

EMKAL^{Inc.}

Information Technology Experts

Prepared by: Ray Angod

NIST CSF 2.0 Lead Implementer and Lead Auditor



NIST CSF 2.0 Cybersecurity Maturity Assessment for Sample Hospital

Current-State Profile, Target-State Profile, Gap Analysis, and
Remediation Roadmap

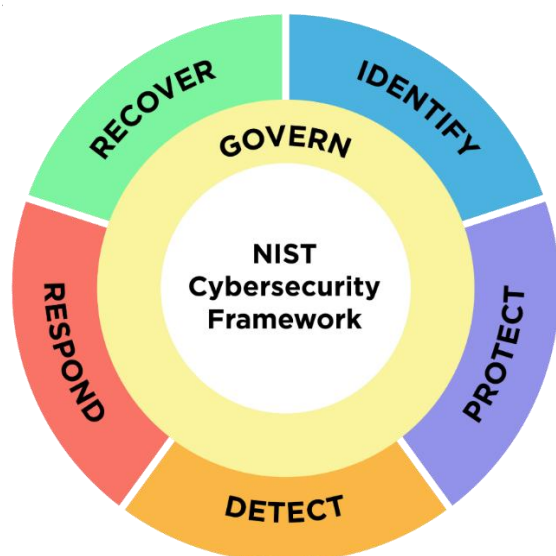
Table of Contents

1. Purpose and Scope.....	2
2. Assessment Methodology	3
3. Executive Scorecard	4
4. Executive Remediation Roadmap	4
5. Category Assessments	6
5.1 GOVERN (GV)	7
5.2 DETECT (DE)	8
6. Remediation Roadmap	9
Risk Rating: Very High	9
Risk Rating: High	10
Risk Rating: Medium	12
Appendix A: Evaluation of Individual Outcomes.....	14
GOVERN	14
GV.OC – Organizational Context	14
GV.RM — Risk Management Strategy	15
GV.RR – Roles, Responsibilities, and Authorities	16
GV.PO – Policy.....	18
GV.OV – Oversight	18
GV.SC – Cybersecurity Supply Chain Management	19
DETECT.....	23
DE.CM – Continuous Monitoring.....	23
DE.AE – Adverse Event Analysis.....	24

1. Purpose and Scope

This sample assessment demonstrates EMKAL's methodology and deliverables when evaluating an organization's cybersecurity risk governance and management practices against the **NIST Cybersecurity Framework (CSF) 2.0**. This report only contains the Govern and Detect functions to provide an example of what our clients should expect.

This report establishes a defensible Current Profile, defines a risk-informed Target Profile, identifies material gaps, and converts those gaps into a prioritized improvement roadmap. The assessment is designed for executive decision-making, operational planning, and reporting to regulators; it is not a certification or a guarantee of security.



Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

This report was created by Ray Angod, a former nuclear medicine technologist who holds an MBA (Health Industry Management) and is a NIST Cybersecurity Lead Implementer and Auditor, with certifications in cybersecurity and disaster recovery. He is also a Certified Training and Development Professional and an experienced facilitator. He combines this unique blend of expertise to help organizations develop cybersecurity programs that strengthen their security posture and meet compliance requirements.

2. Assessment Methodology

For each Category, there exist multiple outcomes (also referred to as “subcategories”), which were assessed through interviews, surveys, document review, configuration inspection, and metrics. This assessment employs a two-tier evaluation methodology:

Tier 2: Specific outcomes are scored using the Capability Maturity Model (CMM) from a range of 0 to 5 (see table below)

Tier 1: The arithmetic average of Tier 2 scores, which approximates the current state of cybersecurity maturity in a single number for each Category.

Score	Maturity level	Description
0	Not Performed	Absent or performed only in an ad-hoc, reactive manner. No documented procedures, assigned ownership, or evidence of outcome achievement exists.
1	Initial	Achieved informally by individual effort rather than organizational practice. Activity occurs occasionally and without repeatable method; results depend on specific people rather than defined processes.
2	Developing	Procedure exists and is followed with some consistency, but is not yet formally documented, standardized, or communicated across the organization.
3	Defined	The outcome is achieved through documented, standardized, and organization-wide practice. Policies, procedures, and roles are established; responsibilities are assigned and understood; evidence of execution is retained. This is the minimum level at which this assessment’s rubric considers the outcome substantively achieved
4	Measured	Outcome achievement is actively measured using defined metrics, tracked against targets, and reviewed at planned intervals. Leadership uses quantitative evidence to direct resources, identify weak areas, and verify effectiveness.
5	Adaptive	The organization continuously improves how it achieves the outcome, incorporating threat landscape changes, lessons learned from incidents, stakeholder feedback, and insights from peer organizations. Improvements are evidence-based and integrated with enterprise risk management cycles.

