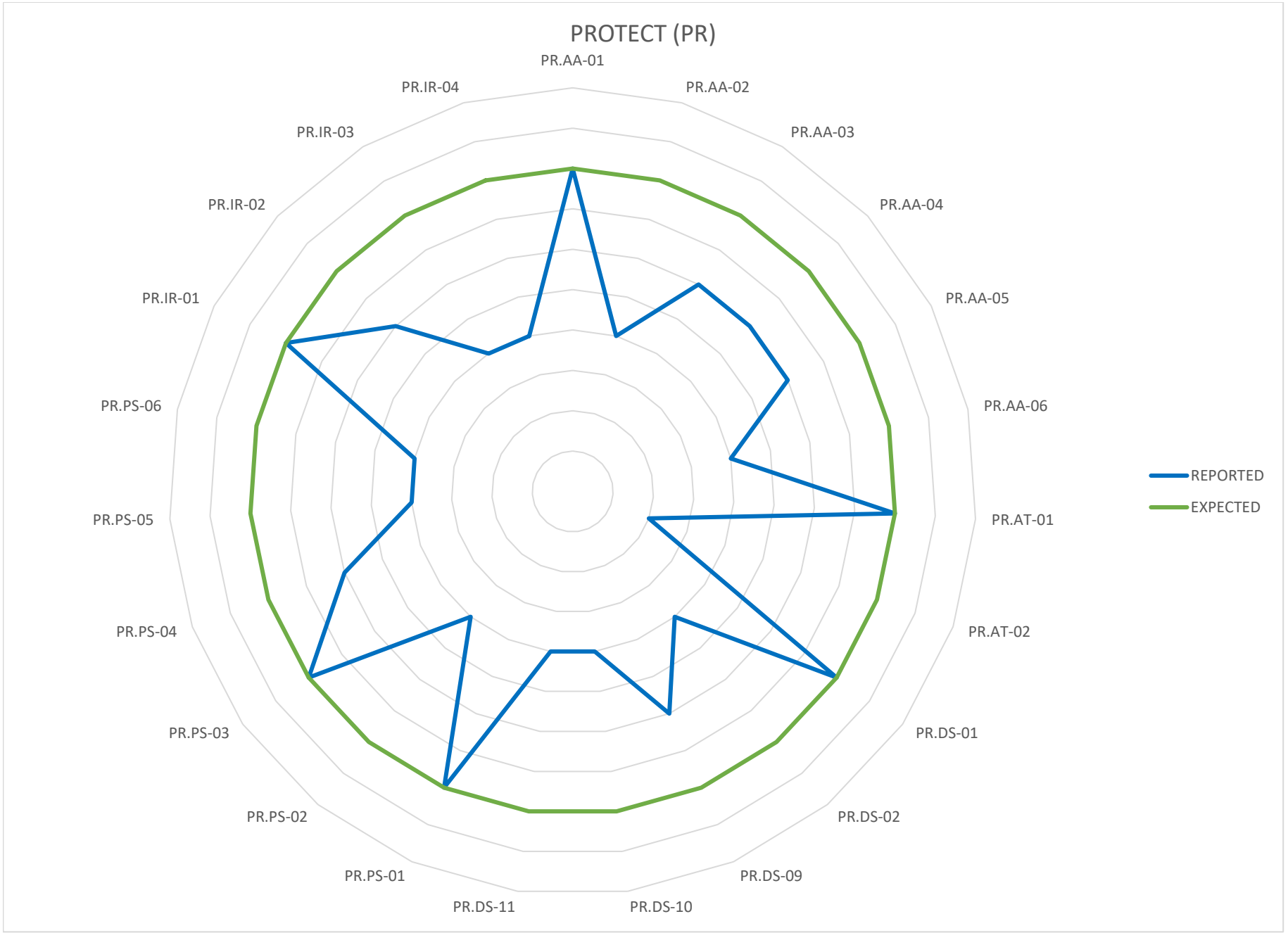
FUNCTION	STATE	EXP	%	CATEGORY	STATE	EXP	%	SUB-CATEGORY		REPORTED	EXPECTED
Govern GV	2.3	4.0	58.6%								
				Organizational Context GV.OC	1.2	4.0	30.0%				
								GV.OC-01	The organizational mission is understood and informs cybersecurity risk management.	2	4
								GV.OC-02	Internal and external stakeholders are determined. and their needs and exoectations reaardina cybersecurity risk manaaement are understood.	1	4
								GV.OC-03	Legal, regulatory, and contractual requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.	1	4
								GV.OC-04	Critical objectives, capabilities, and services that stakeholders depend on or expect from the organization are determined and communicated.	1	4
								GV.OC-05	Outcomes, capabilities, and services that the organization depends on are determined and communicated.	1	4
				Risk Management Strategy GV.RM	2.6	4.0	64.3%				
								GV.RM-01	Risk management objectives are established and agreed to by organizational stakeholders.	3	4
								GV.RM-02	Risk appetite and risk tolerance statements are determined, communicated, and maintained.	2	4
								GV.RM-03	Enterprise risk management processes include cybersecurity risk management activities and outcomes.	4	4
								GV.RM-04	Strategic direction that describes appropriate risk response options is established and communicated.	2	4
								GV.RM-05	Lines of communication across the organization are established for cybersecurity risks. including risks from suppliers and other third parties.	2	4
								GV.RM-06	A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated.	3	4
								GV.RM-07	Strategic opportunities (i.e., positive risks) are identified and included in organizational cybersecurity risk discussions.	2	4
				Cybersecurity Supply Chain Risk Management GV.SC	2.7	4.0	67.5%				
								GV.SC-01	A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders.	2	4
								GV.SC-02	Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally.	3	4
								GV.SC-03	Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes.	2	4
								GV.SC-04	Suppliers are known and prioritized by criticality.	4	4
								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.	3	4
								GV.SC-06	Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships .	2	4
								GV.SC-07	The risks posed by a supplier, their products and services, and other third parties are identified, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship.	3	4
								GV.SC-08	Relevant suppliers and other third parties are included in incident planning, response, and recovery activities.	3	4
								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.	3	4
								GV.SC-10	Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement.	2	4
				Roles, Responsibilities, and Authorities GV.RR	2.8	4.0	68.8%				
								GV.RR-01	Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving.	3	4
								GV.RR-02	Roles. responsibilities. and authorities related to cybersecurity risk manaaement are established. communicated. understood. and enforced.	2	4
								GV.RR-03	Adequate resources are allocated commensurate with cybersecurity risk strategy, roles and responsibilities, and policies.	4	4
								GV.RR-04	Cybersecurity is included in human resources practices.	2	4
				Policies, Processes, and Procedures GV.PO	2.5	4.0	62.5%				
								GV.PO-01	Policies. processes. and procedures for manaaina cybersecurity risks are established based on oraanizational context. cybersecurity strateav. and priorities and are communicated and enforced.	3	4
								GV.PO-02	Policies, processes, and procedures for managing cybersecurity risks are reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission.	2	4
				Oversight GV.OV	2.3	4.0	58.3%				
								GV.OV-01	Cybersecurity risk management strategy outcomes are reviewed to inform and adjust strategy and direction.	3	4
								GV.OV-02	The cybersecurity risk manaaement strateav is reviewed and adiusted to ensure coveraae of oraanizational requirements and risks.	2	4
								GV.OV-03	Organizational cybersecurity risk management performance is measured and reviewed to confirm and adjust strategic direction.	2	4
Identify ID	2.2	4.0	54.9%								
				Asset Management ID.AM	1.1	4.0	28.6%				
								ID.AM-01	Inventories of hardware managed by the organization are maintained.	1	4
								ID.AM-02	Inventories of software. services. and systems managed by the oraanization are maintained.	1	4
								ID.AM-03	Representations of the organization's authorized network communication and internal and external network data flows are maintained.	1	4
								ID.AM-04	Inventories of services provided by suppliers are maintained.	1	4
								ID.AM-05	Assets are prioritized based on classification, criticality, resources, and impact on the mission.	1	4
								ID.AM-07	Inventories of data and corresponding metadata for designated data types are maintained.	1	4
								ID.AM-08	Systems, hardware, software, and services are managed throughout their life cycle.	2	4
				Risk Assessment ID.RA	2.3	4.0	58.3%				
								ID.RA-01	Vulnerabilities in assets are identified, validated, and recorded.	4	4
								ID.RA-02	Cyber threat intelligence is received from information sharing forums and sources.	2	4
								ID.RA-03	Internal and external threats to the oraanization are identified and recorded.	2	4
								ID.RA-04	Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded.	2	4
								ID.RA-05	Threats, vulnerabilities, likelihoods, and impacts are used to determine risk and inform risk prioritization.	2	4
								ID.RA-06	Risk responses are chosen from the available options, prioritized, planned, tracked, and communicated.	2	4
								ID.RA-07	Changes and exceptions are managed, assessed for risk impact, recorded, and tracked.	2	4
								ID.RA-08	Processes for receiving. analyzing. and responding to vulnerability disclosures are established.	3	4
								ID.RA-09	The authenticity and integrity of hardware and software are assessed prior to acquisition and use.	2	4
				Improvement ID.IM	3.0	4.0	75.0%				
								ID.IM-01	Continuous evaluation is applied to identify improvements.	4	4
								ID.IM-02	Security tests and exercises. including those done in coordination with suppliers and relevant third parties. are conducted to identify improvements.	3	4
								ID.IM-03	Lessons learned during execution of operational processes, procedures, and activities are used to identify improvements.	3	4
