CMMIDev/3, ISO 9001, 20000, 27001

Cybersecurity Maturity Model Certification (CMMC) & The Risk Management Framework (RMF)

Chakib Jaber, CTO
Spin Systems Inc. (SpinSys.com)

AGENDA

About SpinSys (2-5 min)

Cybersecurity Maturity Model Certification (CMMC) (20 min)

- Overview
- Framework
- Implementation Approach

- **Quick Discussion (2-5 min)**

Risk Management Framework (RMF) (20 min)

- SpinSys Projects Effort Overview
- About
- Steps

Discussions (15 min)

About SpinSys

www.spinsys.com

Cyber Security Maturity Model Certification

What is CMMC?

CMMC stands for "Cybersecurity Maturity Model Certification." The CMMC will encompass multiple maturity levels that ranges from "Basic Cybersecurity Hygiene" to "Advanced."

All companies doing business within the Department of Defense (DoD) will not be able to bid on contracts unless they have CMMC

Cyber Security Maturity Model Certification

When will the final CMMC framework be released to the public?

- Version 1.0 of the CMMC framework became available to support training requirements in January 2020. In June 2020, industry should begin to see the requirement for CMMC compliance.

Will other Federal (Non-DoD) contracts use CMMC?

- The initial implementation of the CMMC will only be within the DoD.

Over 300,000 DoD contractors will need to comply with CMMC

(including Prime and Subcontractors)

Cyber Security Maturity Model Certification

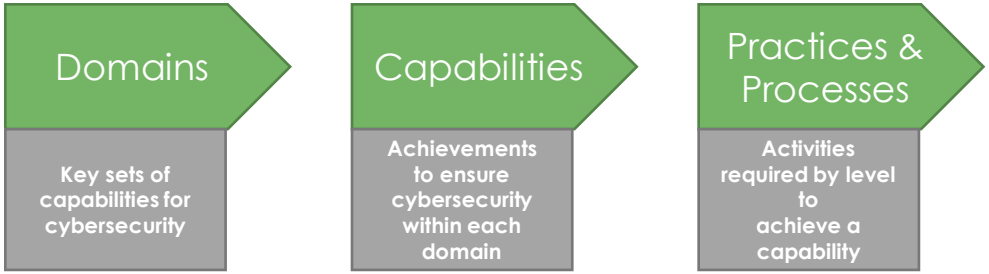
Why is CMMC being created?

DoD is planning to migrate to the new CMMC framework in order to assess and enhance the cybersecurity posture of the Defense Industrial Base (DIB). The CMMC is intended to serve as a verification mechanism to ensure appropriate levels of cybersecurity practices and processes are in place to ensure basic cyber hygiene as well as protect Controlled Unclassified Information (CUI) residing on the Department's industry partners' networks.

CMMC Maturity Level	Technical Practices	Process Maturity
Level 5	***Advanced/Progressive*** Demonstrate a proven ability to optimize capabilities in an effort to repel advanced persistent threats	***Optimized*** Activities are standardized across all applicable organizational units and identified improvements are shared
Level 4	***Proactive*** Demonstrate a substantial and proactive cybersecurity program	***Reviewed*** Activities are reviewed for effectiveness and management is informed of any issues
Level 3	***Good Cyber Hygiene*** Demonstrate good cyber hygiene and effective NIST SP 800-171 Rev 1 security requirements	***Managed*** Activities are reviewed for adherence to policy and procedures and adequately resourced
Level 2	***Intermediate Cyber Hygiene*** Demonstrate intermediate cyber hygiene	***Documented*** Standard operating procedures, policies, and plans are established for all practices
Level 1	***Basic Cyber Hygiene*** Demonstrate basic cyber hygiene, as defined by the Federal Acquisition Regulation (FAR)	***Performed*** N/A - Perform Level 1 practices but no required to exhibit process institutionalization

CMMC - Framework

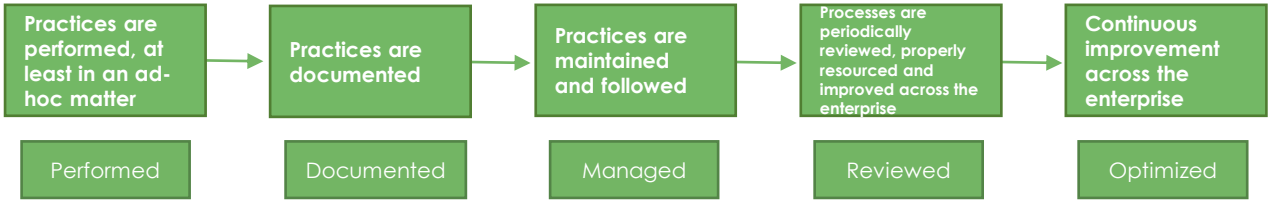
- The Framework consists of **17 Domains** based on cybersecurity best practices
- Domains are comprised of capabilities
- Capabilities are comprised of practices and processes mapped to CMMC level 1 through level 5
- Practices are activities performed at each level for the domain
- Processes detail maturity of institutionalization for the practices



