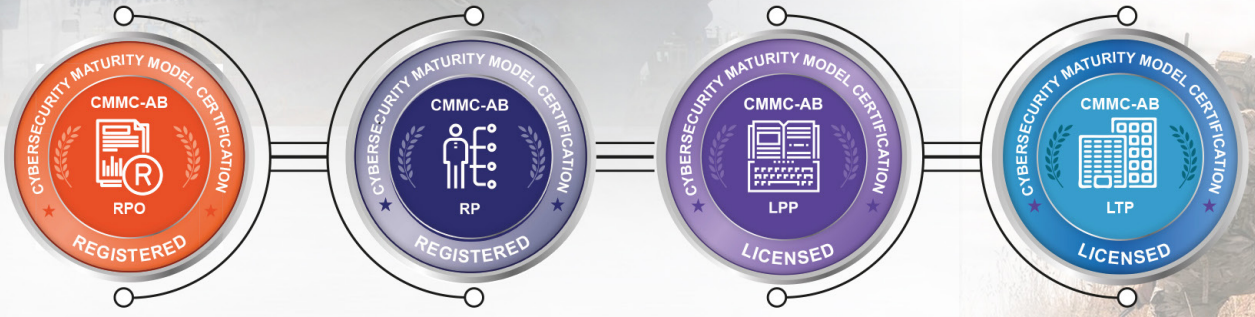
Perfecting the Art of *Active* Cyber Defense

CMMC Readiness Consulting Services

Cybersecurity Maturity Model Certification



ecfirst

Table of Contents

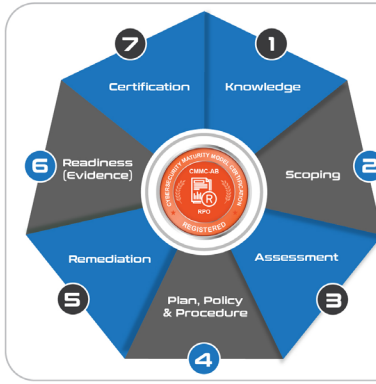
Organizations Seeking Certification OSC

Cybersecurity Maturity Model Certification (CMMC)

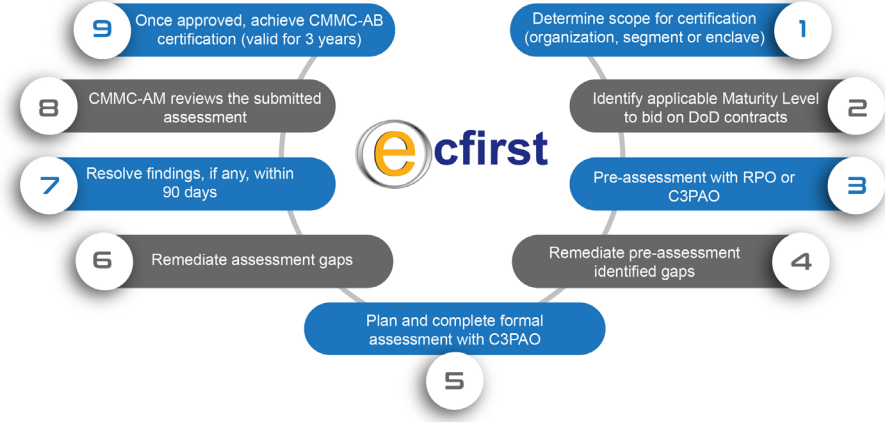
OSC

- OSCs are organizations with the intent to have the maturity of their cybersecurity program(s) certified under CMMC.
- Initially, CMMC-AB will focus on DoD contractors who need certification to respond to an active DoD solicitation.
- CMMC is currently expected to be required at contract award, not at proposal submission.
- Registered Provider Organizations (RPOs) and Certified 3rd Party Assessment Organizations (C3PAOs) assists OSC to create cybersecurity programs that will meet/exceed CMMC requirements and to prepare for an assessment.
- May grow to include other federal agencies in the near future.

Signature Methodology



CMMC-AB Certification | Key Steps



Getting Started with CMMC

On 31 January 2020, the U.S Department of Defense (DoD) introduced a new cybersecurity standard, the Cybersecurity Maturity Model Certification (CMMC)[1]. Every cybersecurity and compliance professional, including senior executives, must raise their awareness of this important and valuable cybersecurity standard developed by the DoD. The CMMC Model v1.02 was introduced on 18 March 2020[2].