3. Executive Scorecard

CSF Function	Current Score	12-Month Target Score
GOVERN (GV)	0.9	2.9
IDENTIFY (ID)		
PROTECT (PR)		
DETECT (DE)	1.3	2.6
RESPOND (RS)		
RECOVER (RC)		

4. Executive Remediation Roadmap

A. Implement Enterprise Risk Management (ERM)

NIST CSF 2.0 is an extension of ERM, and cybersecurity risks should be addressed alongside other high-level risks (e.g., privacy, financial, reputational, etc.). For example, risk appetite statements should be documented to guide decisions about which cybersecurity risks should be accepted, mitigated, transferred, or avoided. It is recommended to implement ERM based on ISO 31000 and ISO 31010 guidelines as best practices recognized internationally and across industries, which would include risk appetite and risk tolerance statements, a risk matrix, and Key Risk Indicators (KRIs).

Benefit: Places cyber risk in the same decision-making framework as other risk such as patient safety and financial sustainability. This approach shifts cybersecurity from a siloed IT problem and connects it with critical services such as patient care, and will make cyber risks easier to evaluate and manage at an executive level.

B. Conduct a Business Impact Analysis (BIA)

In order to determine which services are most vulnerable to a cyberattack and should therefore be most critical to protect, it is first necessary to identify and prioritize the organization's functions and processes, and understand which ones will have the greatest impact should they not be available.

Benefit: Identifies which capabilities are most critical at Sample Hospital, which dictates which supporting IT services should be prioritized. By establishing Maximum Tolerable Downtime, senior leadership will be able to make more informed decisions about cybersecurity investments and how to maintain patient care during cyber incidents.

C. Define Cybersecurity Roles & Responsibilities

Based on survey and interview responses, cybersecurity at Sample Hospital appears to be almost completely under the purview of the IT Department. However, cybersecurity is an enterprise-level risk and requires input from other internal resources, such as Privacy, HR, and Clinical Leadership. To achieve this, it is recommended to prepare a RACI matrix where all NIST CSF outcomes are assigned roles of responsible, accountable, consulted, or informed. This will clarify expectations and reduce the likelihood of gaps due to silos.

Benefit: Ensures that cybersecurity responsibilities are not siloed within the IT Department, and all relevant parties are aware of their role in maintaining and improving cybersecurity at Sample Hospital. It can also reveal where no one is responsible for key aspects of cybersecurity, and these gaps can be filled prior to a cyber incident.

D. Map External Dependencies

Sample Hospital relies on several cloud services, some of which are considered “critical” by clinical leaders. These external dependencies should be mapped to services, with failure points identified that would compromise strategic objectives such as patient care. The risk likelihood and impact of failure points should be assessed based on the ERM, and mitigating controls should be implemented where appropriate.

Benefit: Gain more visibility of how your critical services could be interrupted, and proactively implement controls and/or redundancy measures to mitigate the impact if a cloud service provider experiences downtime. This will provide greater resiliency for Sample Hospital and provide assurance that service delivery will be less easily disrupted.

E. Complete the Legal and Regulatory Obligations Register

There is currently a disconnect between Compliance and the IT Department, where the IT Team is recommending and implementing technical controls without a clear understanding of the legal and regulatory obligations of Sample Hospital. Having access to an updated and maintained register will enable them to prioritize their recommendations to ensure compliance.

Benefit: Provides the IT Department with clearer guidelines of which technical controls should be prioritized in order to keep Sample Hospital compliant. Also promotes communication and collaboration between IT and Compliance to close regulatory gaps.

5. Category Assessments

Each Category's **Current Score** is the Tier 1 score of all associated outcomes.

Each Category's **Target Score** is what could be reasonably achievable over the next 12 months if recommended actions are implemented.

Each Category's **Gap** was calculated by subtracting the Target from the Current Score.

