1. Incident Response (IR)
2. System and information integrity (SI)
3. Recovery (RE)
4. Risk Management (RM)
5. Personnel security (PS)
6. Situational awareness (SA)
7. Asset management (AM)
8. Physical protection (PE)
9. Access control (AC)
10. Identification and authentication (IA)
11. Systems and communications protection (SC)
12. Configuration management (CM)
13. Audit and Accountability (AU)
14. Awareness and training (AT)
15. Media protection (MP)
16. Security assessment (CA)
17. Maintenance (MA)

The first response is to stop the bleed in an emergency, (IR), check for on coming danger (SI), and move to a recovery mode (RE), attempting to prevent further damage (reputational, to system, ect.). Then in quadrant two of Eisenhower Matrix, it is not urgent but important. Risk management (RM), personal security, (PS) and situational awareness (SA) must be assessed. A company that makes smart choices has staff on that is trained to screen individuals, and a culture of awareness will further the company's maturity. Next, the company will work on taking stock of their assets (AM) and how best to protect them (PE). They will have to assure who has access to them (AC), and how they are able to get that access (IA). Finally, the company will round off their maturity by asserting their configurations are managed (CM), they have audits (AU), regular training (AT), protecting nonphysical assets (MP), and making sure there is maintenance (MA).

1. Incident Response (IR) - Develop and implement a response to a declared incident C018 – Level 2 - IR.2.096
3. Recovery (RE) – Manage backups C029 – Level 2 – RE.2.138

5. Personal Security (PS) - Protect CUI during personnel actions C027 – Level 2 – PS.2.128

7. Asset Management (AM) – Identify and document assets C005 – Level 3 – AM.3.036

How to meet the Level

Incident Response: Develop and implement a response to a declared incident

To meet level two of incident response, we will look at several factors such as what is missing, what needs to be built, what tools are needed, training and testing. Reviewing logs can help identify missing forensic artifacts that were touched or altered, checking for unauthorized firmware/software changes, and reviewing hashes. There should also be a documented incident response plan to outline clean procedures with identifying, reporting, containing, eradicating, and how to recover from the incident. There will be a designated incident response leader and communication contactant, as well as other specified roles and responsibilities. Regular audits and training to spot and report potential incidents should be conducted to improve results.

Recovery: Manage Backups

To manage backups for recoveries, we can start with classifying data sets and systems containing CUI's and creating an outline for how long backups are kept, how data is moved offsite, and how often test restore will be performed. Physically managed backups need to be stored in locked cabinets and secured rooms that have restricted access. Offsite storage is acceptable as well. When using cloud providers, they must meet federal risk and authorized management program standards (FedRAMP) or higher requirements. Backups must have immutable storage against ransomware, least privilege administration authority, regular integrity checks to make sure they weren't corrupted, and tests for restoration.

Personal Security: Protect CUI during personnel actions

To protect controlled unclassified information (CUI) during change of staff, the company can focus on accountability and immediate restriction of access. Hardware, as in laptops and mobile devices. Authentication tools such as tokens, smart cards, and keys or build passes, and documents like manuals or printed materials need to be returned. When teammates are terminated or transferred their accesses must be disabled/ adjusted before the induvial even notices. An exit interview is best practice if possible. Data needs to be monitored for unusual information hoarding that may happen before individuals depart. Every aspect of the organization is to take responsibility for quick actions, systems admin & IT, human resources, program management, and security officer.

Asset Management: Identify and document assets

To identify and document assets, the company must be aware of what they have with a documented list, preventing gaps and increasing security. Establishing and maintain centralized assets and inventory that will include hardware, software, software, and cloud-based resources from any environment including on-premises and AWS environment. Location, ownership, configuration, and access levels are tracked as key details for inventory. Roles need to be assigned responsibilities to ensure inventory is updated consistently, such as, cloud engineer keeps track of AWS resources, security manager reviews/ audit to verify accuracy, and IT admin updating software/hardware inventory. Assessing, modifying, and removing as needed. Automated tools are also available to assist such as RMM and Active Directory. With these actions in place, the company can ensure all assets are properly accounted for and secured.

The most important item I learned while working on the CMMC for this week is fact that security hygiene must be accumulated to achieve higher levels, preventing picking and choosing. The goal is to prevent a “Swiss cheese” structure. As a consultant like Brad, it does not matter how much money or tools a company throws at a problem, but their weakest practices define their security. The spreadsheet helps organizations duplicate secure these habits, ensuring they are repeatable across the entire enterprise. It is also great that the CMMC model v1.02 spread sheet also has references to various technical frameworks.

SPS Academic Resource Center. (n.d.). *The Eisenhower Matrix*. https://sps.columbia.edu/sites/default/files/2023-08/Eisenhower%20Matrix.pdf

Ross, R., Pillitteri, V., Dempsey, K., Riddle, M., & Gary Guissanie. (2016). *Protecting controlled unclassified information in nonfederal systems and organizations*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf

A second word document was used to word count, paragraphs were cut and pasted into this document.