So, why the CMMC? Malicious cyberactors continue to target the Defense Industrial Base (DIB) and the supply chain of the DoD. This challenge to U.S. national security, including economic security, is what raised the priority for the DoD to establish a credible and unified cybersecurity standard for organizations that provide services to it, i.e., the cyber supply chain.

Focus of the CMMC

The focus of the CMMC is on Controlled Unclassified Information (CUI). CUI is the information shared with DoD suppliers that requires safeguarding. CUI is, specifically, information the U.S. federal government creates or possesses, or that an entity creates or possesses for or on behalf of the government, that a law, regulation or government wide policy requires or permits an agency to handle only when using safeguarding or dissemination controls. A CUI registry provides information on the specific categories and subcategories of information that the U.S federal government's executive branch protects.

The CMMC is a cybersecurity certification standard. This standard is intended to serve as a verification mechanism to ensure that appropriate levels of cybersecurity practices and processes are in place and to protect CUI that resides on the networks of the DoD's industry partners.

How the CMMC Is Organized

The CMMC combines various cybersecurity standards and maps these best practices and processes to maturity levels, ranging from basic cyber hygiene to highly advanced practices. The CMMC defines 5 distinct levels, which include:[3]

- Level 1—Performed
- Level 2—Documented
- Level 3—Managed
- Level 4—Reviewed
- Level 5—Optimizing

These levels encompass the following:[4]

- 17 capability domains with 43 capabilities
- 5 processes to measure process maturity
- 171 practices to measure technical capabilities

The CMMC framework organizes processes and cybersecurity best practices into a set of domains. There are 17 capability domains that have been defined in the CMMC. Process maturity or process institutionalization characterizes the extent to which an activity is embedded in the operations of an organization. Practices are activities performed at each level for the domain. Each level consists of practices and processes as well as those specified in lower levels. In addition to assessing an organization's implementation of cybersecurity practices, the CMMC also assesses the organization's institutionalization of cybersecurity processes.

Cyber Defense Strategy

The CMMC is designed to provide the DoD assurance that a DIB contractor can adequately protect CUI at a level commensurate with the risk, accounting for flow down to subcontractors in a multitier supply chain. To reduce risk, the DIB sector must enhance its protection of CUI in its networks.

"The CMMC is designed to provide the DoD assurance that a DIB contractor can adequately protect CUI at a level commensurate with the risk, accounting for flow down to subcontractors in a multitier supply chain."

Every organization must establish its own cybersecurity strategy. The recommendation is that all organizations, not just those directly impacted by the mandate, take the first step and establish a deeper understanding of the CMMC standard. The levels defined within CMMC provide a framework that an organization can leverage to establish its cybersecurity strategy and priorities over a 12 to 24 month period. Cyber defense is all about kaizen[5], and the CMMC is an excellent reference that organizations can use to continuously improve their security posture.

Endnotes

[1] Blanchard, C.; R. Lee; et. al.; "DoD Releases Final Cybersecurity Maturity Model Certification Framework and Establishes Cybersecurity Audit and Accreditation Organization," Arnold & Porter, 13 February 2020.
[2] Office of the Under Secretary of Defense for Acquisition and Sustainment-Cybersecurity Maturity Model Certification, "CMMC Model," USA, 2020.
[3] PreVeil, "What Are the 5 Levels of CMMC?" USA, 2020.
[4] Ibid.
[5] Foster, B. "Security Kaizen: Adopting the Practice of Continuous Improvement to Improve Your Security Posture," Security Intelligence, January 5, 2015.

Understanding CMMC Maturity Level 1

The U.S. DoD cybersecurity standard, the CMMC, establishes 5 Maturity Levels.[1] The core objective of the certification is to ensure that vendors providing products and services to the DoD have an appropriate level of implemented cybersecurity capabilities; hence, the CMMC standard. The higher the CMMC Maturity Level, the greater the requirements are to secure the organization. The CMMC combines various cybersecurity standards and maps these best practices and processes to corresponding maturity levels, ranging from basic cyberhygiene to highly advanced practices.