Risk Ratings, which are used to prioritize implementation order, are assigned to each outcome and were determined based on the Gap as categorized below:

2.6 – 3.0: VERY HIGH

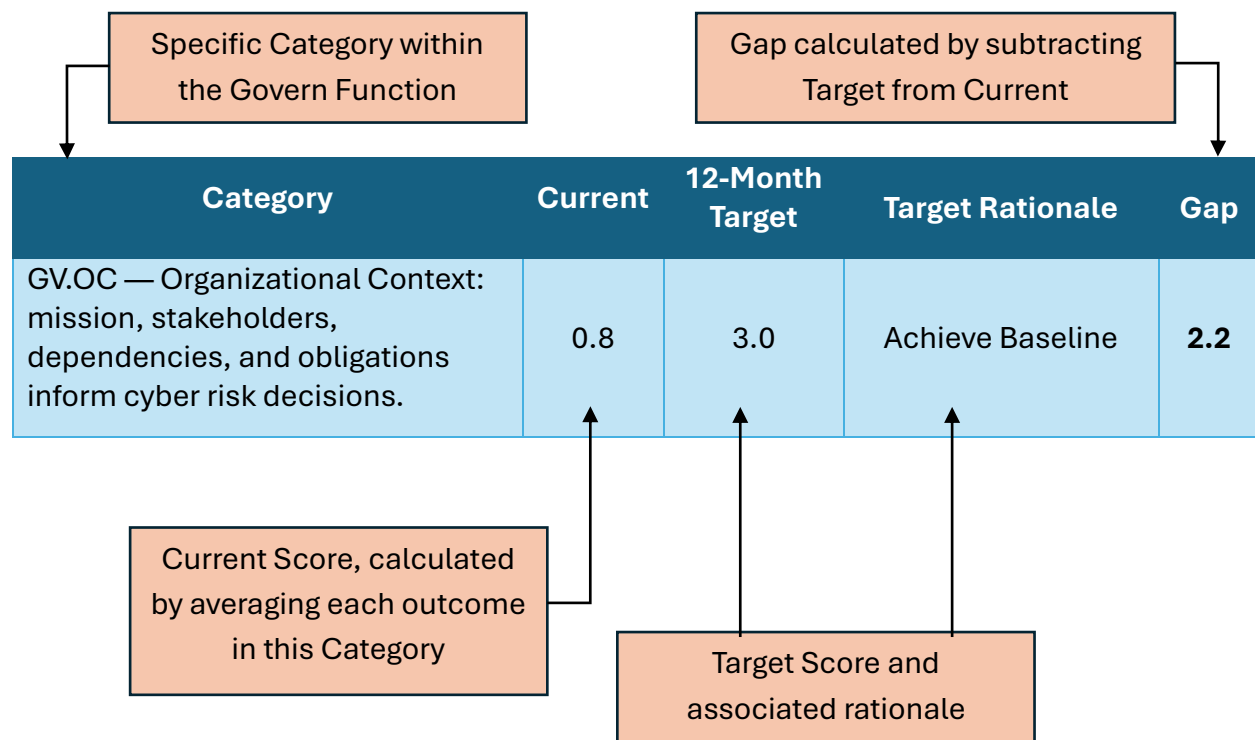
2.1 – 2.5: HIGH

1.1 – 2.0: MEDIUM

1.0 or less: LOW

See Appendix A for detailed notes and scoring for each individual outcome.

Example:



5.1 GOVERN (GV)

Category	Current	12-Month Target	Target Rationale	Gap
GV.OC — Organizational Context: mission, stakeholders, dependencies, and obligations inform cyber risk decisions.	0.8	3.0	Achieve Baseline	2.2
GV.RM — Risk Management Strategy: objectives, appetite, tolerance, methods, and communication are established.	0.6	2.8	Achieve Baseline, except for GV.RM-07, which has a Target of 2.0 critical services are less dependent on it	2.2
GV.RR — Roles, Responsibilities, and Authorities: accountability and adequate resourcing are defined.	1.0	3.0	Achieve Baseline	2.0
GV.PO — Policy: cybersecurity policy is established, communicated, enforced, and maintained.	0.8	3.0	Achieve Baseline	2.2
GV.OV — Oversight: performance and risk-management results are reviewed and adjusted.	0.4	3.0	Achieve Baseline	2.6
GV.SC — Cybersecurity Supply Chain Risk Management: supplier risk is governed throughout the relationship lifecycle.	1.9	2.5	Complete internal improvements before addressing vendor risk	0.6
TOTAL	0.9	2.9		2.0

5.2 DETECT (DE)

Category	Current	12-Month Target	Target Rationale	Gap
DE.CM — Continuous Monitoring: assets, networks, facilities, personnel activity, and external services are monitored for adverse events.	1.4	2.5	Requires new tools and process redesign; resource intensive	1.1
DE.AE — Adverse Event Analysis: events are correlated, characterized, prioritized, and escalated.	1.2	2.5	Requires new tools and process redesign; resource intensive. Exception is DE.CM-09 where the Target was set to 3.0, due to it's criticality in monitoring highly sensitive data.	1.3
TOTAL	1.3	2.6		1.3

6. Remediation Roadmap by Risk Rating

Risk Rating: Very High

Should be most heavily prioritized over the next 12 months:

GV.RM-03: **Enterprise Risk Management must be implemented** for this outcome to be scored.

