Cybersecurity Preparedness

SELF-EVALUATION QUESTIONNAIRE

April 2025

(Version 2.0)

mhcc.maryland.gov

Toll Free: 1-877-245-1762
TTY Number: 1-800-735-2258
Fax: 410-358-1236

4160 Patterson Avenue
Baltimore, MD 21215

INTRODUCTION

Cybersecurity is essential to protect health care provider organizations, including practices, clinics, and health centers (herein referred to as "organizations" throughout) from internal and external cyber threats.[1] Cybersecurity is not limited to just the technology systems that store and transmit patient data; it encompasses people and processes to make sure operations and security are working in tandem. Assessing cybersecurity preparedness helps ensure cyber threats are treated like any other disaster (e.g., fires, floods, outbreaks) and encompasses a review of preventative measures that protect patient privacy and safety and limit disruption to organization operations should a cyber-attack occur.

The Maryland Health Care Commission ("MHCC") developed a *Cybersecurity Preparedness Self-Evaluation Questionnaire* (questionnaire) to assist organizations with understanding, assessing, and prioritizing cybersecurity.[2] The questionnaire includes select elements from the National Institute of Standards and Technology ("NIST")[3] Cybersecurity Framework ("CSF") Version 2.0.[4] The NIST CSF was developed through a collaborative process with experts in the federal government and private sector to create a set of standards, best practices, and recommendations for improving cybersecurity.[5] The six core functions of the NIST CSF include: Govern ("GV"), Identify ("ID"), Protect ("PR"), Detect ("DE"), Respond ("RS"), and Recover ("RC").[6] Each function has a list of categories and subcategories that define specific cybersecurity activities that should be performed continuously and concurrently. Users of the questionnaire are encouraged to review the NIST CSF at: www.nist.gov/cyberframework.

INSTRUCTIONS

The questionnaire consists of a series of self-evaluation statements intended to help users identify potential gaps in cybersecurity and prioritize areas for improvement. Statements are grouped by people, processes, and technology and reference the NIST CSF function, category, and subcategory and applicable page numbers in the NIST CSF (Version 2.0, February 2024). Click on the source that follows each self-evaluation statement for more information.[7] For each statement, select one response from the options that most accurately reflects how you would categorize your organization's ability to effectively detect, understand, and contain cyber threats:

- Lacking – Unaware or unable to take effective action
- Minimal – Some basic structures are in place to react if a problem should surface
- Satisfactory – Necessary structures are in place to address current problems
- Advanced – Structures are being identified and implemented to anticipate and address emerging problems
- N/A – Not applicable

After selecting a response for each self-evaluation statement, tally your responses to understand how operational security corresponds to cybersecurity maturity of your organization.

LIMITATIONS

This questionnaire is for informational purposes and does not guarantee compliance with federal, state, or local laws. The scope of the self-evaluation statements is not intended to be exhaustive or the only source to assess cybersecurity readiness. Some information may not be applicable to certain users. Results do not serve as legal advice for reducing risks to privacy and security.

The NIST CSF offers a taxonomy of high-level cybersecurity outcomes regardless of an organization's size, sector, or maturity. It does not prescribe how outcomes should be achieved and, instead, links to online resources that provide guidance on practices and controls that could be used to achieve those outcomes.[8]

QUESTIONNAIRE FEEDBACK

The MHCC would greatly appreciate your feedback on the utility of this questionnaire by responding to a brief survey at the following link: forms.gle/XE6ZRJoSVXXWFKPA9.

PEOPLE

1. Organizational leadership is responsible for managing cybersecurity and maintains a risk-aware and ethical culture that focuses on continuous improvement.

   - Example: Conduct reviews of and training on roles and responsibilities to foster accountability and improved performance

   ☐ **Lacking** ☐ **Minimal** ☐ **Satisfactory** ☐ **Advanced** ☐ **N/A**

   Source: GV.RR-01 (p. 17)

2. Cybersecurity roles, responsibilities, needs, and authorities for internal and external stakeholders are established, communicated, understood, and enforced and adequate resources are allocated consistent with cybersecurity needs.