The CMMC defines 5 distinct Maturity Levels, which include:[2]

- Level 1—Performed (Basic Cyber Hygiene)
- Level 2—Documented (Intermediate Cyber Hygiene)
- Level 3—Managed (Good Cyber Hygiene)
- Level 4—Reviewed (Proactive)
- Level 5—Optimizing (Advanced/Progressive)

Organizations need to examine the CMMC model and its applicability to secure the cybersecurity supply chain. Maturity Level 1 (ML1), which is the first step to establishing the foundation of resilience in the cybersecurity supply chain is examined here. Achieving ML1 certification establishes a credible foundation for the CMMC levels that follow.

> "Organizations need to examine the CMMC model and its applicability to secure the cybersecurity supply chain."

ML1 addresses the protection of U.S. Federal Contract Information (FCI). This level encompasses the basic safeguarding requirements for FCI, which are specified in the U.S. Federal Acquisition Regulation (FAR) Clause 52.204-21.[3] FCI is "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 websites) or simplified transactional information, such as necessary to process payments." DoD contracts that specify the need for a contractor to process, store or transmit FCI require the organization to comply with CMMC Maturity Level 1 practices. There is no process maturity assessed at Level 1.

Organization of the CMMC Framework

The CMMC framework organizes cybersecurity processes and best practices into a set of domains. There are 17 capability domains defined in the CMMC. Process maturity, or process institutionalization, characterizes the extent to which an activity is embedded in the operations of an organization. Practices are activities performed at each level for the domain. Each level consists of practices and processes as well as those specified in lower levels. In addition to assessing an organization's implementation of cybersecurity practices, the CMMC also assesses the organization's institutionalization of cybersecurity processes.

ML1 Domains, Practices and Capabilities

ML1 includes practice requirements associated with the following domains:

- Domain 1—Access Control (AC), 4 Practices
- Domain 6—Identification and Authentication (IA), 2 Practices
- Domain 9—Media Protection (MP), 1 Practice
- Domain 11—Physical Protection (PE), 4 Practices
- Domain 16—System and Communications Protection (SC), 2 Practices
- Domain 17—System and Information Integrity (SI), 4 Practices

ML1 requirements include 17 Practices across 6 Domains. This level establishes requirements for 16 capabilities and requires an organization to perform the practices specified within. Since the organization may only be able to perform these practices in an ad hoc manner and may or may not rely on documentation, process maturity is not assessed for ML1.

The CMMC maturity levels and associated sets of processes and practices across domains are cumulative. For an organization to achieve a specific CMMC level, it must also demonstrate achievement of the preceding lower levels. ML1 is the starting point defined in the CMMC model. Organizations that process FCI data and CUI are required to meet the criteria of higher Maturity Levels, such as Maturity Level 2 or Maturity Level 3. The highest Maturity Level that an organization can achieve is Maturity Level 5 (ML5). The objective of ML5 is to ensure that the organization is prepared to address Advanced Persistent Threats (APTs) using implemented capabilities.

A good starting point for any organization interested in the CMMC is ML1. Get started and perform a readiness assessment to address the requirements associated with ML1.

Endnotes

[1] Office of the Under Secretary of Defense for Acquisition and Sustainment-Cybersecurity Maturity Model Certification; CMMC Model, USA, 2020.
[2] PreVeil; "What Are the 5 Levels of CMMC?" USA, 2020.
[3] Carnegie Mellon University, Pittsburgh, Pennsylvania, USA, and The Johns Hopkins University Applied Physics Laboratory LLC, Baltimore, Maryland, USA, CMMC Version 1.02, 18 March 2020.

Maturity Level 1 Consulting Services

Cybersecurity Maturity Model Certification

ecfirst

CMMC-AB Registered Provider Organization™	CMMC-AB Registered Practitioner™	CMMC-AB Licensed Partner Publisher™	CMMC-AB Licensed Training Provider™
RPO – REGISTERED	RP – REGISTERED	LPP – LICENSED	LTP – LICENSED

CMMC Readiness Services!

- CMMC Readiness Assessment
- CMMC Policy Updates
- CMMC Procedure Draft
- CMMC Evidence Guidance
- CMMC Training Program
- CMMC Remediation

CMMC Signature Methodology!