GV.RM-02: As part of implementing Enterprise Risk Management, develop **risk appetite and risk tolerance** statements.

GV.OC-04: Complete a **Business Impact Assessment (BIA)** to determine the criticality of services, the impact and likelihood of these services being disrupted, and the maximum tolerable downtime for each service (response time objectives)

GV.RR-02: Establish a **RACI matrix** for cybersecurity to clearly define who is accountable, who is responsible, who has decision-making authority, who owns risk, etc. Document the process to report cyber risks and incidents to leadership.

GV.RM-06: CISO currently estimates cybersecurity risk based on their expertise. Moving forward, this evaluation should be calculated by considering likelihood and impact across several dimensions (clinical, privacy, financial, etc.) and developing a **risk matrix** to prioritize risks. This would be supported by first completing a BIA.

GV.OC-03: Complete the **legal and regulatory obligations register**, document and implement a process for communicating compliance requirements to other departments with reporting requirements to senior leadership.

GV.OC-05: Complete a **register of all external dependencies**, map them to services, and identify failure points that would compromise critical services

GV.RR-03: After prioritizing risks, **determine which controls are required to mitigate the most severe risks**, which is a natural extension of the BIA. Senior leadership has a responsibility to ensure that these resources are available. Cost-benefit analysis could be conducted to evaluate the cost effectiveness of the proposed controls.

GV.OV-03: **Develop Key Risk Indicators (KRIs)** based on existing performance KPIs, and measure and report them to senior leadership/the board. KRIs could include cybersecurity training completion, MFA coverage, number of tabletop simulations completed per year, etc.

Risk Rating: High

Should then be prioritized over the next 12 months after Very High Risk:

GV.PO-01: After the deployment of ERM at your organization, **align the existing cybersecurity risk management policy to that overarching framework** and include required information such as management intent, expectations, and direction. Create an official process for department heads to request approval for policies specific to their department, where the risk is evaluated based on criteria defined in the ERM. Document and disseminate expectations to department heads about policy review cadence and how to retain records of signed acceptance of policies from employees.

GV.OV-01: **Develop metrics for the cybersecurity risk management strategy**, assign targets based on historical performance and, if possible, regulatory requirements/contractual obligations, measure and report them to senior leadership and the board.

GV.OV-02: Develop stronger mechanisms to provide assurance that cybersecurity risk management covers all relevant organizational requirements and risks. This is best done when organizational risks are determined and documented in a risk register as part of the ERM. **Establish formalized Roles & Responsibilities for cybersecurity that extend beyond the IT department.** Develop a process to investigate minor incidents and near misses, with a process to incorporate lessons learned into cybersecurity risk management.

GV.PO-02: After the cybersecurity risk management framework has been modified to align with an overarching ERM, evaluate existing departmental policies against this framework and **systematically look for gaps where policies need to be revised to align with the cybersecurity risk management framework.** The cybersecurity risk management framework should also have guidance on how department heads should communicate changes in legal/regulatory requirements to the appropriate parties, and how policies must change as a result. Investigate how "Shadow AI" is being used in the organization, and develop appropriate policies and if necessary technical controls (if the associated risks are beyond your risk appetite as per the ERM).

DE.AE-08: Although IT staff claim to have a general understanding of what constitutes "incident criteria", there is no **documentation or guidance about how to identify or evaluate these incident criteria.** IT, privacy, and clinical leaders should collaborate to define these criteria with severity levels and receive senior leadership approval.

DE.CM-09: Email filtering assists with preventing malicious emails from entering the environment, but to help secure data and prevent loss, **a data loss prevention (DLP) solution, such as Microsoft Purview, should be deployed**. The organization should also define approved security configurations and what constitutes a healthy endpoint. From there, they will be in a better position to detect deviations using tools such as Microsoft Defender and Intune. Regarding hardware tampering, leadership should identify which roles should have this responsibility, document protocols on how to check for tampering, and include these responsibilities in the appropriate job descriptions.

Risk Rating: Medium

Should then be prioritized after the initial 12-month period:

GV.OC-01: **Evaluate the organizational mission** and determine if it provides high-level guidance on how cybersecurity risk should be managed.

GV.RM-01: **For each cybersecurity risk management objective, define the target metric, measurement method, reporting frequency, and accountable owner.**

GV.RM-04: Develop a **shared responsibility policy and vendor responsibility matrix** to formally document security responsibilities with third-party vendors.

GV.RM-07: Include **discussion on positive risks** during senior leadership meetings in the agenda, and develop a methodology to evaluate which positive risks should be pursued.

