Small Business Cybersecurity Self Assessment

Why Cybersecurity is important...

Small businesses represent an opportunity for hackers and cyber criminals. Here are a few reasons why:

- Small businesses are a soft target – No/Limited Cybersecurity
- You have desirable data:
  - ◊ Credit Card Info
  - ◊ HIPPA data
  - ◊ PII – Personal Identity Info
  - ◊ Young Adult / Children's PII
- Small businesses may have access to larger companies' and government systems
- You have a legal obligation to protect the data and access you maintain

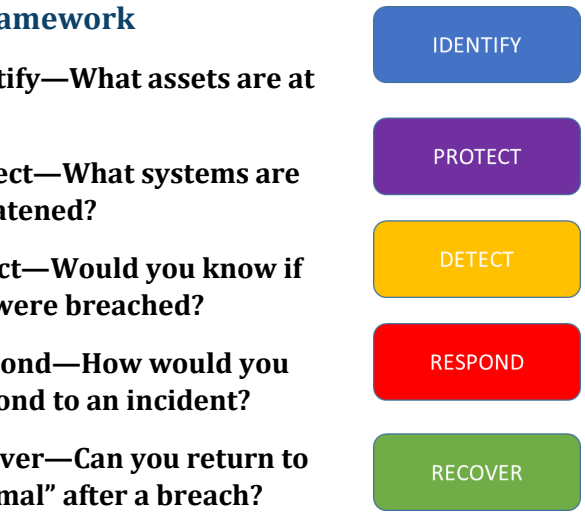
Cybersecurity Maturity Model Certification (CMMC)

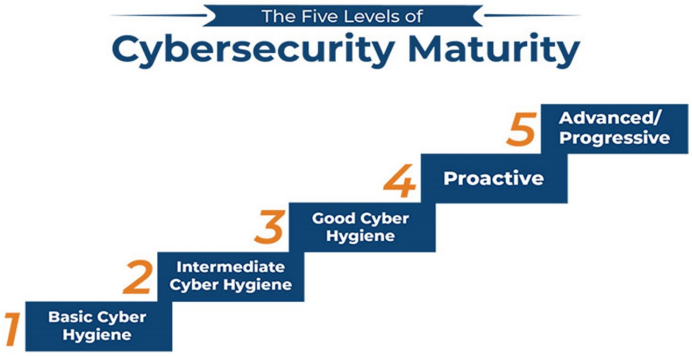
CMMC Model version 1.02, specifically the 17 requirements provided by CMMC and adopted by the Department of Defense for Level 1 maturity. CMMC Level 1 requirements match 2016 "17 Critical FAR controls"

Guidelines & Assessment Foundation

NIST Framework

- **Identify—What assets are at risk?**
- **Protect—What systems are threatened?**
- **Detect—Would you know if you were breached?**
- **Respond—How would you respond to an incident?**
- **Recover—Can you return to "normal" after a breach?**





SC SBDC Resources

- **South Carolina Cyber Breach Law**
- **Small Business Cybersecurity Self-Assessment**
- **Small Business Cybersecurity Guide & Workbook**

SCSBDC.com/cyber || 803.777.4907

CONSULTING * EDUCATION * RESOURCES

Access Control

Access refers to the ability people or devices have to gain entry and use your data processing systems. You control access by granting or denying requests to use information, process data or enter into a network or facility. The goal should be to only provide access to authorized users, or processes implemented by authorized users, devices or other data processing systems. Controls should also include the ability to limit data exposure and processes to only the needed areas within the business and its data processing systems.

Identification and Authentication

Identification and Authentication (IA) is the most basic defense put in place to stop unauthorized access to data resources within a business. Done properly it verifies the identity of a user, process or device and determines what data and systems are approved for access. IA also provides a means of tracking each individual along their passage within a network or system. Normally, identity of a user is authenticated using a combination of a passphrase, a device only the user has access to, and a biometric input (fingerprint, facial recognition, voice pattern). Care should be taken to not only verify identity at the point of entry but to maintain that the person originally verified continues to be the same person throughout the user session.

