CMMC V1.02

LEVEL 1 REQUIREMENTS

DISCLAIMER

Implementing the actions suggested in this presentation does not guarantee certification to CMMC Level 1. The final requirements for certification have not yet been published.

LEVEL 1 SUGGESTIONS

- While Level 1 requires the implementation of the fewest number of practices (17), understanding each practice requires knowledge of IT systems. If a company out-sources its IT functions, it will be necessary to go over these practices with the IT company to help ensure compliance.

- Although Level 1 certification does not require formal policies and procedures, it is a best practice – and good business – to formally document all policies and procedures to ensure a repeatable, quality result and reduce cyber risk; and to develop and implement a training program for all employees. (Note: this will also improve the maturity of your system)

LEVEL 1 OVERVIEW

- Level 1 focuses on the protection of *Federal Contract Information (FCI) and consists only of practices that correspond to basic safeguarding requirements specified in 48 CFR 52.204-2.
- Process maturity is not assessed for Level 1. In other words, the practices may be performed but not documented (no written processes), and may be done in an ad-hoc manner. Processes are not institutionalized (ingrained) across the organization, nor are they optimized.
- There are 17 practices in Level 1

- *Note: Federal contract information means information not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public Web sites) or simple transactional information, such as necessary to process payments.

LEVEL 1 – NUMBER OF PRACTICES IN EACH DOMAIN

- Access Control – 4
- Asset Management – 0
- Audit & Accountability – 0
- Awareness & Training – 0
- Configuration Management – 0
- Identification & Authentication – 2
- Incident Response – 0
- Maintenance – 0
- Media Protection - 1
- Personnel Security – 0
- Physical Protection – 4
- Recovery – 0
- Risk Management – 0
- Security Assessment – 0
- Situational Awareness – 0
- System & Communications Protection – 2
- System & Information Integrity - 4

LEVEL 1 PRACTICES – ACCESS CONTROL DOMAIN

- AC.1.001 – *Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).*
  - ✓Control who can use company computers and who can log onto the company network
    - ❖Every employee has a username and strong password – no one can use a computer without them
    - ❖Disable username and password when employee leaves the company
  - ✓Limit the services and devices (like printers) that can be accessed by company computers
    - ❖New devices – like printers – must be authorized to be used on the network
  - ✓Set up your system so that unauthorized users and devices cannot get on the company network

LEVEL 1 PRACTICES – ACCESS CONTROL DOMAIN

- AC.1.002 – ***Limit information system access to the types of transactions and functions that authorized users are permitted to execute.*** Not everyone in the company needs access to every type of account.
  - ✓ Identify who the authorized users need to be for each type of account
  - ✓ Keep a current list of accounts and users – see example below (will differ by company)
  - ✓ Review and update list regularly

NAME	HR	Finance	IT	Payroll	Operations	Change Log
Mary Jones	Yes	No	No	No	Yes	1/3/19 – added new employee
John Smith	No	No	No	Yes	Yes	2/10/19 – removed from HR
Sue Baker	No	No	Yes	No	Yes	5/6/19 – added operations
Frank Simpson	No	No	No	No	Yes	7/17/19 – removed from network

LEVEL 1 PRACTICES – ACCESS CONTROL DOMAIN

- AC.1.003 - ***Verify and control/limit connections to and use of external information systems.***
  - ✓*Employees should be connecting to secured external information systems only.* Example: Employees should not be working at a coffee shop using an unsecured network.
  - ✓Limit/control access of 3rd parties, such as contractors, teammates, etc.
  - ✓Limit/control access by other systems internal to the company. For example, if you have an information system for processing FCI and a system that does not process FCI, the system that does not process FCI should be treated as an external system, and there must be adequate controls in place to restrict access.