GV.RR-01: Formally document Roles & Responsibilities for cybersecurity in a RACI matrix. Individuals who are identified in the RACI matrix should meet at least annually to review cybersecurity governance and their roles. **Tabletop exercises should be conducted to prepare for possible incidents.**

GV.SC-05: Security requirements are clearly articulated in vendor contracts. To further improve, **vendor requirements should be mapped to service criticality**, which should be derived from a BIA. Furthermore, vendor contracts can be strengthened by including provisions regarding the disclosure of vulnerabilities, inventory lists, insider due diligence, conformance to best practices (such as NIST CSF 2.0), and vendor responsibilities with regard to cybersecurity risks.

GV.SC-07: While there are many strengths in the initial evaluation of a vendor, assessments do not continue throughout the lifecycle of the relationship. Moving forward, processes should be put in place to **confirm that vendors are meeting their ongoing cybersecurity obligations** through security questionnaires, incident reviews, and contract compliance checks.

GV.SC-08: The organization has an updated list of contact information of critical suppliers, however there are no crisis communication protocols about what information must be conveyed throughout an incident. **Critical vendors should be included in tabletop exercises** to better prepare for incident response, and this provision should be written into the Master Service Agreement.

DE.CM-01: Network monitoring tools are in place to detect potentially adverse events such as suspicious connections and unauthorized devices. This approach can be strengthened by **creating a network diagram as a baseline** to better understand suspicious network flows which fall outside of expected network behaviour.

DE.CM-03: Configure Microsoft XDR for detection of unusual user behaviour and trigger alerts to the IT Department to investigate. **Prepare a protocol of how the IT Department should respond when unusual user behaviour is detected.** Expand unusual sign-in activity reporting to all users, not just administrators. Microsoft XDR can also be configured to set up honeypots to detect unauthorized access on the network, which should send an alert when this deception mechanism is triggered. The organization should also consider data loss prevention (DLP) technologies, such as Microsoft Purview, to check for suspicious user behaviour and protect against a data breach.

DE.AE-02: Better **leverage the findings in the cyber threat intelligence feed with log events** to determine if a possible incident is associated with known malicious activity. Senior leadership should create an expectation of regular reports which should drive decision-making about cybersecurity controls and policies.

DE.AE-04: **Include a manual review and evaluation of the scope and impact reported by the SIEM**, with established and documented criteria of how to measure scope and impact.

DE.AE-07: Although telemetry from networking appliances and workstations are well integrated into the SIEM, there is an "over-reliance" on them according to the IT manager. **IT staff should cross-reference SIEM telemetry with other data points**, such as asset criticality and vulnerability information in order to determine severity and response actions. Furthermore, roles are not clear regarding who should action threat intelligence or third-party vulnerabilities.

Appendix A: Evaluation of Individual Outcomes

GOVERN

GV.OC – Organizational Context

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

Score: 1.0

Gap: 2.0

Risk Rating: MEDIUM

Findings: Evaluate the organizational mission and determine if it provides high-level guidance on how cybersecurity risk should be managed.

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

Score: 2.5

Gap: 0.5

Risk Rating: LOW

Findings: Internal stakeholder register created for BoD, senior leadership team, clinical leaders, privacy officer, and IT department. External stakeholder register created for Ontario Health, Insurer, and EHR vendor, but not yet created for other vendors and patients. Relevant additional external stakeholders are still being identified.

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

Score: 0.3

Gap: 2.7

Risk Rating: VERY HIGH

Findings: Complete the legal and regulatory obligations register, document and implement a process for communicating compliance requirements to other departments with reporting requirements to senior leadership.

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

Score: 0.3

Gap: 2.7

Risk Rating: VERY HIGH

Findings: Complete a Business Impact Assessment (BIA) to determine the criticality of services, the impact and likelihood of these services being disrupted, and the maximum tolerable downtime for each service (response time objectives)

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

Score: 0.0

Gap: 3.0

Risk Rating: VERY HIGH

Findings: Complete a register of all external dependencies, map them to services, and identify failure points that would compromise critical services

GV.RM — Risk Management Strategy

GV.RM-01: Risk management objectives are established and agreed to by organizational stakeholders

Score: 1.0

Gap: 2.0

Risk Rating: MEDIUM

Findings: For each cybersecurity risk management objective, define the target metric, measurement method, reporting frequency, and accountable owner.

GV.RM-02: Risk appetite and risk tolerance statements are established, communicated, and maintained

Score: 0.0

Gap: 3.0

Risk Rating: VERY HIGH

Findings: As part of implementing Enterprise Risk Management, develop risk appetite and risk tolerance statements.