CMMC - Domains

(DOD, 2020)

CMMC Capabilities - Processes



CMMC Capabilities - Practices

	Description of Level Practices	CMMC Rev 0.3 Practices	New CMMC Rev 0.4 Material	CMMC Rev 0.4 Practices	Rev 0.4 New Content Sources
CMMC Level 1	Basic Cyber Hygiene	17	+18 practices	35	• DIB SCC TF WG Top 10 • NIST Cybersecurity Framework 1.1 • ISO 27001:2013 • AIA NAS 9933 • CIS Critical Security Controls 7.1 • CERT Resilience Management Model® • Additional DIB Inputs • Subject Matter Experts
CMMC Level 2	Intermediate Cyber Hygiene	46	+69 practices	115	
CMMC Level 3	Good Cyber Hygiene	63	+28 practices	91	
CMMC Level 4	Proactive	10	+85 practices	95	
CMMC Level 5	Advanced / Progressive	4	+30 practices	34	

Cybersecurity Maturity Model Certification (CMMC)

Physical Access

1. Limit Physical Access
2. Control Physical Access
3. Maintain Physical Access Log
4. Always Escort and Monitor Visitors

Operations & Maintenance

1. Software Supported by Original Vendor
2. System Configuration Baselines in Place
3. System Configuration Management Performed
4. System Maintenance is Performed
5. Install Anti-Virus Protection
6. Keep Anti-Virus Protection Updated
7. Use Anti-Virus Protection in Real-Time
8. Events are Reported
9. Incidents are Declared
10. Incidents are Resolved
11. System Flaws are Corrected
12. Audit Logs Retained
13. Audit Logs Reviewed
14. Properly Sanitize Media Containing CUI

Documentation & Knowledge Sharing

1. Guidelines in Place
2. CUI is Identified and Controlled
3. Assets are Tracked
4. Define Security Controls
5. Stay Informed on Cyber Threats
6. Share Cyber Threat Information with Team
7. Cybersecurity Objectives Defined
8. Cybersecurity Objectives Implemented

System Access

1. Identify Authorized Users, Processes and Devices
2. Screen People Before Giving Access to CUI
3. Protect CUI During Personnel Actions
4. Authenticate System Access
5. Limit Unsuccessful Logon Attempts
6. Limit System Access to Authorized Users
7. Limit System Access to Approved Activity
8. Separate Public Facing Systems from Internal Systems
9. Protect Communications at System Boundaries

Based on the 59 pages of DoD's rev 0.4 draft.
This is meant to serve as a guide when understanding the LOE to be compliant with CMMC Level 1.

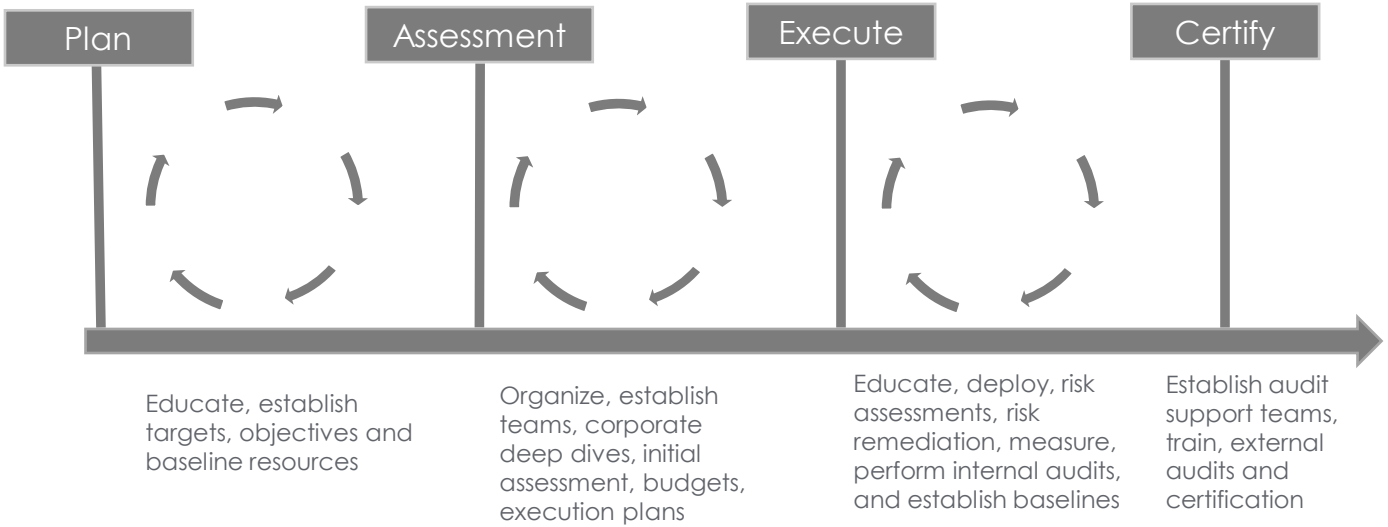
Cyber Security Maturity Model Certification

- For many companies, DoD contracts make up a substantial percentage of their revenue, and because CMMC certification will now be an absolute requirement for contract awards, it is extremely important that contractors pass the CMMC audit on the first pass and avoid the need for re-certification.

- If a contractor fails a CMMC audit, they will be unable to offer products and services to the DoD for an extended period due to:

1. The time it takes to implement NIST 800-171 controls effectively
2. The time it takes for another CMMC audit to become certified

Implementation Approach



Implementation Cost/Budget Considerations

Soft Costs

- Cost of planning
- Cost of learning
- Cost of training
- Cost of new internal hires
- Cost of new process and implementations
- Cost of ongoing projects

Acquisition Costs

- Cost of consulting services
- Cost of training
- Cost of new products/services

Certification Costs

- Cost of auditors
- Cost of certifications

Implementation Cost/Budget Variables

Mature SP 800-171 complaint environnement*

- Consulting costs (mid size organization) -
  - CMMC gap assessment
    - Estimated cost $15,000-20,000
  - Gap remediation
    - Estimated cost $10,000 - $25,000
- Hard costs prep - (depending current on investment)
  - Additional budget ($10,000 - $25,000)
    - End point protection
    - Multi factor authentication
    - Mobile device management
    - Log monitoring
- Hard costs for audit
  - Not defined yet
  - Budget guess ($20,000 - $50,000)

Not Mature SP 800-171 complaint environnement*

- Consulting costs (mid size organization) -
  - CMMC gap assessment
    - Estimated cost $30,000-50,000
  - Gap remediation
    - Estimated cost $10,000 - $40,000
- Hard costs prep - (depending on investment)
  - Budget estimates ($20,000 -$90,000)
    - End point protection
    - Multi factor authentication, code reviews
    - Mobile device management
    - Log monitoring, backups
- Hard costs for audit
  - Not defined yet
  - Budget Guess ($20,000 - $50,000)

***: Costs are estimates and will depend on size and maturity of organization(s), based on our own estimates**

SPIN SYS

CMMIDev/3, ISO 9001, 20000, 27001

Discussions

Risk Management Framework (RMF)

RMF Agenda

About SpinSys programs

Risk Management Framework (RMF)

- About
- Steps

Program Overview

SpinSys provides worldwide enterprise Health Information Technology (IT) engineering support in the following areas of interest for customers within the Medical Community:

- System engineering
- Enterprise infrastructure
- Enterprise network
- Network security
- Infrastructure engineering
- Infrastructure operations
- Network operations
- Platform infrastructure engineering
- Systems testing
- Systems integration
- Infrastructure and network migration services
- Enterprise portals
- Data exchange
- Big Data Solutions
- Information assurance

