LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

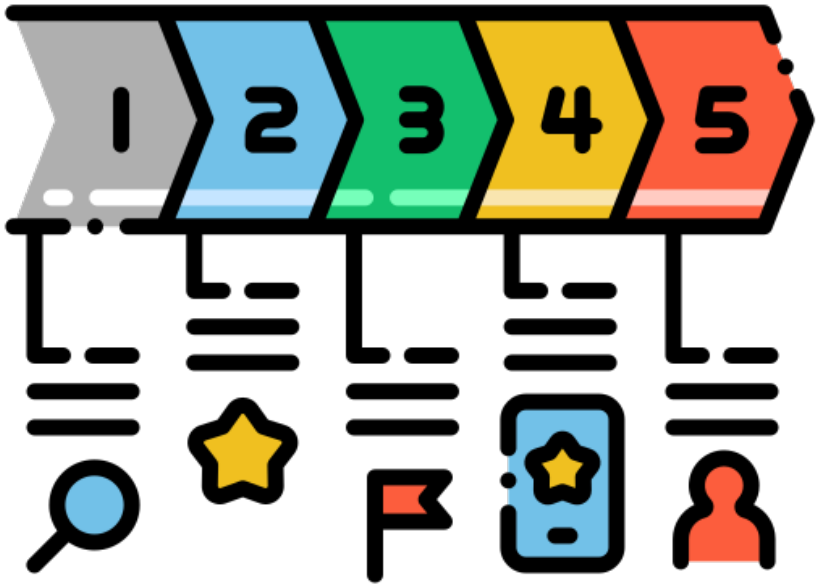
HC3 Intelligence Briefing
Cybersecurity Maturity Models

08/06/2020

Report #: 202008061030

Agenda

- Executive Summary
- Background
  - What is Cybersecurity Maturity Model(CMM)
  - History of CMM
  - Why use CMM
  - How to use CMM
- Notable Cybersecurity Maturity Models
  - Cybersecurity Capability Maturity Model (C2M2)
  - NIST Cybersecurity Framework
  - Cybersecurity Maturity Model Certification
- How can CMM be used to protect the Health/Public Health Sector
  - Using CMMs to provide customer with continuous service
  - Using CMMs to protect sensitive information
  - Using CMMs to comply with laws and regulations



Slides Key:

Non-Technical: managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

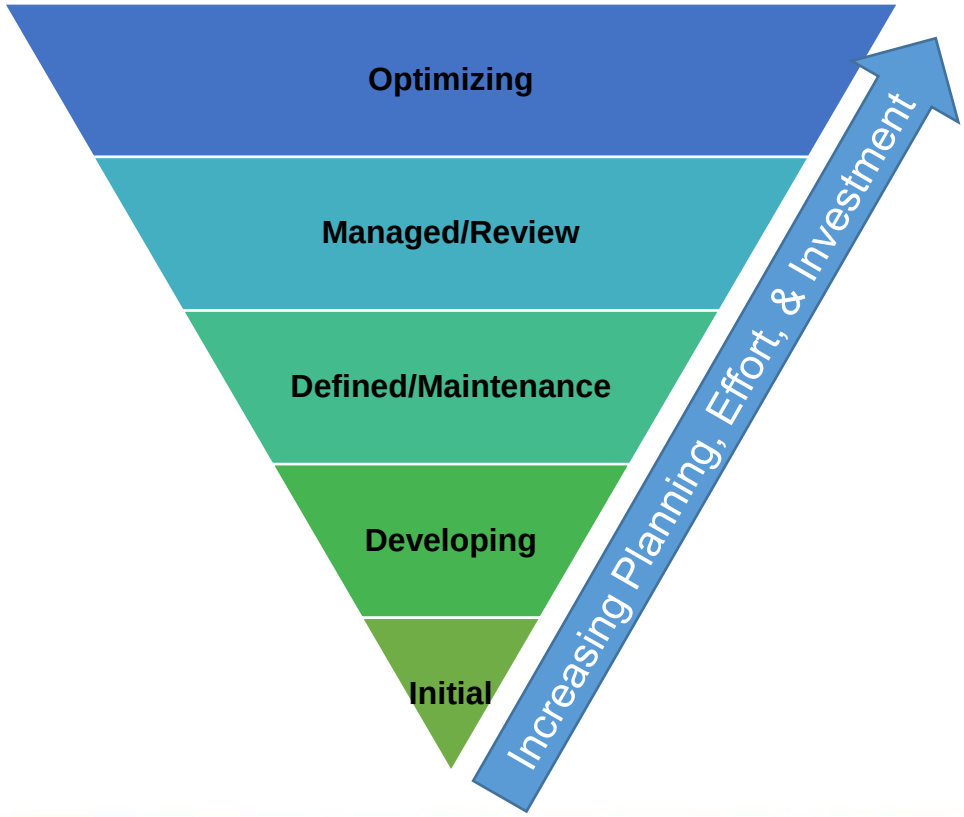
Executive Summary

- Cybersecurity Maturity Models:
  - Attempt to collect the best cybersecurity practices;
  - Are developed by a collaboration of experts from diverse backgrounds;
  - Consider the dispersion in size, knowledge, skills, abilities, and experience of organizations that will use the model;
  - Take a life cycle and continuous improvement approach to cybersecurity

- Cybersecurity Models help organizations
  - Provide services for their customers without interruption;
  - Protect sensitive customer and proprietary information; and
  - Comply with laws and regulations that govern their operations.

