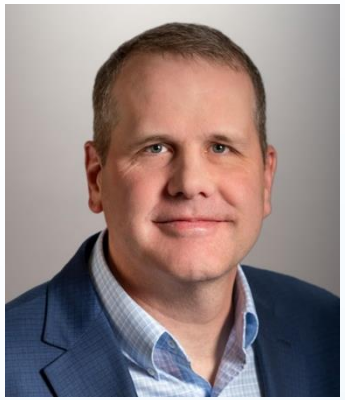
McKONLY & ASBURY

What's New in CMMC & The Top 10 Not-Met Controls

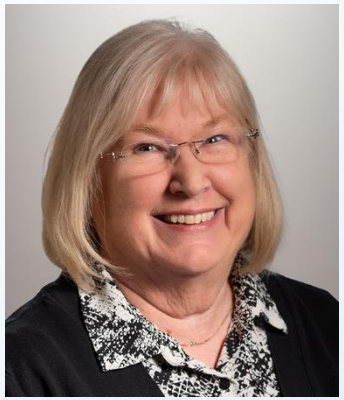
macpas.com

Introductions



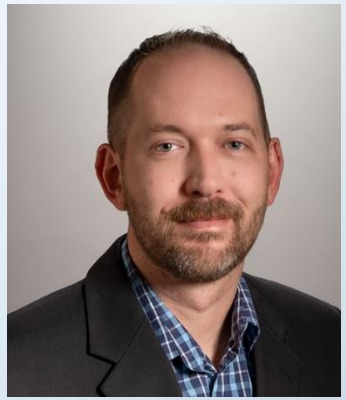
Dave Hammarberg, Partner
CISSP, CISA, CCA

Leads the SOC, Cybersecurity, Forensic Examination, Information Technology, CMMC, and Internal Audit practices. He has been an integral part of the Firm for over 20 years, serving clients in a variety of information technology and accounting capacities and leading the firms Information Technology Department.



Elaine Nissley, Director
CISA, CCA

Leads the Internal Audit (IA) and CMMC practices. She has been an integral part of the Firm for 20 years, serving clients providing a variety of IA risk assessment services including assessments and consulting on of NIST 800-53 based Information Security frameworks. She has an extensive information technology (IT) and IT Audit experience.



Michael Murray, Supervisor
CCA

Member of the Internal Audit Services group providing internal and external IT focused services for clients in the manufacturing, construction, and retail segments. Mike is one of the founding members of our CMMC C3PAO assessment team, implementing CMMC practices within the firm in preparation for our DIBCAC Level 2 assessment.

Firm Overview

Helping You Thrive!

McKonly & Asbury

M&A is a team of CPAs and Business Advisors serving clients from our offices in Camp Hill, Lancaster, Bloomsburg, and Philadelphia.

accountingTODAY 2024 Best Firms to Work For

accountingTODAY 2024 Best Firms for Young Accountants

accountingTODAY 2024 Best Firms for Women

BEST PLACES to work in PA 2024

Services Provided

- SOC, HITRUST, CMMC & Technology Consulting
- Advisory & Business Consulting
- Audit & Assurance
- Tax
- Entrepreneurial Support & Outsourced Accounting

Industries Served

- Affordable Housing
- Architecture, Engineering, and Construction (AEC)
- Entrepreneurial
- Family-owned Business
- Franchises
- Healthcare
- Manufacturing & Distribution
- Nonprofit
- Public Companies

Agenda

- **The 10 Most Failed Security Requirements**
  - SC.L2-3.13.11: FIPS-Validated Cryptography.
  - IA.L2-3.5.3: Multifactor Authentication.
  - SI.L2-3.14.1: Identify, report, correct system flaws.
  - RA.L2-3.11.1: Periodically assess risk.
  - RA.L2-3.11.2: Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.
  - AU.L2-3.3.3: Review and update logged events.
  - AU.L2-3.3.4: Audit logging process failure alerts.
  - AU.L2-3.3.5: Audit record review, analysis, and reporting.
  - IR.L2-3.6.3: Test incident response capability .
  - CM.L2-3.4.1: Establish/maintain baseline configuration.
- **Q & A**

10 Most-Failed Security Requirements

- The Defense Contracts Management Agency (DCMA) published a list of the 10 most failed security requirements based on DIBCAC assessments.