GV.RM-03: Cybersecurity risk management activities and outcomes are included in enterprise risk management processes

Score: 0.0

Gap: 3.0

Risk Rating: VERY HIGH

Findings: Enterprise Risk Management must be implemented for this outcome to be scored.

GV.RM-04: Strategic direction that describes appropriate risk response options is established and communicated

Score: 1.0

Gap: 2.0

Risk Rating: MEDIUM

Findings: Develop a shared responsibility policy and vendor responsibility matrix to formally document security responsibilities with third-party vendors.

GV.RM-06: A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated

Score: 0.0

Gap: 3.0

Risk Rating: VERY HIGH

Findings: CISO currently estimates cybersecurity risk based on their expertise. Moving forward, this evaluation should be calculated by considering likelihood and impact across several dimensions (clinical, privacy, financial, etc.) and developing a risk matrix to prioritize risks. This would be supported by first completing a BIA.

GV.RM-07: Strategic opportunities (i.e., positive risks) are characterized and are included in organizational cybersecurity risk discussions

Score: 0.0

Gap: 2.0* → Manually reduced Target to 2.0 due to less dependency on critical services

Risk Rating: MEDIUM

Findings: Include discussion on positive risks during senior leadership meetings in the agenda, and develop a methodology to evaluate which positive risks should be pursued.

GV.RR – Roles, Responsibilities, and Authorities

GV.RR-01: Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving

Score: 1.5

Gap: 1.5

Risk Rating: MEDIUM

Findings: Formally document Roles & Responsibilities for cybersecurity in a RACI matrix. Individuals who are identified in the RACI matrix should meet at least annually to review cybersecurity governance and their roles. Tabletop exercises should be conducted to prepare for possible incidents.

GV.RR-02: Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced

Score: 0.0

Gap: 3.0

Risk Rating: VERY HIGH

Findings: Establish a RACI matrix for cybersecurity to clearly define who is accountable, who is responsible, who has decision-making authority, who owns risk, etc. Document the process to report cyber risks and incidents to leadership.

GV.RR-03: Adequate resources are allocated commensurate with the cybersecurity risk strategy, roles, responsibilities, and policies

Score: 0.0

Gap: 3.0

Risk Rating: VERY HIGH

Findings: After prioritizing risks, determine which controls are required to mitigate the most severe risks. Senior leadership has a responsibility to ensure that these resources are available. Cost-benefit analysis could be conducted to evaluate the cost effectiveness of the proposed controls.

GV.RR-04: Cybersecurity is included in human resources practices

Score: 2.5

Gap: 0.5

Risk Rating: LOW

Findings: Incorporate cybersecurity knowledge into hiring, training, and retention decisions.

GV.PO – Policy

GV.PO-01: Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced

Score: 0.8

Gap: 2.2

Risk Rating: HIGH

Findings: After the deployment of ERM at your organization, align the existing cybersecurity risk management policy to that overarching framework and include required information such as management intent, expectations, and direction. Create an official process for department heads to request approval for policies specific to their department, where the risk is evaluated based on criteria defined in the ERM. Document and disseminate expectations to department heads about policy review cadence and how to retain records of signed acceptance of policies from employees.

GV.PO-02: Policy for managing cybersecurity risks is reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission

Score: 0.8

Gap: 2.2

Risk Rating: HIGH

Findings: After the cybersecurity risk management framework has been modified to align with an overarching ERM, evaluate existing departmental policies against this framework and systematically look for gaps where policies need to be revised to align with the framework. The cybersecurity risk management framework should also have guidance on how department heads should communicate changes in legal/regulatory requirements to the appropriate parties, and how policies must change as a result. Investigate how "Shadow AI" is being used in the organization, and develop appropriate policies and if necessary technical controls (if the associated risks are beyond your risk appetite as per the ERM).

GV.OV – Oversight

GV.OV-01: Cybersecurity risk management strategy outcomes are reviewed to inform and adjust strategy and direction

Score: 0.5

Gap: 2.5

Risk Rating: HIGH

Findings: Develop metrics for the cybersecurity risk management strategy, assign targets based on historical performance and, if possible, regulatory requirements/contractual obligations, measure and report them to senior leadership and the board.

GV.OV-02: The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks

Score: 0.7

Gap: 2.3

Risk Rating: HIGH

Findings: Develop stronger mechanisms to provide assurance that cybersecurity risk management covers all relevant organizational requirements and risks. This is best done when organizational risks are determined and documented in a risk register as part of the ERM. Establish formalized Roles & Responsibilities for cybersecurity that extend beyond the IT department. Develop a process to investigate minor incidents and near misses, with a process to incorporate lessons learned into cybersecurity risk management.