								ID.IM-04	Cybersecurity plans that affect operations are communicated, maintained, and improved.	2	4
Protect PR	2.7	4.0	67.6%								
				Identity Management, Authentication, and Access Control PR.AA	2.8	4.0	70.8%				
								PR.AA-01	Identities and credentials for authorized users. services. and hardware are manaaed by the oraanization.	4	4
								PR.AA-02	Identities are proofed and bound to credentials based on the context of interactions.	2	4
								PR.AA-03	Users, services, and hardware are authenticated.	3	4
								PR.AA-04	Identity assertions are protected, conveyed, and verified.	3	4
								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.	3	4
								PR.AA-06	Physical access to assets is managed, monitored, and enforced commensurate with risk.	2	4
				Awareness and Training PR.AT	2.5	4.0	62.5%				
								PR.AT-01	Users are provided awareness and training so they possess the knowledge and skills to perform general tasks with security risks in mind.	4	4
								PR.AT-02	Individuals in specialized roles are provided awareness and training so they possess the knowledge and skills to perform relevant tasks with security risks in mind.	1	4
				Data Security PR.DS	2.6	4.0	65.0%				
								PR.DS-01	The confidentiality, integrity, and availability of data-at-rest are protected.	4	4
								PR.DS-02	The confidentiality. integrity. and availability of data-in-transit are protected.	2	4
								PR.DS-09	Data is managed throughout its life cycle, including destruction.	3	4
								PR.DS-10	The confidentiality, integrity, and availability of data-in-use are protected.	2	4
								PR.DS-11	Backups of data are created, protected, maintained, and tested.	2	4
				Platform Security PR.PS	2.8	4.0	70.8%				
								PR.PS-01	Configuration management practices are applied.	4	4
								PR.PS-02	Software is maintained, replaced, and removed commensurate with risk.	2	4
								PR.PS-03	Hardware is maintained, replaced, and removed commensurate with risk.	4	4
								PR.PS-04	Log records are generated and made available for continuous monitoring.	3	4
								PR.PS-05	Installation and execution of unauthorized software are prevented.	2	4
								PR.PS-06	Secure software development practices are integrated and their performance is monitored throughout the software development life cycle.	2	4
				Technology Infrastructure Resilience PR.IR	2.8	4.0	68.8%				
								PR.IR-01	Networks and environments are protected from unauthorized logical access and usage.	4	4
								PR.IR-02	The oraanization's technoloav assets are protected from environmental threats.	3	4
								PR.IR-03	Mechanisms are implemented to achieve resilience requirements in normal and adverse situations.	2	4
								PR.IR-04	Adequate resource capacity to ensure availability is maintained.	2	4
Detect DE	2.6	4.0	63.8%								
				Continuous Monitoring DE.CM	2.6	4.0	65.0%				
								DE.CM-01	Networks and network services are monitored to find potentially adverse events.	4	4
								DE.CM-02	The physical environment is monitored to find potentially adverse events	2	4
								DE.CM-03	Personnel activity and technology usage are monitored to find potentially adverse events.	3	4
								DE.CM-06	External service provider activities and services are monitored to find potentially adverse events.	2	4
								DE.CM-09	Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events.	2	4
				Adverse Event Analysis DE.AE	2.5	4.0	62.5%				
								DE.AE-02	Potentially adverse events are analyzed to better understand associated activities.	4	4
								DE.AE-03	Information is correlated from multiple sources.	2	4
								DE.AE-04	The estimated impact and scope of adverse events are determined.	3	4
								DE.AE-06	Information on adverse events is provided to authorized staff and tools.	2	4
								DE.AE-07	Cyber threat intelligence and other contextual information are integrated into the analysis.	2	4
								DE.AE-08	Incidents are declared when adverse events meet the defined incident criteria.	2	4
Respond RS	2.4	4.0	60.6%								
				Incident Management RS.MA	1.2	4.0	30.0%				
								RS.MA-01	The incident response plan is executed once an incident is declared in coordination with relevant third parties.	1	4
								RS.MA-02	Incident reports are triaged and validated.	2	4
								RS.MA-03	Incidents are categorized and prioritized.	1	4
								RS.MA-04	Incidents are escalated or elevated as needed.	1	4
								RS.MA-05	The criteria for initiating incident recovery are applied.	1	4
				Incident Analysis RS.AN	2.5	4.0	62.5%				
								RS.AN-03	Analysis is performed to determine what has taken place during an incident and the root cause of the incident.	4	4
								RS.AN-06	Actions performed during an investigation are recorded and the records' integrity and provenance are preserved.	2	4
								RS.AN-07	Incident data and metadata are collected, and their integrity and provenance are preserved.	2	4
								RS.AN-08	The incident's magnitude is estimated and validated.	2	4
				Incident Response Reporting and Communication RS.CO	3.0	4.0	75.0%				
								RS.CO-02	Internal and external stakeholders are notified of incidents.	4	4
								RS.CO-03	Information is shared with designated internal and external stakeholders.	2	4
				Incident Mitigation RS.MI	3.0	4.0	75.0%				
								RS.MI-01	Incidents are contained.	4	4
								RS.MI-02	Incidents are eradicated.	2	4
Recover RC	2.8	4.0	68.8%								
				Incident Recovery Plan Execution RC.RP	2.5	4.0	62.5%				
								RC.RP-01	The recovery portion of the incident response plan is executed once initiated from the incident response process.	4	4
								RC.RP-02	Recovery actions are determined, scoped, prioritized, and performed.	2	4
								RC.RP-03	The integrity of backups and other restoration assets is verified before using them for restoration.	2	4
								RC.RP-04	Critical mission functions and cybersecurity risk management are considered to establish post/incident operational norms.	3	4
								RC.RP-05	The integrity of restored assets is verified. systems and services are restored. and normal operating status is confirmed.	2	4
								RC.RP-06	The criteria for determining the end of incident recovery are applied, and incident-related documentation is completed.	2	4
				Incident Recovery Communication RC.CO	3.0	4.0	75.0%				
								RC.CO-03	Recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders.	4	4
								RC.CO-04	Public updates on incident recovery are properly shared using approved methods and messaging.	2	4

