The CMMC is Here, Are You Ready?

(2-Part Series)

The JAMIS CMMC Readiness Group

October 12, 2021

About JAMIS

JAMIS provides innovative and agile cloud ERP solutions designed exclusively for government contractors

- JAMIS Prime ERP was built in the Cloud from day one
- Decades of experience built into modern tech
- The process automation expertise from nearly 1,000 implementations

Purpose & Background

- The CMMC will impact ALL government contractors.
- Bring a panel of experts together to provide awareness and education to JAMIS customers, partners, and the general federal contracting market.
- Data security is a very high priority for JAMIS, and staying engaged with industry cybersecurity professionals and our customers on this journey to a new frontier is the best way for us to prepare for a new regulatory environment.

JAMIS CMMC Readiness Group

RISCPoint

DHG
DIXON HUGHES GOODMAN LLP

HK
Holland & Knight

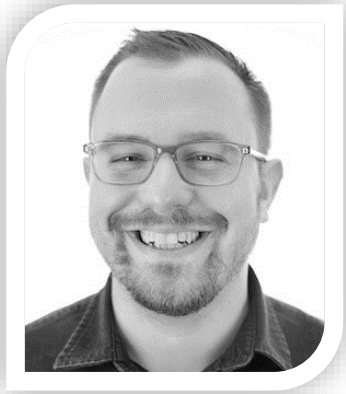
Cask
GOVERNMENT SERVICES

EDWARDS
PERFORMANCE SOLUTIONS

NEVERFAIL
CONTINUOUS CONTROLS

Meet the CMMC Readiness Group Panel of Experts

Dan Rusert
Vice President
Of Marketing, JAMIS



Jacob Nix
CEO, RISCPoint
& JAMIS vCISO

Eric Crusius
Partner, Holland &
Knight

Tom Tollerton
Managing Director,
DHG

Stacy High-Brinkley
VP Compliance
Solutions, Cask
Government Solutions

Kris Martel
CISO, Neverfail
Continuous Controls

Brian Hubbard
Director Commercial &
Cybersecurity, Edwards
Performance Solutions

Eric Levitas
Director of BD,
Edwards Performance
Solutions

Join Our LinkedIn Group!

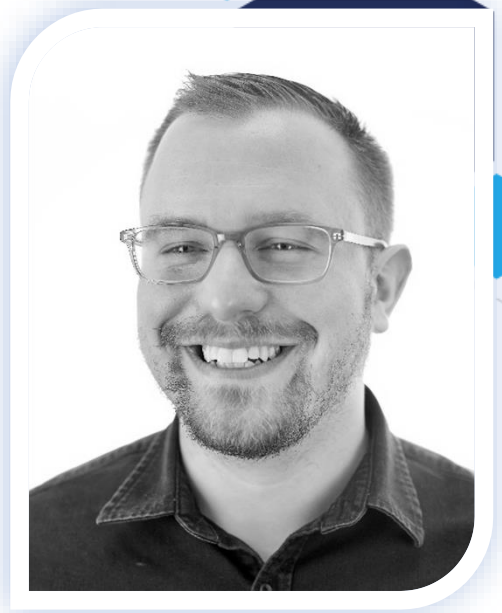
Direct Link to the JAMIS CMMC Readiness Group

https://www.linkedin.com/groups/13969347/

Introducing the CMMC Panel of Experts Group Leader

RISCPoint JAMIS®

- As CEO of RISCPoint, Nix leverages the knowledge gained during his time in leadership roles at global audit and consulting firms to build a team of experts to help organizations build a balanced environment, tailored to their regulatory and compliance requirements, while also helping them to efficiently achieve their business goals.
- Jake also serves as JAMIS' virtual Chief Information Security Officer. JAMIS and RISCPoint have a shared focus on security and compliance excellence.