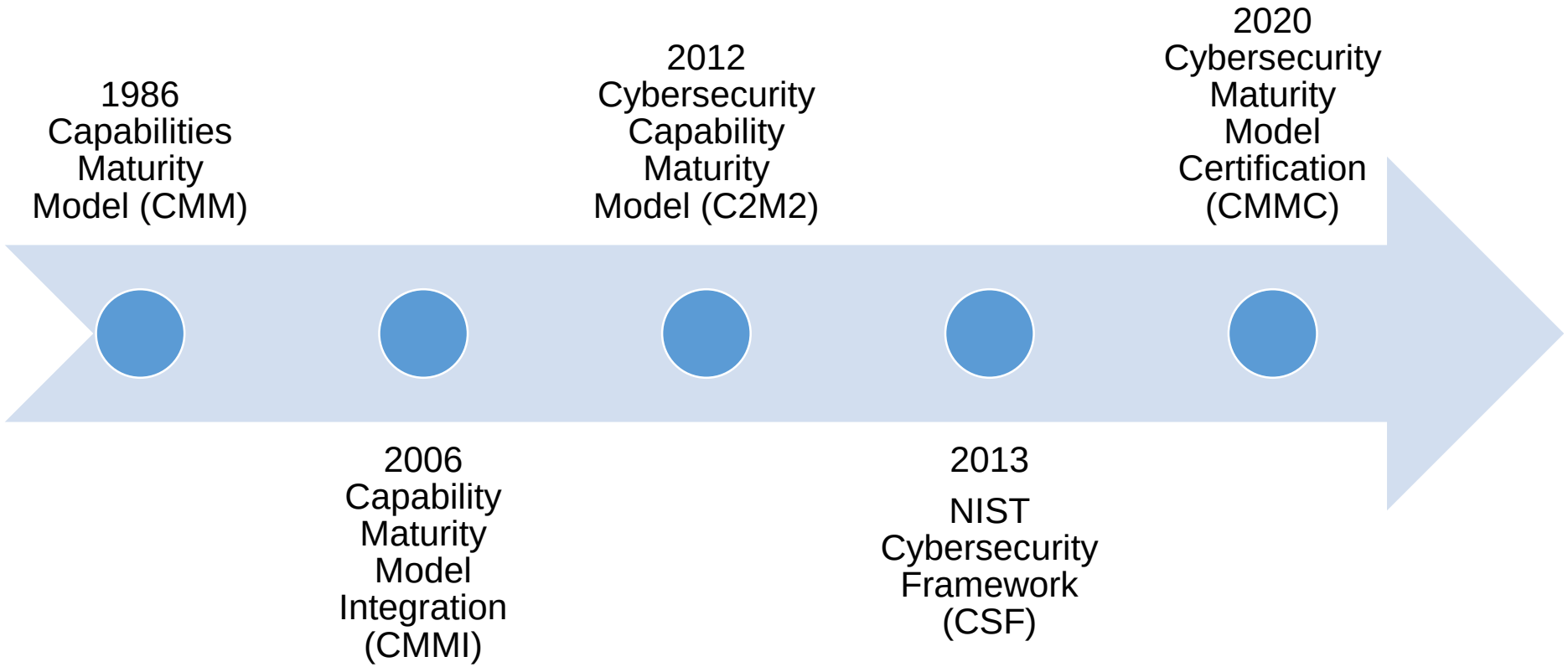
Cybersecurity Maturity Model

- Provides a structure for organizations to baseline current capabilities in cybersecurity workforce planning, establishing a foundation for consistent evaluation
- Management tool for leadership in identifying opportunities for growth and evolution

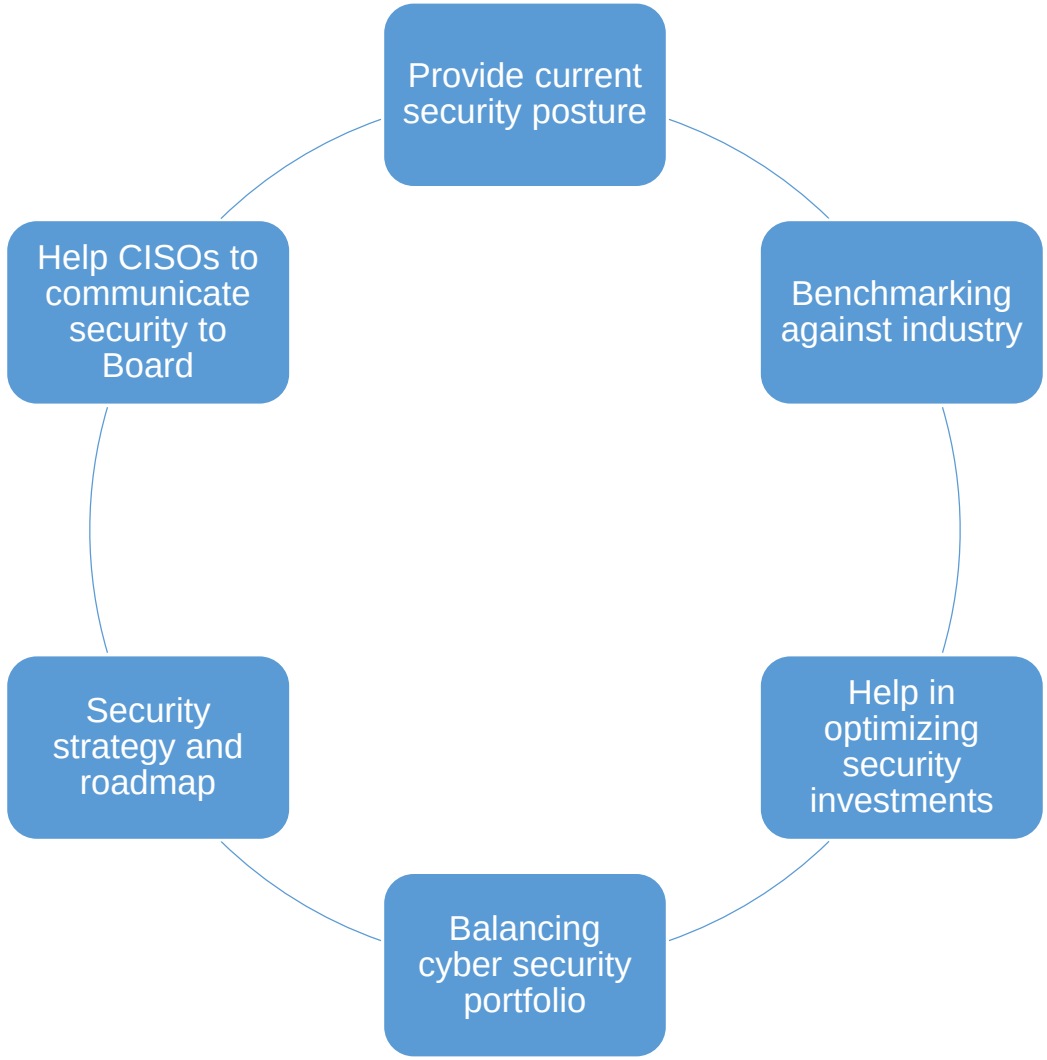


NICCS (2014)