The RMF security framework is at the core of everything we do

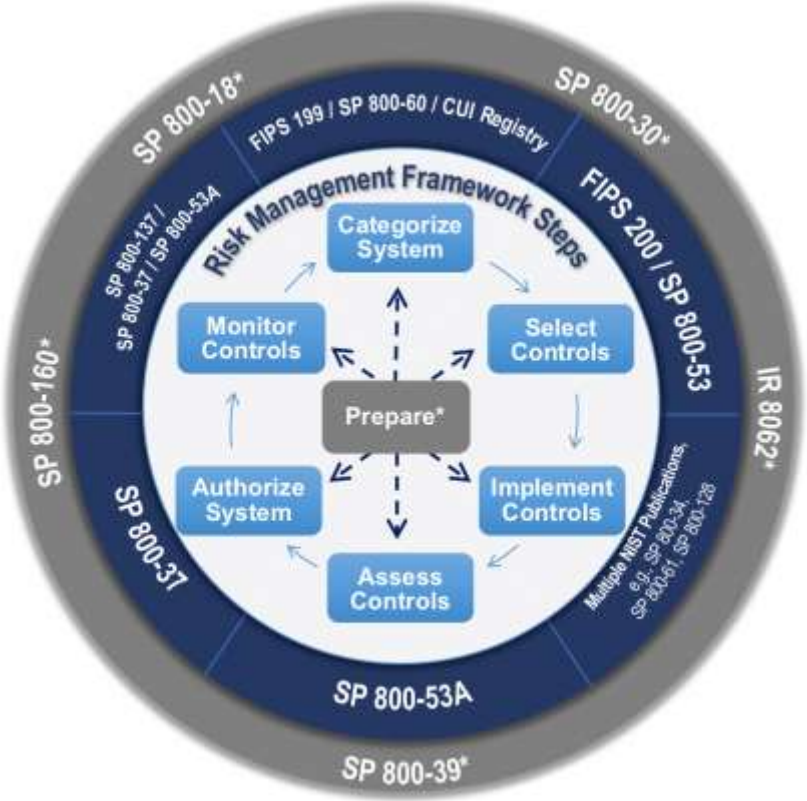
Focus on Success – Meeting Our Goals

- Proven expertise and customer relationships with each program within the scope of this task order
- Focus on customer satisfaction and customer relationships
- Core focus on providing innovative solutions: improving the user experience, promoting cost savings, and improving quality
- CMMI Level 3 accredited Agile processes will provide focus on customer satisfaction, quality, and cross-team collaboration
- Lean processes will provide measured and visible incremental success; will achieve more with smaller teams, reduce cost and produce faster time to market
- Support consolidation and cost reduction while maintaining and delivering enterprise grade solutions
- Secure and manage resources and infrastructure

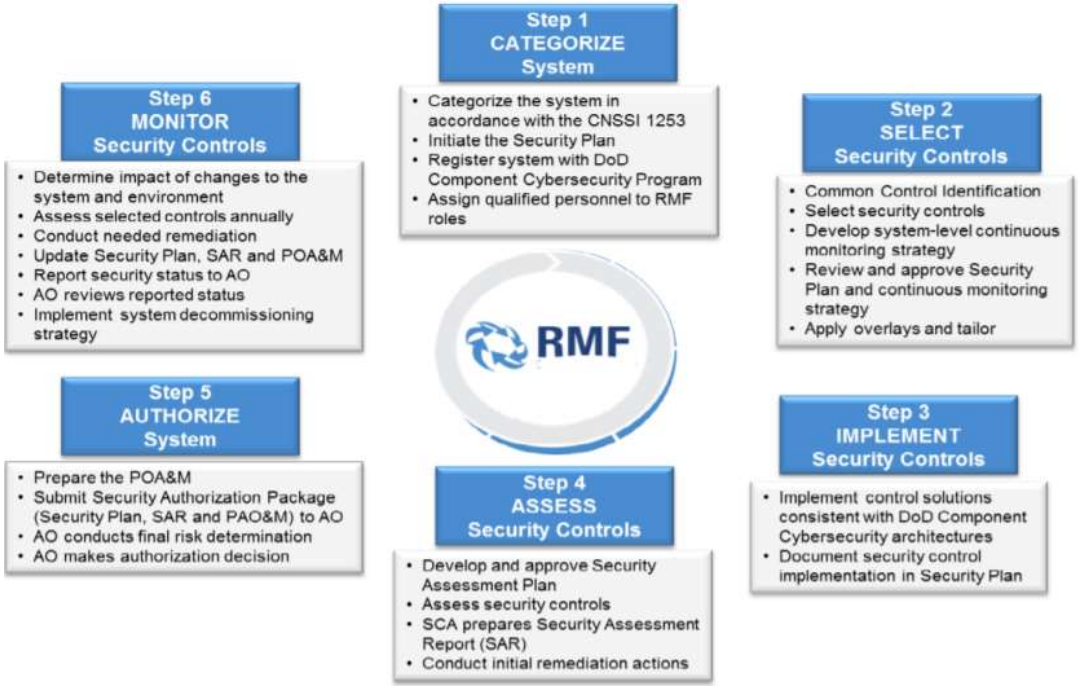
Security is imbedded in every step of the project lifecycle