Jacob Nix
Chief Executive Officer, CPA, CISA, CDPSE, ISO LI, CCSFP

JAMIS®

Agenda

- CMMC Rollout and Training Timeline
- NIST 800-171 vs CMMC Level 3
- Remediation Planning & Approach
- Q&A

CMMC Rollout & Training Timeline

Eric Levitas, Director of Business Development
Edwards Performance Solutions

EDWARDS
PERFORMANCE SOLUTIONS

- Edwards Performance Solutions helps clients increase operational performance by finding ways to improve productivity, profitability, and security.
- With two decades of experience working with both government and commercial clients, we ensure operational excellence to drive overall mission success.
- More than project managers; we're trusted advisors in healthcare, training, cybersecurity, and business process.

Eric Levitas
Director, Business Development, Connector, Podcaster

JAMIS®

CMMC CCP Training Timeline

OCTOBER 2021

25

10/25 – 10/29 (Virtual) CCP Exam Prep EDT

9:00 AM - 5:00 PM (EDT)

Instructor: Amira Armond Jeff Baldwin Joy Beland Sara Deaton

Location: Zoom Virtual Classroom

$3720.00

Class Size:	25
Seats Remaining:	23
Starts:	October 25, 2021 9:00 AM EDT
Ends:	October 25, 2021 5:00 PM EDT
Recurrence:	Daily View 5 Recurrences

Course Date and Time

- Monday, October 25, 2021 9:00:00 AM - 5:00 PM EDT
- Tuesday, October 26, 2021 9:00:00 AM - 5:00 PM EDT
- Wednesday, October 27, 2021 9:00:00 AM - 5:00 PM EDT
- Thursday, October 28, 2021 9:00:00 AM - 5:00 PM EDT
- Friday, October 29, 2021 9:00:00 AM - 5:00 PM EDT

Key Training Notes

- CCP Course will begin being distributed in Oct. 2021
  - Official Test for CCP will be in Feb 2022
- Edwards is first LPP to distribute their curriculum to train CCP's
  - This is a solid step in the right direction!
- CCA1 & CCA3 classes will be administered in 2022
- There are a little over 100 PAs who will begin the formal assessments
- We don't know when assessments will begin – the DOD keeps pausing until they publish the final scoping guidelines.
- CCP's can participate in the formal assessments
- CCP is the next logical phase of RP's
  - This is critical for proper advisement
- OCS's will want in house people trained to better implement and consult on CMMC / 800-171.

JAMIS®

BREAKDOWN

CCA · CCP · RPO · RP · C3PAO

CERTIFIED PROFESSIONALS

- Create CMMC-based cybersecurity programs
- Consult with OSCs on assessment preparation
- Maintain CMMC compliance of OSC systems
- Participate on formal CMMC Assessment Teams

CCP REQUIREMENTS

- Take 5-day course, pass exam, prove 2 years IT or Cybersecurity Experience

INTENDED AUDIENCE

- Employees of Organizations Seeking CMMC Certification (OSC)
- Information Technology (IT) and Cybersecurity Professionals
- Regulatory Compliance Officers
- Legal and Contract Compliance Professionals
- Management Professionals
- Cybersecurity and Technology Consultants
- Federal Employees
- Candidate CMMC Assessment Team Members

CERTIFIED ASSESSORS

- Create CMMC-based cybersecurity programs
- Consult with OSCs on assessment preparation
- Maintain CMMC compliance of OSC systems
- Participate on formal CMMC Assessment Teams
- Lead a formal assesstment

CCA REQUIREMENTS

- For any Assessor Level, take 5-day Certified Professional course and pass exam
- Level 1: Take 5-day Course, pass exam, 2 years IT or Security Experience, pass Tier 3 Background Check, be a US citizen
- Level 2: Level 1 + be a US citizen (L2 or higher)
- Level 3: Hold Level 1 Certified Assessor, 4 years IT or Cyber Experience
- Level 5: Hold Level 3 Certified Assessor, 4 years IT or Cyber Experience, and completed 15 CMMC ML-3 Assessments

REGISTERED PROVIDER ORGANIZATIONS (RPOs) & **REGISTERED PRACTITIONERS (RPs)** provide a necessary service in preparation for an assessment.