LEVEL 1 PRACTICES – ACCESS CONTROL DOMAIN

- **AC.1.004 – *Control information posted or processed on publicly accessible information systems.***
  - ✓Designate employees who are authorized to post information publicly – on website, LinkedIn, Twitter, etc.
  - ✓Train the designated employees to ensure that publicly accessible information does not contain nonpublic information
  - ✓Review and approve information prior to posting, and review sites frequently

LEVEL 1 PRACTICES – ACCESS CONTROL DOMAIN

Good Business - not required but relatively easy to implement

- Prohibit the use of personal portable storage devices on internal systems – don't allow employees to use personal flash drives, CDs/DVDs, or external hard drives
- Limit the use of personal computers, tablets and mobile phones to those registered with the IT department. Personal mobile devices should not connect to the company network without permission
- Limit unsuccessful logon attempts – typically 3 attempts, then account is locked
- Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity
- Authorize wireless access prior to allowing such connections
- Monitor and control remote access sessions – use VPN

LEVEL 1 PRACTICES – ASSET MANAGEMENT (AM) DOMAIN

- *There are currently no practices in the Asset Management Domain at Level 1*

- ***Good Business***
  - ✓ ***Keep a log of all IT assets – computers, monitors, keyboards, software, etc., including who the assets are issued to and the date issued and returned.***

LEVEL 1 PRACTICES – AUDIT & ACCOUNTABILITY (AU) DOMAIN

- *There are currently no practices in the Audit and Accountability domain at Level 1*

LEVEL 1 PRACTICES – AWARENESS & TRAINING (AT) DOMAIN

- *There are no currently practices in the Awareness and Training domain at Level 1*

- **Good Business**
  - ✓ ***Ensure that all employees are made aware of the security risks associated with their job and provide training to mitigate the risks***

LEVEL 1 PRACTICES – CONFIGURATION MANAGEMENT (CM) DOMAIN

- *There are no currently practices in the Configuration Management domain at Level 1*
- *Good Business*
    - *Document the software and configuration settings of your system*
    - *Remove software that is not needed*
    - *Analyze the security impact of changes prior to implementation*
    - *Limit installed software to items that the organization has approved*

LEVEL 1 PRACTICES – IDENTIFICATION & AUTHENTICATION (IA) DOMAIN

- ***IA.1.076 – Identify information system users, processes acting on behalf of users, or devices***. You need to know who is using or viewing your system.
  - ✓Assign individual, unique identifiers – like user names – to all employees/users who access company systems
  - ✓Confirm the identities of user, processes, or devices before allowing them access the company’s information system – usually done through passwords.

LEVEL 1 PRACTICES – IDENTIFICATION & AUTHENTICATION (IA) DOMAIN

- ***IA.1.077 – Authenticate (or verify) the identity of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.***
  - ✓All authorized system users have usernames and strong passwords
  - ✓Change default/temporary usernames/passwords

LEVEL 1 PRACTICES – INCIDENT RESPONSE (IR) DOMAIN

- *There are currently no practices in the Incident Response domain at Level 1*

- **Good Business –**
  - ✓ **Establish ways to detect an incident**
    - ❖ **Alerts from sensors or antivirus software**
    - ❖ **A file name that looks unusual**
  - ✓ **Establish a way to report incidents internally**
  - ✓ **Establish a system for tracking incidents**
  - ✓ **Determine a place and a way to store evidence of an incident**

LEVEL 1 PRACTICES – MAINTENANCE (MA) DOMAIN

- *There are currently no practices in the Maintenance domain at Level 1*

- **Good Business – Perform maintenance on your machines**
  - ✓**Corrective maintenance – repairing problems**
  - ✓**Preventative maintenance – updates to prevent potential problems**
  - ✓**Supervise maintenance activities of 3rd party providers**
  - ✓**Sanitize equipment removed for off-site maintenance**

LEVEL 1 PRACTICES – MEDIA PROTECTION (MP) DOMAIN

- ***MP.1.118 – Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.***

- ***Good Business –***
  - ✓ ***Physically control and securely store system media containing FCI, both paper and digital***

NOTE: Per FAR 4.705, contractors are required to retain financial and accounting records and acquisition/supply records for four years.

LEVEL 1 PRACTICES – PERSONNEL SECURITY (PS) DOMAIN

- ***There are currently no practices in the Personnel Security domain at Level 1***
- ***Good Business***
  - ✓***Screen individuals prior to authorizing access to organizational systems***
    - ❖***Background checks***
    - ❖***Drug tests***
    - ❖***Other employment screening pertinent to your company***
  - ✓***Make sure employees no longer have access to FCI when they change jobs or leave the company***
    - ❖***Disable accounts***
    - ❖***ID, access cards/keys returned***
    - ❖***Exit interview – remind them of their responsibility not to discuss FCI***

LEVEL 1 PRACTICES – PHYSICAL PROTECTION (PE) DOMAIN

- ***PE.0.131- Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.***
  - ✓Visitors must sign in and out and be provided a numbered badge that they wear while they are at your facility.
  - ✓Limit visitor access to only the areas necessary.