Media Protection

Media Protection (MP) refers to both digital and non-digital data stored in formats such as internal/external hard-drives, thumb/flash drives, disks, film, and paper. Just like data systems, media should be protected with access controls through physical and digital security. Only authorized personnel should have physical or virtual access to digital and non-digital data. All media should remain in a controlled atmosphere until sanitized and/or disposed of properly.

Physical Access

Protecting the actual building, system and environment used to process your data is what Physical Access (PE) is all about. Normally we are talking about the facilities (building, room, datacenter, file cabinets, office, etc.) and the hardware (networks, computer cabinets, enclosures, etc.) Common threats within this category include unauthorized access, natural disasters, civil unrest, environmental fluctuations and human error. Controls range from simple door locks to complex redundant infrastructures with guarded access.

System and Communication

Protections for Systems and Communication (SC) are both physical and virtual and involve protecting stored data and data in transit. Stored data can be protected by physically separating it from exposure to external networks. Data in transit can be encrypted and transmitted over virtual private networks as a form of protection. Creating boundaries with firewalls and restricted and monitored network access points would also fall into this category.

System and Information Integrity

System and information (SI) integrity can be maintained by continuously monitoring for unusual activity, malware, and active attacks. Most companies will accomplish this through antivirus software, network monitoring services and regularly updating software and hardware to the latest security standards. Maintaining data integrity includes not only detecting and removing data abnormalities but also responding in an appropriate and timely manner. Reporting and correcting shortfalls within the security infrastructure is key to ongoing system and information integrity.

ACCESS CONTROL	Standard	Y / N or NA	Notes or Alternate Solution
Are there any devices used by both employees and clients?	Best Practice		
Who owns the mobile devices used within the company?	Best Practice		
Do you allow employees to use personal devices to access company data (BYOD)?	Best Practice		
Who has access and authorization to distribute web/social media content?	Best Practice		
Does the company own and manage all web property and social media accounts internally?	Best Practice		
Can the company remotely lock / wipe a lost device?	Best Practice		
Does someone monitor login activity?	Best Practice		
Do all employees have web access and is it monitored?	Best Practice		
Do you use passphrases for system and software access?	CMMC AC.1.001		
Do you authenticate users before allowing access?	CMMC AC.1.001		
Are logins required to gain access vs. group or shared access?	CMMC AC.1.001		
Are new account requests authorized before system access is granted?	CMMC AC.1.001		
Do you use access control lists to limit access to systems, applications, and data based on role/identity?	CMMC AC.1.002		
Can you separate and enforce access control rights within your systems?	CMMC AC.1.002		
Do you limit external access to only authorized individuals?	CMMC AC.1.003		
Are you providing guidelines/restrictions on personal or external system access?	CMMC AC.1.003		
Have external systems with access been verified to meet guidelines/restrictions?	CMMC AC.1.003		
Are you limiting the number of system access points for better management of inbound/outbound traffic?	CMMC AC.1.003		
Are you controlling who posts information to publicly accessible systems?	CMMC AC.1.004		
Do employees receive training on what is classified/protected information that cannot be publicly posted?	CMMC AC.1.004		
Is there a review process for all public postings to ensure non-public information is not posted?	CMMC AC.1.004		

IDENTITY AND AUTHENTICATION	Standard	Y / N or NA	Notes or Alternate Solution
Can employees reset any passphrases or lock out owners from any device, in any way?	Best Practice		
Is hardware/software maintained internally?	Best Practice		
How many users have admin level access to their devices?	Best Practice		
Do you assign accounts for unique access by individuals?	CMMC IA.1.076		
Have you separated duties of those who assign permissions from those who assign access?	CMMC IA.1.076		
Is there a centralized account management process that can delete/ lock accounts when needed?	CMMC IA.1.076		
Have you centralized account management into a central identity management system?	CMMC IA.1.077		
Is there an account provisioning (set-up) process in place?	CMMC IA.1.077		
Do you assign unique accounts to new employees, contractors and subcontractors?	CMMC IA.1.077		
Is there a random passphrase generated for each new account and is a passphrase reset required upon first access?	CMMC IA.1.077		
Does your passphrase policy include at least 12 characters with upper/lower case, numbers and special characters?	CMMC IA.1.077		
MEDIA PROTECTION	**Standard**	**Y / N or NA**	**Notes or Alternate Solution**
Are cloud data storage services being used with limited access and sharing disabled?	Best Practice		
What non-data-processing equipment is connected to the internet via your network (IoT)?	Best Practice		
Is there a secure method for equipment / data / paper disposal?	Best Practice		
Is there an inventory of devices and software installed on each?	Best Practice		
Is there a regular accounting of data and where it is stored?	Best Practice		
Are you assigning unique inventory/asset control identifiers to all data processing equipment?	CMMC MP.1.118		
Have all removable media and mobile devices been marked and tracked?	CMMC MP.1.118		