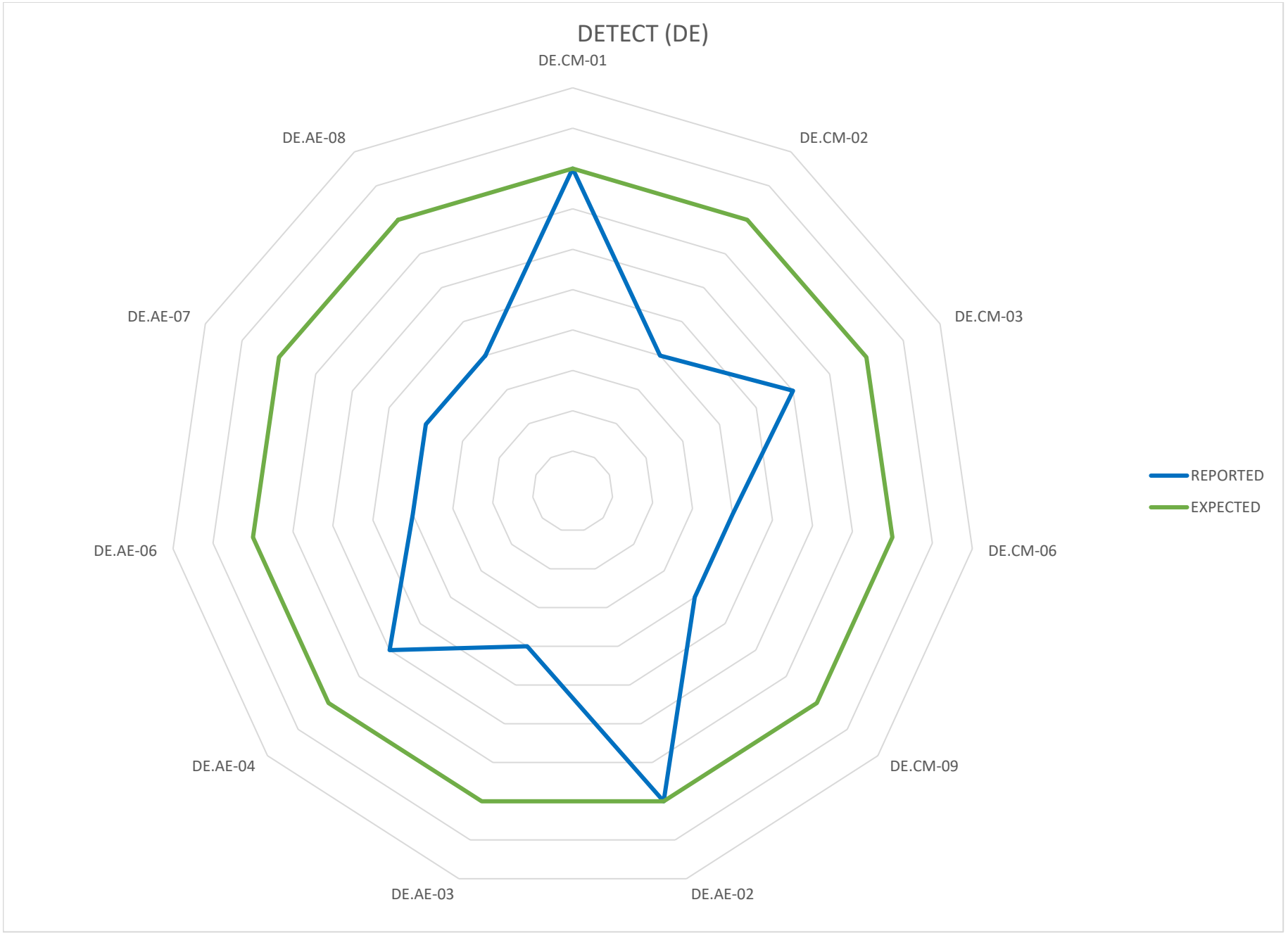
Q4 2023 NIST CSF 2.0 CYBER HYGIENE PROFILE SCORECARD ©SWOPE

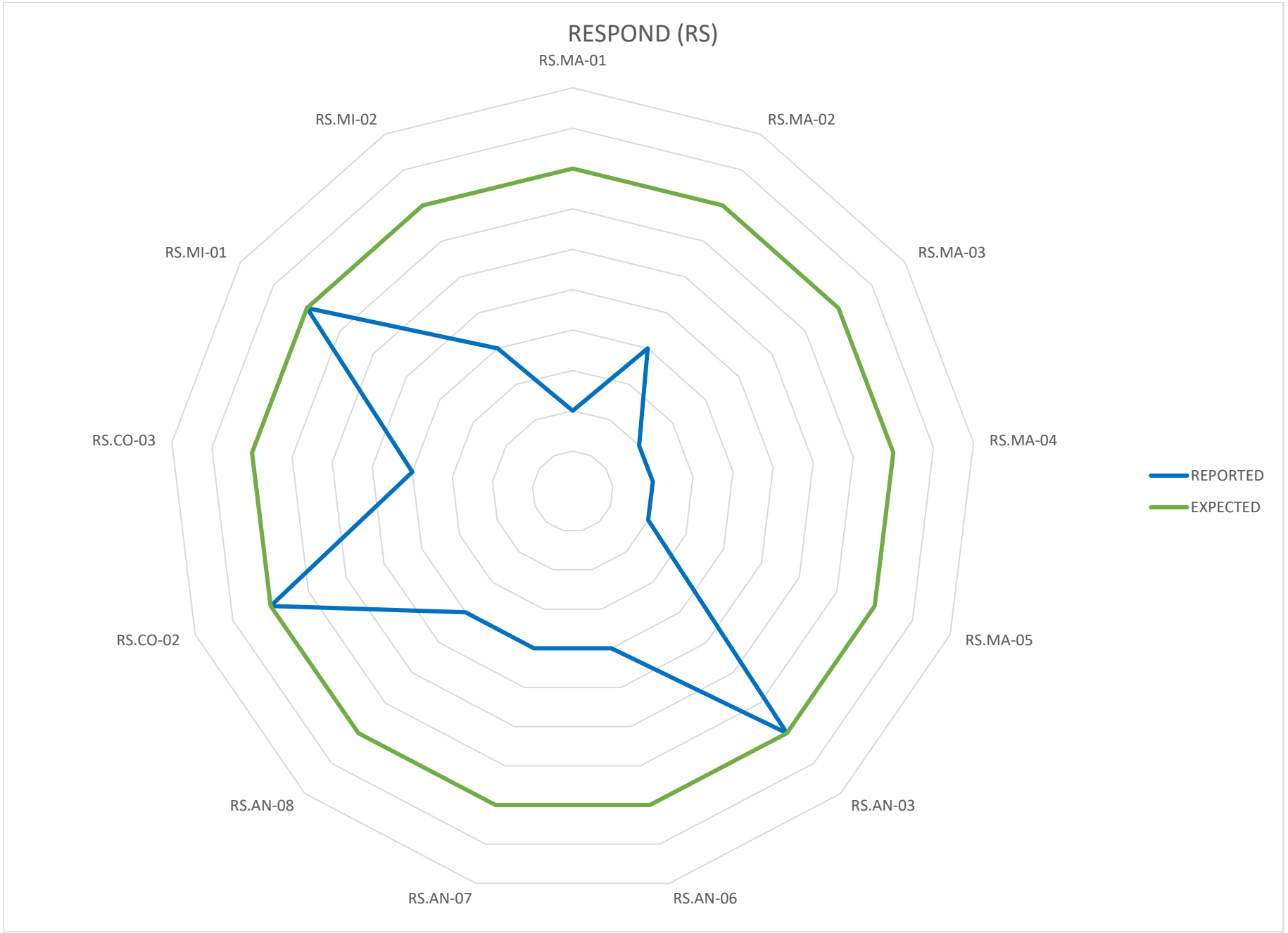
Govern GV	**58.6%**		
		Organizational Context GV.OC	30.0%
		Risk Management Strategy GV.RM	64.3%
		Cybersecurity Supply Chain Risk Management GV.SC	67.5%
		Roles, Responsibilities, and Authorities GV.RR	68.8%
		Policies, Processes, and Procedures GV.PO	62.5%
		Oversight GV.OV	58.3%
Identify ID	**54.0%**		
		Asset Management ID.AM	28.6%
		Risk Assessment ID.RA	58.3%
		Improvement ID.IM	75.0%
Protect PR	**67.6%**		
		Identity Management, Authentication, and Access Control PR.AA	70.8%
		Awareness and Training PR.AT	62.5%
		Data Security PR.DS	65.0%
		Platform Security PR.PS	70.8%
		Technology Infrastructure Resilience PR.IR	68.8%