Maturity Model History

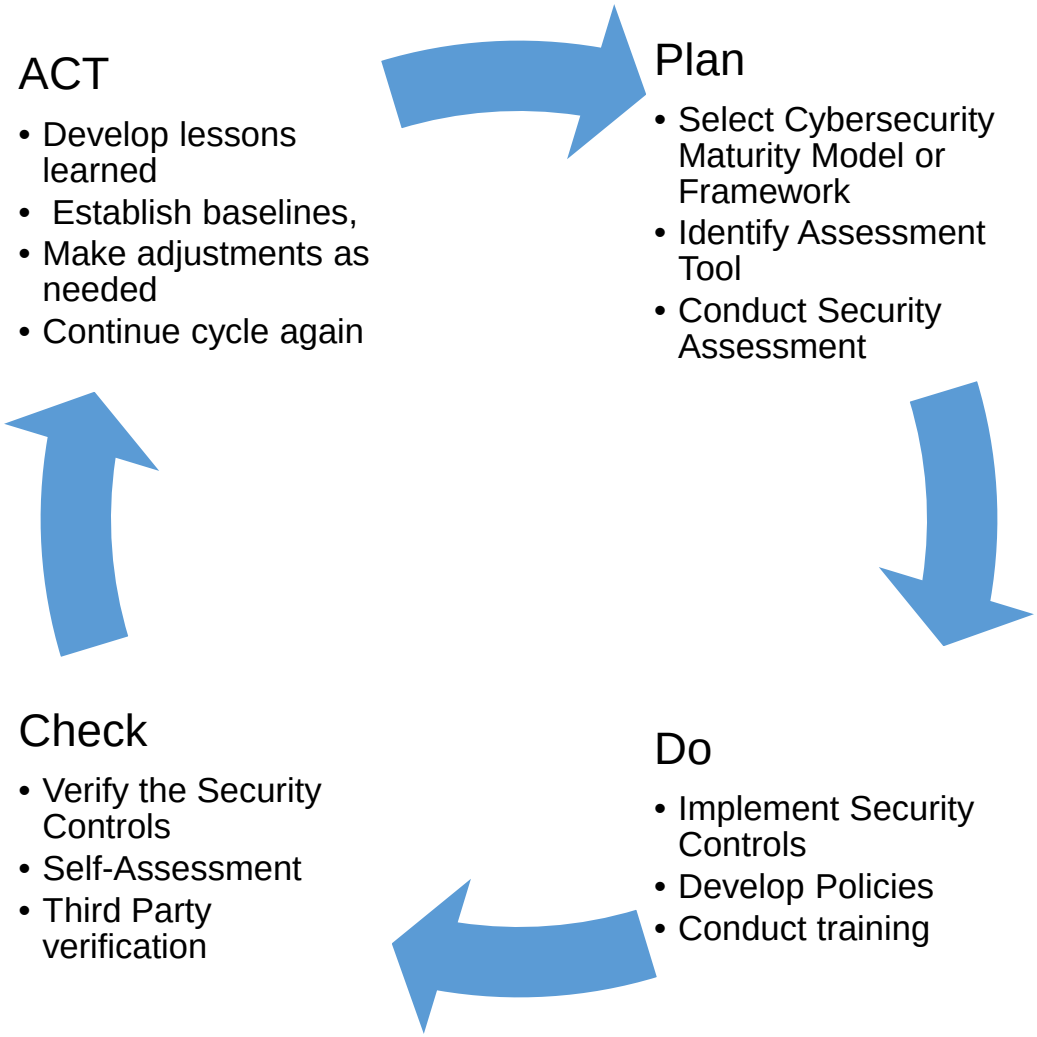


Why do you need a Cybersecurity Maturity Model



NICCS (2014)

How to use a Cybersecurity Maturity Model



NICCS (2014)
Demming, E. W. (1982)

Notable Cybersecurity Maturity Models

Cybersecurity Capabilities Maturity Model (C2M2)

- Developed in 2012, updated in 2014 and 2019.
- Developed collaboratively with an industry advisory group from government, Industry, and academia led by the Department of Energy in partnership with the Department of Homeland Security.
- Derived from cybersecurity best practices from government and industry.
- Originally developed for critical infrastructure but updated to be applied to all sectors with information and operations technology. [1]

NIST Cybersecurity Framework (CSF)

- Published first in 2014. Updated in 2017 and 2018.
- Collaborative effort of industry, academia, and government coordinated by the National Institute of Standards and Technology (NIST).
- Mandated by the Cybersecurity Enhancement Act of 2014 (CEA).
- Brings best practices from industry and government but practices are derived directly from NIST 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013.
- Developed to improve cybersecurity risk management for critical infrastructure but can be used by any sector or community. [2]

DOD Cybersecurity Maturity Model Certification

- Created in 2019 and updated in 2020.
- Developed in concert with Department of Defense stakeholders, University Affiliated Researchers, Federally Funded Research Centers, and the Defense Industrial Base and led by the Office of the Under Secretary of Defense for Acquisition and Sustainment.
- From NIST SP 800-171, Security Requirements for Controlled Unclassified Information, and the Defense Acquisition Supplement.
- For Defense Industrial Base Contractors and will require a third- party certification. [3]

[1] Department of Energy (n.d.) [2] NIST (n.d.) [3] CMMC (2020)

Notable Cybersecurity Maturity Models

Model	Cybersecurity Capabilities Maturity Model (C2M2)	NIST Cybersecurity Framework (CSF)	Cybersecurity Maturity Model Certification
Maturity Levels Functions/Tiers	3	5/4	5
Security Domains/Categories	10	21	17
Processes/Subcategories/Capabilities	38	108	44
Practices/Controls (Maximum)	210	240	171
Type of Assessment	Self-Assessed	Self-Assessed	Third Party Certification

[1] Department of Energy (n.d.) [2] NIST (n.d.) [3] CMMC (2020

Notable Cybersecurity Maturity Models: Cybersecurity Capabilities Maturity Model (C2M2)

10 Domains

1. **Risk Management**
2. Asset Identification, Change, and Configuration Management
3. Identity and Access Management
4. Threat and Vulnerability Management
5. Situational Awareness
6. Information Sharing and Communications
7. Event and Incident Response, Continuity of Operations, and Service Restoration
8. Vendor Security Management
9. Workforce Management
10. Cybersecurity Program Management

