Cyber Security maturity model certification (CMMC), v1.10 (January 2020)

The Cybersecurity Maturity Model Certification (CMMC) is a unified standard for implementing cybersecurity across the defense industrial base (DIB), which includes over 300,000 companies in the supply chain. The CMMC is the DoD's response to significant compromises of sensitive defense information located on contractors' information systems.

CMMC Model v1.0 encompasses the following:

- ✓ 17 capability domains; 43 capabilities
- ✓ 5 processes across five levels to measure process maturity
- ✓ 171 practices across five levels to measure technical capabilities Section 7. Power of Commissioner

CMMC model framework organizes processes and cybersecurity best practices into a set of domains:

- Process maturity or process institutionalization characterizes the extent to which an activity is embedded or ingrained in the operations of an organization. The more deeply ingrained an activity, the more likely it is that:
  - ✓ An organization will continue to perform the activity – including under times of stress – and
  - ✓ The outcomes will be consistent, repeatable and of high quality.
- Practices are activities performed at each level for the domain

The CMMC establishes five certification levels that reflect the maturity and reliability of a company's cybersecurity infrastructure to safeguard sensitive government information on contractors' information systems. The five levels are tiered and build upon each other's technical requirements. Each level requires compliance with the lower-level requirements and institutionalization of additional processes to implement specific cybersecurity-based practices.

Target Audience?

DoD contractors, required to learn the standard and follow the required guidelines and comply.

How can we help?

Check Point family of blades includes in depth GENV protection, supporting customers when ensuring the overall detection and prevention of cyber security risks.

When adhering to comply and follow this methodology, Check Point family of products can be enabled to ensure proper alignment and consistent compliance with this set of standard requirements.

Check Point Compliance governs multiple blades within the Check Point protection suite and can provide a wide view of your compliance with the requirements presented within this standard, and allows required recommendation to ensure wider compliance while strengthening your security posture when utilizing Check Point family of products.

The following blades need to be enabled to get the full Standard coverage:

- Anti Bot
- Anti Spam & Mail
- Anti Virus
- Application Control
- URL filtering
- DLP
- Identity Awareness
- Gateway Properties Configuration
- Gateway Operating System Configuration
- Firewall Rule Base Configuration
- Firewall and Management Configuration
- IPS Configuration

- VPN Configuration
- Threat Emulation

The Check Point DLP blade can enable the below controls and Check Point Compliance controls has the proper validation process for it.

In addition, there are few other Check Point solutions (i.e.: endpoint suite), which can also be of assistance to enterprises in need to comply with this standard.

How can Check Point Compliance Blade help you (example & partial list of controls)?

CMMC Control Example	Which Control would Check Point Compliance Blade validate?
Access Control, AC.2.009 Limit unsuccessful logon attempts. • NIST SP 800-171 Rev 1 3.1.8 • NIST CSF v1.1 PR.AC-7 • NIST SP 800-53 Rev 4 AC-7	Firewall: 1. Check the 'Accounts expiration indication' setting for User Accounts 2. Check the Expiration notification for Administrator Accounts 3. Check the 'Accounts expiration indication' setting for Administrator Accounts 4. Check that 'Lockout Administrator's account after' is selected
Audit and accountability, AU.2.041 Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions. • NIST SP 800-171 Rev 1 3.3.2 • CIS Controls v7.1 16.8, 16.9 • NIST CSF v1.1 DE.CM-1, DE.CM-3, DE.CM-7 • CERT RMM v1.2 MON:SG1.SP3 • NIST SP 800-53 Rev 4 AU-2, AU-3, AU-3(1), AU-6, AU-11, AU-12	FW: 1. Check that all audit trails include date, time and user identification GAIA: 1. Check that the Audit logs are being sent to the Management server 2. Check that the Audit logs are being sent to the Syslog server
System and communication protection, SC.3.186 Terminate network connections	FW: 1. Check the TCP Start Timeout in the Stateful

associated with communications sessions at the end of the sessions or after a defined period of inactivity. • NIST SP 800-171 Rev 1 3.13.9 • NIST SP 800-53 Rev 4 SC-10	Inspection settings 2. Check the TCP Session Timeout in the Stateful Inspection settings 3. Check the TCP End Timeout in the Stateful Inspection settings
<u>System and communication protection, SC.4.229</u> Utilize a URL categorization service and implement techniques to enforce URL filtering of websites that are not approved by the organization. • CMMC • CIS Controls v7.1 7.4	Application Control: 1. Check that Access Policy is blocking File storage and sharing applications and sites 2. Check that Access Policy is blocking Share files applications and sites 3. Check that Access Policy is blocking Supports file transfer applications and sites 4. Check that the Access Policy has a defined Instant Messaging policy URL Filtering: 1. Check that Sex education-related Sites are being blocked by an Access Policy 2. Check that sites categorized as Tasteless are being blocked by an Access Policy 3. Check that Spam-related Sites are being blocked by an Access Policy 4. Check that Alcohol-related Sites are being blocked by an Access Policy
<u>System and information integrity, SI.1.211</u>	Anti Bot:

Provide protection from malicious code at appropriate locations within organizational information systems. • FAR Clause 52.204-21 b.1.xiii • NIST SP 800-171 Rev 1 3.14.2 • CIS Controls v7.1 8.1 • NIST CSF v1.1 DE.CM-4 • CERT RMM v1.2 VAR:SG3.SP1 • NIST SP 800-53 Rev 4 SI-3 • AU ACSC Essential Eight	1. Check that each Gateway's Anti-Bot configuration is activated according to the policy Anti-Virus: 2. Check that Archive scanning in the Anti-Virus is enabled 3. Check that the HTTP protocol is enabled in the Anti-Virus settings 4. Check that the SMTP protocol is enabled in the Anti-Virus settings 5. Check the Anti-Virus Mail Configuration settings 6. Check that the Anti-Virus blocks files when the nesting level is exceeded 7. Check that Anti-Virus is activated according to the policy Threat Emulation: 1. Check the HTTP protocol setting of each Threat Emulation profile 2. Check the SMTP protocol setting of each Threat Emulation profile Threat Prevention: 1. Check that the Malware DNS Trap is enabled 2. Check the 'High Confidence' setting in the

	Threat Prevention Profile 3. Check the 'Medium Confidence' setting in the Threat Prevention Profile
System and Information Integration, SI.2.216 Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks. • NIST SP 800-171 Rev 1 3.14.6 • CIS Controls v7.1 12.6 • NIST CSF v1.1 DE.CM-1 • CERT RMM v1.2 MON:SG1.SP3 • NIST SP 800-53 Rev 4 SI-4	IPS: 1. Check that the IPS Blade has an updated protection package 2. Check the IPS Protection: TCP Window Size Enforcement 3. Check the IPS Protection: SYN Attack Threat Emulation: 1. Check the frequency of scheduled Threat Emulation images in the Threat Emulation blade 2. Check the Emulation Connection Handling Mode of each Threat Emulation profile 3. Check the frequency of scheduled updates of Threat Emulation engine 4. Check the Protected Scope of each Threat Emulation profile 5. Check the HTTP protocol setting of each Threat Emulation profile
System and Information Integration, SI.3.218	Anti Spam & Mail: 1. Check the Content-based Anti-Spam setting is

Employ spam protection mechanisms at information system access entry and exit points. • CMMC • NIST SP 800-53 Rev 4 SI-8	set to at least Medium 2. Check the IP Reputation Anti-Spam setting is set to High 3. Check the Block List Anti-Spam setting is set to Block