Detect DE	**63.8%**		
		Continuous Monitoring DE.CM	65.0%
		Adverse Event Analysis DE.AE	62.5%
Respond RS	**60.6%**		
		Incident Management RS.MA	30.0%
		Incident Analysis RS.AN	62.5%
		Incident Response Reporting and Communication RS.CO	75.0%
		Incident Mitigation RS.MI	75.0%
Recover RC	**68.8%**		
		Incident Recovery Plan Execution RC.RP	62.5%
		Incident Recovery Communication RC.CO	75.0%

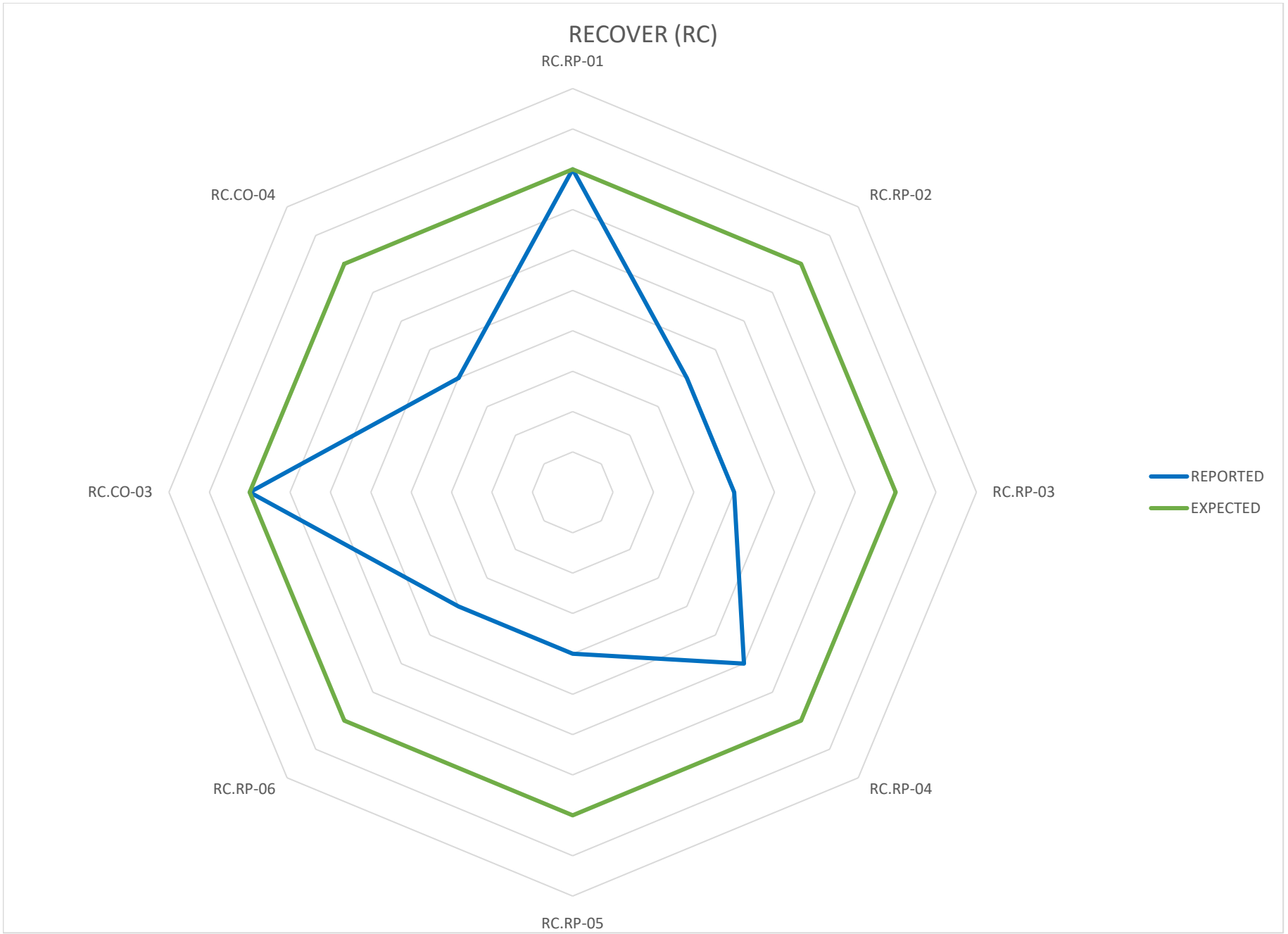

GOVERN (GV)
GV.OC-01
GV.OC-02
GV.OC-03
GV.OC-04
GV.OC-05
GV.RM-01
GV.RM-02
GV.RM-03
GV.RM-04
GV.RM-05
GV.RM-06
GV.RM-07
GV.SC-01
GV.SC-02
GV.SC-03
GV.SC-04
GV.SC-05
GV.SC-06
GV.SC-07
GV.SC-08
GV.SC-09
GV.SC-10
GV.RR-01
GV.RR-02
GV.RR-03
GV.RR-04
GV.PO-01
GV.PO-02
GV.OV-01
GV.OV-02
GV.OV-03
REPORTED
EXPECTED