   - Example: IT Operations Manual; Employee Handbook; Business Associates Agreements that outline roles and responsibilities for cybersecurity; Human Resources practices; Periodic reviews of cybersecurity roles, responsibilities, needs and authorities

   ☐ **Lacking** ☐ **Minimal** ☐ **Satisfactory** ☐ **Advanced** ☐ **N/A**

   Source: GV.OC-02 (p. 16), GV.RR-02 (p. 17), GV.RR-03 (p. 17), GV.RR-04 (p. 17), GV.SC-02 (p. 17)

3. Personnel are provided with training tailored to their specialized roles to demonstrate the knowledge and skills necessary to perform tasks with consideration of the relevant cybersecurity risks.

   - Example: Employee Handbook; Position requirements; Employee training program including testing and exercises

   ☐ **Lacking** ☐ **Minimal** ☐ **Satisfactory** ☐ **Advanced** ☐ **N/A**

   Source: PR.AT-01 (p. 20); PR.AT-02 (p. 20)

4. Personnel and third parties demonstrate understanding of the legal, regulatory, and contractual requirements governing cybersecurity and their rights and obligations related to cybersecurity.

   - Example: Signed attestations in compliance with HIPAA and HITECH; Data security standards; Breach reporting

   ☐ **Lacking** ☐ **Minimal** ☐ **Satisfactory** ☐ **Advanced** ☐ **N/A**

   Source: GV.OC-03 (p. 16)

5. The organization has established lines of communication to share risk statements outlining the acceptable level of risk with personnel and third parties.

   - Example: Translate risk statements into action items; Share statements as part of onboarding and at regular points

   ☐ **Lacking** ☐ **Minimal** ☐ **Satisfactory** ☐ **Advanced** ☐ **N/A**

   Source: GV.RM-02 (p. 16), GV.RM-05 (p. 16)

6. The organization monitors and reviews personnel and external service provider activity and technology usage, such as internet use, maintenance activities, logs from access systems, creation of new users, e-mail spam, file downloads, and use of portable external devices (e.g., flash drive).

   - Example: Audits of IT system logs and e-mail accounts

   ☐ **Lacking** ☐ **Minimal** ☐ **Satisfactory** ☐ **Advanced** ☐ **N/A**

   Source: PR.PS-04 (p. 20), DE.CM-03 (p. 21), DE.CM-06 (p. 21)

---

7. Information pertaining to cybersecurity processes and recovery is communicated with authorized employees and third parties.

   - Example: Communication and/or cybersecurity plans include steps for informing employees of adverse events; Cyber incident reports are generated and shared with relevant clients; Response activities that comply with State and federal law are presented in online forums, stakeholder advisory groups and/or other information sharing sessions

   ☐ **Lacking** ☐ **Minimal** ☐ **Satisfactory** ☐ **Advanced** ☐ **N/A**

   Source: DE.AE-06 (p. 21), RS.CO-02 (p. 22), RS.CO-03 (p. 22), RC.CO-04 (p. 22)

---

8. All users and devices undergo a standard authentication process prior to use and all system identities and credentials are protected and verified.

   - Example: Require multifactor authentication and minimum strength of passwords and similar authenticators; Encrypt data and use signature validation to ensure all identities and credentials are protected and verified

   ☐ **Lacking** ☐ **Minimal** ☐ **Satisfactory** ☐ **Advanced** ☐ **N/A**

   Source: PR.AA-03 (p. 19), PR.AA-04 (p.19)

---

9. All users are authorized and credentialed and user permissions and access privileges for IT systems, devices, software, and files are limited to only what is necessary to perform job functions.