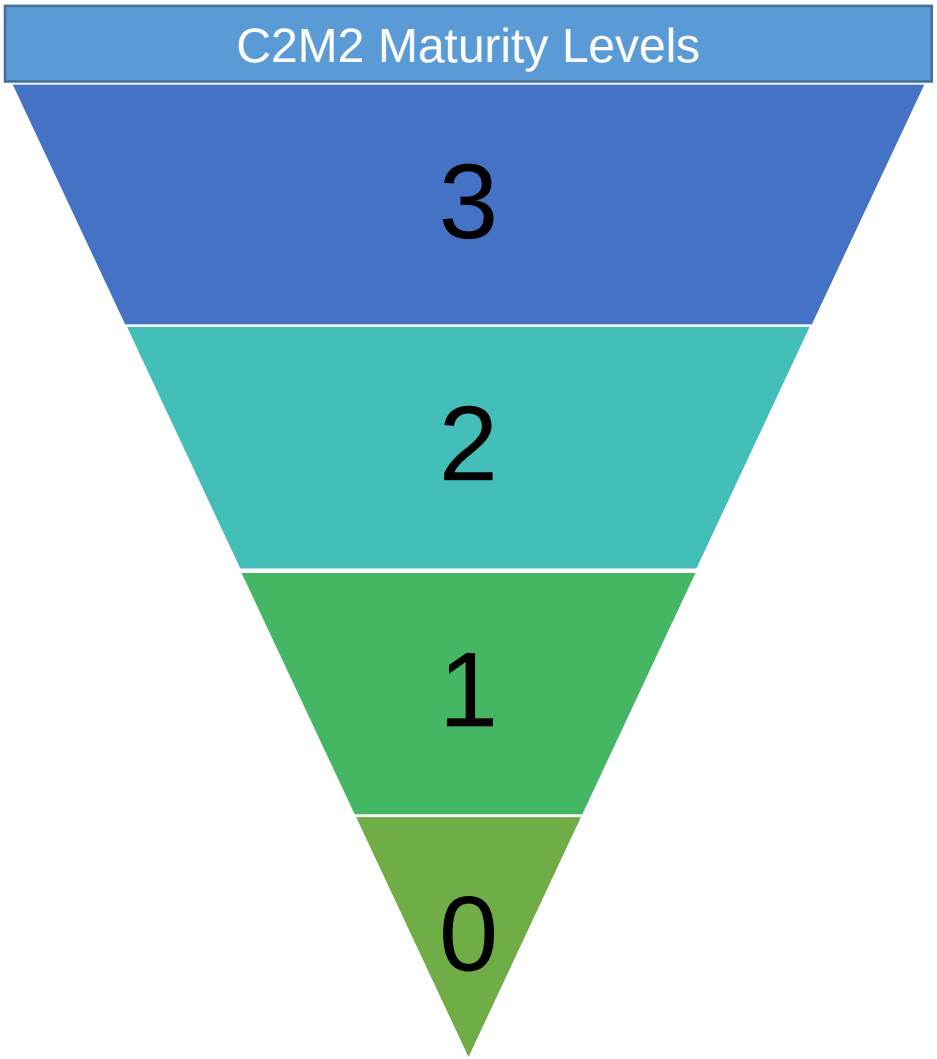
Each Domain is Organized by Objectives

For example, the **Risk Management Domain** has the following 3 Objectives:

1. Manage Cybersecurity Risk
2. Establish Cybersecurity Risk Management Strategy
3. Management Practices

Cybersecurity Capability Maturity Model (C2M2) Program. (n.d.

C2M2: Risk Management Domain, Manage Cybersecurity Risk Objective Practices by Maturity Level

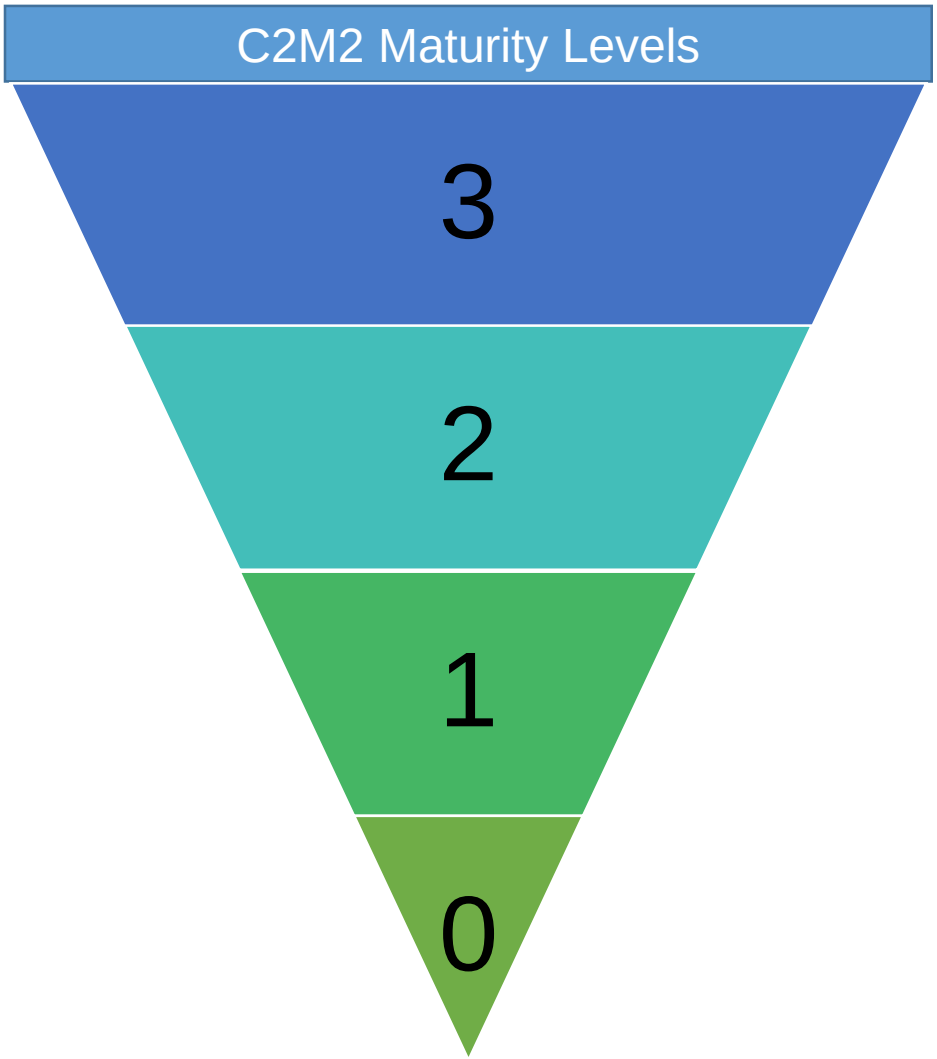


- **Level 3:**
- Risk assessments include all assets and activities that are critical to the achievement of the organization's mission
- The risk management program defines and operates risk management policies and procedures
- A current cybersecurity architecture is used to inform risk analysis
- The risk register includes all risks identified through cybersecurity risk assessments and is used to support risk management activities

- **Level 2:**
- Risk assessments are performed to identify risks according to organization-defined triggers
- Risks are recorded in a risk register
- Risks are analyzed to select and prioritize risk responses using defined risk criteria
- Risks are tracked to ensure that risk responses are implemented

Cybersecurity Capability Maturity Model (C2M2) Program. (n.d.).