IDENTIFY (ID)
ID.AM-01
ID.AM-02
ID.AM-03
ID.AM-04
ID.AM-05
ID.AM-07
ID.AM-08
ID.RA-01
ID.RA-02
ID.RA-03
ID.RA-04
ID.RA-05
ID.RA-06
ID.RA-07
ID.RA-08
ID.RA-09
ID.IM-01
ID.IM-02
ID.IM-03
ID.IM-04
REPORTED
EXPECTED


PROTECT (PR)
PR.AA-01
PR.AA-02
PR.AA-03
PR.AA-04
PR.AA-05
PR.AA-06
PR.AT-01
PR.AT-02
PR.DS-01
PR.DS-02
PR.DS-09
PR.DS-10
PR.DS-11
PR.PS-01
PR.PS-02
PR.PS-03
PR.PS-04
PR.PS-05
PR.PS-06
PR.IR-01
PR.IR-02
PR.IR-03
PR.IR-04
REPORTED
EXPECTED


DETECT (DE)
DE.CM-01
DE.CM-02
DE.CM-03
DE.CM-06
DE.CM-09
DE.AE-02
DE.AE-03
DE.AE-04
DE.AE-06
DE.AE-07
DE.AE-08
REPORTED
EXPECTED


RESPOND (RS)
RS.MA-01
RS.MA-02
RS.MA-03
RS.MA-04
RS.MA-05
RS.AN-03
RS.AN-06
RS.AN-07
RS.AN-08
RS.CO-02
RS.CO-03
RS.MI-01
RS.MI-02
REPORTED
EXPECTED


RECOVER (RC)
RC.RP-01
RC.RP-02
RC.RP-03
RC.RP-04
RC.RP-05
RC.RP-06
RC.CO-03
RC.CO-04
REPORTED
EXPECTED

NIST CSF 2.0
6 Functional Areas
22 Categories
106 Subcategories

Public Draft: The NIST Cybersecurity Framework 2.0

SCALE
5.0 "World class, setting the standard"
4.5 "Standard Operating Procedure, aligned with the business, aligned with best practices"
4.0 "Standard Operating Procedure, Business as Usual (BAU)"
3.5 "Occurs, consistently, aligned with ERM business risk and adversarial threat"
3.0 "Occurs, consistently, aligned with CSRM technical vulnerabilities and the attack surface"
2.5 "Occurs, not consistently, structured"
2.0 "Occurs, not consistently, unstructured"
1.5 "Initial process and documentation in place"
1.0 "ADHOC or only when necessary"
0.5 "Awareness and acceptance of the need exists"
0.0 "Not doing this at all"

Cyber Hygiene Profile Mapping

COST PROJECTIONS
1 Labor Hour $ cost per each 106 Subcategories = 106 Labor Hours to fill out ATO Attestation Form/Questions
Knowledge Management/Intelligence = 14 Labor Hours to convert ATO data to KM Repo & Executive Dashboard
TOTAL = 120 Labor Hours using Microsoft Suite (Excel, Sharepoint, PowerBI) x $72hr average FTE = **$8640 COST**
*AI (GPT, LLMs) could increase efficiency (ex. ChatBots) & improve cost savings

Authorization to Operate / Attestation of Security Assessment (irs.gov)

GV.OC-01 The organizational mission is understood and informs cybersecurity risk management.

Level 5.0: "World class, setting the standard"

1. Has your organization's cybersecurity risk management been recognized by a leading industry authority for its excellence in aligning with the organizational mission? [YES/NO]
2. Does your organization actively contribute to setting global standards for cybersecurity risk management in relation to organizational missions? [YES/NO]
3. Are your cybersecurity policies and practices regularly benchmarked against top-performing organizations and adjusted to maintain a leading edge? [YES/NO]
4. Does your organization conduct continuous, proactive threat intelligence to anticipate and mitigate risks before they impact business operations, consistently aligned with the organizational mission? [YES/NO]
5. Is there a dedicated function within your organization that ensures ongoing alignment of cybersecurity practices with evolving business strategies and organizational mission? [YES/NO]

Level 4.5: "Standard Operating Procedure, aligned with the business, aligned with best practices"

1. Are your cybersecurity standard operating procedures (SOPs) fully integrated with business objectives and the organizational mission? [YES/NO]
2. Do your SOPs reflect current best practices in cybersecurity and are they reviewed regularly for continuous improvement? [YES/NO]
3. Is there a systematic and formal process for updating your cybersecurity practices in line with changes in the organizational mission? [YES/NO]
4. Does your organization have a track record of successful audits that confirm the alignment of cybersecurity SOPs with the business and organizational mission? [YES/NO]
5. Are decision-makers across the business units held accountable for enforcing cybersecurity SOPs that are aligned with the organizational mission? [YES/NO]

Level 4.0: "Standard Operating Procedure, Business as Usual (BAU)"

1. Are cybersecurity practices deeply embedded in your organization's daily operations and business as usual activities? [YES/NO]
2. Do your employees receive regular training to ensure that cybersecurity SOPs are followed as part of their daily responsibilities? [YES/NO]
3. Are your cybersecurity SOPs documented, well communicated across the organization, and adhered to by all departments? [YES/NO]
4. Is adherence to cybersecurity SOPs a criterion in performance evaluations for relevant staff within your organization? [YES/NO]
5. Does your organization's leadership routinely demonstrate commitment to cybersecurity SOPs through their directives and actions? [YES/NO]

Level 3.5: "Occurs, consistently, aligned with ERM business risk and adversarial threat"

1. Does your cybersecurity strategy include a clear and consistent alignment with enterprise risk management (ERM) that addresses both business risks and adversarial threats? [YES/NO]
2. Are threat assessments and business risk analyses conducted regularly to inform and adjust cybersecurity practices? [YES/NO]
3. Is the cybersecurity team equipped with the tools and authority to act upon ERM insights in a manner consistent with the organizational mission? [YES/NO]
4. Does your organization use a formalized process to ensure that cybersecurity measures address specific ERM-identified threats and risks? [YES/NO]
5. Are the outcomes of aligning cybersecurity with ERM and adversarial threats reviewed and reported to the senior management periodically? [YES/NO]

Level 3.0: "Occurs, consistently, aligned with CSRM technical vulnerabilities and the attack surface"