   - Example: Configure user profiles and software based on role; Use key cards or fobs to limit access to sensitive areas/materials

   ☐ **Lacking** ☐ **Minimal** ☐ **Satisfactory** ☐ **Advanced** ☐ **N/A**

   Source: PR.AA-01 (p. 19), PR.AA-02 (p. 19), PR.AA-05 (p. 20), PR.AA-06 (p. 20), PR.PS-01 (p. 20), PR.IR-01 (p. 20)

PROCESSES

10. The mission, objectives, and activities of the organization are understood and inform cybersecurity risk management.

    - Example: The organization's mission and objectives are clearly defined and integrated with the organization's cybersecurity risk management plan and processes as described in an organizational operation manual, employee handbook, memorandums, business associate agreements, contracts with third parties, and/or other risk management plans

    ☐ **Lacking** ☐ **Minimal** ☐ **Satisfactory** ☐ **Advanced** ☐ **N/A**

    Source: GV.OC-01 (p. 16)

---

11. The organization develops a method for calculating, documenting, categorizing, and prioritizing cybersecurity risk, establishes a policy for managing cybersecurity based on the organization's strategy and priorities, periodically reviews and updates the policy to reflect the changing cyber-landscape and organizational needs, and communicates the policy with stakeholders.

    - Example: Create and disseminate a risk policy; Update policy based on reviews of cybersecurity risk

    ☐ **Lacking** ☐ **Minimal** ☐ **Satisfactory** ☐ **Advanced** ☐ **N/A**

    Source: GV.RM-06 (p. 16), GV.PO-01 (p. 17), GV.PO-02 (p. 17)

---

12. Cybersecurity risk management strategy objectives and outcomes are established, evaluated, reviewed, and adjusted to inform the enterprise risk management process.

    - Example: Perform cybersecurity audits and make adjustments to organizational policies and procedures based on audit findings

    ☐ **Lacking** ☐ **Minimal** ☐ **Satisfactory** ☐ **Advanced** ☐ **N/A**

    Source: GV.RM-01 (p. 16), GV.RM-03 (p. 16), GV.OV-01 (p.17), GV.OV-02 (p. 17), GV.OV-03 (p. 17)

13. The organization has a mapping of how information and data move through IT systems and networks and has prioritized all activities, systems, software, and data that are essential for its operation.

    - Example: Workflow charts for communication and data transmission processes; Evaluate potential effects from an interruption in critical business operations and share results with employees and third parties

    ☐ **Lacking** ☐ **Minimal** ☐ **Satisfactory** ☐ **Advanced** ☐ **N/A**

    Source: ID.AM-03 (p. 18), ID.AM-05 (p. 18)

---

14. The organization communicates and understands cybersecurity risk management goals, capabilities, and services that external stakeholders depend on from the organization.

    - Example: Business Impact Analysis; IT Risk Assessment Report; IT Operations Manual

    ☐ **Lacking** ☐ **Minimal** ☐ **Satisfactory** ☐ **Advanced** ☐ **N/A**

    Source: GV.OC-04 (p. 16), GV.OC-05 (p. 16)

---

15. A strategic direction is established and communicated that includes risk response options and opportunities (positive risks).

    - Example: Document criteria for accepting and avoiding risk; Cybersecurity insurance; Strengths, weaknesses, opportunities, and threats (SWOT) analysis

    ☐ **Lacking** ☐ **Minimal** ☐ **Satisfactory** ☐ **Advanced** ☐ **N/A**

Source: GV.RM-04 (p. 16); GV.RM-07 (p. 16)

---

16. The organization manages risks in the cyber supply chain by documenting and prioritizing suppliers and other third parties by importance to the infrastructure, performing due diligence before entering into a contractual relationship for a technology product or service, managing risk throughout the life cycle of a technology product or service, and ensuring the ongoing integration and monitoring of supply chain risk management.

- Example: Ensure contractual requirements and other provisions are established and understood when an agreement concludes

☐ **Lacking** ☐ **Minimal** ☐ **Satisfactory** ☐ **Advanced** ☐ **N/A**

Source: GV.SC-01 (p. 17), GV.SC-03 (p. 17), GV.SC-04 (p. 17), GV.SC-05 (p. 18), GV.SC-06 (p. 18), GV.SC-07 (p. 18), GV.SC-09 (p. 18), GV.SC-10 (p. 18)

---

17. Processes for incident response and disaster recovery that encompass relevant suppliers and other third parties are established, communicated, maintained, and improved.