C2M2: Risk Management Domain, Manage Cybersecurity Risk Objective Practices by Maturity Level



- **Level 1:**
- Cybersecurity risks are identified and documented, at least in an ad hoc manner
- Risks are mitigated, accepted, avoided, or transferred at least in an ad hoc manner

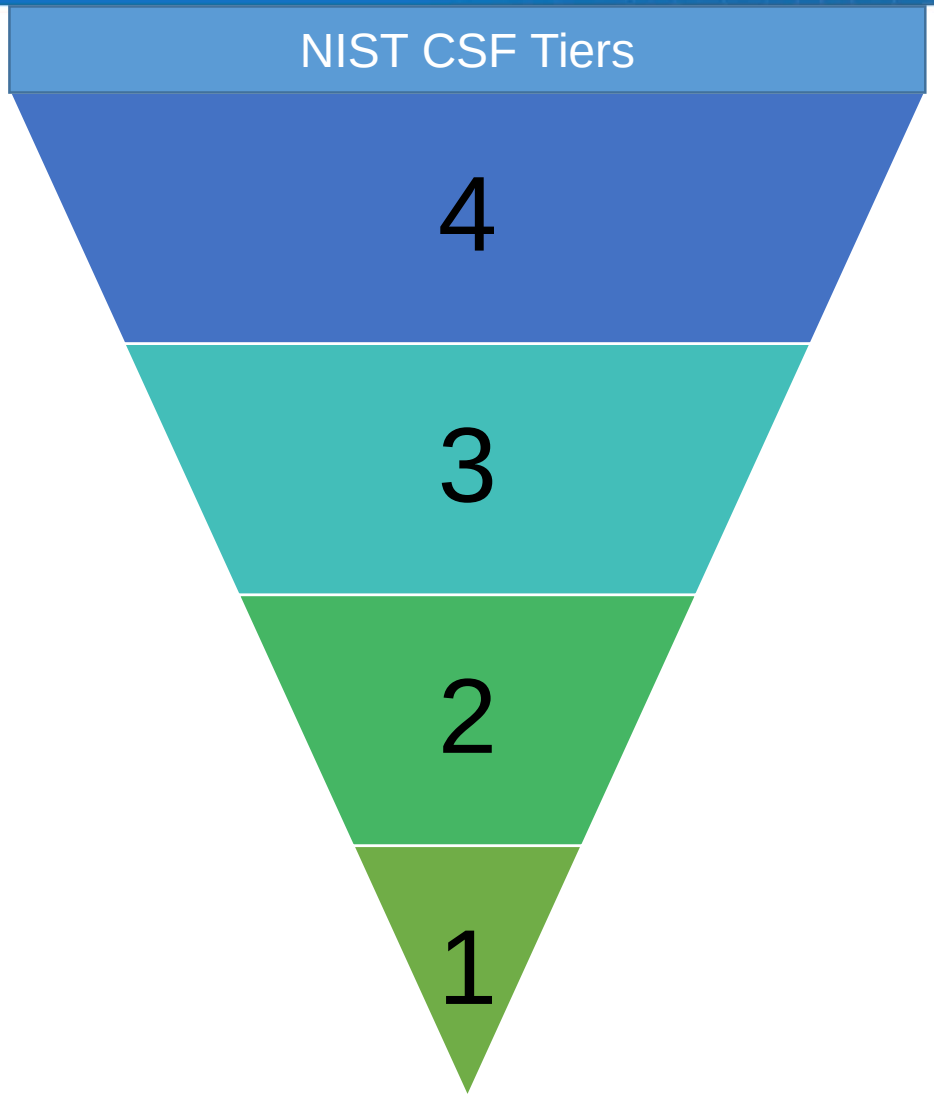
- **Level 0:**
- Practices not performed.

Cybersecurity Capability Maturity Model (C2M2) Program. (n.d.).

Notable Cybersecurity Maturity Models: NIST Cybersecurity Framework

CORE Functions	Categories
Identify Cybersecurity risk to systems, people, assets, data, and capabilities.	• Asset Management • Business Environment • Governance • Risk Assessment • Risk Management Strategy • Supply Chain Risk Management
Protect Develop and implement appropriate safeguards to ensure delivery of critical services.	• Identity Management and Access Control • Awareness and Training • Data Security • Information Protection Processes and Procedures • Maintenance • Protective Technology
Detect Develop and implement appropriate activities to identify the occurrence of a cybersecurity event	• Anomalies and Events • Security Continuous Monitoring • Detection Processes
Respond Develop and implement appropriate activities to take action regarding a detected cybersecurity incident	• Response Planning • Communications • Analysis • Mitigation • Improvements
Recover Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.	• Recovery Planning • Improvements • Communications

