SCUEP

Examination Statements		
Information Security Program – Assessment Factor		
Policies & Procedures – Component		
Stmt #	**Statement / Sub-statement**	**Exam-level**
Stmt 1	**The credit unions written information security Policies/Procedures/Plans include the following:**	SCUEP
Stmt 1.1	Are approved by the Board of Directors	SCUEP
Stmt 1.2	Documents access controls and authentication requirements for accessing critical applications and systems	SCUEP
Stmt 1.3	Documents access restrictions used at physical locations where member data is stored	SCUEP
Stmt 1.4	Documents data encryption requirements	SCUEP
Stmt 1.5	Documents when key or critical controls will be tested	SCUEP
Stmt 1.6	Documents segregation of duty requirements	SCUEP
Stmt 1.7	Documents data destruction and media sanitization criteria	SCUEP
Stmt 1.8	Assigns specific responsibility for the security program's implementation	SCUEP
Governance – Component		
Stmt #	**Sub-statement**	**Exam-level**
Stmt 2	**The annual report to the Board on the overall status of the information security program includes the following:**	SCUEP
Stmt 2.1	Results from the information security risk assessment	SCUEP
Stmt 2.2	Control arrangements with service providers	SCUEP
Stmt 2.3	Results of testing key or critical controls	SCUEP
Stmt 2.4	Security incidents and management's response to security incidents	SCUEP
Risk Assessment – Component		
Stmt #	**Sub-statement**	**Exam-level**
Stmt 3	**The information security risk assessment process includes the following:**	SCUEP
Stmt 3.1	Identification of reasonable and foreseeable threats to critical assets	SCUEP
Stmt 3.2	Documenting key or critical controls	SCUEP
Stmt 3.3	Testing the adequacy of identified key or critical controls	SCUEP
Stmt 3.4	Assessing the likelihood those threats may be exploited by a weakness or vulnerability	SCUEP
Stmt 3.5	Assessing the potential damage or impact from those threats if successfully exploited	SCUEP
Training – Component		
Stmt #	**Sub-statement**	**Exam-level**
Stmt 4	**The information security training program includes the following:**	SCUEP
Stmt 4.1	New Employee Training and background checks	SCUEP

Stmt 4.2	Employee training provided to all employees	SCUEP
Stmt 4.3	Incident response, current cyber threats, and emerging issues	SCUEP
Stmt 4.4	Social Engineering training such as phishing scams, pretexting, spear phishing	SCUEP
Stmt 4.5	Documented training records	SCUEP
Incident Response – Component		
Stmt #	**Sub-statement**	**Exam-level**
Stmt 5	**The incident response program includes the following:**	SCUEP
Stmt 5.1	Assessment of the nature and scope of an incident	SCUEP
Stmt 5.2	Measures to contain and control an incident	SCUEP
Stmt 5.3	The identification of member information that has been accessed or misused	SCUEP
Stmt 5.4	Filing a timely Suspicious Activity Report (SAR), when applicable	SCUEP
Stmt 5.5	Prompt notification to the NCUA Regional Director, and/or State Supervisory Authority	SCUEP
Stmt 5.6	Notification to appropriate law enforcement authorities	SCUEP
Stmt 5.7	Notification of members when warranted	SCUEP
Technology Service Providers– Component		
Stmt #	**Sub-statement**	**Exam-level**
Stmt 6	**Third party management process includes the following:**	SCUEP
Stmt 6.1	Maintain a vendor management policy	SCUEP
Stmt 6.2	A process for performing due diligence	SCUEP
Stmt 6.3	Maintaining a listing of all critical vendors and contracts	SCUEP
Stmt 6.4	Appropriate information security measures within service provider contracts	SCUEP
Business Continuity / Disaster Recovery– Component		
Stmt #	**Sub-statement**	**Exam-level**
Stmt 7	**The Disaster Recovery / Business Continuity program includes the following components:**	SCUEP
Stmt 7.1	Backup and recovery plans for critical systems and services in the event of a disaster or incident	SCUEP
Stmt 7.2	A process of identifying the potential impact of disruptive events to an entity's functions and processes (Business Impact Analysis)	SCUEP
Stmt 7.3	Methods for training and testing contingency plans	SCUEP
Stmt 7.4	Reports to the Board on the status of the business continuity program and/or results from testing	SCUEP
Cybersecurity Controls– Component		
Stmt #	**Sub-statement**	**Exam-level**
Stmt 8	**Select the cybersecurity controls the credit union currently maintains:**	SCUEP
Stmt 8.1	Anti-virus/Anti-malware	SCUEP
Stmt 8.2	Email Protection (such as SPAM filtering, encrypted e-mail)	SCUEP

