Wisconsin Procurement Institute

An APEX Accelerator

Cyber Friday:

Building a CMMC Program: 3.1.3 Audit and Accountability Policy, Log Review Procedure

July 19 | 11:00 am - Noon

Presented by:

Matt Frost, Wisconsin Procurement Institute

NCMA NATIONAL CONTRACT MANAGEMENT ASSOCIATION WISCONSIN

Webinar Etiquette

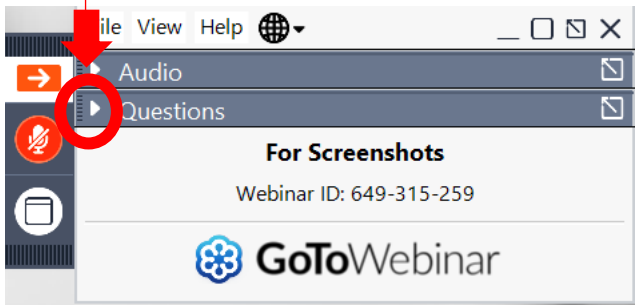
PLEASE

- Log into the GoToWebinar session with the name that you registered with online
- Place your phone or computer on MUTE
- Use the QUESTIONS option to ask your question(s).
  - We will share the questions with our guest speaker who will respond to the group

THANK YOU!

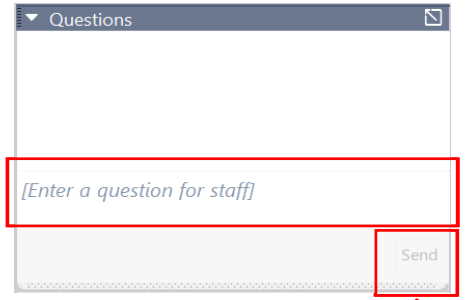
OPENING THE QUESTIONS BOX

Click here to access within the Control Panel



USING THE QUESTIONS BOX

Type questions here at any time during a presentation



Click Send when ready to submit a question

Wisconsin Procurement Institute

An APEX Accelerator

Assisting Wisconsin businesses compete in the government marketplace.

WPI is Wisconsin's APEX ACCELERATOR

The APEX Accelerators program, under management of the Department of Defense (DOD) Office of Small Business Programs (OSBP), plays a critical role in the Department's efforts to identify and engage with a wide range of businesses entering and participating in the defense supply-chain. The program provides the education and training that all businesses need to participate to become capable of participating in DOD and other government contracts.

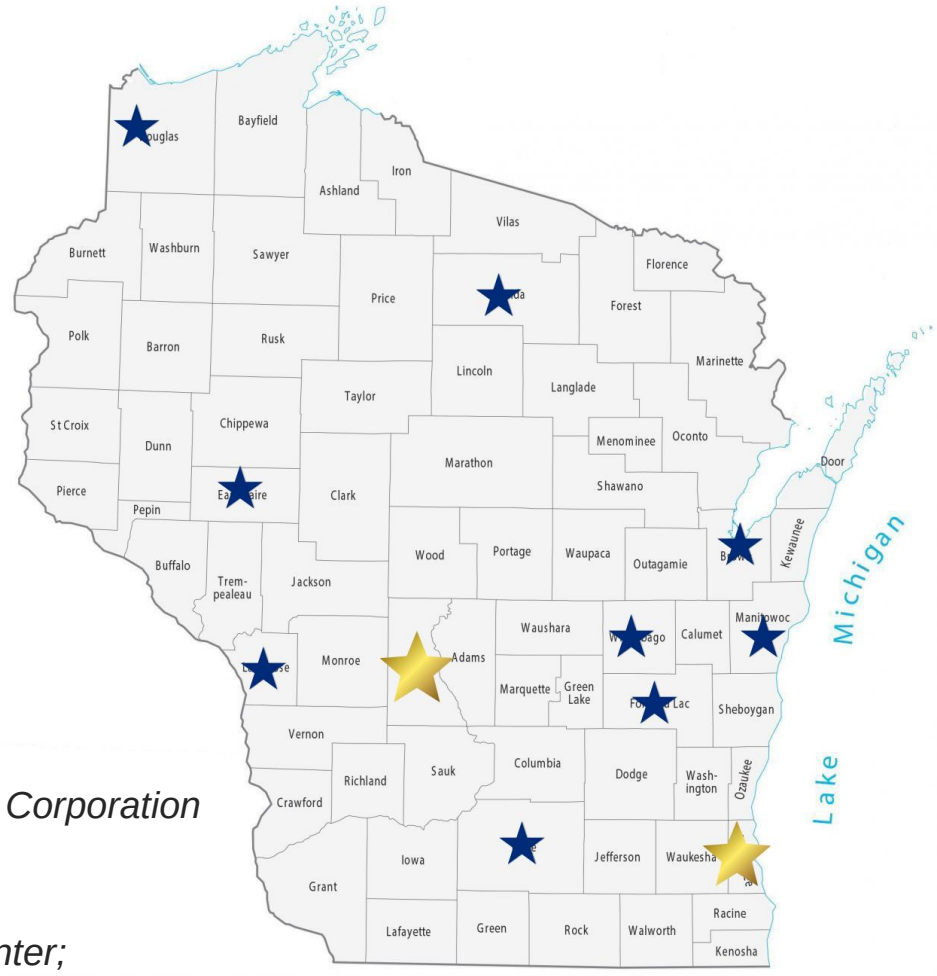
WPI provides services to all of Wisconsin's 72 counties

- Individual counseling at our offices, client's facility or virtually
- Small group training – webinars and workshops
- Conferences including one on one buyer meetings – Marketplace, The Contracting Academy, Small Business Academy, Wisconsin Federal Contractor Forum, Acquisition Hour, Cyber Fridays, DOD Roadmap series, Government Opportunities Business Conference, End of Year Federal Contractor Update, Annual DOD Contract Management Update, Evening FAR sessions and more……