- Understand what the requirements are asking of you.
  - NIST 800-171 is not prescriptive
  - NIST 800-171A does not provide examples that will fit every enterprise

10 Most-Failed Security Requirements

1. **SC.L2-3.13.11: FIPS-Validated Cryptography (3 or 5)**
   Ensures encryption methods are compliant with FIPS standards.

   [a] Determine if FIPS-validated cryptography is employed to protect the confidentiality of CUI.

10 Most-Failed Security Requirements

1. SC.L2-3.13.11: FIPS-Validated Cryptography (3 or 5)

Ensures encryption methods are compliant with FIPS standards.

Good to know:

- *This control will be scored 3 if non-FIPS validated encryption is used.*

- FIPS validated algorithms and FIPS validated modules are not the same.

- NIST performs validation of FIPS modules
  - *https://csrc.nist.gov/Projects/cryptographic-module-validation-program/validated-modules/*

10 Most-Failed Security Requirements

2. IA.L2-3.5.3: Multifactor Authentication (3 or 5)

Requires additional verification steps beyond a password

[a] Privileged accounts are identified.

[b] Multifactor authentication is implemented for local access to privileged accounts.

[c] Multifactor authentication is implemented for network access to privileged accounts.

[d] Multifactor authentication is implemented for network access to non-privileged accounts.

10 Most-Failed Security Requirements

3. SI.L2-3.14.1: Identify, report, correct system flaws (5)

Regularly discovering and fixing vulnerabilities.

[a] The time within which to identify system flaws is specified.
[b] System flaws are identified within the specified time frame.
[c] The time within which to report system flaws is specified.
[d] System flaws are reported within the specified time frame.
[e] The time within which to correct system flaws is specified.
[f] System flaws are corrected within the specified time frame.

10 Most-Failed Security Requirements

4. RA.L2-3.11.1: Periodically assess risk (3)

Continuous risk assessment is vital

[a] The frequency to assess risk to organizational operations, organizational assets, and individuals is defined.

[b] Risk to organizational operations, organizational assets, and individuals resulting from the operation of an organizational system that processes, stores, or transmits CUI is assessed with the defined frequency.

10 Most-Failed Security Requirements

5. **RA.L2-3.11.2: Scan for vulnerabilities in organizational systems and applications periodically *and* when new vulnerabilities affecting those systems and applications are identified. (5)**
   Frequent vulnerability scanning to spot weaknesses

   [a] The time within which to identify system flaws is specified.

   [b] System flaws are identified within the specified time frame.

   [c] The time within which to report system flaws is specified.

   [d] System flaws are reported within the specified time frame.

   [e] The time within which to correct system flaws is specified.

10 Most-Failed Security Requirements

6. AU.L2-3.3.3: Review and update logged events (1)

Keep security logs up to date

[a] A process for determining when to review logged events is defined.

[b] Event types being logged are reviewed in accordance with the defined review process.

[c] Event types being logged are updated based on the review.

10 Most-Failed Security Requirements

7. AU.L2-3.3.4: Audit logging process failure alerts (1)

Timely detection and alerting for logging failures

[a] Personnel or roles to be alerted in the event of an audit logging process failure are identified.

[b] Types of audit logging process failures for which alert will be generated are defined.

[c] Identified personnel or roles are alerted in the event of an audit logging process failure.

10 Most-Failed Security Requirements

8. AU.L2-3.3.5: Audit record review, analysis, and reporting (5)

Regularly review and analyze audit logs

[a] Audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity are defined.

[b] Defined audit record review, analysis, and reporting processes are correlated.

10 Most-Failed Security Requirements

9. IR.L2-3.6.3: Test incident response capability (1)

Ensure incident response plans are practical and effective

[a] Determine if the incident response capability is tested.

10 Most-Failed Security Requirements

10. CM.L2-3.4.1: Establish/maintain baseline configuration (5)

Document and enforce standard configurations

[a] A baseline configuration is established.

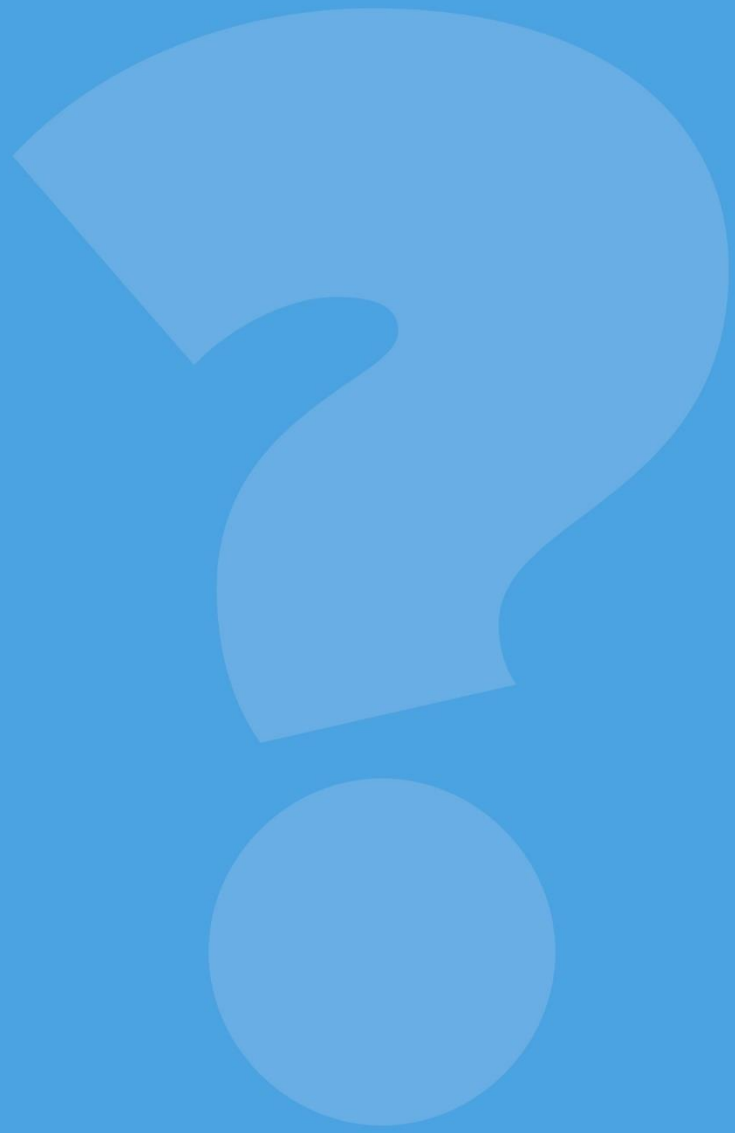
[b] The baseline configuration includes hardware, software, firmware, and documentation.

[c] The baseline configuration is maintained (reviewed and updated) throughout the system development life cycle.

[d] The system inventory includes hardware, software, firmware, and documentation.

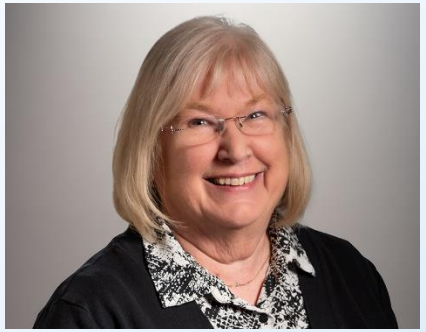
[e] The inventory is maintained (reviewed and updated) throughout the system development life cycle.

Questions?

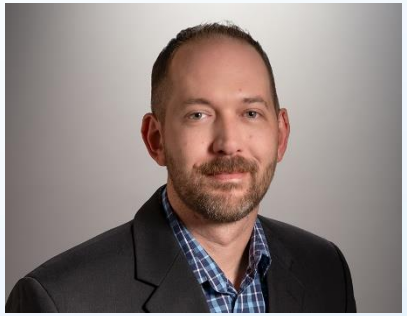


Contact Information

Dave Hammarberg, CISSP, CISA, CCA
Partner
dhammarberg@macpas.com
717-972-5723



Elaine Nissley, CCA
Director
enissley@macpas.com
717-972-5728

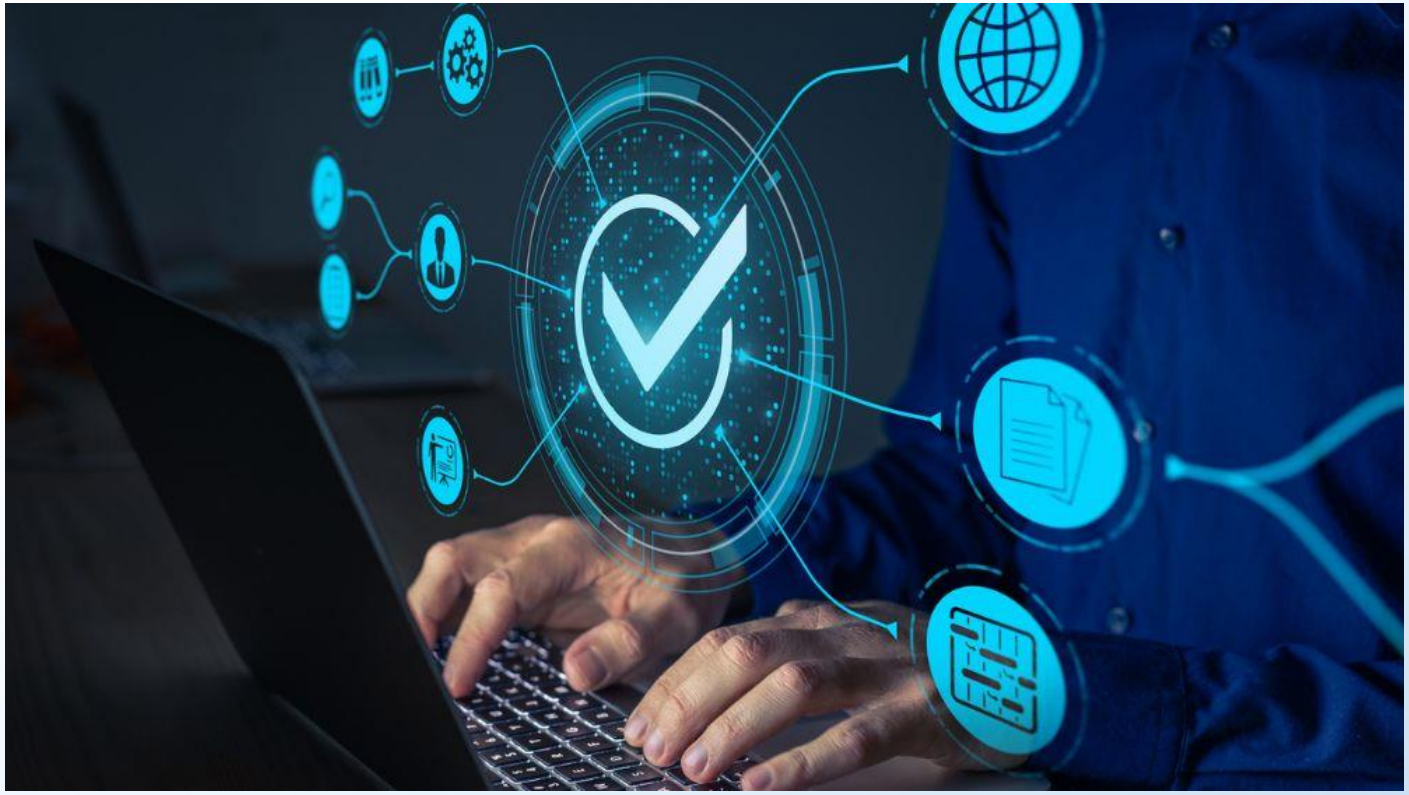


Mike Murray, CCA
Supervisor
mmurray@macpas.com
570-317-9524

McKONLY & ASBURY

Upcoming Events

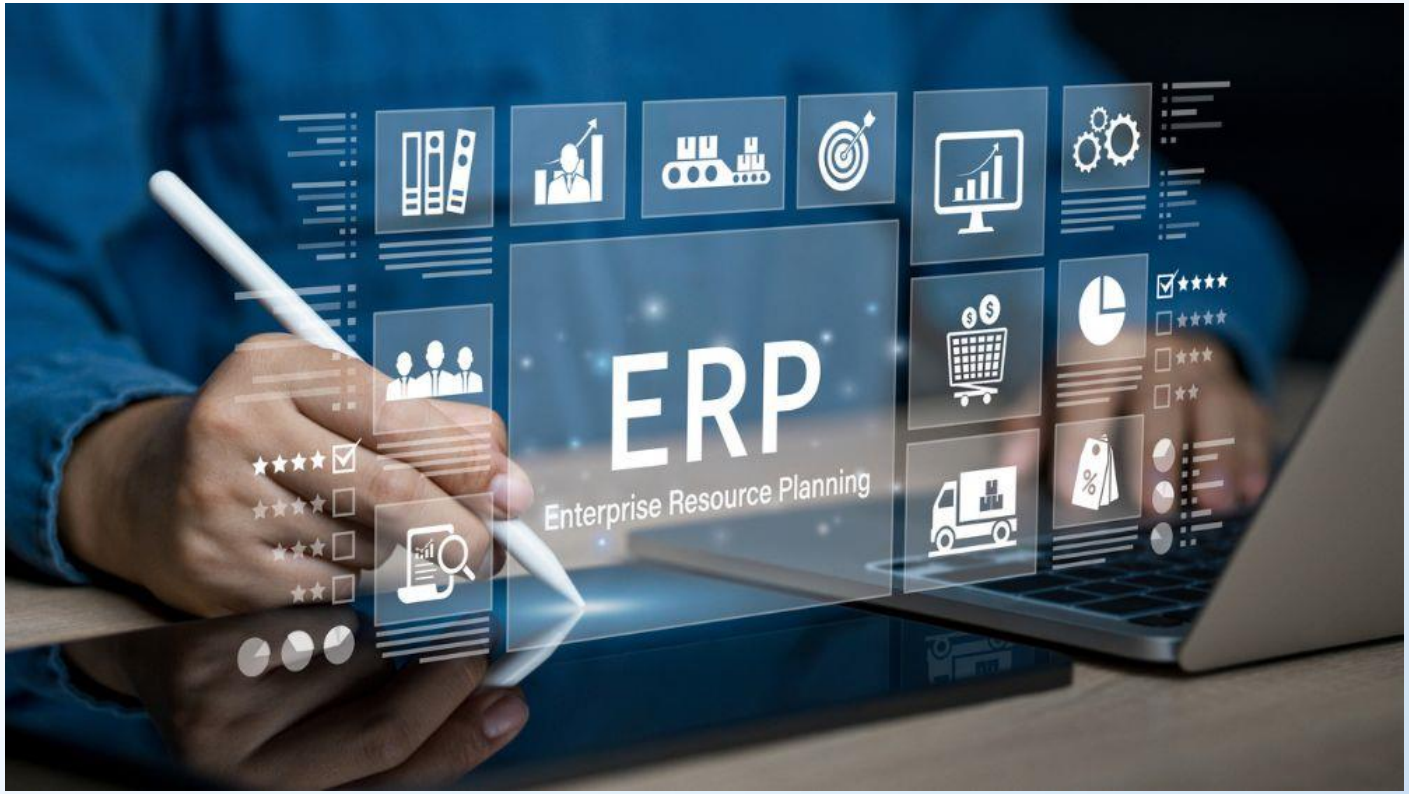
May 8 Webinar



The Essentials of SOC 1 – All You Need to Know

REGISTER NOW

May 29 Webinar



Your Business Evolved, But Has Your ERP?

REGISTER NOW