CMMC ML1 Readiness

- Readiness Assessment
- Gap Remediation Guidance
- Policy Development
- System Security Plan (SSP) Development
- Procedure Guidance
- Evidence Guidance

Perfecting the Art of *Active* Cyber Defense

1000s of Clients | Clients in all 50 States | Clients on 5 Continents

CMMC Timeline

ecfirst

CMMC Facts

- 5 Maturity Levels
- 17 Domains
- 43 Capabilities
- 171 Practices
- 5 Processes

2021 – 2025	Defense Dept (DoD) Phased Rollout Requiring CMMC Certification
CMMC-AB CCP, CCA-1 and CCA-3 Exams Expected to be Available	**June 2021**
April 2021	CMMC-AB Expected to Approve LPP Courseware
CMMC v2.0 Expected Release Date	**March 2021**
February 2021	ecfirst Approved as a CMMC-AB Licensed Training Provider (LTP)
ecfirst Approved as Registered Provider Organization (RPO)	**November 2020**
October 2020	ecfirst Amongst the Early Approved Licensed Partner Publisher (LPP)
ecfirst Team Member Approved as Registered Practitioner (RP)	**September 2020**
March 2020	CMMC v1.02 Released
CMMC v1.0 Released	**January 2020**

Maturity Level 3: Securing DoD's CUI

Maturity Level 3 (ML3) establishes the minimal requirements for securing CUI in the U.S. DoD cybersecurity standard, CMMC. CMMC is designed to provide increased assurance to the DoD that a DIB contractor can adequately protect CUI at a level commensurate with the risk, accounting for information flow down to its subcontractors in a multi-tier supply chain. Level 3 is about managed processes and practices to demonstrate "Good Cyber Hygiene". The focus of this brief is on Maturity Level 3 and its associated requirements to appropriately secure CUI.

CMMC Model

The CMMC model measures cybersecurity maturity with five levels and aligns a set of processes and practices with the type and sensitivity of information to be protected and the associated range of threats.

The threat is significant. The aggregate loss of intellectual property and certain unclassified information from the DoD supply chain can undercut U.S. technical advantages and innovation as well as significantly increase risk to national security. The CMMC maturity levels serve as a way to measure an organization's process maturity.

> "Maturity Level 3 establishes the minimal requirements for securing CUI. Organizations must ensure capabilities, processes, and practices are aligned. While the focus of ML1 is on FCI, with ML3 it is on FCI and CUI. Higher maturity levels are designed to address APT."

Beyond FCI. CUI.

The CMMC Model encompasses the basic safeguarding requirements for FCI specified in FAR Clause 52.204-21 and the security requirements for CUI specified in NIST SP 800-171 per Defense Federal Acquisition Regulation Supplement (DFARS) Clause 252.204-7012. Level 3 of CMMC addresses the protection of FCI and CUI. FCI is information provided by or generated for the Government under contract not intended for public release. CUI is information that requires safeguarding or dissemination controls pursuant to and consistent with laws, regulations, and government-wide policies.

ML3 Processes and Practices

The term 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 that the outcomes will be consistent, repeatable and of high quality.

Level 3 requires that an organization establish, maintain, and resource a plan demonstrating the management of activities for practice implementation. The plan may include information on missions, goals, project plans, resourcing, required training, and involvement of relevant stakeholders. Level 3 focuses on the protection of CUI and encompasses all of the security requirements specified in NIST SP 800-171 as well as additional practices from other standards and references to mitigate threats.

Three maturity processes are required at ML3. The ML3 required processes are:

1. Establish policy (required at ML2 and higher maturity levels)
2. Document the CMMC practices to implement the policy (required at ML2 and higher maturity levels)
3. Establish, maintain, and resource a plan that includes requirements of domains (required at ML3 and higher maturity levels)

Process institutionalization provides additional assurances that the practices associated at each level are implemented effectively. The CMMC model, further, measures the implementation of practices. The CMMC practices provide a range of mitigation across the levels, starting with safeguarding at ML1, moving to a broad protection of CUI at ML3, and culminating with reducing the risk from APTs at ML4 and ML5. 130 practices are required to be implemented at ML3.

Conclusion

Organizations across industries can apply the same concepts to secure all confidential and sensitive information with the same requirements as we see in ML3. When implementing CMMC, an organization can achieve a specific CMMC level for its entire enterprise network or for particular segment(s) or enclave(s), depending upon where the information to be protected is handled and stored.

The CMMC maturity levels and the associated sets of processes and practices across domains are cumulative. For an organization to achieve a specific CMMC level it must also demonstrate achievement of the preceding lower levels. An organization must demonstrate both the requisite institutionalization of processes and the implementation of practices for a specific CMMC level and the preceding lower levels in order to achieve that level. Hence ML3 includes the requirements associated with ML1 and ML2. Maturity Level 3 is the starting point to secure all CUI. Get started and perform a readiness assessment to identify gaps with the ML3 requirements. ML3 is all about ensuring a credible, evidence-based cyber defense to secure CUI.