Stmt 8.3	Patch Management (patching critical applications and systems)	SCUEP
Stmt 8.4	Password Management	SCUEP
Stmt 8.5	Firewalls	SCUEP
Stmt 8.6	Intrusion Detection System (IDS) / Intrusion Prevention system (IPS)	SCUEP

CORE

Examination Statements		
Information Security Program – Assessment Factor		
Policies & Procedures – Component		
Stmt #	**Statement / Sub-statement**	**Exam-level**
Stmt 1	**The credit unions written information security Policies/Procedures/Plans include the following:**	CORE
Stmt 1.1	Are approved by the Board of Directors	CORE
Stmt 1.2	Documents access controls and authentication requirements for accessing critical applications and systems	CORE
Stmt 1.3	Documents access restrictions used at physical locations where member data is stored	CORE
Stmt 1.4	Documents data encryption requirements	CORE
Stmt 1.5	Documents when key or critical controls will be tested	CORE
Stmt 1.6	Documents segregation of duty requirements	CORE
Stmt 1.7	Documents data destruction and media sanitization criteria	CORE
Stmt 1.8	Assigns specific responsibility for the security program's implementation	CORE
Governance – Component		
Stmt #	**Sub-statement**	**Exam-level**
Stmt 2	**The annual report to the Board on the overall status of the information security program includes the following:**	CORE
Stmt 2.1	Results from the information security risk assessment	CORE
Stmt 2.2	Control arrangements with service providers	CORE
Stmt 2.3	Results of testing key or critical controls	CORE
Stmt 2.4	Security incidents and management's response to security incidents	CORE
Asset Inventory – Component		
Stmt #	**Sub-statement**	**Exam-level**
Stmt 3	**The inventory of information assets (software/hardware) includes the following:**	CORE
Stmt 3.1	Workstations and Laptops (including operating systems)	CORE
Stmt 3.2	Servers (including operating systems)	CORE
Stmt 3.3	Security Devices (e.g., Firewall, IDS/IPS, etc.)	CORE
Stmt 3.4	Network Devices (e.g., Switches, Routers, etc.)	CORE
Stmt 3.5	Software Applications (including version and number of instances)	CORE
Risk Assessment – Component		
Stmt #	**Sub-statement**	**Exam-level**

Stmt 4	**The information security risk assessment process includes the following:**	CORE
Stmt 4.1	Identification of reasonable and foreseeable threats to critical assets	CORE
Stmt 4.2	Documenting key or critical controls	CORE
Stmt 4.3	Testing the adequacy of identified key or critical controls	CORE
Stmt 4.4	Assessing the likelihood those threats may be exploited by a weakness or vulnerability	CORE
Stmt 4.5	Assessing the potential damage or impact from those threats if successfully exploited	CORE
Controls Testing – Component		
Stmt #	**Sub-statement**	**Exam-level**
Stmt 5	**The Independent testing of critical controls includes the following:**	CORE
Stmt 5.1	Information Technology Controls Audit	CORE
Stmt 5.2	Internal Vulnerability Scanning	CORE
Stmt 5.3	External Vulnerability Scanning	CORE
Stmt 5.4	Internal Penetration Testing	CORE
Stmt 5.5	External Penetration Testing	CORE
Stmt 5.6	Social Engineering Testing	CORE
Corrective Actions – Component		
Stmt #	**Sub-statement**	**Exam-level**
Stmt 6	**The process for tracking formal issues, exceptions, and/or corrective actions includes the following:**	CORE
Stmt 6.1	A process for resolving identified issues, exceptions and/or corrective actions	CORE
Stmt 6.2	Methods for tracking and reporting issues to resolution	CORE
Training – Component		
Stmt #	**Sub-statement**	**Exam-level**
Stmt 7	**The information security training program includes the following:**	CORE
Stmt 7.1	New Employee Training and background checks	CORE
Stmt 7.2	Employee training provided to all employees	CORE
Stmt 7.3	Incident response, current cyber threats, and emerging issues	CORE
Stmt 7.4	Social Engineering training such as phishing scams, pretexting, spear phishing	CORE
Stmt 7.5	Documented training records	CORE
Incident Response – Component		
Stmt #	**Sub-statement**	**Exam-level**
Stmt 8	**The incident response program includes the following:**	CORE
Stmt 8.1	Assessment of the nature and scope of an incident	CORE
Stmt 8.2	Measures to contain and control an incident	CORE