- Example: Disaster response and recovery plan is established and inclusive of third parties

☐ **Lacking** ☐ **Minimal** ☐ **Satisfactory** ☐ **Advanced** ☐ **N/A**

Source: GV.SC-08 (p. 18), ID.IM-04 (p. 19), RS.MA-05 (p. 22)

---

18. Internal and external threats are identified and validated through various information sharing sources, and the potential impacts and likelihood of the threats are understood.

- Example: Conduct a risk analysis; Use cyber threat intelligence and hunting; Develop a risk identification process

☐ **Lacking** ☐ **Minimal** ☐ **Satisfactory** ☐ **Advanced** ☐ **N/A**

Source: ID.RA-01 (p. 18), ID.RA-02 (p. 19), ID.RA-03 (p. 19), ID.RA-04 (p. 19), DE.AE-02 (p. 21), DE.AE-03 (p. 21)

---

19. Risks are prioritized and tracked with the consideration of critical mission functions.

- Example: Vulnerability management plans; Annual risk assessments

☐ **Lacking** ☐ **Minimal** ☐ **Satisfactory** ☐ **Advanced** ☐ **N/A**

Source: ID.RA-05 (p. 19), ID.RA-06 (p. 19), RC.RP-04 (p. 23)

---

20. Document lessons learned from incident investigations, security tests, and other exercises conducted for the organization and relevant third parties to ensure effective response of recovery.

- Example: Business impact analysis and disaster recovery testing and reports

☐ **Lacking** ☐ **Minimal** ☐ **Satisfactory** ☐ **Advanced** ☐ **N/A**

Source: ID.RA-08 (p. 19), ID.IM-01 (p. 19); ID.IM-02 (p. 19), ID.IM-03 (p. 19), DE.AE-04 (p. 21), DE.AE-07 (p. 21), RS.AN-03 (p. 22); RS.AN-06 (p. 22), RS.AN-07 (p. 22), RS.AN-08 (p. 22)

---

21. The incident response and recovery plan is executed based on defined criteria in coordination with third parties, and incidents are triaged, validated, categorized, prioritized, and escalated or elevated, as needed.

- Example: Develop and review incident reports and categorize and prioritize incidents based on type (e.g., data breach, ransomware, etc.)

☐ **Lacking** ☐ **Minimal** ☐ **Satisfactory** ☐ **Advanced** ☐ **N/A**

Source: RS.MA-01 (p. 22); RS.MA-02 (p. 22); RS.MA-03 (p. 22); RS.MA-04 (p. 22), RC.RP-01 (p. 22), RC.RP-02 (p. 23)

---

22. The organization contains and eradicates cyber incidents to mitigate risk.

- Example: Use of firewalls, VPNs, email security software and anti-malware software

☐ **Lacking** ☐ **Minimal** ☐ **Satisfactory** ☐ **Advanced** ☐ **N/A**

Source: RS.MI-01 (p. 22), RS.MI-02 (p.22)

---

23. Incidents are characterized by defined criteria, stakeholders are notified of incidents, and recovery concludes once incident-related documentation is completed.

- Example: Operations manual; Disaster recovery plan

☐ **Lacking** ☐ **Minimal** ☐ **Satisfactory** ☐ **Advanced** ☐ **N/A**

Source: DE.AE-08 (p. 21), RS.CO-02 (p. 22), RC.RP-06 (p.23)

TECHNOLOGY

24. Assets, such as hardware, software, services, systems, data, and metadata, managed by the organization and third parties are inventoried and maintained.

- Example: Catalogue of all computers, mobile devices, electronic medical devices, printers, scanners, fax machines, copiers, and other machines located off site that are accessed virtually by the organization, programs installed on computers, data, and electronic health record systems

☐ Lacking ☐ Minimal ☐ Satisfactory ☐ Advanced ☐ N/A

Source: ID.AM-01 (p. 18), ID.AM-02 (p. 18), ID.AM-04 (p. 18), ID.AM-07 (p. 18), ID.AM-08 (p. 18)

25. Hardware, software, and critical suppliers are assessed prior to acquisition to ensure authenticity and integrity.

- Example: IT Operations Manual outlines the process for analysis, design, development, testing, installation, maintenance, evaluation, and disposal of IT systems and software

☐ Lacking ☐ Minimal ☐ Satisfactory ☐ Advanced ☐ N/A

Source: ID.RA-09 (p. 19), ID.RA-10 (p. 19), PR.IR-01 (p. 20)

26. The organization monitors all software and hardware for unauthorized access and maintains, replaces, and removes commensurate with risk.