1. Are your cybersecurity activities consistently focused on identifying and mitigating technical vulnerabilities relative to your organization's attack surface? [YES/NO]
2. Does your organization have a comprehensive inventory of assets that is regularly updated to reflect the current attack surface for vulnerability management? [YES/NO]
3. Are cybersecurity controls reviewed and adjusted consistently to mitigate known and emerging technical vulnerabilities? [YES/NO]
4. Does your organization employ continuous monitoring to detect changes in the attack surface and technical vulnerabilities? [YES/NO]
5. Are the efforts to address technical vulnerabilities and the attack surface documented and aligned with the cybersecurity risk management framework? [YES/NO]

Level 2.5: "Occurs, not consistently, structured"

1. Are there structured protocols for cybersecurity risk management that are sometimes not consistently followed? [YES/NO]
2. Does your organization periodically review the alignment of cybersecurity activities with the organizational mission, even if not on a regular basis? [YES/NO]
3. Are there defined processes in place for cybersecurity risk management that require further integration into everyday business practices? [YES/NO]
4. Does your cybersecurity team have a structured approach to risk management which is applied in an ad-hoc manner during certain projects or in specific departments? [YES/NO]
5. Is there inconsistency in the way cybersecurity risk management informs decision-making across different levels of the organization? [YES/NO]

Level 2.0: "Occurs, not consistently, unstructured"

1. Does your organization carry out cybersecurity activities informed by the organizational mission without a formal structure? [YES/NO]
2. Are cybersecurity risk management practices in place that lack a formal framework and occur sporadically across the organization? [YES/NO]
3. Do some departments or teams consider cybersecurity in their processes more than others, leading to an unstructured approach organization-wide? [YES/NO]
4. Is there a recognition of the organizational mission within cybersecurity discussions, even if this is not reflected in a structured policy or process? [YES/NO]
5. Are efforts to manage cybersecurity risks done based on individual initiative rather than an organization-wide structured approach? [YES/NO]

Level 1.5: "Initial process and documentation in place"

1. Has your organization developed initial documentation for cybersecurity risk management processes? [YES/NO]
2. Are there basic cybersecurity policies in place that reference the organizational mission, although not fully operationalized? [YES/NO]
3. Does your organization have foundational cybersecurity risk management processes that are not yet fully integrated into business practices? [YES/NO]
4. Is there an initial effort to communicate the importance of the organizational mission within the realm of cybersecurity to the relevant stakeholders? [YES/NO]
5. Are the documented processes for cybersecurity risk management occasionally referred to during strategic planning or crisis management? [YES/NO]

Level 1.0: "ADHOC or only when necessary"

1. Does your organization address cybersecurity in relation to the organizational mission only when specific issues arise? [YES/NO]
2. Are cybersecurity risk management practices initiated as a reaction to incidents rather than as a proactive measure? [YES/NO]
3. Do discussions regarding the alignment of cybersecurity activities with the organizational mission occur on an ad-hoc basis? [YES/NO]
4. Is there a lack of a routine or consistent approach to cybersecurity risk management across the organization? [YES/NO]
5. Are cybersecurity measures primarily implemented in an uncoordinated fashion following an incident or breach? [YES/NO]

Level 0.5: "Awareness and acceptance of the need exists"

1. Is there a general awareness within your organization of the need to align cybersecurity risk management with the organizational mission, but no formal action taken? [YES/NO]
2. Has the organization identified the necessity for cybersecurity risk management, yet lacks a comprehensive strategy or policy? [YES/NO]
3. Does your organization recognize the importance of cybersecurity to support the organizational mission without having established a clear path to integration? [YES/NO]
4. Are there informal talks about the potential impact of cybersecurity on achieving the organizational mission without concrete plans? [YES/NO]
5. Is there a consensus among leadership on the importance of cybersecurity, but no alignment with business objectives or mission-driven actions? [YES/NO]

Level 0.0: "Not doing this at all"

1. Does your organization completely lack a cybersecurity risk management plan that addresses the organizational mission? [YES/NO]
2. Are there no cybersecurity policies, processes, or documentation that reference or incorporate the organizational mission? [YES/NO]
3. Is there a total absence of cybersecurity considerations in strategic business decisions related to the organizational mission? [YES/NO]
4. Does your organization have no defined cybersecurity leadership or dedicated resources to align with the organizational mission? [YES/NO]
5. Is your organization without any form of cybersecurity awareness or training that relates to the organizational mission? [YES/NO]

GV.OC-02 Internal and external stakeholders are determined, and their needs and expectations regarding cybersecurity risk management are understood.

Level 5.0: "World class, setting the standard"

1. Has your organization's approach to engaging with stakeholders in cybersecurity risk management been recognized as a best practice leader by industry peers or standards bodies? [YES/NO]
2. Does your organization engage with stakeholders to co-develop cybersecurity strategies and innovative risk management solutions that set industry benchmarks? [YES/NO]
3. Are stakeholder relationships managed through a centralized system that ensures their needs and expectations are exceeded, influencing industry trends in cybersecurity? [YES/NO]
4. Is there a continuous feedback loop with stakeholders that contributes to the evolution of cybersecurity practices, which in turn shapes global standards? [YES/NO]
5. Are your stakeholder engagement processes in cybersecurity risk management audited externally and shown to achieve excellence beyond compliance? [YES/NO]

Level 4.5: "Standard Operating Procedure, aligned with the business, aligned with best practices"

1. Are stakeholder needs and expectations systematically integrated into your cybersecurity SOPs and reviewed against best practices regularly? [YES/NO]
2. Does your organization maintain up-to-date profiles for all stakeholders, including their specific cybersecurity needs and expectations? [YES/NO]
3. Are there established channels for continuous stakeholder communication that are evaluated and refined as part of your cybersecurity SOPs? [YES/NO]
4. Do your cybersecurity SOPs include routine stakeholder engagement that aligns with both business objectives and recognized best practices? [YES/NO]
5. Is there a process to ensure stakeholder feedback is incorporated into risk management procedures, keeping them aligned with business and best practice changes? [YES/NO]

Level 4.0: "Standard Operating Procedure, Business as Usual (BAU)"

1. Are stakeholder engagement activities in cybersecurity risk management included in the routine responsibilities of relevant staff? [YES/NO]
2. Does your organization have established SOPs for regularly identifying and updating stakeholder needs and expectations in cybersecurity? [YES/NO]
3. Are there formal procedures for involving stakeholders in periodic reviews of cybersecurity risks and controls as part of BAU? [YES/NO]
4. Do SOPs require all business units to engage with relevant stakeholders when new cybersecurity initiatives are undertaken? [YES/NO]
5. Are training and awareness programs in place for staff to understand how stakeholder needs inform cybersecurity risk management within their roles? [YES/NO]

Level 3.5: "Occurs, consistently, aligned with ERM business risk and adversarial threat"

1. Is stakeholder input consistently sought and factored into the ERM process to address both business risks and adversarial threats? [YES/NO]
2. Does your organization have a formal mechanism to ensure stakeholder concerns are addressed when updating cybersecurity measures? [YES/NO]
3. Are regular risk assessments conducted with stakeholder involvement to ensure alignment with their needs in managing adversarial threats? [YES/NO]
4. Are stakeholder expectations documented and considered in the consistent application of cybersecurity controls against identified risks? [YES/NO]
5. Is there a regular review process with stakeholders to discuss and align on ERM strategies and threat mitigation tactics? [YES/NO]