NIST Cybersecurity Framework: Tiers

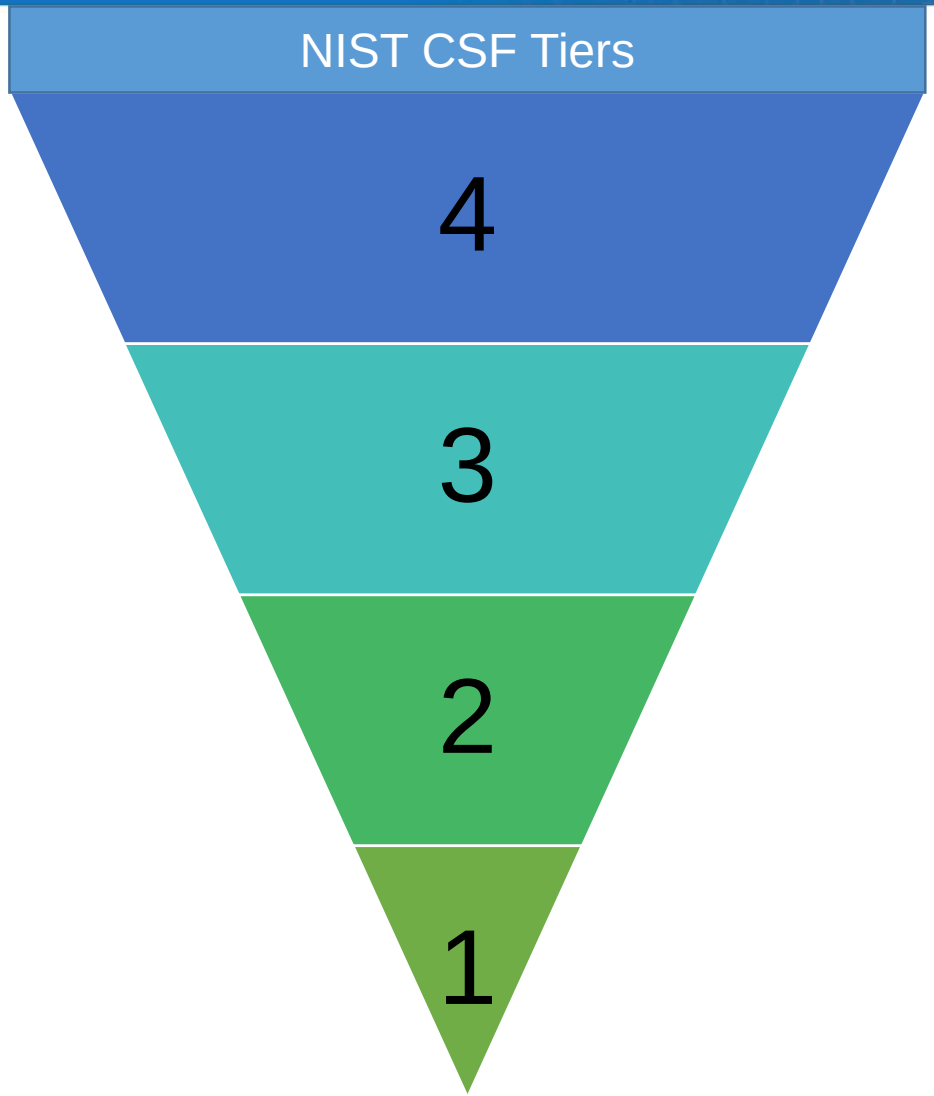


- **Tier 4: Adaptive**
- Risk Management Process – The organization adapts its cybersecurity practices based on previous and current cybersecurity activities, including lessons learned and predictive indicators
- Integrated Risk Management Program – There is an organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events.

- **Tier 3: Repeatable**
- Risk management Process - practices are formally approved and expressed as policy.
- Integrated Risk Management Program – There is an organization wide approach to manage cybersecurity risk.
- External Participation - The organization understands its role, dependencies, and dependents in the larger ecosystem and may contribute to the community's broader understanding of risks.

NIST (2018

NIST Cybersecurity Framework: Tiers



- **Tier 2: Risk Informed**
- Risk Management Process – Risk management practices are approved by management but may not be established as organizational-wide policy.
- Integrated Risk Management Program – There is an awareness, but an organizational approach has not been established.
- External Participation – Generally, organization understands its role in larger ecosystem with respect to either its own dependencies or dependents, but not both

- **Tier 1: Partial**
- Risk Management Process Organizational cybersecurity risk management practices are not formalized,
- Integrated Risk Management Program limited awareness of cybersecurity risk at organizational level.
- External Participation Organization does not understand role in larger ecosystem with respect to its dependencies or dependents.

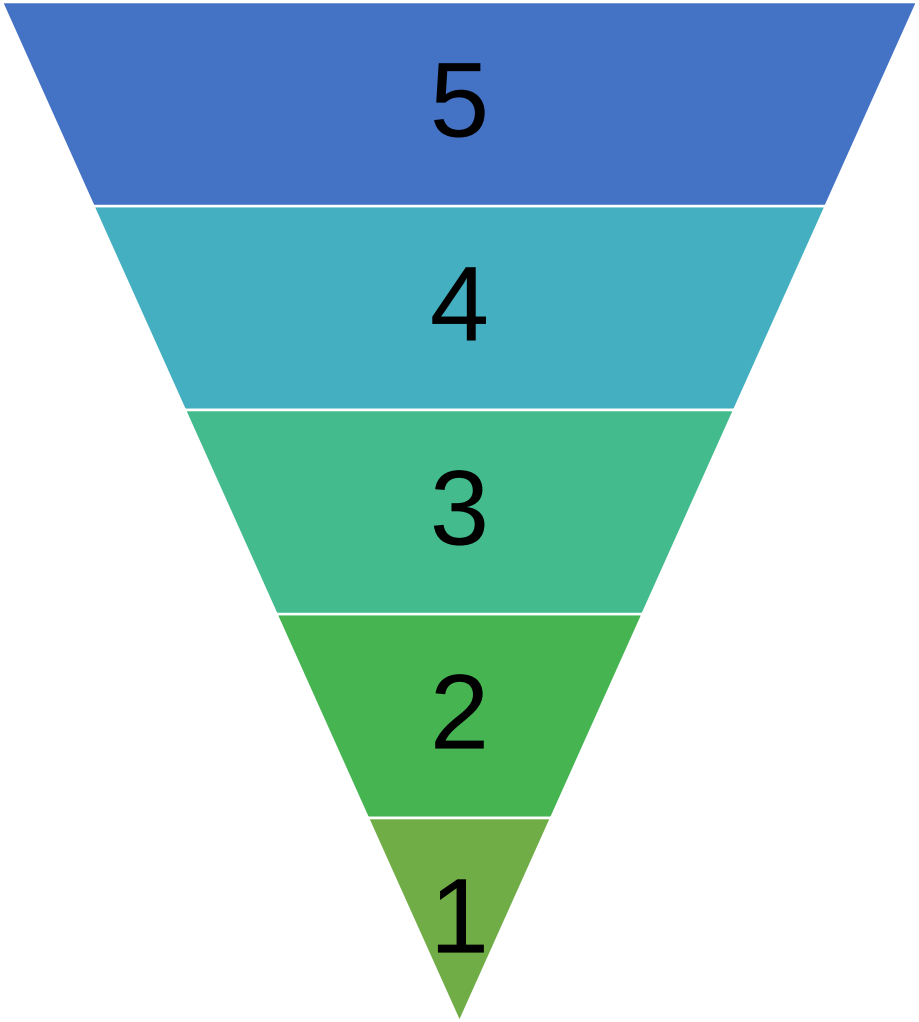
NIST (2018

Notable Cybersecurity Maturity Models: Cybersecurity Maturity Model Certification 17 Domains

- Access Control
- Asset Management
- Awareness and Training
- Audit and Accountability
- Configuration Management
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Personnel Security
- System and Information Integrity
- System and Communications Protection
- Situational Awareness
- Security Assessment
- Physical Protection
- Risk Management
- Recovery

Cybersecurity Maturity Model Certification (CMMC). (2020, March 20).