PHYSICAL ACCESS	Standard	Y / N or NA	Notes or Alternate Solution
Are networking and data processing equipment physically secured?	Best Practice		
Are hard copy files locked?	Best Practice		
Do you regularly audit/search facilities for passwords being left out?	Best Practice		
Have you identified sensitive areas within your locations and set up appropriate physical security to limit access to authorized personnel?	CMMC PE.1.131		
Do your printers and other output devices remain within physically secured areas?	CMMC PE.1.131		
Do you maintain a list of authorized personnel with appropriate access credentials for sensitive areas?	CMMC PE.1.131		
Are all visitors escorted by authorized personnel while on premises?	CMMC PE.1.132		
Are visitors provided security and access policies and monitored for compliance?	CMMC PE.1.132		
Are logs maintained on all personnel entering/leaving sensitive areas?	CMMC PE.1.133		
Are visitor access logs maintained and archived for future reference?	CMMC PE.1.133		
Do you use physical access devices (locks, card readers, biometrics) and are they checked regularly?	CMMC PE.1.134		
Is there a process to update access devices due to personnel changes?	CMMC PE.1.134		
Are all codes, keys and access devices secured and audited regularly?	CMMC PE.1.134		
SYSTEMS AND COMMUNICATION	**Standard**	**Y / N or NA**	**Notes or Alternate Solution**
Is a virtual private network (VPN) being used for remote access?	Best Practice		
Are devices set to auto connect to bluetooth and wifi networks?	Best Practice		
Have you established network communication limitations/ boundaries?	CMMC SC.1.175		
Are there systems in place to monitor/manage communications across network boundaries?	CMMC SC.1.175		
Do policies exist to manage access points and acceptable server interfaces via gateways, routers, firewalls, VPNs?	CMMC SC.1.175		
Do you use subnetworks, perimeter networks or "demilitarized zones" to buffer internal networks from outside access?	CMMC SC.1.176		

SYSTEM AND INFORMATION INTEGRITY	Standard	Y / N or NA	Notes or Alternate Solution
Is there a breach/data loss recovery plan in place?	Best Practice		
Is there a system security plan (SSP) in place?	Best Practice		
Has a list of acceptable software been established?	Best Practice		
Are classes or cybersecurity news updates performed regularly?	Best Practice		
Does the company randomly test employees regarding cyber threats?	Best Practice		
Does the company have a copy of applicable breach/incident reporting laws?	Best Practice		
Is there a backup plan identifying what data is backed up and the frequency of the backups?	Best Practice		
Are backups stored in a separate location?	Best Practice		
Does the company use cloud based back up services?	Best Practice		
Are hardware and software being used, less than 5 years old?	Best Practice		
Is encryption being used where applicable?	Best Practice		
Is there an inventory of all equipment?	Best Practice		
Are firewalls in place (hardware/software)?	Best Practice		
Are company owned devices encrypted?	Best Practice		
Has the company performed a test restoration of data lately?	Best Practice		
Does anyone monitor who is accessing/storing data remotely?	Best Practice		
Are regulatory guidelines being followed (HIPPA, DoD, PCI)?	Best Practice		
Has anyone been assigned to monitor web traffic for company information?	Best Practice		
Is web security in place for vendors, suppliers and international transactions?	Best Practice		
Are there processes in place to identify, report and correct system flaws and security issues?	CMMC SI.1.210		
Do you perform software updates in a timely manner, in accordance with your system security plan (SSP)?	CMMC SI.1.210		
Have you turned on auto updates for security software and hardware?	CMMC SI.1.210		
Do you use malware detection on all inbound and outbound network traffic?	CMMC SI.1.211		
Have you loaded malware detection on all devices accessing your networks?	CMMC SI.1.211		
Are all malware, anti-virus and other protection systems updated within 5 days of update release?	CMMC SI.1.212		
Do you perform periodic scans for malware?	CMMC SI.1.213		
Are you scanning files from external sources in real-time as they are downloaded, opened or executed?	CMMC SI.1.213		
Does your malware protection automatically disinfect and/or quarantine suspect files?	CMMC SI.1.213		