- ***PE.1.132 – Escort visitors and monitor visitor activity.***
  - ✓Visitors must be escorted at all times.

Note: These physical protection requirements are also contained in the ITAR

LEVEL 1 PRACTICES – PHYSICAL PROTECTION (PE) DOMAIN

- ***PE.1.133 – Maintain audit logs of physical access.***
  - ✓Keep sign-in/out logs secure and available for audit

- ***PE.1.134 – Control and manage physical access devices.***
  - ✓ Keep logs of who has keys, combinations, entry cards, etc.

LEVEL 1 PRACTICES – RECOVERY (RE) DOMAIN

- *There are currently no practices in the Recovery domain at Level 1*

- ***Good Business***
  - ✓ *Regularly perform and test systems and data backups so you can recover it in the event of a failure or malware infection occurs*

LEVEL 1 PRACTICES – RISK MANAGEMENT (RM) DOMAIN

- *There are currently no practices in the Risk Management domain for Level 1*

- *Good Business*
  - ✓ *Organizations should assess the risk to their operations and assets at regular internals, and create a plan to eliminate/mitigate those risks*

LEVEL 1 PRACTICES – SECURITY ASSESSMENT (CA) DOMAIN

- *There are currently no practices in the Security Assessment domain at Level 1*

- ***Good Business***
  - ✓ ***Reassess existing controls (practices) at periodic intervals to validate their usefulness***

LEVEL 1 PRACTICES – SITUATIONAL AWARENESS (SA) DOMAIN

- ***There are currently no practices in the Situational Awareness domain at Level 1***

- Good Business – Periodically assess the security controls in organizational systems to determine if the controls are effective in their application. In other words, are the controls you have in place working as they should.

LEVEL 1 PRACTICES – SYSTEM & COMMUNICATIONS PROTECTION (SC) DOMAIN

- SC.1.175 – Monitor, control, and protect organizational communications (information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of information systems.
  - ✓Web Proxy – when an employee uses a company computer to go to a website, a web proxy makes the request on the user's behalf, looks at the web request, and decides if it should let the employee go to the website.
  - ✓A firewall controls access from the inside and outside, protecting valuable information and resources stored on the company's network. A firewall stops unwanted traffic on the internet from passing through an outside "fence" to the company's networks and information systems.

LEVEL 1 PRACTICES – SYSTEM AND COMMUNICATIONS PROTECTION (SC) DOMAIN

- ***SC.1.176 – Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.***
  - ✓Subnetworks that are separated from internal networks are referred to as demilitarized zones (DMZs).
  - ✓DMZs are typically implemented with boundary control devices and techniques that include routers, gateways, firewalls, virtualization, or cloud-based technologies.

EXAMPLE: You want to launch a website to post job openings and allow the public to download an application form. You must create a DMZ to do this to protect your internal network (options: router and firewall, cloud)

LEVEL 1 PRACTICES – SYSTEM INFORMATION INTEGRITY (SI) DOMAIN

- ***SI.1.210 - Identify, report, and correct information and information system flaws in a timely manner.***
  - ✓Enable all security updates for your software, including the operating system and applications
  - ✓Purchase the maintenance packages for new hardware and operating systems

LEVEL 1 PRACTICES – SYSTEM AND COMMUNICATIONS PROTECTION (SC) DOMAIN

- ***SI.1.211 - Provide protection from malicious code at appropriate locations within the organizational information systems.***
  - ✓Install ant-malware software

- ***SI.1.212 - Update malicious code protection mechanisms when new releases are available***
  - ✓Configure anti-malware software to automatically update to the latest antivirus code and definitions of all known malware

LEVEL 1 PRACTICES – SYSTEM INFORMATION INTEGRITY (SI) DOMAIN

- ***SI.1.213 - Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.***
  - ✓Develop a plan for how often scans are conducted
    - ❖Real-time scans look at the system whenever new files are downloaded, opened, and saved
    - ❖Periodic scans check previously saved files against updated malware information

- ***Good Business***
  - ***Use SPAM filters on inbound and outbound emails***

CMMC V1.02

LEVEL 1 REQUIREMENTS