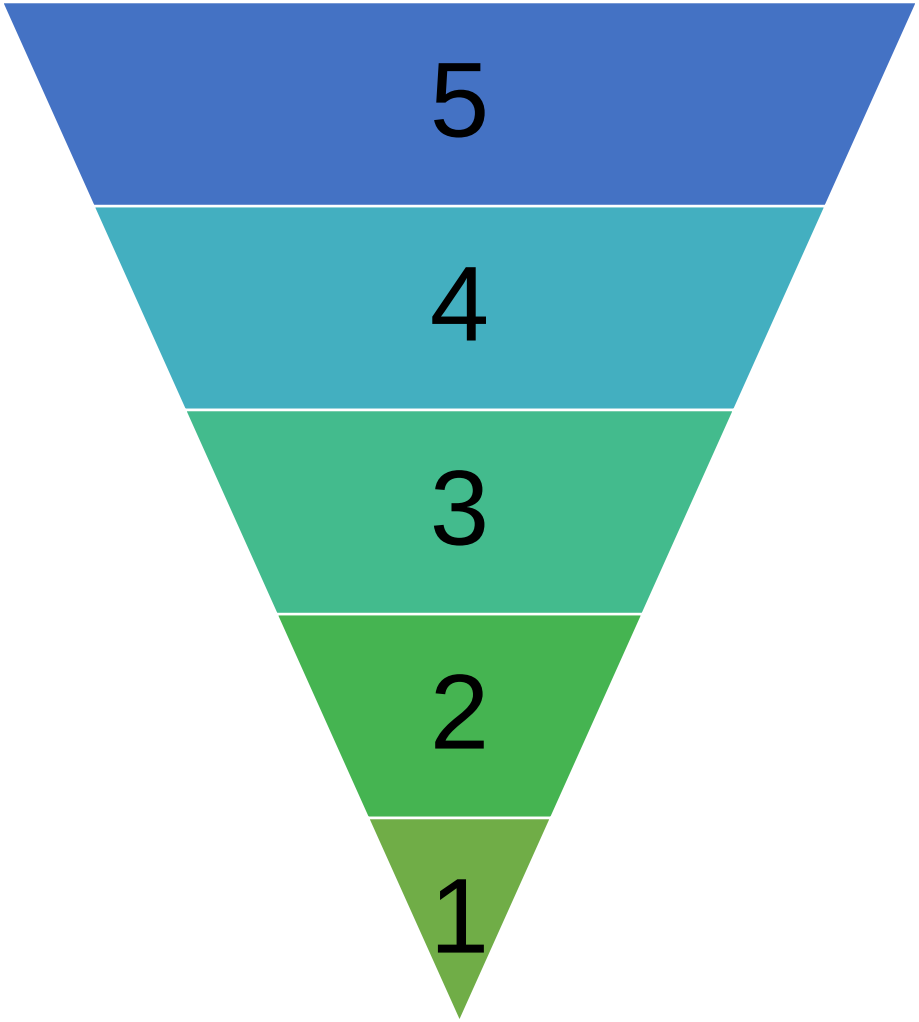
CMMC Increases Security Controls as Level Progresses



- **Level 5: Advanced/Progressive**
- 171 Cybersecurity Practices
- Comply with the Federal Acquisition Regulation (FAR)
  48 CFR 52.204-21
- Encompasses all practices from NIST SP 800-171 r1
- Includes a select subset of 4 practices from Draft NIST SP 800-171B
- Additional 11 practices to demonstrate advanced cybersecurity program
- **Level 4: Proactive**
- 156 Cybersecurity Practices
- Comply with the FAR
- Encompasses all practices from NIST SP 800-171 r1
- Includes a select subset of 11 practices from Draft NIST SP 800-171B
- Includes add'l 15 practices to demonstrate proactive cybersecurity program

Cybersecurity Maturity Model Certification (CMMC). (2020, March 20).

CMMC Increases Security Controls as Level Progresses



- **Level 3: Good Cyber-hygiene**
- 130 Cybersecurity Practices
- Comply with the FAR
- Encompasses all practices from NIST SP 800-171 r1
- Includes an additional 20 practices to support good cyber hygiene
- **Level 2: Intermediate Cyber-hygiene**
- 72 Cybersecurity Practices
- Comply with the FAR
- Includes a select subset of 48 practices from NIST SP 800-171 r1
- Includes an additional 7 practices to support intermediate cyber hygiene
- **Level 1: Basic Cyber-hygiene**
- 17 Cybersecurity Practices
- Equivalent to all practices in FAR

Cybersecurity Maturity Model Certification (CMMC). (2020, March 20).

Why should the Healthcare Sector use Cybersecurity Maturity Models

Continuity of Service

- Ransomware attacks on healthcare organizations have resulted in distributed denial of service attacks
  - In 2016, a private hospital suffered a ransomware attack resulting in the freeze of all computer systems. The attack forced the hospital to revert to pen and paper during the downtime to maintain patient and data records. With the systems down, schedules, documents, and patient data were unavailable, requiring the transfer of some patients to nearby health care institutions for more complete care.
  - A rural hospital had to replace its entire computer network after a ransomware cyber-attack froze the hospital's electronic health record system. Doctors were unable to review their patients' medical histories or transmit laboratory and pharmacy orders.

Protecting Information

- Healthitsecurity.com reported that so far this year the top 10 Healthcare Sector data breaches accounted for almost 3 million patient records being compromised [1]
- A 2020 Verizon Data Breach Report found that:
  - data breaches in the Health Sector were up 71% from the 2019 Report;
  - almost half of data breaches were by company insiders;
  - The majority of data stolen was personal and medical information; and
  - security awareness training was recommended as a top security control [2].

NICCS (2014)

[1] (Healthitsecurity.com, 2020), [2] (Verizon, 2020

Why should the Healthcare Sector use Cybersecurity Maturity Models

Compliance with Laws and Regulations

- Healthcare Sector organizations may fall under one or more of these common regulations and guidelines.
  - Health Insurance Portability and Accountability Act (HIPAA)
  - Health Information Technology for Economic and Clinical Health (HITECH) Act
  - Gramm-Leach-Bliley Act (GLBA)
  - Payment Card Industry Data Security Standard (PCI DSS)
  - Federal Privacy Act of 1974
  - Federal Information Security Management Act of 2002
  - State laws such as The California Consumer Privacy Act (CCPA

NICCS (2014), Harris & Maymi (2019)

Health Sector Specific Resources

Below are some links to some trusted government websites that can provide free resources that can help organization to assess their cybersecurity maturity and keep informed of vulnerabilities, threats, and general information affecting the Health Sector.

- HIPAA Security Rule Crosswalk
  - https://www.hhs.gov/hipaa/for-professionals/security/nist-security-hipaa-crosswalk/index.html
- Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients
  - https://www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx
- Health Sector Cybersecurity Coordination Center (HC3)
  - https://www.hhs.gov/hc3

NICCS (2014)

Health Sector Recommendations and Mitigations

The HHS 405(d) Program published the Health Industry Cybersecurity Practices (HICP), which is a free resource that identifies the top five cyber threats and the ten best practices to mitigate them. Below are examples from HICP that can be used to mitigate some common threats.

Ten Best Cybersecurity Practices	405(d) HICP Sub Practice Reference
1. Email Protection Systems	1.A-C
2. Endpoint Protection Systems.	2.5.A
3. Access Management	3.5.A
4. Data Protection and Loss Prevention	4.5.A,B
5. Asset Management	5.5.A-C
6. Network Management	6.5.A-C
7. Vulnerability Management	7.5.A
8. Incident Response	8.5.A,B
9. Medical Device Security	9.5.A
10. Cybersecurity Policies	10.5.A

HHS (2018)

Summary

- Cybersecurity Maturity Models:
  - attempt to collect the best cybersecurity practices;
  - are developed by a collaboration of experts from diverse backgrounds;
  - consider the dispersion in size, knowledge, skills, abilities, and experience of organizations that will use the model;
  - take a life cycle and continuous improvement approach to cybersecurity;
- Cybersecurity Models help organizations
  - provide services for their customers without interruption;
  - protect sensitive customer and proprietary information; and
  - comply with laws and regulations that govern their operations.
- Although the Health Sector does not have a uniform sector-wide cybersecurity maturity model, many resources exist to assist organizations throughout the cybersecurity life cycle.

Reference Materials

References

- Curtis, P., Stevens, J., & Mehravari, N. (2015). Cybersecurity Capability Maturity Model for Information Technology Services (C2M2 for IT Services),. Carnegie Mellon University, Software Engineering Institute. Carnegie Mellon University. Retrieved July 2020 from
  - https://apps.dtic.mil/dtic/tr/fulltext/u2/1026943.pdf
- Cybersecurity Maturity Model Certification (CMMC). (2020, March 20). Retrieved July 2020 from
  - https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf
- Davis, J. (2020). UPDATE: The 10 Biggest Healthcare Data Breaches of 2020, So Far. Retrieved July 2020 from https://healthitsecurity.com/news/the-10-biggest-healthcare-data-breaches-of-2020-so-far
- Department of Energy. (n.d.) Cybersecurity Capability Maturity Model (C2M2) Program. Retrieved July 2020 from
  - https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity-0
- Demming, E. W. (1982). Out of the Crisis. Cambridge, MASS: Massachusetts Institute of Technology. P.88
- DHS. (2014). Cybersecurity Capability Maturity Model White Paper. United States. Department of Homeland Security. Retrieved July 2020 from
  - https://www.hsdl.org/?abstract&did=798503
- Harris, S. and Maymi, F. (2019). All in One CISSP, Exam Guide Eighth Edition. McGraw-Hill Education. P 79-81
- HHS. (2016). HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework. Health and Human Services. DHHS Office for Civil Rights. Retrieved July 2020 from
  - https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf

References

- HHS. (2018). Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients. Retrieved July 2020 from
  - https://www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx
- *Understanding Cyber Security Models*. (2020, March 3). Retrieved July 2020, from huntsmansecurity.com: https://www.huntsmansecurity.com/blog/understanding-cyber-security-maturity-models/
- NICCS (2014)Capability Maturity Model White Paper. Retrieved Jul 20, 2020, from https://niccs.us-cert.gov/sites/default/files/Capability%20Maturity%20Model%20White%20Paper.pdf?trackDocs=Capability%20Maturity%20Model%20White%20Paper.pdf
- NIST. (n.d.). NIST Cybersecurity Framework. Retrieved July 2020 from
  - https://www.nist.gov/cyberframework
- NIST. (2015, Jan 22). NIST Special Publication 800-53(4). National Institute of Standards and Technology. Retrieved July 2020 from
  - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
- NIST. (2018). Framework for Improving Critical Infrastructure for Cybersecurity. National Institute of Standards and Technology. Retrieved July 2020 from
  - https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
- Verizon. (2020) 2020 Data Breach Investigations Report. Retrieved July 2020 from
  - https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf

Questions

Questions

Upcoming Briefs

- COVID-19 Cyber Threats (Update) - August 13, 2020
- 5G Security (Update) - August 20, 2020
- CIS 20 Controls and HPH – September 3, 2020

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to **HC3@HHS.GOV** or call us Monday-Friday, between 9am-5pm (EST), at **(202) 691-2110.**

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback. If you wish to provide feedback please complete the HC3 Customer Feedback Survey.

HC3 Customer Feedback

Disclaimer

These recommendations are advisory and are not to be considered as Federal directives or standards. Representatives should review and apply the guidance based on their own requirements and discretion. HHS does not endorse any specific person, entity, product, service, or enterprise.

About Us

HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector

Products

Sector & Victim Notifications

Directed communications to victims or potential victims of compromises, vulnerable equipment or PII/PHI theft and general notifications to the HPH about currently impacting threats via the HHS OIG

White Papers

Document that provides in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

Threat Briefings & Webinar

Briefing document and presentation that provides actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

Need information on a specific cybersecurity topic or want to join our listserv? Send your request for information (RFI) to HC3@HHS.GOV or call us Monday-Friday, between 9am-5pm (EST), at (202) 691-2110.
Visit us at: www.HHS.Gov/HC3

Contact

www.HHS.GOV/HC3

(202) 691-2110

HC3@HHS.GOV