References

https://www.isaca.org/resources/news-and-trends/industry-news/2021/resilience-in-the-cybersecurity-supply-chain

https://www.isaca.org/resources/news-and-trends/industry-news/2020/getting-started-with-cmmc-a-us-dod-mandate-for-cybersecurity

Maturity Level 3 Consulting Services

Cybersecurity Maturity Model Certification

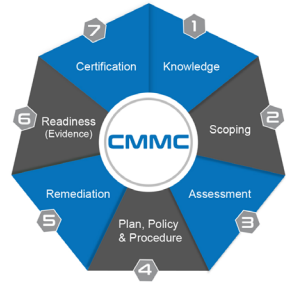
ecfirst

CMMC-AB Registered Provider Organization™	CMMC-AB Registered Practitioner™	CMMC-AB Licensed Partner Publisher™	CMMC-AB Licensed Training Provider™
RPO – REGISTERED	RP – REGISTERED	LPP – LICENSED	LTP – LICENSED

CMMC Readiness Services!

- CMMC Readiness Assessment
- CMMC Policy Updates
- CMMC Procedure Draft
- CMMC Evidence Guidance
- CMMC Training Program
- CMMC Remediation

CMMC Signature Methodology!



CMMC ML3 Readiness

- Readiness Assessment
- Gap Remediation Guidance
- Policy Development
- System Security Plan (SSP) Development
- Procedure Guidance
- Evidence Guidance

Perfecting the Art of *Active* Cyber Defense

1000s of Clients | Clients in all 50 States | Clients on 5 Continents

HITRUST CSF® Services

ecfirst | HITRUST® Authorized External Assessor

As a HITRUST Authorized External Assessor, ecfirst can assist your efforts for Readiness Assessment, Validated Assessment, HITRUST CSF Certification, Interim Assessment, and Re-certification. Talk to us about your journey to achieve HITRUST CSF Certification, and beyond. Jump-start your initiatives with ecfirst.

ecfirst a full suite of HITRUST services enabling your organization to achieve and manage certification, including:

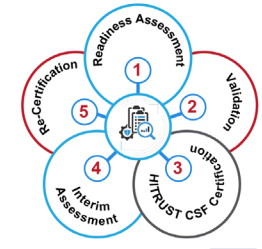
- Perform a comprehensive HITRUST pre-assessment to identify compliance and cyber gaps.
- Develop a customized HITRUST policy and procedure set to meet your requirements.
- Perform a guided HITRUST Readiness Assessment.
- Guidance on the development of implementation evidence.
- Conduct a HITRUST Validated Assessment towards Certification.
- Complete a HITRUST Interim Assessment.

Your Trusted Partner | ecfirst

- ecfirst Customized Policies
- ecfirst Customized Procedures
- ecfirst Evidence Readiness
- ecfirst Readiness Assessment
- ecfirst Validated Assessment
- ecfirst HITRUST CSF Certification
- ecfirst Interim Assessment
- ecfirst Re-Certification

Signature Methodology

Achieving Certification



Virtual! HITRUST Cybersecurity Workshop

CEU 4 Hours

- Examine the fundamentals of the HITRUST CSF.
- Leveraging the HITRUST CSF to implement the NIST Cybersecurity Framework.
- Addressing regulatory mandates such as GDPR, CCPA, HIPAA, and FISMA.
- Getting organized: From Readiness Assessment, thru Validation to Certification.
- Roadmap to HITRUST and NIST certification.

Complimentary! HITRUST Exec Brief

Achieving Certification

Ask about our free 29-minute exec brief to walk-thru the roadmap for achieving HITRUST CSF Certification. Understand key steps for readiness assessment.