Important Information

Name of person responsible for Cybersecurity:

Current Data Inventory (PII, CC, HIPPA, HR, Financials, IP)

Data Type	Location of Data

Equipment/Device Inventory: (Attach additional sheets if needed)

Equipment Type		Owner	Location	ID Number

Operating Systems (Windows, Apple OS, Linux, Other)

Type	Version	Date No Longer Supported

Approved Software

Title	Purpose	Owner	Version

User Identities (Attach additional sheets if needed)

UID	Name	Access Level	Remote Access	Multi- User	Multi- Factor
			Y / N	Y / N	Y / N
			Y / N	Y / N	Y / N
			Y / N	Y / N	Y / N
			Y / N	Y / N	Y / N

Passphrase Management

Complexity	Upper and Lower case letter, at least one numeric and one symbol
Length	Minimum of 12 characters
Change Frequency	Change at a minimum of 180 days
Reuse	No resuse of the past 6 passphrases
Lockout	15 minute lockout after 3 unsuccessful attempts

Data Encryption Checklist

Type	In Place	Needed
Database(s)		
Server Storage		
Laptop Hard Drive(s)		
Mobile Devices		
Email		
Other		

Virtual Private Network (VPN) software in use:

Endpoint Protection Checks & Scanning

Type	Name
Antivirus	
Vulnerability Scan	
Anomaly Detection	
Intrusion Detection	
Active Response	
Alerting/Notification	
Historical Analysis and Stats	
Reporting	
Other	

Firewall

Type	Brand	Software Version

Backup Procedures

Full System			
Frequency		Stored at:	
User Files Only			
Frequency		Stored at:	
File Change Only			
Frequency		Stored at:	

Incident Response Team

Type	Company	Contact	Phone	Email

Authorities

Type	Company	Contact	Phone	Email
Local Police				
Forensics				
Other				

Cybersecurity Insurance

Type	Company	Contact	Phone	Email

Questions?

SCSBDC.com/Cyber
803.777.4907

Small Business Cybersecurity Tips

Guidelines for "Non-Techy" Entrepreneurs

Common Do's and Don't of Cybersecurity

- DO Maintain physical control of cyber assets
- DO Stay updated on threats
- DO Remove unused apps/software
- DO Enable password protection
- DO Turn off Bluetooth
- DO Use encryption
- DO Understand device app permissions
- DO Watch auto-installs
- DO Configure your browser correctly
- Do NOT use public USB ports
- Do NOT use public wi-fi (without VPN)
- Do NOT scan random QR codes
- Do NOT download apps from unknown sources
- Do NOT set laptop to auto-connect to networks

For more information:

SC Title 39 Trade and Commerce – Section 39-1-90
https://www.scstatehouse.gov/code/title39.php

CMMC Requirements
https://www.cmmcab.org/

NIST Protection Framework
https://www.nist.gov/cyberframework

To Report a Breach:

Notify local law enforcement, the local office of the FBI or the U.S. Secret Service.
For incidents involving mail theft, contact the U.S. Postal Inspection Service.

SC SBDC Contact Information:

Phone: 803.777.4907

Web: SCSBDC.com/cyber

Office: 1014 Greene St., Columbia, SC 29208

Funded in part through a Cooperative Agreement with the Small Business Administration.

CONSULTING * EDUCATION * RESOURCES