RPOs

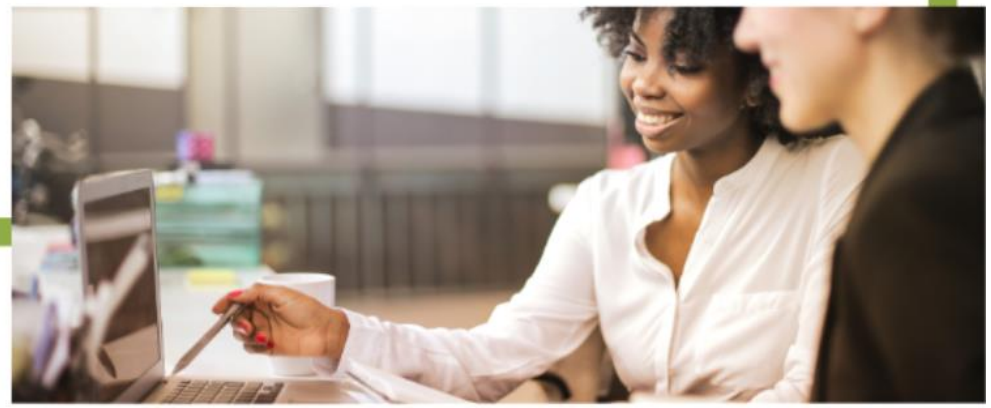
- Deliver non-certified CMMC consulting services
- Signifies you agreed to CMMC-AB Code of Professional Conduct
- Listed on CMMC-AB Marketplace

RPs

- Consult with OSCs on cybersecurity program development
  - Design/implement practices
  - Create process documentation
- Consult with OSCs on assessment preparation
  - Scoping
  - Objective evidence collection and storage
- Not authorized to participate on formal Assessment Teams

CERTIFIED THIRD-PARTY ASSESSOR ORGANIZATIONS (C3PAOs) are organizations employing CAs and CPs, providing quality assurance of the assessment process and results.

- Identify gaps associated with an organization's cybersecurity posture
- Provide detailed findings followed by directional roadmaps designed to guide organizations to full compliance in regards to organizational needs
- Provide senior management with deliverable that justifies compliance funding or support
- C3PAOs cannot perform both the official assessment and pre-assessment for the same organization