About RMF

- Risk Management Framework (for Information Systems and Organizations)
- RMF must be continuously assessed
- Primarily used by DoD
- Defined in NIST 800-37r2


SP 800-18*
FIPS 199 / SP 800-60 / CUI Registry
SP 800-30*
SP 800-137 / SP 800-37 / SP 800-534
Risk Management Framework Steps
FIPS 200 / SP 800-53
SP 800-160*
IR 8062*
Categorize System
Monitor Controls
Select Controls
Prepare*
Authorize System
Implement Controls
Assess Controls
SP 800-37
Multiple NIST Publications, e.g., SP 800-34, SP 800-61, SP 800-128
SP 800-53A
SP 800-39*

RMF - Steps



SCA: Security Control Official
AO: Authorizing official
POA&M: Plan of Actions & Milestones

RMF Steps

01 - Prepare > 02 - Categorize > 03 - Select > 04 - Implement > 05 - Assess > 06 - Authorize > 07 - Monitor

Prepare carries out essential activities at the organization, mission and business process, and information system levels of the enterprise to help prepare the organization to manage its security and privacy risks using the Risk Management Framework

RMF Steps

01 - Prepare > 02 - Categorize > 03 - Select > 04 - Implement > 05 - Assess > 06 - Authorize > 07 - Monitor

Categorize:

The system and the information processed, stored, and transmitted by that system based on an impact analysis.

Security Objectives: Confidentiality, Integrity, Availability
Impact Values: Low, Moderately, High
Specific category of information (e.g., Privacy, medical, Proprietary, financial, investigative, contractor-sensitive, security management), defined by an organization

RMF Steps

01 - Prepare > 02 - Categorize > 03 - Select > 04 - Implement > 05 - Assess > 06 - Authorize > 07 - Monitor

Select:
An initial set of baseline security controls for the system based on the security categorization; tailor and supplement the security control baseline as needed based on organization assessment of risk and local conditions

RMF Steps

01 - Prepare > 02 - Categorize > 03 - Select > 04 - Implement > 05 - Assess > 06 - Authorize > 07 - Monitor

Implement:
the security controls and document how the controls are deployed within the system and environment of operation

RMF Steps

01 - Prepare > 02 - Categorize > 03 - Select > 04 - Implement > 05 - Assess > 06 - Authorize > 07 - Monitor

Assess:
the security controls using appropriate procedures to determine:

- Implemented correctly
- Operating as intended
- Producing the desired outcome
- With respect to meeting the security requirements for the system
- NIST800-53A

RMF Steps

01 - Prepare > 02 - Categorize > 03 - Select > 04 - Implement > 05 - Assess > 06 - Authorize > 07 - Monitor

Authorize:
System operation based upon a determination of the risk to organizational operations and assets, individuals, other organizations and the Nation resulting from the operation of the decision that this risk is acceptable.

RMF Steps

01 - Prepare > 02 - Categorize > 03 - Select > 04 - Implement > 05 - Assess > 06 - Authorize > 07 - Monitor

Monitor:
And assess selected security controls in the system on an ongoing basis including assessing security control effectiveness, documenting changes to the system or environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to appropriate organizational officials.

SPIN SYS

CMMIDev/3, ISO 9001, 20000, 27001

Discussions

References

- CMMC FAQ's, Office of the Under Secretary of Defense for Acquisition & Sustainment. Retrieved March 11, 2020, from https://www.acq.osd.mil/cmmc/faq.html
- DOD. (2020, January 30). Cybersecurity Maturity Model Certification (CMMC) v1.0. Retrieved March 11, 2020, from https://www.acq.osd.mil/cmmc/docs/CMMC_Model_Main_20200203.pdf
- Brecht, D. (2019, November 7). DoD's Cybersecurity Maturity Model Certification (CMMC) initiative. Retrieved March 11, 2020, from https://resources.infosecinstitute.com/dods-cybersecurity-maturity-model-certification-cmmc-initiative/#gref
- *Risk Management Framework (Rmf) Overview*. (2019). Retrieved from https://www.youtube.com/watch?v=1LgJVxvE8AY&feature=youtu.be
- Initiative, J. T. F. T. (2014, December 18). Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans. Retrieved March 12, 2020, from https://csrc.nist.gov/publications/detail/sp/800-53a/rev-4/final