GV.OV-03: Organizational cybersecurity risk management performance is evaluated and reviewed for adjustments needed

Score: 0.0

Gap: 3.0

Risk Rating: VERY HIGH

Findings: Develop KRIs based on existing performance KPIs, and measure and report them to senior leadership/the board. KRIs could include cybersecurity training completion, MFA coverage, number of tabletop simulations completed per year, etc.

GV.SC – Cybersecurity Supply Chain Management

GV.SC-01: A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders

Score: 2.8

Gap: N/A

Risk Rating: N/A

Findings: The organization has been building their CSRM capabilities over the past few years and have repeatable processes in place to evaluate vendors on criteria established across multiple departments. CSRM could be improved by using established risk criteria to improve decision-making to be more objective.

GV.SC-02: Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally

Score: 2.8

Gap: N/A

Risk Rating: N/A

Findings: CSRM roles and responsibilities are clearly articulated in a RACI matrix, which is communicated to vendors. The organization also clearly identifies vendor responsibilities, and monitors performance based on contractually-binding commitments. Moving forward, the organization should continue to incorporate SCRM performance goals into job descriptions beyond only the IT department.

GV.SC-03: Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes

Score: 1.8

Gap: 0.7

Risk Rating: LOW

Findings: ERM required for this sub-category. Overall, SCRM requirements advance in lockstep with internal technical improvements.

GV.SC-04: Suppliers are known and prioritized by criticality

Score: 2.0

Gap: 0.5

Risk Rating: LOW

Findings: A supplier register exists and is prioritized, however more assurance must be provided that all vendors are equally and fairly measured against these criteria.

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

Score: 0.8

Gap: 1.7

Risk Rating: MEDIUM

Findings: Security requirements are clearly articulated in vendor contracts. To further improve, requirements should be mapped to service criticality, which should be derived from a BIA. Furthermore, vendor contracts can be strengthened by including provisions

regarding the disclosure of vulnerabilities, inventory lists, insider due diligence, conformance to best practices (such as NIST CSF 2.0), and vendor responsibilities with regard to cybersecurity risks.

GV.SC-06: Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships

Score: 1.5

Gap: 1.0

Risk Rating: LOW

Findings: Vendors could be more rigorously evaluated with an ERM and BIA to provide guidance on risk management and criticality. Vendors should be asked to provide information about data provenance, i.e., where data was originally gathered, who accessed it, and how it was moved and edited over time.

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

Score: 0.8

Gap: 1.7

Risk Rating: MEDIUM

Findings: While there are many strengths in the initial evaluation of a vendor, assessments do not continue throughout the lifecycle of the relationship. Moving forward, processes should be put in place to confirm that vendors are meeting their cybersecurity obligations through security questionnaires, incident reviews, and contract compliance checks.

GV.SC-08: Relevant suppliers and other third parties are included in incident planning, response, and recovery activities

Score: 1.0

Gap: 1.5

Risk Rating: MEDIUM

Findings: The organization has an updated list of contact information of critical suppliers, however there are no crisis communication protocols about what information must be conveyed throughout an incident. Critical vendors should be included in tabletop exercises to better prepare for incident response, and this provision should be written into the Master Service Agreement.

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

Score: 2.2

Gap: 0.3

Risk Rating: LOW

Findings: Continuous monitoring of software versions and vulnerability scanning immediately alerts the IT Department, who either patch/update the software directly or contact the vendor if it is the vendor's responsibility. The IT Department has a target to either directly patch or contact the appropriate vendor within 1 hour for critical patches, 4 hours for high patches, and 8 hours for all other patches. Vendor patch response times are documented in the contract and SLA. Non-compliance is tracked and investigated for systemic causes or human error. Can be further improved by requesting data provenance from vendors regarding their technology products and services.

GV.SC-10: Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement

Score: 3.0

Gap: N/A

Risk Rating: N/A

Findings: A comprehensive vendor register is maintained and includes relevant details such as access to hospital systems and data.

DETECT

DE.CM – Continuous Monitoring

DE.CM-01: Networks and network services are monitored to find potentially adverse events

Score: 1.4

Gap: 1.1

Risk Rating: MEDIUM

Findings: Network monitoring tools are in place to detect potentially adverse events such as suspicious connections and unauthorized devices. This approach can be strengthened by creating a network diagram as a baseline to better understand suspicious network flows which fall outside of expected network behaviour.