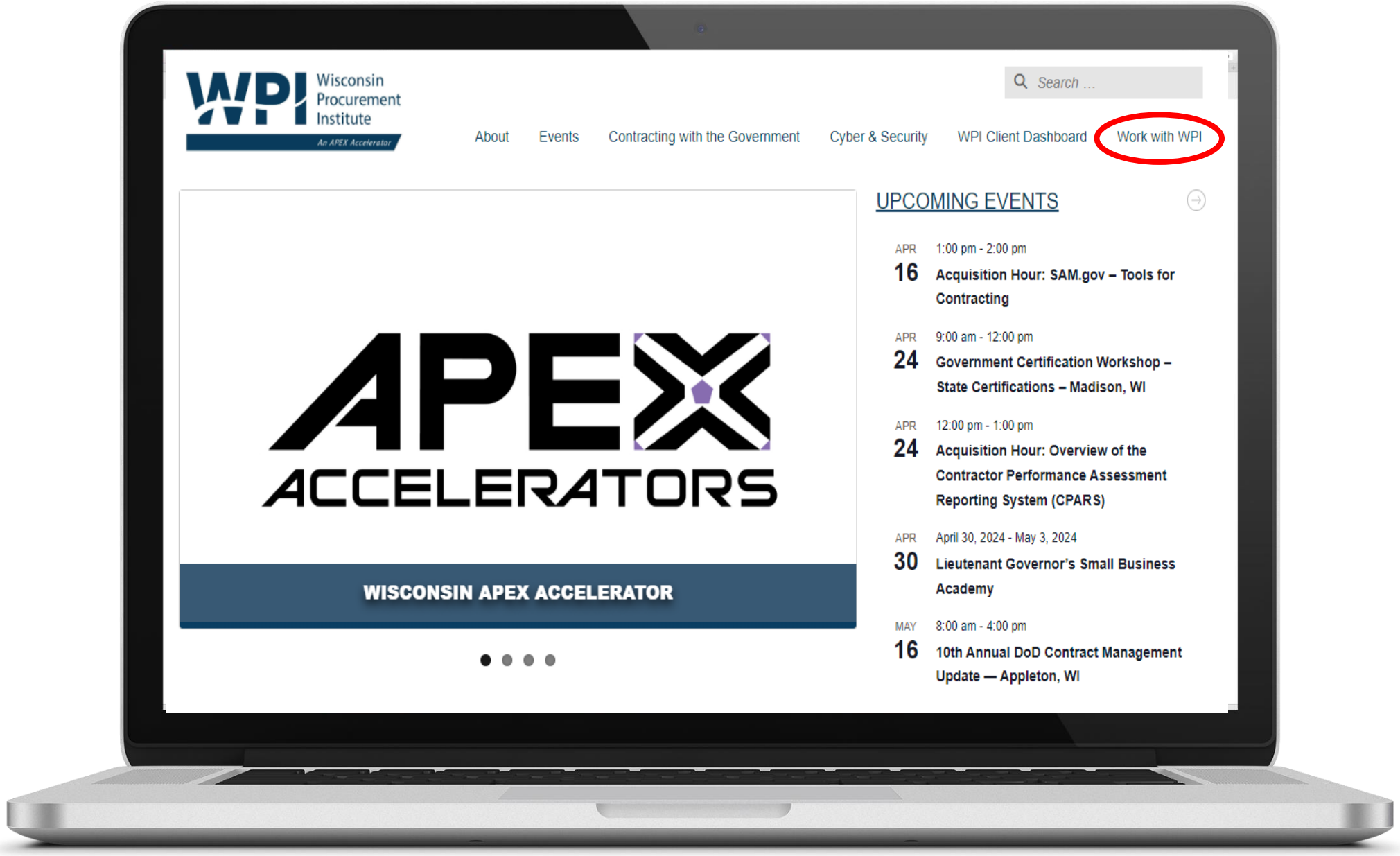
www.wispro.org

WPI OFFICE LOCATIONS

- **MILWAUKEE**
  - *Technology Innovation Center*
- **MADISON**
  - *FEED Kitchens*
  - *Dane County Latino Chamber of Commerce*
  - *Wisconsin Manufacturing Extension Partnership (WMEP)*
  - *Madison Area Technical College (MATC)*
- **CAMP DOUGLAS**
  - *Juneau County Economic Development Corporation (JCEDC)*
- **EAU CLAIRE**
  - *Western Dairyland*
- **FOND DU LAC**
  - *Envision Greater Fond du Lac*
- **GREEN BAY**
  - *NWTC Startup Hub*
- **LACROSSE**
  - *Veterans in Professions*
- **MANITOWOC**
  - *Progress Lakeshore*
- **OSHKOSH**
  - *Greater Oshkosh Economic Development Corporation*
- **SUPERIOR**
  - *Small Business Dev Center; UW Superior*



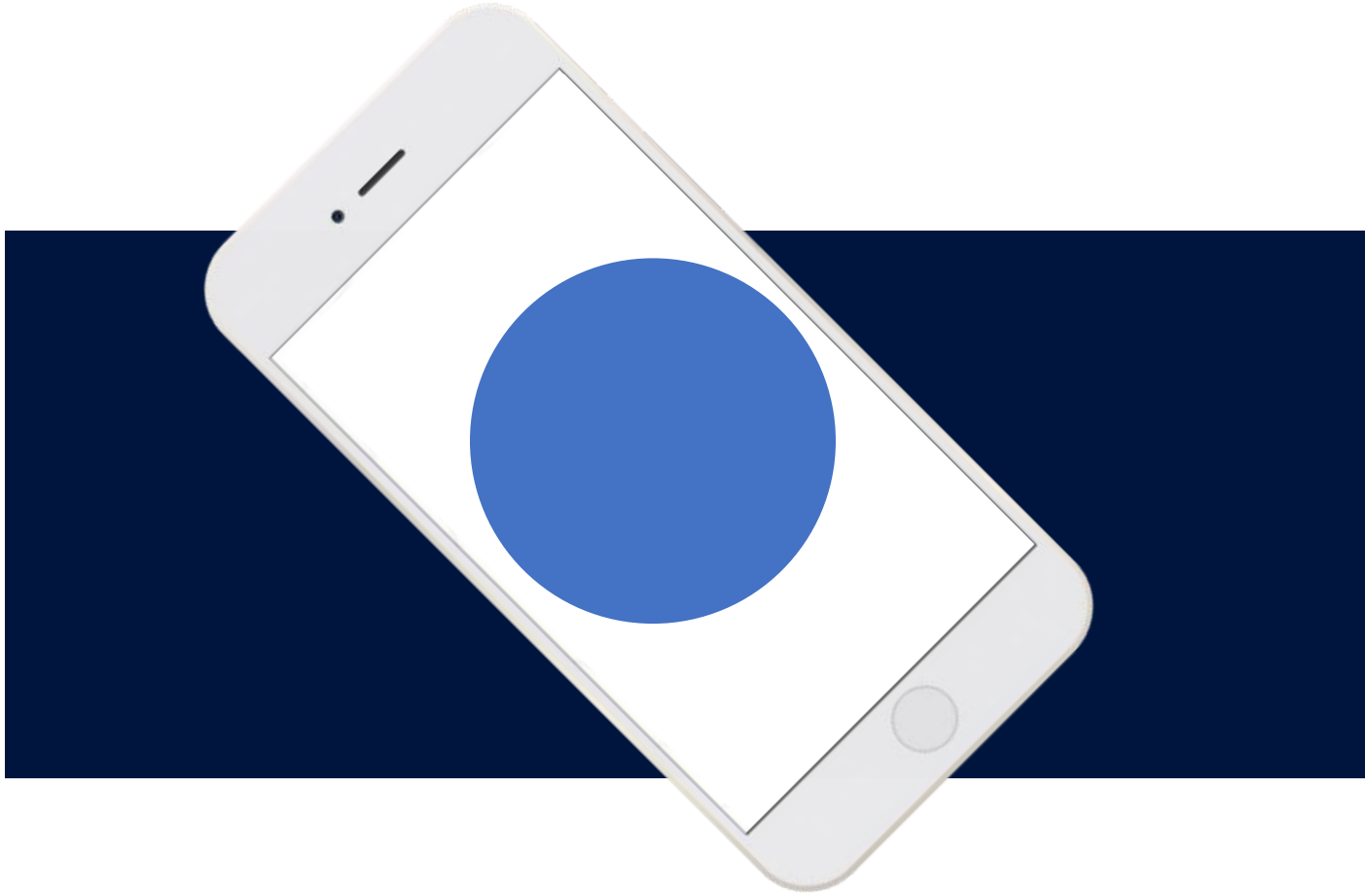
Wisconsin Procurement Institute
An APEX Accelerator


WPI Wisconsin Procurement Institute
An APEX Accelerator
Search ...
About
Events
Contracting with the Government
Cyber & Security
WPI Client Dashboard
Work with WPI
APEX ACCELERATORS
WISCONSIN APEX ACCELERATOR
UPCOMING EVENTS
APR 16 1:00 pm - 2:00 pm
Acquisition Hour: SAM.gov – Tools for Contracting
APR 24 9:00 am - 12:00 pm
Government Certification Workshop – State Certifications – Madison, WI
APR 24 12:00 pm - 1:00 pm
Acquisition Hour: Overview of the Contractor Performance Assessment Reporting System (CPARS)
APR 30 April 30, 2024 - May 3, 2024
Lieutenant Governor's Small Business Academy
MAY 16 8:00 am - 4:00 pm
10th Annual DoD Contract Management Update — Appleton, WI

Documentation for NIST SP 800-171r2 Controls

Wisconsin Procurement Institute

AN APEX ACCELERATOR



CYBER FRIDAY SESSIONS – July 19th, 2024

DFARS 252.204-7012

NIST
National Institute of Standards and Technology

The Contractor shall implement NIST SP 800-171, as soon as practical, but not later than December 31, 2017.

The Contractor shall notify the prime Contractor (or next higher-tier subcontractor) when submitting a request to vary from a NIST SP 800-171 security requirement.

When the Contractor discovers a cyber incident that affects a covered contractor information system or the covered defense information residing therein, or that affects the contractor's ability to perform the requirements of the contract… the Contractor shall rapidly report cyber incidents to DoD.

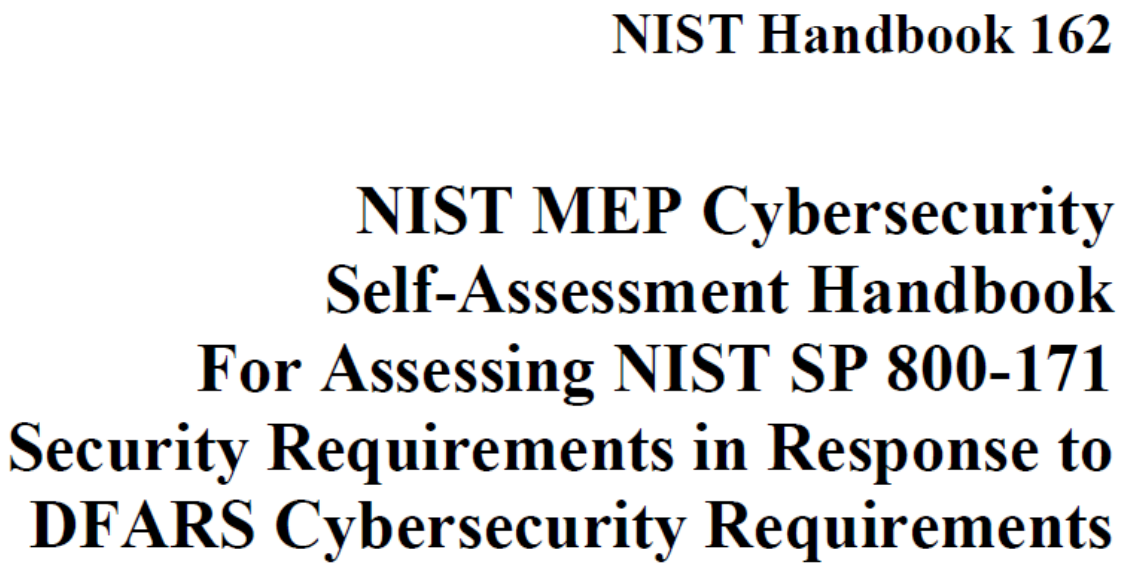
DFARS 252.204-7021

The Cybersecurity Maturity Model Certification (CMMC) is a framework that measures a contractor's cybersecurity maturity to include the implementation of cybersecurity practices…

(b) Requirements. The Contractor shall have a current (i.e. not older than 3 years) CMMC certificate at the CMMC level required by this contract and maintain the CMMC certificate at the required level for the duration of the contract.

14 Families – 110 Controls – 320 Audit Objectives

- Access Control
- Awareness and Training
- **Audit and Accountability**
- Configuration Management
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Personnel Security
- Physical Protection
- Risk Assessment
- Security Assessment
- System and Communications Protection
- System and Information Integrity



1 NIST Handbook 162

NIST MEP Cybersecurity Self-Assessment Handbook for Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements

2 NIST SP 800-171A

NIST Special Publication 800-171A
Assessing Security Requirements for Controlled Unclassified Information

3 NIST SP 800-18r1

NIST Special Publication 800-18
Revision 1
Guide for Developing Security Plans for Federal Information Systems

Reading the Controls

1 — Audit and Accountability Policy

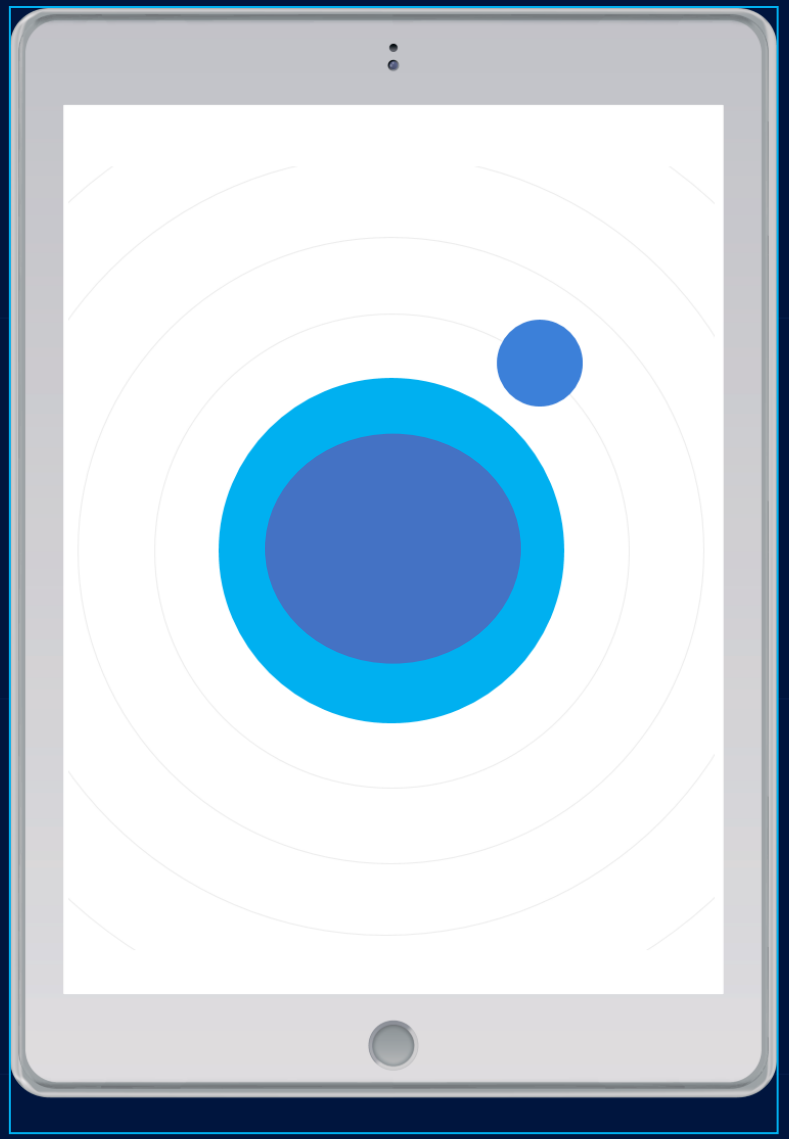
2 — Audit Records

3 — Review and Analysis

3.3.1	**SECURITY REQUIREMENT** Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.3.1[a]	*audit logs needed (i.e., event types to be logged) to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity are specified.*
	3.3.1[b]	*the content of audit records needed to support monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity is defined.*
	3.3.1[c]	*audit records are created (generated).*
	3.3.1[d]	*audit records, once created, contain the defined content.*
	3.3.1[e]	*retention requirements for audit records are defined.*
	3.3.1[f]	*audit records are retained as defined.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* Audit and accountability policy; procedures addressing auditable events; system security plan; system design documentation; system configuration settings and associated documentation; procedures addressing control of audit records; procedures addressing audit record generation; system audit logs and records; system auditable events; system incident reports; other relevant documents or records]. Interview: [*SELECT FROM:* Personnel with audit and accountability responsibilities; personnel with information security responsibilities; personnel with audit review, analysis and reporting responsibilities; system or network administrators]. Test: [*SELECT FROM:* Mechanisms implementing system audit logging].	

Elements of the Policy

1. Purpose
2. Scope
3. Policy Statement
4. Roles and Responsibilities
   - 4.1 System Administrators
   - 4.2 Security Officers
   - 4.3 Compliance Officers
5. Policy Provisions
   - 5.1 Audited Events
     - Logon/Logoff Activities
     - File Access and Modifications
     - Changes to System Configurations
     - Privileged Operations
     - Boundary Events
   - 5.2 Contents of Audit Records
     - Date and Time of Event
     - User Identification
     - Type of Event and Source
     - Success/Failure of Event
   - 5.3 Audit Storage Capacity

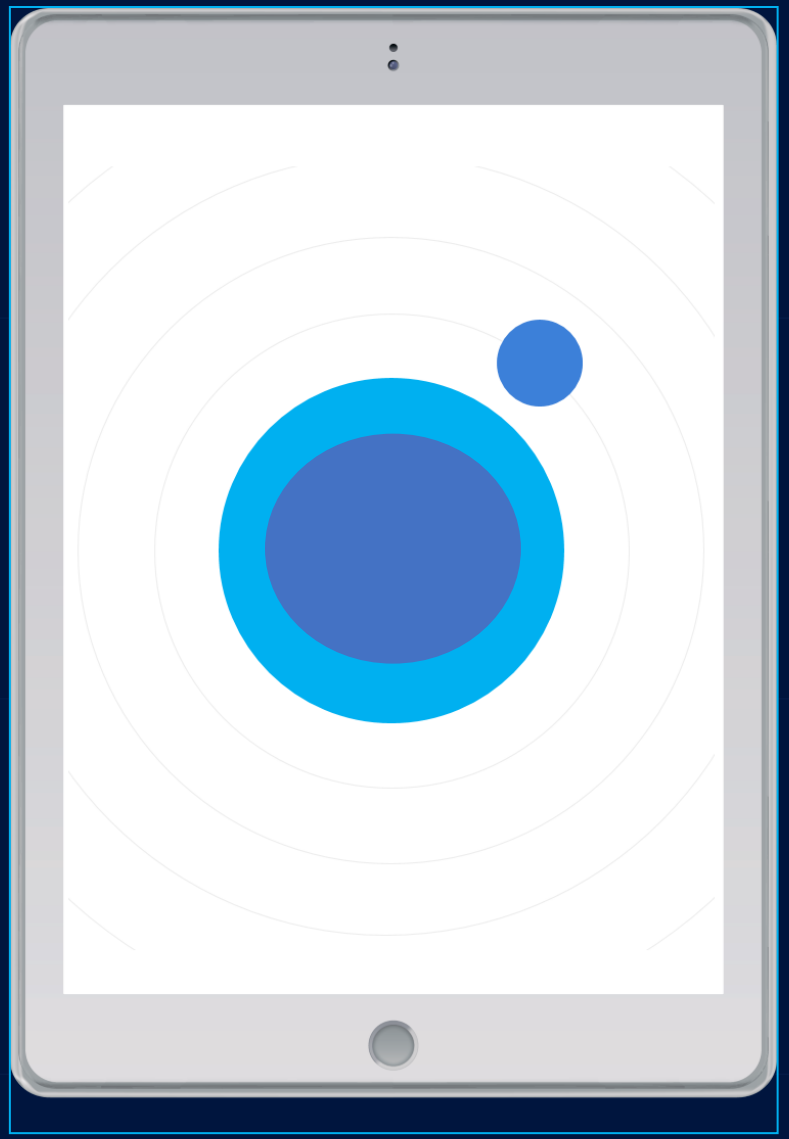


3.3.2	**SECURITY REQUIREMENT** Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.
3.3.7	**SECURITY REQUIREMENT** Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.
3.3.8	**SECURITY REQUIREMENT** Protect audit information and audit logging tools from unauthorized access, modification, and deletion.
3.3.9	**SECURITY REQUIREMENT** Limit management of audit logging functionality to a subset of privileged users.

Elements of the Policy

- 5.4 Response to Audit Processing Failures
- 5.5 Protection of Audit Information
- 5.6 Audit Review, Analysis, and Reporting
- 5.7 Audit Record Retention
- 5.8 Audit Generation

6. Procedures and Guidelines
7. Policy Review and Updates
8. Communication and Training



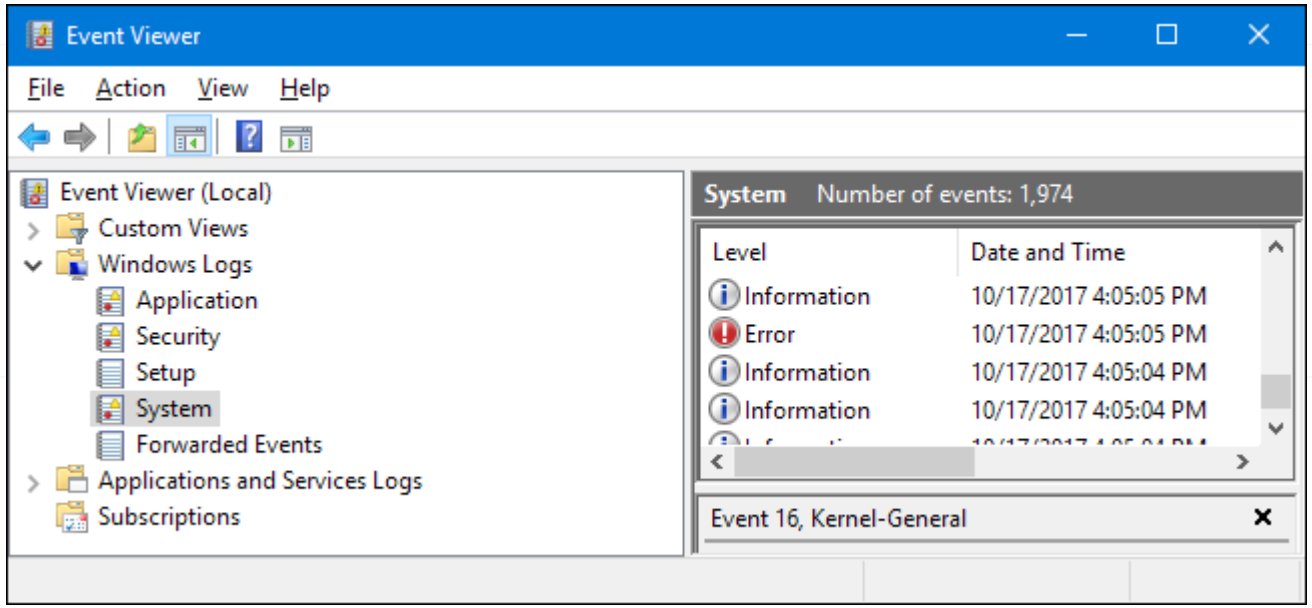
Reading the Controls

1 — Audit and Awareness Policy

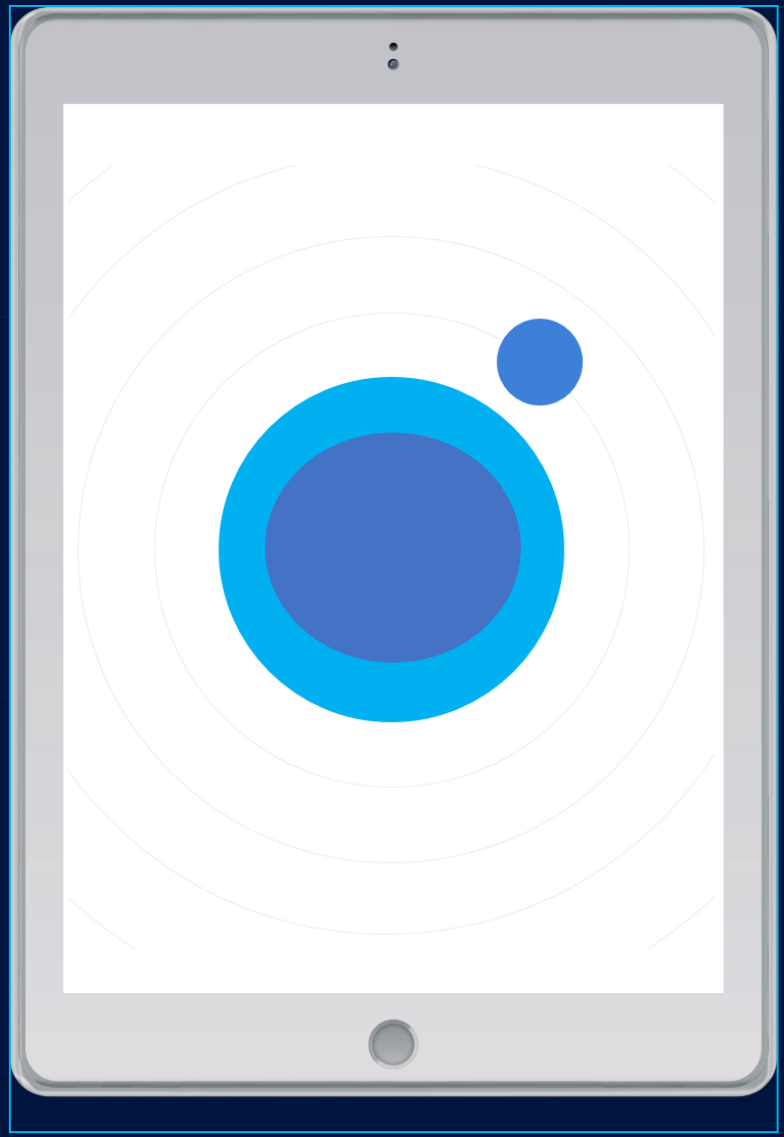
2 — Audit Records

3 — Review and Analysis

3.3.1	**SECURITY REQUIREMENT** Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.3.1[a]	*audit logs needed (i.e., event types to be logged) to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity are specified.*
	3.3.1[b]	*the content of audit records needed to support monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity is defined.*
	3.3.1[c]	*audit records are created (generated).*
	3.3.1[d]	*audit records, once created, contain the defined content.*
	3.3.1[e]	*retention requirements for audit records are defined.*
	3.3.1[f]	*audit records are retained as defined.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* Audit and accountability policy; procedures addressing auditable events; system security plan; system design documentation; system configuration settings and associated documentation; procedures addressing control of audit records; procedures addressing audit record generation; system audit logs and records; system auditable events; system incident reports; other relevant documents or records]. Interview: [*SELECT FROM:* Personnel with audit and accountability responsibilities; personnel with information security responsibilities; personnel with audit review, analysis and reporting responsibilities; system or network administrators]. Test: [*SELECT FROM:* Mechanisms implementing system audit logging].	

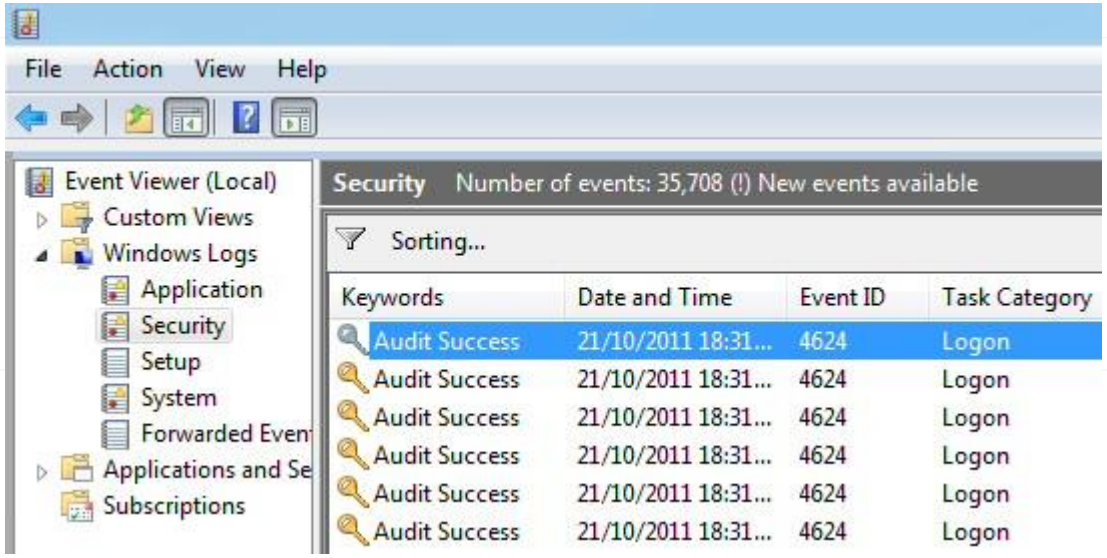


Event Viewer Logs



System Events Logs capture activities related to the system's operation and are essential for understanding system health and detecting anomalies. These logs typically include:

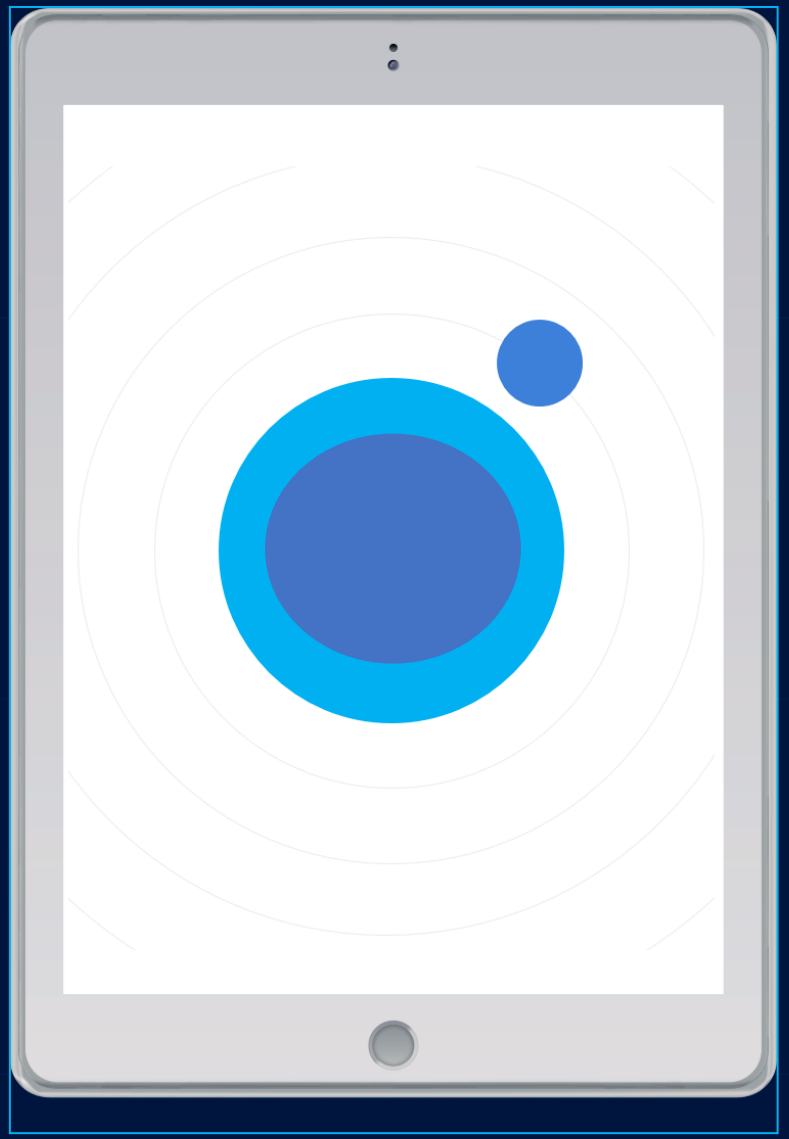
- **System startup and shutdown events**
- **System crashes and hardware failures**
- **Service or application start and stop events**
- **Operating system updates and patches**



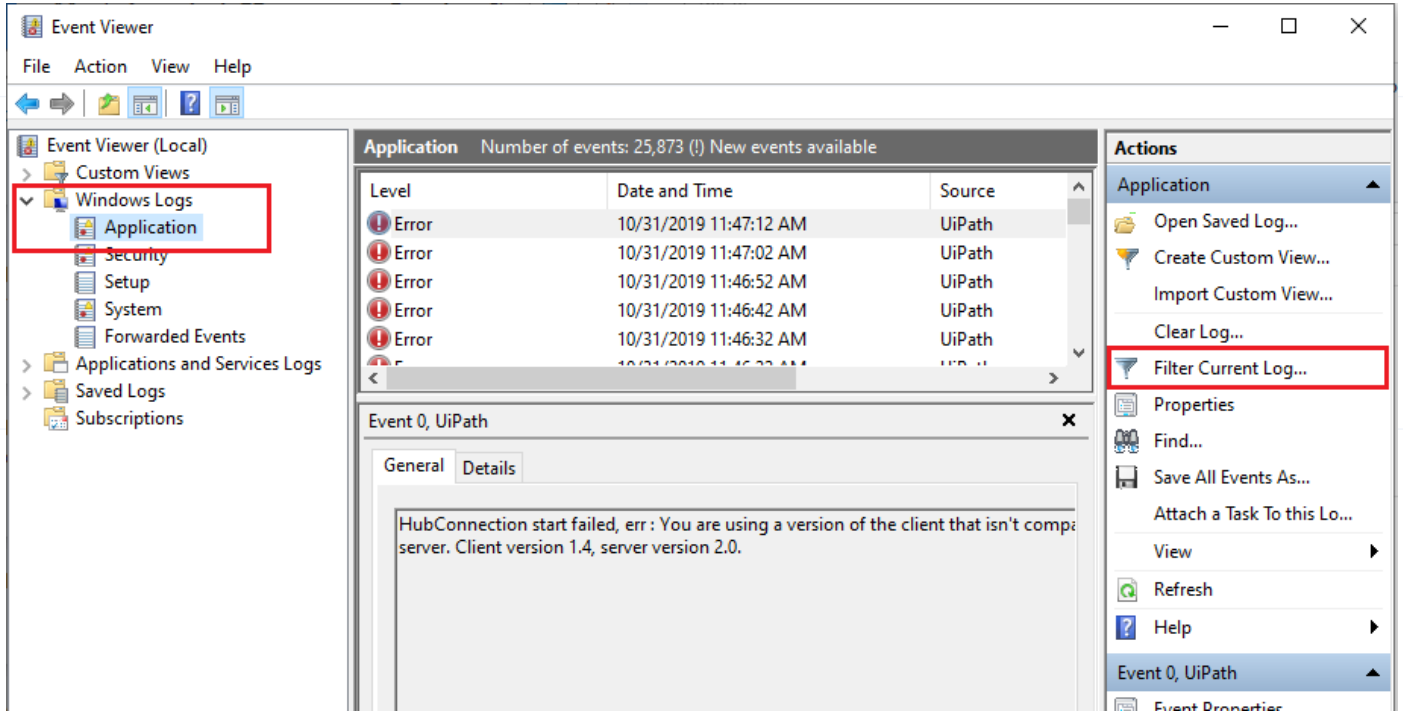
Security Logs focus on security-related events and are vital for detecting and responding to security incidents. These logs capture:

- **Firewall activity (e.g., allowed and blocked traffic)**
- **Intrusion detection/prevention system (IDS/IPS) alerts**
- **Antivirus and anti-malware activity**
- **Access control and authorization changes**
- **Security policy changes**

Event Viewer Logs

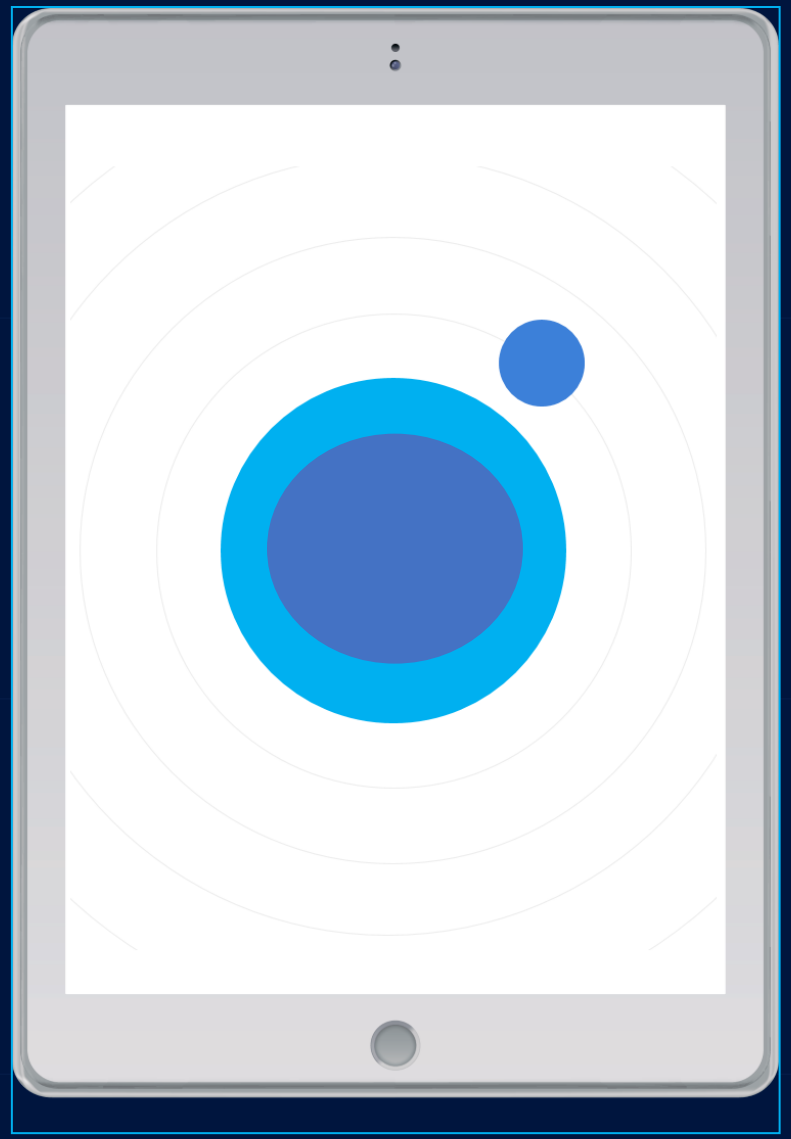


Event Viewer Logs



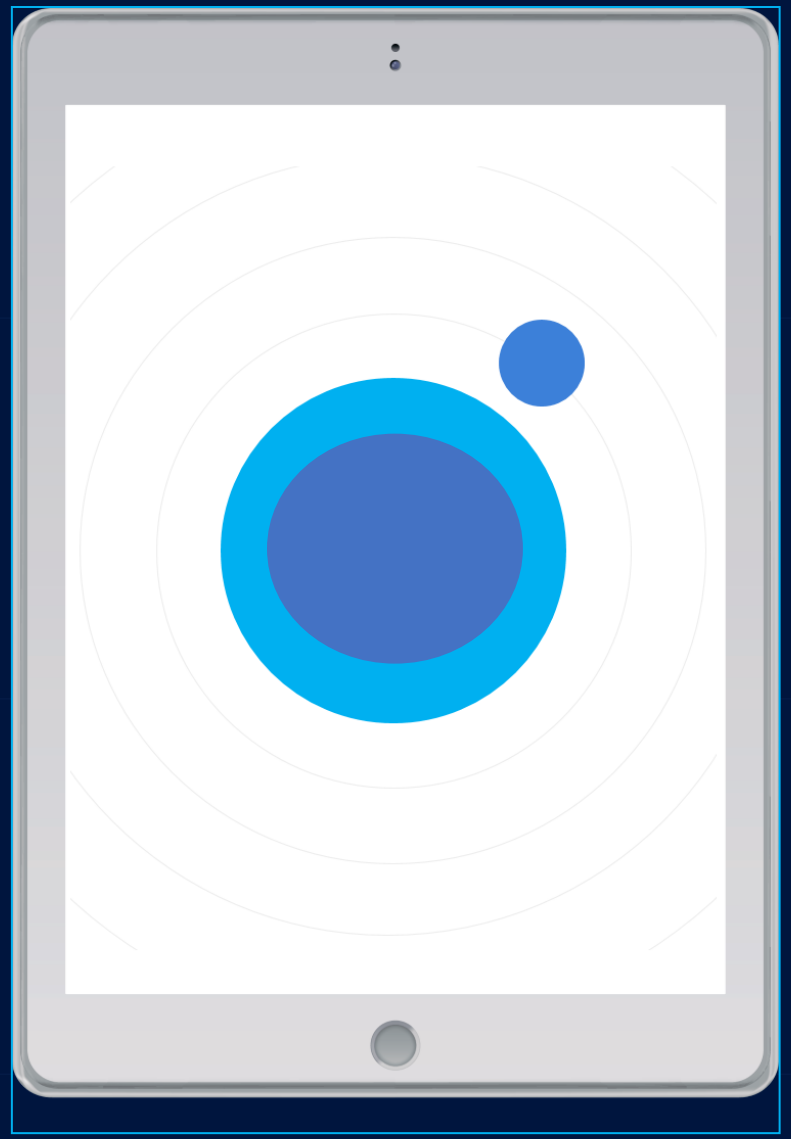
Application Logs detail the operations and errors of applications running on the system. These logs are useful for diagnosing application issues and monitoring application-level security. They include:

- **Application start and stop events**
- **User access to applications**
- **Application errors and exceptions**
- **Application updates and configuration changes**



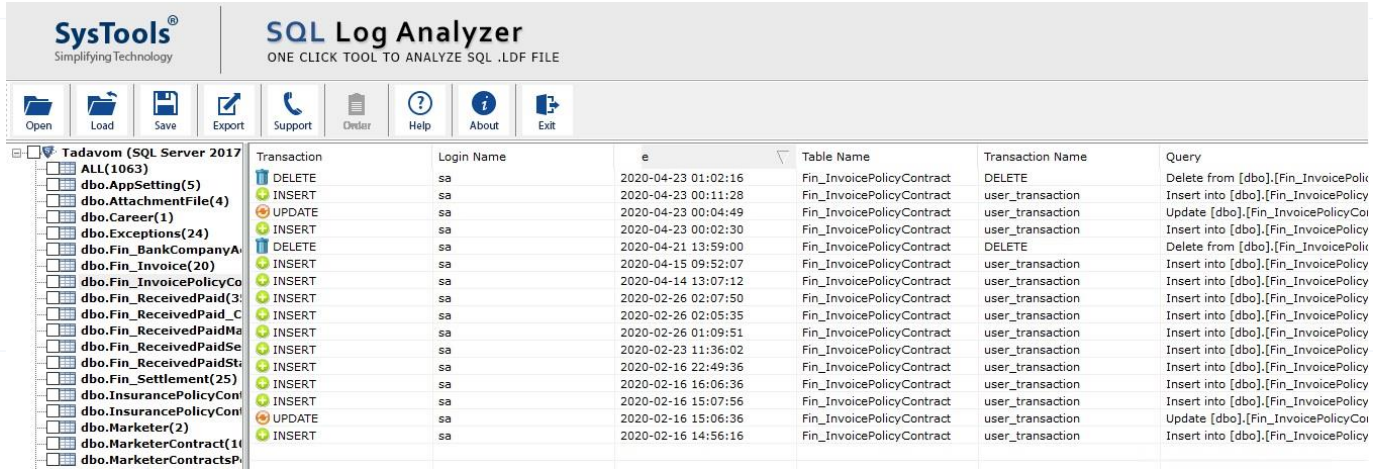
Event Viewer Logs

✖	Sep 10 12:07:11	▶ WAN	Destination_High_Port_Abusers	185.152.66.241:80	TCP:S
✖	Sep 10 12:07:11	▶ WAN	Destination_High_Port_Abusers	185.152.66.241:80	TCP:S
✖	Sep 10 12:07:09	▶ WAN	Destination_High_Port_Abusers	185.152.66.241:80	TCP:S
✖	Sep 10 12:07:09	▶ WAN	Destination_High_Port_Abusers	185.152.66.241:80	TCP:S
✖	Sep 10 12:07:08	▶ WAN	Destination_High_Port_Abusers	185.152.66.241:80	TCP:S



Network Logs provide visibility into network activities and are essential for detecting network-based threats. These logs typically include:

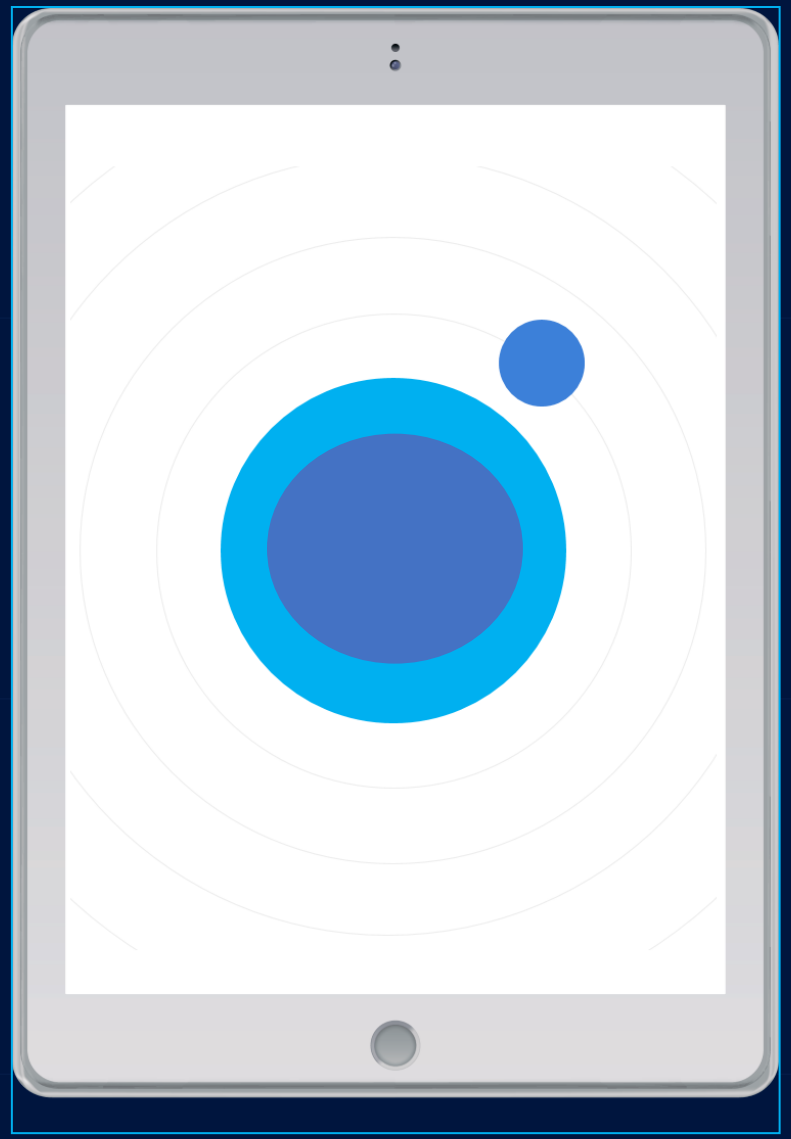
- **Network traffic logs (e.g., NetFlow, packet captures)**
- **VPN and remote access logs**
- **Router and switch logs**
- **DNS query logs**
- **Web proxy logs**



Database Logs record activities related to database operations and are important for tracking data access and modifications. These logs include:

- **Database user logons and logoffs**
- **Database query executions**
- **Changes to database schemas**
- **Database errors and performance issues**

Event Viewer Logs

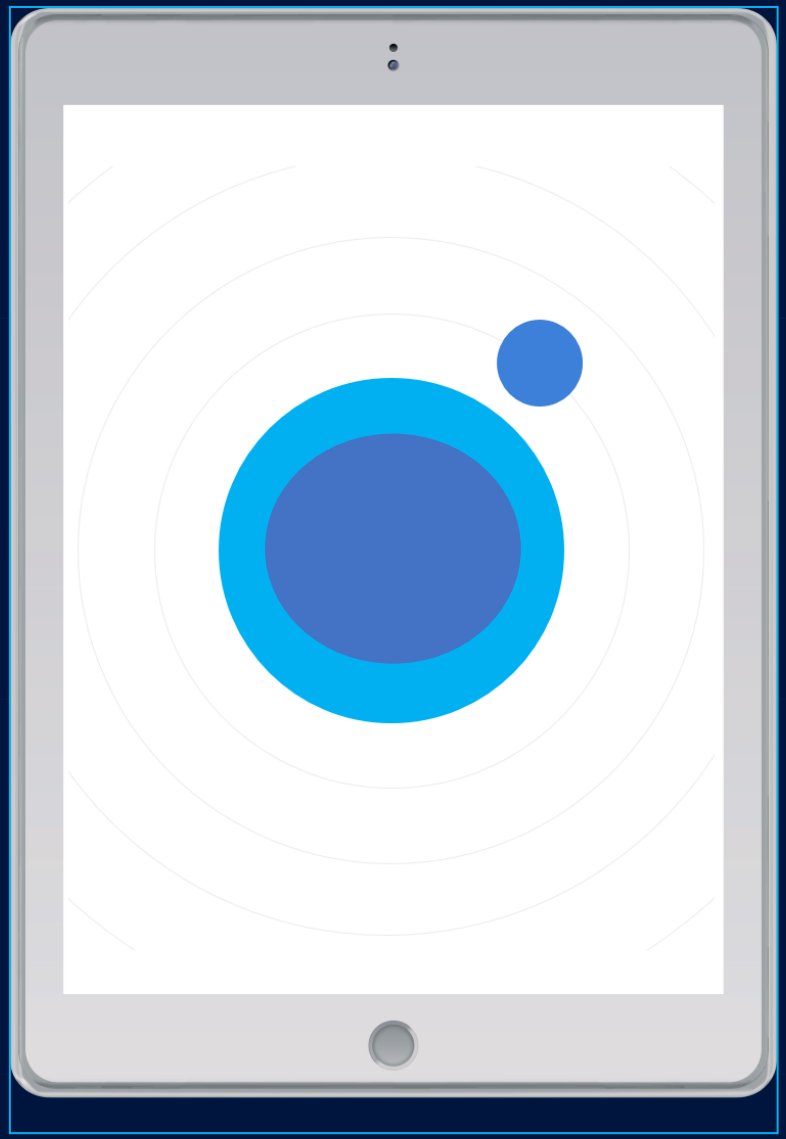


	A	B	C	D
1	Site Id	(All)		
2				
3	Count of Occurred Event			
4	Document Location	Delete	Restore	Grand Total
5	Audit Logs	1		1
6	salesteam/Shared Documents/Office	1		1
7	salesteam/Shared Documents/IT	1		1
8	marketing/Shared Documents/Channel sales	1		1
9	marketing/Shared Documents/Creative	1		1
10	sales/Shared Documents/Sales	1	1	2
11	**Grand Total**	**6**	**1**	**7**

Audit Trail Logs provide a chronological record of all significant events and are critical for forensic analysis and compliance verification. These logs should capture:

- **File access and modifications**
- **Changes to system configurations**
- **Use of privileged accounts**
- **Access to sensitive data (e.g., controlled unclassified information)**

Event Viewer Logs



Reading the Controls

NIST SP 800-171

1

Audit and Accountability Policy

2

Audit Records

3

Review and Analysis

Ways to Review and Analyze Audit Records

Regular Log Reviews

Conduct regular log reviews to identify anomalies and potential security incidents:

- **Daily Reviews**: Focus on critical logs like failed login attempts, privilege escalations, and access to sensitive data.
- **Weekly Reviews**: Broader analysis of user activity logs, system events, and network traffic.
- **Monthly Reviews**: Comprehensive review of all logs to identify trends and patterns.

Automated Log Analysis

Leverage automated tools to assist in log analysis:

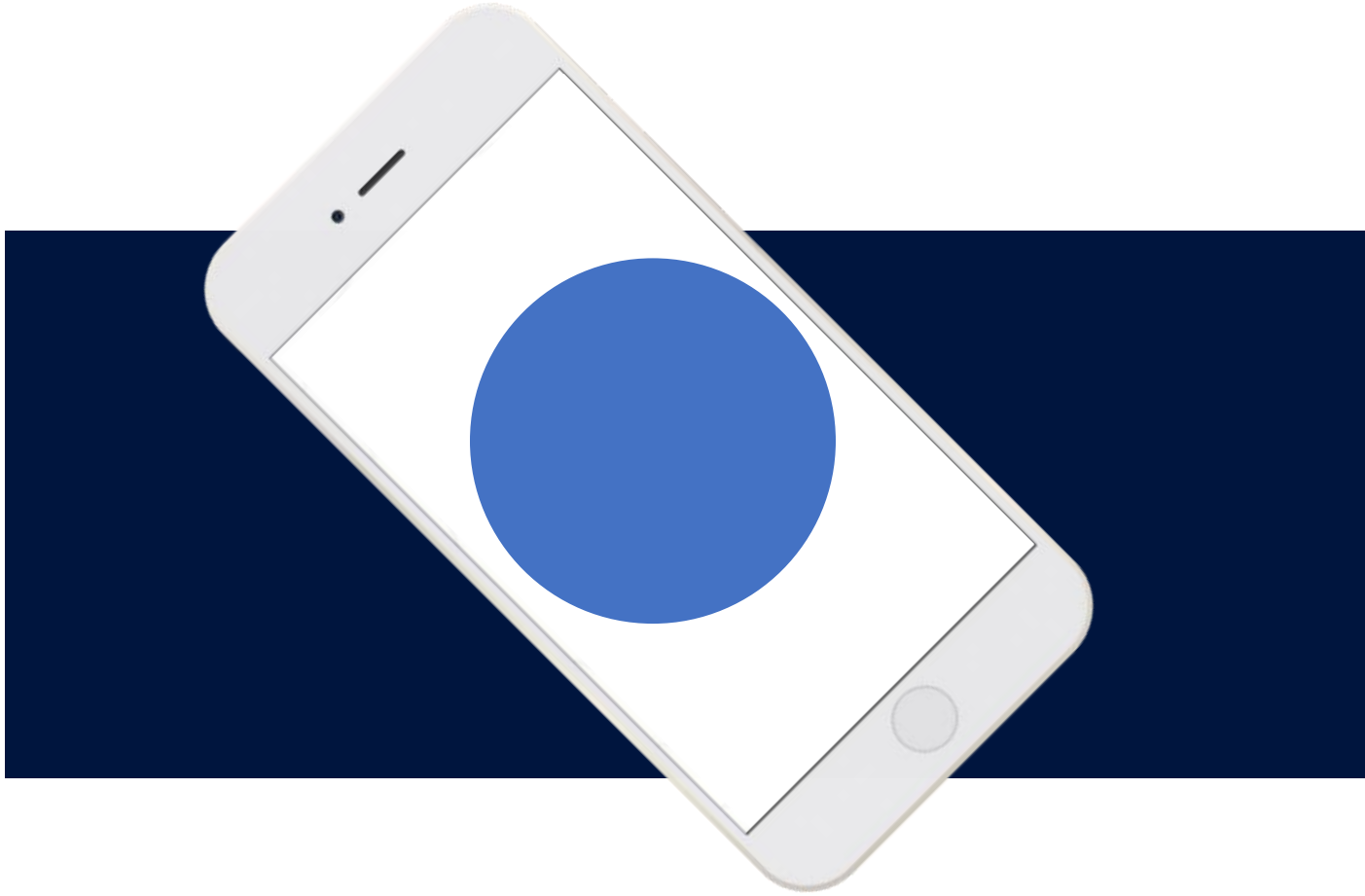
- **SIEM Systems**: Automate the correlation of events and alerting on suspicious activities.
- **Anomaly Detection**: Use machine learning algorithms to detect unusual patterns.
- **Log Parsing**: Use regular expressions and parsing rules to extract relevant information from logs.

Matthew Frost

mattf@wispro.org

Wisconsin Procurement Institute

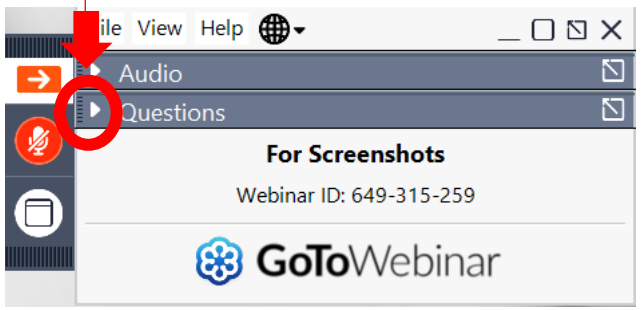
AN APEX ACCELERATOR



QUESTIONS?

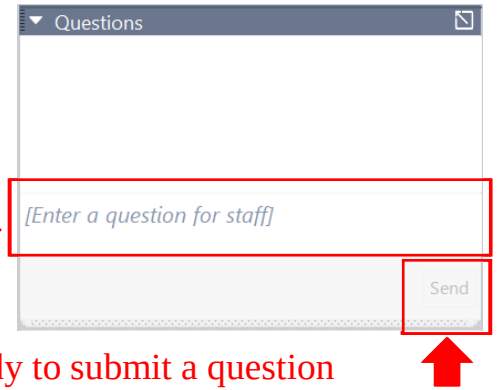
OPENING THE QUESTIONS BOX

Click here to access within the Control Panel



USING THE QUESTIONS BOX

Type questions here at any time during a presentation



Click Send when ready to submit a question

UPCOMING TRAINING - EVENTS

Wisconsin Procurement Institute
An APEX Accelerator

July 19, 2024

NCMA
NATIONAL CONTRACT MANAGEMENT ASSOCIATION
WISCONSIN

CYBER FRIDAY LIVE WEBINAR SERIES

Cyber Friday is a series of one-hour webinars focusing on critical topics for DOD contractors and subcontractors in cyber security, data security, and CMMC. Attendees receive 1 CPE credit for attending.

- **August 23,** 3.1.4 Configuration Management Policy, Change Request Process, Baseline Configurations
- **September 20,** 3.1.6 Incident Response Policy, Incident Response Plan
- **October 18,** 3.1.7 System Maintenance Policy
- **November 22,** 3.1.8 Media Control Policy, Media Destruction Policy and Personnel Security
- **January 24,** 3.1.11 Risk Assessment Policy, Security Assessment Reports

WPI Wisconsin Procurement Institute
An APEX Accelerator

…More information and registrations at wispro.org/events

EMERGING ISSUES WEBINAR SERIES

This series is intended as an information tool and resource for contract managers and those with a compliance function. Attendees receive 1 CPE credit for attending.

- **July 25** – Beyond contracts: Conducting Business with the Federal Government
- **Aug 22** – Regulation Making – The Process and the Important Role Businesses Play
- **Sep 19** – Industry 4.0 – The Next Generation of the DIB
- **Oct 24** – Innovation – What Does Innovation Look Like from DoD's Perspective?
- **Nov 21** – The Critical Role Your Accounting System Plays in SBIR/STTR Success

WPI Wisconsin Procurement Institute
An APEX Accelerator

…More information and registrations at wispro.org/events

- Save the Date -

The Contracting Academy

Developing and Growing Government Contractors

Dec 10

Virtual | 9:00 am - 4:00 pm

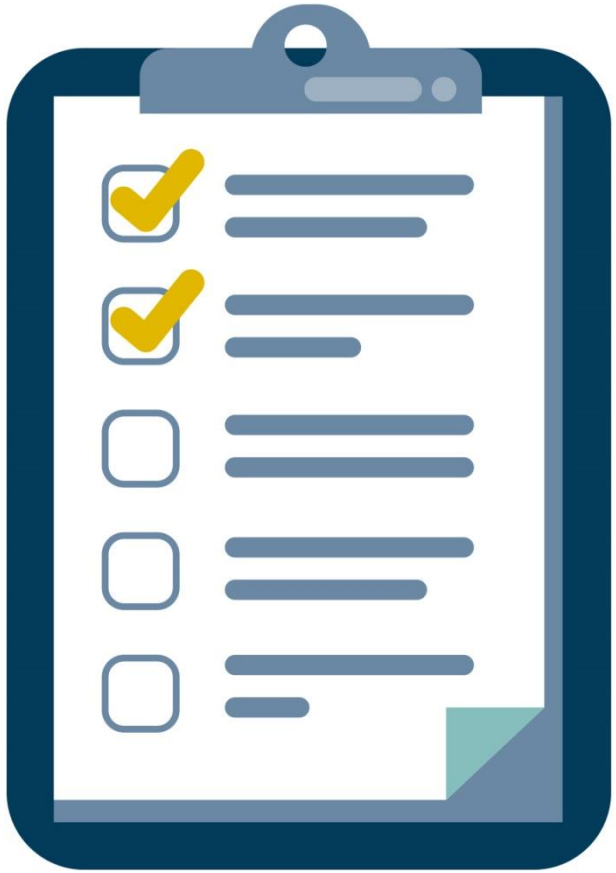
The Contracting Academy (TCA) is an opportunity for businesses to grow their technical knowledge of contracting with Federal Government, State/Local Government, and Government Prime Contractors. The series of workshops will benefit established businesses looking to grow and develop their government sales.

…More information and registrations at wispro.org/events

WPI Wisconsin Procurement Institute
An APEX Accelerator

NCMA National Contract Management Association
WISCONSIN

SURVEY



Wisconsin Procurement Institute
An APEX Accelerator

July 19, 2024

NCMA
NATIONAL CONTRACT MANAGEMENT ASSOCIATION
WISCONSIN

CONTINUING PROFESSIONAL EDUCATION

This webinar is eligible for 1 CPE credit.
For a certificate of this credit please contact:

Neelu Patil
neelagangap@wispro.org

PRESENTED BY

Wisconsin Procurement Institute (WPI)

www.wispro.org

Matt Frost

Wisconsin Procurement Institute

MattF@wispro.org | 608-293-0920

10437 Innovation Drive Suite 320
Milwaukee WI 53226