NIST 800-171 vs. CMMC Level 3

Tom Tollerton, Managing Director
Dixon Hughes Goodman

DHG

DIXON HUGHES GOODMAN LLP

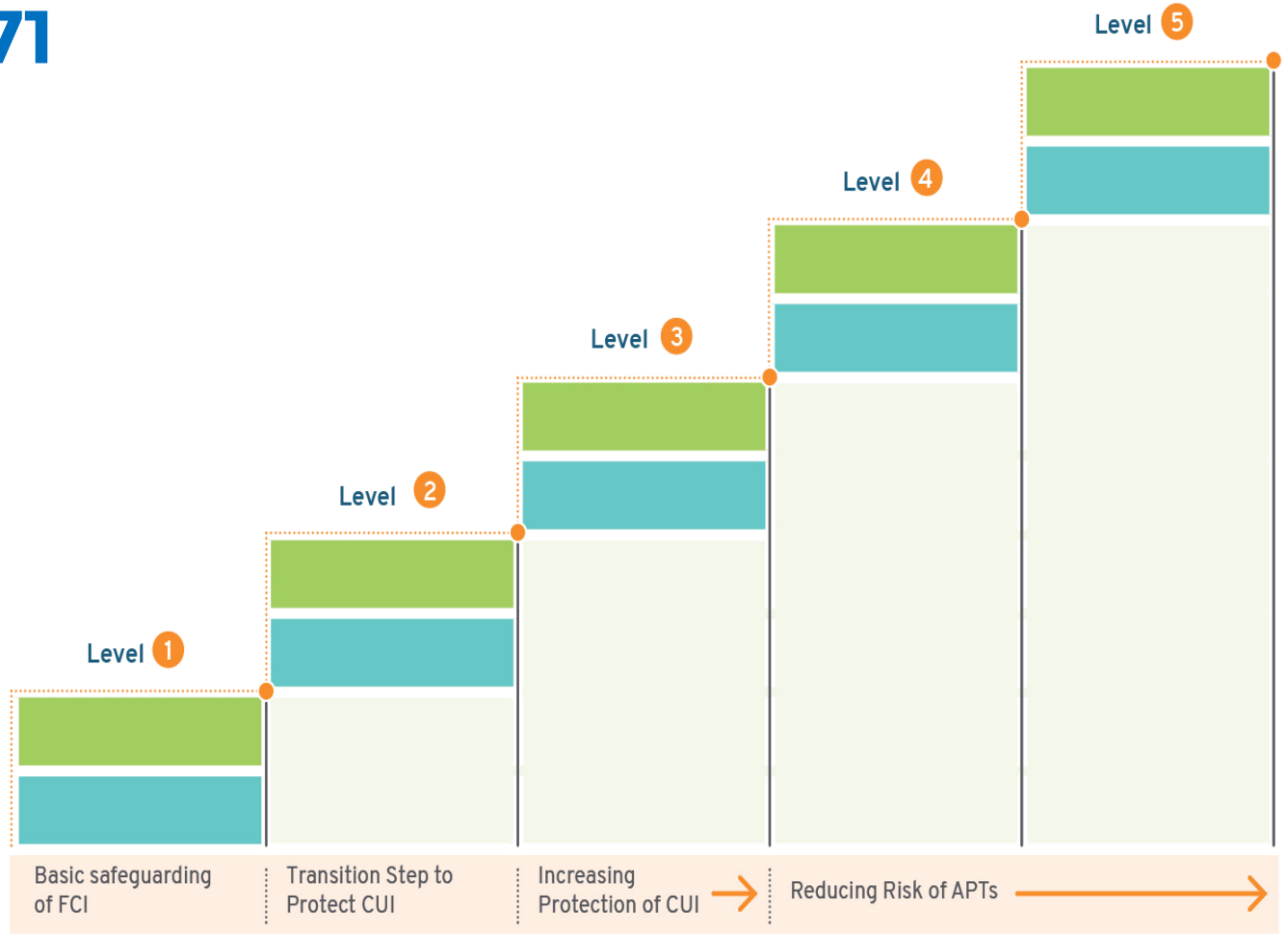
- DHG has an extensive Government Contracting Advisory practice comprised of former DCAA auditors with many years of DCAA audit experience, as well as other professionals with significant experience in government contracts.
- As a result, our industry focused professionals provide advice to our clients in all aspects of finance, accounting and compliance associated with government contracting. Our team delivers comprehensive regulatory compliance solutions to a broad range of contractors from the largest to the smallest.

Tom Tollerton,
CISSP, CPDSE, QSA, CMMC-RP / Managing Director

JAMIS®

General Differences between CMMC and NIST 800-171

- CMMC is a Maturity Model / NIST 800-171 is a Control Set
  - Five levels of maturity
- CMMC Introduces Three New Domains
  - Asset Management
  - Recovery
  - Situational Awareness
- NIST 800-171 Permit POAMS, and CMMC does not



[1]Source: *DoD CMMC framework*

Assessment Scoring

- Scoring dictated by the NIST SP 800-171 DoD Assessment Methodology, Version 1.3.1
- If all security requirements are met, a score of 110 is awarded
- Control scoring is weighted based on impact to the information system
- For each unimplemented control, a weight value of 1, 3, or 5 is subtracted from 110, can potentially lead to scores below 0

JAMIS®

Overview of Self-Assessment

- **3 Levels of Assessment:**

- **Basic** – A contractor self-assessment of implementation status of 110 security controls defined by NIST SP 800-171
  - Based on review of System Security Plan

- **Medium** – Conducted by DoD personnel trained in accordance with DoD Policy
  - Based on review of System Security Plan