Example: IT Operations Manual addresses the maintenance, replacement, and removal of software and hardware

☐ Lacking ☐ Minimal ☐ Satisfactory ☐ Advanced ☐ N/A

Source: PR.PS-02 (p. 20), PR.PS-03 (p. 20), PR.PS-06 (p. 20)

27. Networks, network services, computing hardware and software, runtime environments, data, and external service providers are configured, continuously monitored, and scanned to detect potential adverse events.

- Example: Vulnerability scans; Penetration testing; Reviews of IT system access audit logs

☐ **Lacking** ☐ **Minimal** ☐ **Satisfactory** ☐ **Advanced** ☐ **N/A**

Source: PR.PS-01 (p. 20), PR.IR-01 (p. 20), DE.CM-01 (p. 21), DE.CM-06 (p. 21), DE.CM-09 (p. 21)

---

28. Technology assets are protected from environmental threats (i.e., external factors that affect cybersecurity) and physical access to assets is monitored and enforced to prevent unauthorized access.

- Example: Security employees; Key cards and fobs for access; Auditing of access and visitor logs

☐ **Lacking** ☐ **Minimal** ☐ **Satisfactory** ☐ **Advanced** ☐ **N/A**

Source: PR.AA-06 (p. 20), PR.IR-02 (p. 21), DE.CM-02 (p. 21)

---

29. Changes and exceptions to the IT system are managed by assessing risk impact, which is recorded and tracked, and networks are protected from unauthorized access with log records generated to support continuous monitoring.

- Example: Limit ability to install software to dedicated IT employees; Block external devices (i.e., flash drives and smart phones) from connecting to a computer or network; IT manual details process and procedures for changes and exceptions

☐ **Lacking** ☐ **Minimal** ☐ **Satisfactory** ☐ **Advanced** ☐ **N/A**

Source: ID.RA-07 (p. 19) PR.PS-04 (p. 20), PR.PS-05 (p. 20), PR.IR-01 (p. 20)

30. Data at rest, in transit, and in use are protected to ensure confidentiality, integrity, and availability.

- Example: IT Operations Manual includes information on converting data to code (encrypting); Firewalls are in place

☐ **Lacking** ☐ **Minimal** ☐ **Satisfactory** ☐ **Advanced** ☐ **N/A**

Source: PR.DS-01 (p. 20), PR.DS-02 (p. 20), PR.DS.10- (p. 20)

---

31. Mechanisms are implemented to ensure resilience and availability of data in normal and adverse situations, including creating backups of data that are protected, maintained, tested, and their integrity verified prior to and following restoration.

- Example: Mechanisms such as failsafe, load balancing, and alternative hardware to prevent failure; Back up data restoration policies

☐ **Lacking** ☐ **Minimal** ☐ **Satisfactory** ☐ **Advanced** ☐ **N/A**

Source: PR.DS-11 (p.20), PR.IR-03 (p. 21), PR.IR-04 (p. 21), , RC.RP-03 (p. 23), RC.RP-05 (p. 23)

CYBERSECURITY MATURITY RESULTS

Tally the total number of response options selected for all self-evaluation statements. Then review the corresponding maturity level on the right, which is an indicator of preparedness to detect, understand, and contain cyber incidents and potential breaches. Maturity levels are based on a cybersecurity maturity model that has been validated through extensive research.[9] Results can be used by organizations to identify areas for improvement. In general, higher levels of maturity correspond to better operational security; lower levels of maturity indicate a need to identify and implement cybersecurity improvements in people, processes, and technology.

Response Option	Total Number Selected	Cybersecurity Maturity Level
Lacking	#	Unprepared – Lacking necessary information to take effective action; unaware or unable to respond to current or emerging issues
Minimal	#	Reactive – Basic platforms and structures in place to react to business requirements; unable to proactively prevent problems from arising
Satisfactory	#	Proactive – Platforms, structures, and processes in place to proactively address current issues and challenges
Advanced	#	Anticipatory – Platforms, structures, and processes in place necessary to address future issues and challenges
N/A	#	N/A – Not applicable

More information on the maturity levels:[10]

- **Unprepared**: Lacking people (cybersecurity personnel), technology (anti-virus software, firewalls, etc.), and/or processes (e.g., regular cybersecurity awareness training, incident response plans) to deal with cyber threats.
- **Reactive:** People, technology, and processes are in place to handle cyberattacks after they occur.
- **Proactive:** People, technology, and processes are in place to protect against foreseeable threats (e.g., assigns least required access privileges needed to perform specific tasks, security configurations continuously evaluated, etc.)[11]
- **Anticipatory:** People, technology, and processes are able to protect against cyber threats that could emerge (e.g., looking into potential impacts of new technology such as blockchain).

KEY TERMS

A full list of cybersecurity terms and definitions is available at: csrc.nist.gov/glossary.

RESOURCES

1. ***Security Risk Assessment Tool***, HealthIT.gov. Available at: www.healthit.gov/providers-professionals/security-risk-assessment-tool.
2. ***The NIST Cybersecurity Framework (CSF) Version 2.0,*** NIST February 2024. Available at: nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.
3. ***Security and Privacy Controls for Federal Information Systems and Organizations***, NIST Special Publication 800-53 Revision 5, September 2020. Available at: csrc.nist.gov/pubs/sp/800/53/r5/upd1/final.
4. ***Cyber Guidance for Small Businesses***, Cybersecurity & Infrastructure Security Agency. Available at: www.cisa.gov/cyber-guidance-small-businesses.

ABOUT MHCC

The MHCC is an independent regulatory agency whose mission is to plan for health system needs, promote informed decision-making, increase accountability, and improve access in a rapidly changing health care environment by providing timely and accurate information on availability, cost, and quality of services to policy makers, purchasers, providers and the public. The MHCC is responsible for advancing health information technology statewide and fostering innovation in a way that balances the need for information sharing with the need for strong privacy and security policies.

ENDNOTES

[1] Ready.gov, *Cybersecurity*. Available at: www.ready.gov/cybersecurity.
[2] The MHCC fist developed the Cybersecurity Preparedness Self-Evaluation Questionnaire in 2017 to assist health care organizations with assessing cybersecurity readiness. The questionnaire is periodically updated to reflect changes in the cybersecurity landscape and updates to the *NIST Cybersecurity Framework*.
[3] NIST was established by Congress in 1901 to create a measurement infrastructure for technology. A wide variety of industries, including health care, rely on NIST technology, measurement, and standards. More information is available at: www.nist.gov/about-nist.
[4] The questionnaire uses the functions, categories, and subcategories developed by NIST. Descriptions in this document contain language used in *The NIST Cybersecurity Framework (CSF) Version 2.0* (February 2024), which is available at: nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.
[5] The NIST *Framework for Improving Critical Infrastructure Cybersecurity* was initially released in February 2014 and first updated in April 2018 to reflect industry feedback, which included clarifying cybersecurity measurement language and tactics for improving security within the supply chain. NIST released Version 2.0 in February 2024, renamed the resource to *The NIST Cybersecurity Framework 2.0,* and simplified the way organizations can implement the CSF. Version 2.0 expands coverage beyond critical infrastructure to include all types of industries, sectors, and organizations and adds a sixth function, Govern.
[6] NIST. *NIST Cybersecurity Framework 2.0: Resource & Overview Guide*. Available at: nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1299.pdf.
[7] Page numbers represent document pages, not page numbers indicated by Adobe® PDF Reader.
[8] NIST. *The NIST Cybersecurity Framework 2.0* (February 2024). Available at: nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.
[9] *Ibid.*
[10] See n. 8, *Supra.*
[11] Crowdstrike, *Zero Trust Security Explained: Principals of the Zero Trust Model*, May 2021. Available at: www.crowdstrike.com/cybersecurity-101/zero-trust-security/.