Perfecting the Art of *Active* Cyber Defense

1000s of Clients | Clients in all 50 States | Clients on 5 Continents

ecfirst

Consulting Practice

HIPAA & HITECH | TRACER | CMMC-AB RPO | CMMC-AB RP | CMMC NIST Practice | HIPAA Academy | CCPA & GDPR | HITRUST Authorized External Assessor | Managed Compliance | Virtual ISO & InfoSec Staffing | On-Demand Consulting | Med Device Cybersecurity | NIST Cybersecurity Framework

Certification Training

CHP Certified HIPAA Professional | CSCS Certified Security Compliance Specialist | CCSA Certified Cyber Security Architect | CMMC-AB LPP | CCPA | HIMSS Approved Education Partner | CMMC NIST ecfirst Academy | CMMC-AB LTP

Perfecting the Art of *Active* Cyber Defense

1000s of Clients | Clients in all 50 States | Clients on 5 Continents

Ali Pabrai

Global Cybersecurity & Compliance Expert

MSEE | CISSP (ISSAP | ISSMP) | CMMC RP | HITRUST® (CCSFP) | Security+

Mr. Ali Pabrai, a global cybersecurity & compliance expert, is the chairman & chief executive of ecfirst. A highly sought after professional, he has successfully delivered solutions to U.S. government agencies, IT firms, healthcare systems, legal & other organizations worldwide. His career was launched with the U.S. Department of Energy's nuclear research facility, Fermi National Accelerator Laboratory. He has served as vice chairman and in several senior officer positions with NASDAQ-based firms.

Mr. Pabrai has led numerous engagements worldwide for ISO 27001, PCI DSS, NIST, CMMC, GDPR, CCPA, FERPA, HITRUST CSF and HIPAA/HITECH. Mr. Pabrai served as an Interim CISO for a health system with 40+ locations in USA.

Mr. Pabrai has presented passionate briefs to tens of thousands globally, including the USA, United Kingdom, France, Taiwan, Singapore, Canada, India, UAE, Saudi Arabia, Philippines, Japan, Ireland, Bahrain, Jordan, Egypt, Ghana and other countries.

He is a globally renowned speaker who has been featured as a keynote as well as moderated cybersecurity conferences. Mr. Pabrai is the author of several published works. Clients that Mr. Pabrai has delivered to have included the Defense Intelligence Agency (DIA), and the Naval Surface Warfare Center.

Mr. Pabrai was appointed and served (2017) as a member of the select HITRUST CSF Assessor Council. Mr. Pabrai is a proud member of the InfraGard (FBI).

Ali Pabrai | Ali.Pabrai@ecfirst.com | +1.949.528.5224

CMMC-AB RP REGISTERED | ISACA TOP-RATED SPEAKER ★★★★★

> "We have had the true pleasure of working with Ali Pabrai at conferences all over the world during the past few years – with one unanimous word that keeps resounding among audiences and staff alike – *AWESOME!*"
> Michael Mach | *Conference Program Manager* | *ISACA*

ISACA Trust in, and value from, information systems

FBI Conference

INFRAGARD PARTNERSHIP FOR PROTECTION

> "Pabrai's presentation style is engaging, and he encourages questions and discussions. I would recommend him for future presentations and trainings."
> Josh More | *Cyber Sector Chief* | *Iowa FBI InfraGard*

> "On behalf of the Idaho InfraGard (FBI), I would like to thank Pabrai for presenting at our conference. Pabrai is the kind of speaker you want to bring to executives and staff. He says it in a simple, no nonsense way, in a manner that everyone can understand."
> Rachel Zahn | *President* | *InfraGard (FBI)* | *Idaho Alliance*

> "You delivered a fantastic presentation and we all felt your passion for cyber security."
> James E Lamadrid | *Supervisory Special Agent* | *Federal Bureau of Investigation (FBI)* | *Cyber Task Force*

> "Thank you Pabrai. Your enthusiasm and relevance for the Information Security material you presented at our combined Infragard (FBI) conference in Idaho Falls was very well received and pertinent to both our chapter as an organization and the constituents in attendance."

> "As a government employee, I appreciated the simplified insight of highlighting the importance of compliance and funding compared to information security success beyond qualitative metrics. I heard many times over that your specific information with measurable results made your material directly relevant to individuals, businesses and organizations. Thanks again and I hope you are able to join us again in the future."
> Clark Harshbarger | *FBI*

Published Author

Getting Started with HIPAA — First published book on HIPAA!

UNIX Internetworking — First book on UNIX & Networks!

Internet & TCP/IP Network Security — First book on TCP/IP security!

U.S. Department of Defense

ecfirst | CMMC-AB LTP LICENSED | CMMC-AB LPP LICENSED | CMMC-AB RPO REGISTERED | HITRUST® Authorized External Assessor