Level 3.0: "Occurs, consistently, aligned with CSRM technical vulnerabilities and the attack surface"

1. Are stakeholder needs regarding technical vulnerabilities and attack surface consistently gathered and addressed in your CSRM? [YES/NO]
2. Does your organization have a formalized process for involving stakeholders in understanding and managing the technical aspects of cybersecurity risk? [YES/NO]
3. Are there established intervals at which stakeholders review and provide input on the organization's technical vulnerability assessments? [YES/NO]
4. Does your organization ensure that stakeholder expectations are consistently reflected in the prioritization and remediation of technical vulnerabilities? [YES/NO]
5. Is the dialogue with stakeholders about technical cybersecurity issues and attack surface management a regular part of your risk management cycle? [YES/NO]

Level 2.5: "Occurs, not consistently, structured"

1. Does your organization have structured, though not consistently executed, processes for engaging stakeholders in cybersecurity risk discussions? [YES/NO]
2. Are there defined intervals for stakeholder engagement in cybersecurity that are not always adhered to due to operational challenges? [YES/NO]
3. Is stakeholder input on cybersecurity risks sought during specific events or changes in the threat landscape rather than continuously? [YES/NO]
4. Are there formal mechanisms for stakeholder engagement that are sometimes bypassed or overlooked in the rush of daily operations? [YES/NO]
5. Does your organization have a structured plan for stakeholder engagement that is not fully integrated into all levels of cybersecurity management? [YES/NO]

Level 2.0: "Occurs, not consistently, unstructured"

1. Does your organization recognize the importance of stakeholder input in cybersecurity risk management but lacks a regular structured approach? [YES/NO]
2. Are there informal efforts to understand stakeholder needs that are not systematically captured or addressed in cybersecurity planning? [YES/NO]
3. Do stakeholder engagements happen in an ad-hoc manner, influenced by individual initiative rather than organizational policy? [YES/NO]
4. Is the understanding of stakeholder expectations in cybersecurity sporadic and dependent on the occurrence of incidents or specific demands? [YES/NO]
5. Are there recognized stakeholders whose cybersecurity concerns are only occasionally considered in risk management? [YES/NO]

Level 1.5: "Initial process and documentation in place"

1. Has your organization begun documenting stakeholder needs regarding cybersecurity but not yet operationalized the process? [YES/NO]
2. Are initial processes for stakeholder engagement in place that are not fully developed or regularly utilized? [YES/NO]
3. Is there a rudimentary framework for identifying stakeholder expectations that has yet to be integrated into routine risk management activities? [YES/NO]
4. Does your organization have foundational documentation on stakeholder engagement that is not consistently referenced or updated? [YES/NO]
5. Are there early-stage efforts to align stakeholder expectations with cybersecurity measures that lack depth and consistency? [YES/NO]

Level 1.0: "ADHOC or only when necessary"

1. Does your organization address stakeholder needs in cybersecurity risk management only in response to specific events or requests? [YES/NO]
2. Are engagements with stakeholders regarding cybersecurity performed sporadically and without a predefined process? [YES/NO]
3. Is the consideration of stakeholder expectations in cybersecurity initiatives taken on a case-by-case basis rather than systematically? [YES/NO]
4. Does your organization lack a routine mechanism for capturing and addressing stakeholder needs, leading to ad-hoc engagement practices? [YES/NO]
5. Are stakeholder concerns regarding cybersecurity risks occasionally discussed but not formally documented or consistently acted upon? [YES/NO]

Level 0.5: "Awareness and acceptance of the need exists"

1. Is there awareness within your organization of the need to understand stakeholder expectations in cybersecurity, but no formal action has been taken? [YES/NO]
2. Has the organization identified the importance of stakeholder engagement but lacks any structured approach to capturing their needs? [YES/NO]
3. Are there informal discussions about stakeholder needs in cybersecurity that are not yet part of an official engagement strategy? [YES/NO]
4. Is there a general consensus on the relevance of stakeholder expectations to cybersecurity, yet no practical steps toward integration? [YES/NO]
5. Do leaders recognize the value of stakeholder input for cybersecurity risk management without it being reflected in business practices? [YES/NO]

Level 0.0: "Not doing this at all"

1. Does your organization completely disregard stakeholder needs and expectations in the context of cybersecurity risk management? [YES/NO]
2. Are there no established processes or plans in place to engage with stakeholders on cybersecurity matters? [YES/NO]
3. Is there a lack of recognition of who the internal and external stakeholders are in the realm of cybersecurity within your organization? [YES/NO]
4. Does your organization have no formal or informal means of understanding or addressing stakeholder expectations in cybersecurity? [YES/NO]
5. Is there an absence of any documented evidence that stakeholder needs have been considered in the development of cybersecurity policies or practices? [YES/NO]

GV.OC-03 Legal, regulatory, and contractual requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.

Level 5.0: "World class, setting the standard"

1. Does the organization proactively participate in shaping global cybersecurity regulations and privacy standards? [YES/NO]
2. Has the organization's cybersecurity legal and regulatory compliance been validated by third-party auditors against international standards? [YES/NO]
3. Is there a documented and proven track record of zero compliance violations or breaches related to cybersecurity regulations, privacy, and civil liberties over the past five years? [YES/NO]
4. Does the organization have a dedicated cross-functional team that continuously monitors and implements changes in cybersecurity laws and regulations worldwide? [YES/NO]
5. Are all new products, services, and processes subject to a comprehensive legal and regulatory cybersecurity review before being released or implemented? [YES/NO]

Level 4.5: "Standard Operating Procedure, aligned with the business, aligned with best practices"

1. Are cybersecurity legal and regulatory requirements integrated into the daily procedures of the organization's cybersecurity team? [YES/NO]
2. Does the organization routinely update its cybersecurity policies to reflect current legal and regulatory standards and best practices? [YES/NO]
3. Is there a formal program in place to train all employees on cybersecurity legal and regulatory changes relevant to their role? [YES/NO]
4. Has the organization established and maintained a compliance calendar that schedules all necessary legal and regulatory cybersecurity reviews and updates? [YES/NO]
5. Does the organization have an established process to ensure contractual obligations related to cybersecurity are always met and documented? [YES/NO]

Level 4.0: "Standard Operating Procedure, Business as Usual (BAU)"

1. Are all employees aware of and do they adhere to the cybersecurity legal and regulatory requirements that affect their work? [YES/NO]
2. Does the organization have a formalized process for regularly reviewing and updating its cybersecurity policies to comply with legal and regulatory changes? [YES/NO]
3. Are legal and regulatory requirements regarding cybersecurity reviewed and incorporated into the organization's risk management process? [YES/NO]
4. Does the company maintain an updated repository of all relevant cybersecurity laws, regulations, and contractual obligations? [YES/NO]
5. Is there an assigned role or team responsible for tracking compliance with cybersecurity legal and regulatory requirements? [YES/NO]

Level 3.5: "Occurs, consistently, aligned with ERM business risk and adversarial threat"

1. Has the organization identified and documented all cybersecurity legal, regulatory, and contractual requirements specific to its industry and operating regions? [YES/NO]
2. Does the organization's Enterprise Risk Management (ERM) program specifically address compliance with cybersecurity legal and regulatory requirements? [YES/NO]
3. Are there regular audits performed to ensure compliance with cybersecurity legal and regulatory requirements? [YES/NO]
4. Has the organization faced any legal or regulatory non-compliance issues that have been addressed and resolved in the past two years? [YES/NO]
5. Does the organization evaluate new threats in the context of legal and regulatory compliance to adjust its cybersecurity posture accordingly? [YES/NO]

Level 3.0: "Occurs, consistently, aligned with CSRM technical vulnerabilities and the attack surface"

1. Is there a process to ensure that technical vulnerabilities are assessed in light of current cybersecurity laws and regulations? [YES/NO]
2. Does the organization consider legal and regulatory requirements in its Cybersecurity Risk Management (CSRM) framework? [YES/NO]
3. Are incident response plans updated to comply with legal and regulatory reporting obligations? [YES/NO]
4. Does the organization conduct regular training for technical staff on compliance with cybersecurity legal and regulatory requirements? [YES/NO]
5. Are cybersecurity controls tested against legal and regulatory requirements to ensure effectiveness? [YES/NO]

Level 2.5: "Occurs, not consistently, structured"

1. Has the organization identified legal and regulatory requirements pertaining to cybersecurity, even if not fully integrated into cybersecurity practices? [YES/NO]
2. Is there a designated individual or team responsible for understanding and communicating cybersecurity legal and regulatory requirements to the relevant parts of the organization? [YES/NO]
3. Are there documented instances of the organization acting upon identified legal and regulatory requirements? [YES/NO]
4. Does the organization have a formal but irregularly updated policy for cybersecurity legal and regulatory compliance? [YES/NO]
5. Are efforts to comply with cybersecurity legal and regulatory requirements typically reactive rather than proactive? [YES/NO]

Level 2.0: "Occurs, not consistently, unstructured"

1. Is there awareness among the management team of the legal and regulatory obligations concerning cybersecurity? [YES/NO]
2. Has the organization taken steps to comply with known cybersecurity legal and regulatory requirements without a formal strategy? [YES/NO]
3. Are there informal procedures that occasionally reference cybersecurity legal and regulatory compliance? [YES/NO]
4. Does the organization rely on external counsel or ad hoc measures to address cybersecurity legal and regulatory issues as they arise? [YES/NO]
5. Has the organization responded to any legal or regulatory compliance issues after they have occurred? [YES/NO]

Level 1.5: "Initial process and documentation in place"

1. Has the organization begun documenting cybersecurity legal and regulatory requirements relevant to its operations? [YES/NO]
2. Is there an initial process in place for incorporating cybersecurity legal and regulatory compliance into business practices? [YES/NO]
3. Has the organization identified a point of contact for cybersecurity legal and regulatory matters? [YES/NO]
4. Are there initial efforts to communicate the importance of cybersecurity legal and regulatory compliance to employees? [YES/NO]
5. Does the organization have a basic understanding of the penalties for non-compliance with cybersecurity regulations? [YES/NO]

Level 1.0: "ADHOC or only when necessary"

1. Does the organization address cybersecurity legal and regulatory requirements on an as-needed basis? [YES/NO]
2. Are cybersecurity legal and regulatory matters handled in an ad hoc manner by whichever team member is available? [YES/NO]
3. Is the compliance with cybersecurity regulations only considered in response to external prompts, such as a legal challenge or a direct threat? [YES/NO]
4. Does the organization have any documented evidence of compliance with cybersecurity legal and regulatory requirements, even if not systematic? [YES/NO]
5. Is there a reliance on external parties to alert the organization to its cybersecurity legal and regulatory obligations? [YES/NO]

Level 0.5: "Awareness and acceptance of the need exists"

1. Is there an awareness at the leadership level that cybersecurity legal and regulatory compliance needs to be addressed? [YES/NO]
2. Does the organization recognize the importance of complying with cybersecurity legal and regulatory requirements, although it has not yet taken action? [YES/NO]
3. Has the organization expressed an intention to develop strategies for managing cybersecurity legal and regulatory compliance? [YES/NO]
4. Are there informal discussions about the impact of cybersecurity legal and regulatory requirements on the organization? [YES/NO]
5. Is there a general acknowledgment among staff that cybersecurity legal and regulatory compliance is important? [YES/NO]

Level 0.0: "Not doing this at all"

1. Does the organization completely lack a process for identifying and managing cybersecurity legal and regulatory requirements? [YES/NO]
2. Is the organization unaware of the legal and regulatory requirements pertaining to cybersecurity in its jurisdiction? [YES/NO]
3. Has the organization never conducted an audit or assessment of its compliance with cybersecurity regulations? [YES/NO]
4. Are there no resources allocated to manage cybersecurity legal and regulatory risks? [YES/NO]
5. Does the organization lack any form of policy or procedure documentation regarding cybersecurity legal and regulatory compliance? [YES/NO]

GV.OC-04 Critical objectives, capabilities, and services that stakeholders depend on or expect from the organization are determined and communicated.

Level 5.0: "World class, setting the standard"

[YES/NO]
[YES/NO]
[YES/NO]
[YES/NO]
[YES/NO]

Level 4.5: "Standard Operating Procedure, aligned with the business, aligned with best practices"

[YES/NO]
[YES/NO]
[YES/NO]
[YES/NO]
[YES/NO]

Level 4.0: "Standard Operating Procedure, Business as Usual (BAU)"

[YES/NO]
[YES/NO]
[YES/NO]
[YES/NO]
[YES/NO]

Level 3.5: "Occurs, consistently, aligned with ERM business risk and adversarial threat"

[YES/NO]
[YES/NO]
[YES/NO]
[YES/NO]
[YES/NO]

Level 3.0: "Occurs, consistently, aligned with CSRM technical vulnerabilities and the attack surface"

[YES/NO]
[YES/NO]
[YES/NO]
[YES/NO]
[YES/NO]

Level 2.5: "Occurs, not consistently, structured"

[YES/NO]
[YES/NO]
[YES/NO]
[YES/NO]
[YES/NO]

Level 2.0: "Occurs, not consistently, unstructured"

[YES/NO]
[YES/NO]
[YES/NO]
[YES/NO]
[YES/NO]

Level 1.5: "Initial process and documentation in place"

[YES/NO]
[YES/NO]
[YES/NO]
[YES/NO]
[YES/NO]

Level 1.0: "ADHOC or only when necessary"

[YES/NO]
[YES/NO]
[YES/NO]
[YES/NO]
[YES/NO]

Level 0.5: "Awareness and acceptance of the need exists"

[YES/NO]
[YES/NO]
[YES/NO]
[YES/NO]
[YES/NO]

Level 0.0: "Not doing this at all"

[YES/NO]
[YES/NO]
[YES/NO]
[YES/NO]
[YES/NO]

GV.OC-05 Outcomes, capabilities, and services that the organization depends on are determined and communicated.