DE.CM-02: The physical environment is monitored to find potentially adverse events

Score: 2.0

Gap: 0.5

Risk Rating: LOW

Findings: Modern badge readers and associated software allow for real-time tracking of employee access throughout the facility. Sign-in forms should ideally be replaced with a digital solution with data retained for 6 years on the on-premise server, with a retention policy to purge all records over 6 years old. This would allow Security and other relevant parties to more quickly and accurately search logs when required. Cameras should also be modernized so that motion and detected suspicious behaviour can generate real-time alerts to Security, which will allow for a quicker response time.

DE.CM-03: Personnel activity and technology usage are monitored to find potentially adverse events

Score: 0.7

Gap: 1.8

Risk Rating: MEDIUM

Findings: Configure Microsoft XDR for detection of unusual user behaviour and trigger alerts to the IT Department to investigate. Prepare a protocol of how the IT Department should respond when detected. Expand unusual sign-in activity reporting to all users, not just administrators. Microsoft XDR can also be configured to set up honeypots to detect unauthorized access on the network, which should send an alert when this deception mechanism is triggered. The organization should also consider data loss prevention (DLP)

technologies, such as Microsoft Purview, to check for suspicious user behaviour and protect against a data breach.

DE.CM-06: External service provider activities and services are monitored to find potentially adverse events

Score: 2.0

Gap: 0.5

Risk Rating: LOW

Findings: Further strengthen on-site maintenance activities of third-party vendors by informing the Security team, who could monitor their activity via camera feeds. Define what "expected behaviour" looks like for cloud services, configure alerts when activity deviates from this behaviour, and create protocols of how the IT Department should respond.

DE.CM-09: Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events

Score: 0.8

Gap: 2.2 → Manually increased Target to 3.0 due to risk toward critical services

Risk Rating: HIGH

Findings: Email filtering assists with preventing malicious emails from entering the environment, but to help secure data and prevent loss, a data loss prevention (DLP) solution, such as Microsoft Purview, should be deployed. The organization should also define approved security configurations and what constitutes a healthy endpoint. From there, they will be in a better position to detect deviations using tools such as Microsoft Defender and Intune. Regarding hardware tampering, leadership should identify which roles should have this responsibility, document protocols on how to check for tampering, and include these responsibilities in the appropriate job descriptions.

DE.AE – Adverse Event Analysis

DE.AE-02: Potentially adverse events are analyzed to better understand associated activities

Score: 1.0

Gap: 1.5

Risk Rating: MEDIUM

Findings: Better leverage the findings in the cyber threat intelligence feed with log events to determine if a possible incident is associated with known malicious activity. Senior

leadership should create an expectation of regular reports which should drive decision-making about cybersecurity controls and policies.

DE.AE-03: Information is correlated from multiple sources

Score: 2.0

Gap: 0.5

Risk Rating: LOW

Findings: Update the documentation of selecting and adding new services to consider if new data sources can be added to SIEM telemetry. In addition, integrate cyber threat intelligence with log sources to identify correlations.

DE.AE-04: The estimated impact and scope of adverse events are understood

Score: 0.5

Gap: 2.0

Risk Rating: MEDIUM

Findings: Include a manual review and evaluation of the scope and impact reported by the SIEM, with established and documented criteria of how to measure scope and impact.

DE.AE-06: Information on adverse events is provided to authorized staff and tools

Score: 2.5

Gap: N/A

Risk Rating: N/A

Findings: The SIEM is configured to generate and send alerts to specific, defined members of the IT Department with incident response capabilities. However, their ability to respond is limited because only the IT Director has access to the log analysis findings. Providing access to incident responders will assist in more rapid remediation. The SIEM automatically creates tickets into the ticketing system which includes severity levels (high, medium, low) to assist with triage, with data analysis of ticket trends to identify patterns and assist in decision-making for strengthening controls. The overall approach can be improved by documenting what "indicators of compromise" means, and training IT staff to look for these signals.

DE.AE-07: Cyber threat intelligence and other contextual information are integrated into the analysis

Score: 1.0

Gap: 1.5

Risk Rating: MEDIUM

Findings: Although telemetry from networking appliances and workstations are well integrated into the SIEM, there is an "over-reliance" on them according to the IT manager, as IT staff do not cross-reference this telemetry with other data points, such as asset criticality and vulnerability information in order to determine severity and response actions. Furthermore, roles are not clear regarding who should action threat intelligence or third-party vulnerabilities.

DE.AE-08: Incidents are declared when adverse events meet the defined incident criteria

Score: 0.0

Gap: 2.5

Risk Rating: HIGH

Findings: Although IT staff claim to have a general understanding of what constitutes "incident criteria", there is no documentation or guidance about how to identify or evaluate these criteria. IT, privacy, and clinical leaders should collaborate to define these criteria with severity levels and receive senior leadership approval.