- **High** – Conducted by DoD personnel trained in accordance with DoD Policy
  - Assessment will be conducted by reviewing appropriate evidence or demonstration of controls

JAMIS®

Key Considerations

- **Applicability:** Contractors handling CUI, as indicated by the inclusion of the DFARS 252.204-7012 clause within DoD Contracts, must complete a NIST 800-171 assessment to be eligible for contract awards after November 30, 2020.
    - Handling of Federal Contract Information does not automatically require a NIST 800-171 self-assessment to be completed
- **Scoping:** Distinct assessments should be performed for each System Security Plan.
    - Boundaries of the system, and relevant controls must be identified described in each security plan
    - All systems processing, storing, or transmitting CUI and supporting or connected systems should be included in assessment scope
    - If an "Enclave" approach is utilized, architectural or other controls should be identified in the security plan to evidence separation from other environments deemed to be out of scope
- **Assessment Recommendations:** The self-assessment should be performed by a qualified party, with assessment objectivity and independence in mind.

Plans of Action and Milestones (POAMs)

- Now is the time to use them!
- Develop POAMs honestly
- Assignment of Responsibility for completion
- Focus on documentation

JAMIS®

Remediation Planning & Approach

Jake Nix, CEO at RISCPoint & vCISO at JAMIS
Kris Martel, CISO at Neverfail Continuous Controls

NEVERFAIL
CONTINUOUS CONTROLS

- Headquartered in Austin, TX, Neverfail delivers Continuous IT Controls and Availability solutions to some of the most highly recognizable brands in the world.
- More than 5,000 customers in over 60 countries depend on Neverfail to reduce risk through zero trust compliance and continuity solutions without the worry, time, or cost of traditional methods.

Kris Martel
Chief Information Security Officer
C|CISO, CISSP, CISM, CGEIT, CRISC, CDPSE, C|EH, BTA-CBBF, BTA-CBSA

JAMIS®

CMMC Remediation

The plans you need to make, and the path to get there.

We'll focus the next section on discussing how you can prepare your organization for CMMC Certification, and how you can maintain your certification once you attain you desired maturity level, this will focus on:

- The role of readiness and gap assessments
- The methodologies you can leverage to provide structure to the process
- The most common difficulties organizations face
- Ways to reduce risk, and effort for your internal resources

JAMIS®

Knowing Your Current State

Organizations often have existing Security and Compliance programs. When existing tools, and controls exist It is important to get a sense for:

- How well your existing controls operate and if your documentation will meet CMMC standards
- Whether your existing tools can support CMMC requirements
- What gaps exist between your current program and the stringent standards for CMMC

JAMIS®

Focused Remediation

While CMMC can be a challenge due to the stringent and structured requirements, it naturally lends itself to remediation. By applying existing CMMC methodologies, you'll be able to plan, track, and validate your journey. Some Examples and common challenges include:

- The Plan of Action and Milestone (POAM) methodology can provide structure and a starting point
- POAM listings are a great starting point, and reporting mechanism, however, they are often inaccurate and do not provide granular enough reporting for some of the technical tasks to achieve compliance
- CMMC has specific requirements and obtaining certification is expected to be difficult, Organizations often do not consider the complex nature of the standard and can incorrectly validate remediation without the appropriate expertise on staff or through an advisor.

JAMIS®

Optimization and Risk Reduction

Organization's can help reduce risk and on-going effort through a variety of means. Partnering with a Registered Provider Organization. Additionally, with CMMC automation of control implementation and testing is on the rise, finding a skilled technology partner can help, the following should be considered to help reduce overall risk through partnerships

- Work with organizations certified in the CMMC Ecosystem
- Work with technology partners that enable you to do once but leverage or use many times
- POA&M automation. Manually creating and managing POA&Ms should be limited

JAMIS®

Questions & Answers

Thank You

Contact Info:

JAMIS Software Corporation
Phone: (703) 215-9969
Email: info@jamis.com
Website: www.jamis.com

Visit JAMIS CMMC Readiness Group Page:

https://jamis.com/cmmc-readiness-group/

Find us on social media: