NCUA Information Security Examination, Automated Cybersecurity Evaluation Toolbox (ACET), and Tandem Mapping

Introduction

On January 18, 2023, the National Credit Union Administration (NCUA) published their 2023 Supervisory Priorities, which stated that examiners will use new Information Security Examination (ISE) procedures in upcoming exams.

The priorities went on to state that credit unions are still encouraged to conduct cybersecurity self-assessments using the Automated Cybersecurity Evaluation Toolbox (ACET). According to the priorities, “the toolbox works in coordination with and will prepare you for an Information Security Examination.”

This resource is for information purposes only. It serves to provide Tandem’s opinion of the Small Credit Union Examination Program (SCUEP) and CORE ISE procedures and how they relate to the ACET. You may use this resource to assist in your preparation for an upcoming exam, but you should interpret the procedures and coordinate with your examiner, as appropriate, for your credit union.

This resource also serves to identify areas in Tandem where topics from the examination procedures are addressed and does not guarantee that a credit union using Tandem achieves the expectations.

About Tandem: Tandem is a tool designed to assist with compliance goals and improve cybersecurity through the development of an information security program. There are multiple Tandem products referenced in this mapping which can help address the requirements of the updated procedures. These products include Risk Assessment, Policies, Vendor Management, Audit Management, Business Continuity Plan, and Incident Management.

If you do not have access to the Tandem products referenced by this mapping, but would like to learn more, contact us at info@tandem.app or on our website, Tandem.App/Contact.

NCUA ISE Component	NCUA ISE Statement	ACET Declarative Statement	Tandem References
Policies & Procedures The credit union's written information security Policies/Procedures/Plans include the following:	**SCUEP #1.1, CORE #1.1** Are approved by the Board of Directors	**Cyber Risk Management and Oversight | Governance | Strategy / Policies** The institution has board-approved policies commensurate with its risk and complexity that address information security.	**Policies** • Revision/Approval Log
	SCUEP #1.2, CORE #1.2 Documents access controls and authentication requirements for accessing critical applications and systems	**Cybersecurity Controls | Preventative Controls | Access & Data Management** Identification and authentication are required and managed for access to systems, applications, and hardware.	**Policies** • Access Control Policy • Remote Access Policy • User Authentication Policy
	SCUEP #1.3, CORE #1.3 Documents access restrictions used at physical locations where member data is stored	**Cybersecurity Controls | Preventative Controls | Access & Data Management** Physical security controls are used to prevent unauthorized access to information systems and telecommunication systems.	**Policies** • Access Control Policy • Physical Security of Sensitive Information Policy
	SCUEP #1.4, CORE #1.4 Documents data encryption requirements	**Cybersecurity Controls | Preventative Controls | Access & Data Management** Confidential data are encrypted when transmitted across public or untrusted networks (e.g., Internet).	**Policies** • Encryption Policy
	SCUEP #1.5, CORE #1.5 Documents when key or critical controls will be tested	**Cyber Risk Management and Oversight | Risk Management | Audit** Independent audit or review evaluates policies, procedures, and controls across the institution for significant risks and control issues associated with the institution's operations, including risks in new products, emerging technologies, and information systems.	**Audit Management** **Policies** • Security Testing Policy

NCUA ISE Component	NCUA ISE Statement	ACET Declarative Statement	Tandem References
	SCUEP #1.6, CORE #1.6 Documents segregation of duty requirements	**Cybersecurity Controls | Preventative Controls | Access & Data Management** Employee access to systems and confidential data provides for separation of duties.	**Policies** • Access Control Policy
	SCUEP #1.7, CORE #1.7 Documents data destruction and media sanitization criteria	**Cybersecurity Controls | Preventative Controls | Access & Data Management** Data is disposed of or destroyed according to documented requirements and within expected time frames.	**Policies** • Data Retention and Destruction Policy
	SCUEP #1.8, CORE #1.8 Assigns specific responsibility for the security program's implementation	**Cyber Risk Management and Oversight | Resources | Staffing** Information security roles and responsibilities have been identified.	**Policies** • Introduction • Security Committee Policy
Governance The annual report to the Board on the overall status of the information security program includes the following:	**SCUEP #2.1, CORE #2.1** Results from the information security risk assessment	**Cyber Risk Management and Oversight | Governance | Oversight** Management provides a written report on the overall status of the information security and business continuity programs to the board or an appropriate board committee at least annually.	**Resources** • Annual Report to the Board • Information Security Program **Download Documents** • Risk Assessment: Information Security Risk Assessment • Vendor Management: Vendor Oversight • Audit Management: Finding and Response Summary • Incident Management: Incident Summary
	SCUEP #2.2, CORE #2.2 Control arrangements with service providers		
	SCUEP #2.3, CORE #2.3 Results of testing key or critical controls		
	SCUEP #2.4, CORE #2.4 Security incidents and management's response to security incidents		

NCUA ISE Component	NCUA ISE Statement	ACET Declarative Statement	Tandem References
Asset Inventory The inventory of information assets (software/hardware) includes the following:	**CORE #3.1** Workstations and Laptops (including operating systems) **CORE #3.2** Servers (including operating systems) **CORE #3.3** Security Devices (e.g., Firewall, IDS/IPS, etc.) **CORE #3.4** Network Devices (e.g., Switches, Routers, etc.) **CORE #3.5** Software Applications (including version and number of instances)	**Cyber Risk Management and Oversight | Governance | IT Asset Management** An inventory of organizational assets (e.g., hardware, software, data, and systems hosted externally) is maintained.	**Business Continuity Plan** • Software • Systems/Equipment **Risk Assessment** • Information Assets **Custom Fields** can be created on each of these pages for tracking specific details as part of the inventory.
Risk Assessment The information security risk assessment process includes the following:	**SCUEP #3.1, CORE #4.1** Identification of reasonable and foreseeable threats to critical assets	**Cyber Risk Management and Oversight | Risk Management | Risk Assessment** A risk assessment focused on safeguarding customer information identifies reasonable and foreseeable internal and external threats, the likelihood and potential damage of threats, and the sufficiency of policies, procedures, and customer information systems.	**Risk Assessment** • Threats

NCUA ISE Component	NCUA ISE Statement	ACET Declarative Statement	Tandem References
	SCUEP #3.2, CORE #4.2 Documenting key or critical controls	N/A – While there is not a singular declarative statement which addresses this concept, it is implied through the completion of a cybersecurity controls self-assessment, like the ACET.	**Risk Assessment** • Controls
	SCUEP #3.3, CORE #4.3 Testing the adequacy of identified key or critical controls	**Cyber Risk Management and Oversight | Risk Management | Audit** Independent audit or review evaluates policies, procedures, and controls across the institution for significant risks and control issues associated with the institution's operations, including risks in new products, emerging technologies, and information systems.	**Audit Management** **Risk Assessment** • Verifications • Control Audit History Report

	SCUEP #3.4, CORE #4.4
	Assessing the likelihood those threats may be exploited by a weakness or vulnerability
		Cyber Risk Management and Oversight | Risk Management | Risk Assessment
		A risk assessment focused on safeguarding customer information identifies reasonable and foreseeable internal and external threats, the likelihood and potential damage of threats, and the sufficiency of policies, procedures, and customer information systems.
			Risk Assessment
			• Threats
			  ○ Likelihood
			  ○ Potential Damage

	SCUEP #3.5, CORE #4.5 Assessing the potential damage or impact from those threats if successfully exploited		
Controls Testing The Independent testing of critical controls includes the following:	**CORE #5.1** Information Technology Controls Audit	**Cyber Risk Management and Oversight | Risk Management | Audit** Independent audit or review evaluates policies, procedures, and controls across the institution for significant risks and control issues associated with the institution's operations, including risks in new products, emerging technologies, and information systems.	**Audit Management** **Phishing** **Policies** • Security Testing Policy **Tandem Partners** offer security testing services.

NCUA ISE Component	NCUA ISE Statement	ACET Declarative Statement	Tandem References
	CORE #5.2 Internal Vulnerability Scanning	**Cybersecurity Controls | Detective Controls | Threat & Vulnerability Detection** Independent testing (including penetration testing and vulnerability scanning) is conducted according to the risk assessment for external-facing systems and the internal network.	
	CORE #5.3 External Vulnerability Scanning		
	CORE #5.4 Internal Penetration Testing		
	CORE #5.5 External Penetration Testing		
	CORE #5.6 Social Engineering Testing	**Cyber Risk Management and Oversight | Training and Culture | Training** The institution validates the effectiveness of training (e.g., social engineering or phishing tests).	
Corrective Actions The process for tracking formal issues, exceptions, and/or corrective actions includes the following:	**CORE #6.1** A process for resolving identified issues, exceptions and/or corrective actions	**Cyber Risk Management and Oversight | Risk Management | Audit** Issues and corrective actions from internal audits and independent testing/assessments are formally tracked to ensure procedures and control lapses are resolved in a timely manner.	**Audit Management** • Findings
	CORE #6.2 Methods for tracking and reporting issues to resolution		
Training The information security training program includes the following:	**SCUEP #4.1, CORE #7.1** New Employee Training and background checks	**Cyber Risk Management and Oversight | Resources | Staffing** Employment candidates, contractors, and third parties are subject to background verification proportional to the confidentiality of the data accessed, business requirements, and acceptable risk.	**Policies** • Employee Security Awareness Training Policy • Personnel Security Policy

NCUA ISE Component	NCUA ISE Statement	ACET Declarative Statement	Tandem References
	SCUEP #4.2, CORE #7.2 Employee training provided to all employees	**Cyber Risk Management and Oversight | Training and Culture | Training** Annual information security training is provided.	**Training** • Phishing Training • Security Awareness Training • Security Incident Management Training
	SCUEP #4.3, CORE #7.3 Incident response, current cyber threats, and emerging issues	**Cyber Risk Management and Oversight | Training and Culture | Training** Annual information security training includes incident response, current cyber threats (e.g., phishing, spear phishing, social engineering, and mobile security), and emerging issues.	
	SCUEP #4.4, CORE #7.4 Social Engineering training such as phishing scams, pretexting, spear phishing		

	SCUEP #4.5, CORE #7.5
	Documented training records
		N/A – While there is not a singular declarative statement which addresses this concept, it could be implied through the completion of “annual information security training.”	**Training**
			• Download Documents
			  ○ Training Report
			  ○ Transcript

Incident Response The incident response program includes the following:	**SCUEP #5.1, CORE #8.1** Assessment of the nature and scope of an incident	**Cyber Incident Management and Resilience | Detection, Response, & Mitigation | Response & Mitigation** Analysis of security incidents is performed in the early stages of an intrusion to minimize the impact of the incident.	**Incident Management** • Incident Handling Process: Analysis
	SCUEP #5.2, CORE #8.2 Measures to contain and control an incident	**Cyber Incident Management and Resilience | Detection, Response, & Mitigation | Response & Mitigation** Appropriate steps are taken to contain and control an incident to prevent further unauthorized access to or use of customer information.	**Incident Management** • Incident Handling Process: Containment

NCUA ISE Component	NCUA ISE Statement	ACET Declarative Statement	Tandem References
	SCUEP #5.3, CORE #8.3 The identification of member information that has been accessed or misused	N/A – While there is not a singular declarative statement which addresses this concept, it could be implied through declarative statements which discuss how to handle incidents which "[involve] the unauthorized access to or use of sensitive customer information."	**Incident Management** • Action Plans: Data Breach
	SCUEP #5.4, CORE #8.4 Filing a timely Suspicious Activity Report (SAR), when applicable	**Cyber Incident Management and Resilience | Detection, Response, & Mitigation | Escalation & Reporting** Procedures exist to notify customers, regulators, and law enforcement as required or necessary when the institution becomes aware of an incident involving the unauthorized access to or use of sensitive customer information.	**Incident Management** • Additional Documentation: Third-Party Communication
	SCUEP #5.5, CORE #8.5 Prompt notification to the NCUA Regional Director, and/or State Supervisory Authority		
	SCUEP #5.6, CORE #8.6 Notification to appropriate law enforcement authorities		
	SCUEP #5.7, CORE #8.7 Notification of members when warranted		**Incident Management** • Additional Documentation: Member Communication
Technology Service Providers Third party management process includes the following:	**SCUEP #6.1, CORE #9.1** Maintain a vendor management policy	**Cyber Risk Management and Oversight | Governance | Strategy / Policies** The institution has policies commensurate with its risk and complexity that address the concepts of external dependency or third-party management.	**Policies** • Vendor Management Policy

NCUA ISE Component	NCUA ISE Statement	ACET Declarative Statement	Tandem References
	SCUEP #6.2, CORE #9.2 A process for performing due diligence	**External Dependency Management | Relationship Management | Due Diligence** Risk-based due diligence is performed on prospective third parties before contracts are signed, including reviews of their background, reputation, financial condition, stability, and security controls.	**Vendor Management** • Contracts • Documents • Reviews
	SCUEP #6.3, CORE #9.3 Maintaining a listing of all critical vendors and contracts	**External Dependency Management | Relationship Management | Due Diligence** A list of third-party service providers is maintained.	**Vendor Management** • Contact Information
	SCUEP #6.4, CORE #9.4 Appropriate information security measures within service provider contracts	**External Dependency Management | Relationship Management | Contracts** Formal contracts that address relevant security and privacy requirements are in place for all third parties that process, store, or transmit confidential data or provide critical services.	**Vendor Management** • Contracts • Documents • Reviews
Business Continuity / Disaster Recovery The Disaster Recovery / Business Continuity program includes the following components:	**SCUEP #7.1, CORE #10.1** Backup and recovery plans for critical systems and services in the event of a disaster or incident	**Cyber Incident Management and Resilience | Incident Resilience Planning & Strategy | Planning** A formal backup and recovery plan exists for all critical business lines.	**Business Continuity Plan** • Backup Profiles • Systems/Equipment • Recovery Point Objectives **Policies** • Data Backup

	SCUEP #7.2, CORE #10.2
	A process of identifying the potential impact of disruptive events to an entity's functions and processes (Business Impact Analysis)
		Cyber Incident Management and Resilience | Incident Resilience Planning & Strategy | Planning
		Business impact analyses have been updated to include cybersecurity.
			Business Continuity Plan
			• Business Processes
			  ○ Business Impact Analysis
			  ○ Potential Impacts

NCUA ISE Component	NCUA ISE Statement	ACET Declarative Statement	Tandem References
	SCUEP #7.3, CORE #10.3 Methods for training and testing contingency plans	**Cyber Incident Management and Resilience | Incident Resilience Planning & Strategy | Testing** Recovery scenarios include plans to recover from data destruction and impacts to data integrity, data loss, and system and data availability.	**Business Continuity Plan** • Exercises & Tests • Scenarios
	SCUEP #7.4, CORE #10.4 Reports to the Board on the status of the business continuity program and/or results from testing	**Cyber Risk Management and Oversight | Governance | Oversight** Management provides a written report on the overall status of the information security and business continuity programs to the board or an appropriate board committee at least annually.	**Business Continuity Plan** • Revision/Approval Log **Resources** • Annual Report to the Board
Vulnerability & Patch Management The patch management process includes the following:	**CORE #11.1** Patching schedules	**Cybersecurity Controls | Corrective Controls | Patch Management** A patch management program is implemented and ensures that software and firmware patches are applied in a timely manner.	**Policies** • Vulnerability & Patch Management Policy **Risk Assessment** • Vulnerability Scans Control
	CORE #11.2 A process for applying patches in a timely manner		
	CORE #11.3 A process that produces and reviews reports of missing security patches	**Cybersecurity Controls | Corrective Controls | Patch Management** Patch management reports are reviewed and reflect missing security patches.	
Cybersecurity Controls Select the cybersecurity controls the credit union currently maintains:	**SCUEP #8.1** Anti-virus/Anti-malware	**Cybersecurity Controls | Detective Controls | Threat & Vulnerability Detection** Antivirus and anti-malware tools are used to detect attacks.	**Policies** • Malicious Software Protection Policy **Risk Assessment** • Anti-Malware Software Control

NCUA ISE Component	NCUA ISE Statement	ACET Declarative Statement	Tandem References
	SCUEP #8.2 Email Protection (such as SPAM filtering, encrypted e-mail)	**Cybersecurity Controls | Detective Controls | Threat & Vulnerability Detection** Email protection mechanisms are used to filter for common cyber threats (e.g., attached malware or malicious links).	**Policies** • Email Security Policy **Risk Assessment** • SPAM Filter
	SCUEP #8.3 Patch Management (patching critical applications and systems)	**Cybersecurity Controls | Corrective Controls | Patch Management** A patch management program is implemented and ensures that software and firmware patches are applied in a timely manner.	**Policies** • Vulnerability & Patch Management Policy **Risk Assessment** • Patch Management Control
	SCUEP #8.4 Password Management	**Cybersecurity Controls | Preventative Controls | Access & Data Management** Identification and authentication are required and managed for access to systems, applications, and hardware.	**Policies** • User Authentication Policy **Risk Assessment** • Password Complexity
	SCUEP #8.5 Firewalls	**Cybersecurity Controls | Preventative Controls | Infrastructure Management** Network perimeter defense tools (e.g., border router and firewall) are used.	**Policies** • Firewall Policy **Risk Assessment** • Firewall Control
	SCUEP #8.6 Intrusion Detection System (IDS) / Intrusion Prevention system (IPS)	**Cybersecurity Controls | Preventative Controls | Infrastructure Management** Antivirus and intrusion detection/prevention systems (IDS/IPS) detect and block actual and attempted attacks or intrusions.	**Policies** • Intrusion Detection and Prevention Policy **Risk Assessment** • Intrusion Detection / Prevention System Control

NCUA ISE Component	NCUA ISE Statement	ACET Declarative Statement	Tandem References
Anti-Virus / Anti-Malware Anti-virus/Anti-Malware controls include the following:	**CORE #12.1** Workstations/Servers receive automatic updates	**Cybersecurity Controls | Detective Controls | Threat & Vulnerability Detection** Antivirus and anti-malware tools are updated automatically.	**Policies** • Malicious Software Protection Policy **Risk Assessment** • Anti-Malware Software Control
	CORE #12.2 Active alerting functions	**Cybersecurity Controls | Detective Controls | Threat & Vulnerability Detection** Mechanisms (e.g., antivirus alerts, log event alerts) are in place to alert management to potential attacks.	
	CORE #12.3 Antivirus reporting	N/A – While there is not a singular declarative statement which addresses this concept, it could be implied through the statement, “Responsibilities for monitoring and reporting suspicious systems activity have been assigned.”	
Access Controls Limiting access to sensitive information and systems includes the following:	**CORE #13.1** The use of unique passwords following industry best practices	**Cybersecurity Controls | Preventative Controls | Access & Data Management** Access controls include password complexity and limits to password attempts and reuse.	**Policies** • User Authentication Policy **Risk Assessment** • Password Complexity
	CORE #13.2 A process to ensure inactive user accounts are disabled	**Cybersecurity Controls | Preventative Controls | Access & Data Management** Changes to physical and logical user access, including those that result from voluntary and involuntary terminations, are submitted to and approved by appropriate personnel.	**Policies** • Personnel Security Policy • User Authentication Policy **Risk Assessment** • Employee Termination Procedures Control

NCUA ISE Component	NCUA ISE Statement	ACET Declarative Statement	Tandem References
	CORE #13.3 Periodic user access reviews	**Cybersecurity Controls | Preventative Controls | Access & Data Management** User access reviews are performed periodically for all systems and applications based on the risk to the application or system.	**Policies** • User Authentication Policy **Risk Assessment** • Logical Access Controls
Network Security Network defense and perimeter devices include the following:	**CORE #14.1** The use of firewalls to prevent unauthorized access into or out of a computer network	**Cybersecurity Controls | Preventative Controls | Infrastructure Management** Network perimeter defense tools (e.g., border router and firewall) are used.	**Policies** • Firewall Policy **Risk Assessment** • Firewall Control
	CORE #14.2 Intrusion Prevention/Detection System(s) to monitor a network for malicious activity	**Cybersecurity Controls | Preventative Controls | Infrastructure Management** Antivirus and intrusion detection/prevention systems (IDS/IPS) detect and block actual and attempted attacks or intrusions.	**Policies** • Intrusion Detection and Prevention Policy **Risk Assessment** • Intrusion Detection / Prevention System Control
Data Leakage Protection Email and internet browser controls include the following:	**CORE #15.1** The use of only fully supported browsers and email clients are allowed	**Cybersecurity Controls | Preventative Controls | Infrastructure Management** Controls for unsupported systems are implemented and tested.	**Policies** • IT Asset Management Policy
	CORE #15.2 Web content filtering	N/A – While there is not a singular declarative statement which addresses this concept, it could be implied through the statement, “Network perimeter defense tools (e.g., border router and firewall) are used.”	**Policies** • Network Monitoring and Log Management Policy **Risk Assessment** • Web Content Filter Control

NCUA ISE Component	NCUA ISE Statement	ACET Declarative Statement	Tandem References
	CORE #15.3 Email server anti-malware protections are deployed, such as inbound attachment scanning	**Cybersecurity Controls | Detective Controls | Threat & Vulnerability Detection** Email protection mechanisms are used to filter for common cyber threats (e.g., attached malware or malicious links).	**Policies** • Email Security Policy **Risk Assessment** • SPAM Filter Control
	CORE #15.4 Blocking unnecessary file types from entering the email gateway	N/A – While there is not a singular declarative statement which addresses this concept, it could be implied through the statement, “Emails and attachments are automatically scanned to detect malware and are blocked when malware is present.”	
Change & Configuration Management The process for making changes to information assets include the following:	**CORE #16.1** A process describing how changes to systems, applications, and user access are reviewed and approved, such as hardware, operating systems, software applications, and system configurations.	**Cyber Risk Management and Oversight | Governance | IT Asset Management** A change management process is in place to request and approve changes to systems configurations, hardware, software, applications, and security tools.	**Policies** • Change Management Policy **Risk Assessment** • Change Management Control
	CORE #16.2 Procedures to document requests and approvals	**Cyber Risk Management and Oversight | Governance | IT Asset Management** Baseline configurations cannot be altered without a formal change request, documented approval, and an assessment of security implications.	