Stmt 8.3	Plans for identifying member information that has been accessed or misused	CORE
Stmt 8.4	Filing a timely Suspicious Activity Report (SAR), when applicable	CORE
Stmt 8.5	Prompt notification to the NCUA Regional Director, and/or State Supervisory Authority	CORE
Stmt 8.6	Notification to appropriate law enforcement authorities	CORE
Stmt 8.7	Notification of members when warranted	CORE
Third-Party Risk Management - Component		
Stmt #	**Sub-statement**	**Exam-level**
Stmt 9	**Third party management process includes the following:**	CORE
Stmt 9.1	Maintain a vendor management policy	CORE
Stmt 9.2	A process for performing due diligence	CORE
Stmt 9.3	Maintaining a listing of all critical vendors and contracts	CORE
Stmt 9.4	Appropriate information security measures within service provider contracts	CORE
Business Continuity / Disaster Recovery – Component		
Stmt #	**Sub-statement**	**Exam-level**
Stmt 10	**The Disaster Recovery / Business Continuity program includes the following components:**	CORE
Stmt 10.1	Backup and recovery plans for critical systems and services in the event of a disaster or incident	CORE
Stmt 10.2	A process of identifying the potential impact of disruptive events to an entity's functions and processes (Business Impact Analysis)	CORE
Stmt 10.3	Methods for training and testing contingency plans	CORE
Stmt 10.4	Reports to the Board on the status of the business continuity program and/or results from testing	CORE
Vulnerability & Patch Management – Component		
Stmt #	**Sub-statement**	**Exam-level**
Stmt 11	**The patch management process includes the following:**	CORE
Stmt 11.1	Patching schedules	CORE
Stmt 11.2	A process for applying patches in a timely manner	CORE
Stmt 11.3	A process that produces and reviews reports of missing security patches	CORE
Anti-Virus / Anti-Malware Component		
Stmt #	**Sub-statement**	**Exam-level**
Stmt 12	**Anti-virus/Anti-Malware controls include the following:**	CORE
Stmt 12.1	Workstations/Servers receive automatic updates	CORE
Stmt 12.2	Active alerting functions	CORE
Stmt 12.3	Antivirus reporting	CORE

Access Controls– Component		
Stmt #	**Sub-statement**	**Exam-level**
Stmt 13	**Limiting access to sensitive information and systems includes the following:**	CORE
Stmt 13.1	The use of unique passwords following industry best practices	CORE
Stmt 13.2	A process to ensure inactive user accounts are disabled	CORE
Stmt 13.3	Periodic user access reviews	CORE
Network Security – Component		
Stmt #	**Sub-statement**	**Exam-level**
Stmt 14	**Network defense and perimeter devices include the following:**	CORE
Stmt 14.1	The use of firewalls to prevent unauthorized access into or out of a computer network	CORE
Stmt 14.2	Intrusion Prevention/Detection System(s) to monitor a network for malicious activity	CORE
Data Leakage Protection – Component		
Stmt #	**Sub-statement**	**Exam-level**
Stmt 15	**Email and internet browser controls include the following:**	CORE
Stmt 15.1	The use of only fully supported browsers and email clients are allowed	CORE
Stmt 15.2	Web content filtering	CORE
Stmt 15.3	Email server anti-malware protections are deployed, such as inbound attachment scanning	CORE
Stmt 15.4	Blocking unnecessary file types from entering the email gateway	CORE
Change & Configuration Management – Component		
Stmt #	**Sub-statement**	**Exam-level**
Stmt 16	**The process for making changes to information assets include the following:**	CORE
Stmt 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.	CORE
Stmt 16.2	Procedures to document requests and approvals	CORE

CORE+

CORE+ Statements	
Information Security Program – Assessment Factor	
Policies & Procedures - Component	
Statement / Sub-statement	**Exam-level**
The credit unions written information security Policies/Procedures/Plans:	CORE+
Delineate clear lines of responsibility and communicate accountability for information security	CORE+
Describe board, management, and staff training on the information security program	CORE+
Document how information systems are monitored for intrusions	CORE+
Establish appropriate policies, standards, and procedures to support the program	CORE+
Demonstrate policies are adjusted over time to compensate for changes to the program	CORE+
Governance - Component	
Statement / Sub-statement	**Exam-level**
The annual report to the Board on the overall status of the information security program includes the following:	CORE+
Overseeing the risk mitigation activities that support the information security program	CORE+
Implementing a risk acceptance process	CORE+
Approving risk thresholds relating to information security threats or incidents	CORE+
Monitoring reports related to patching, vulnerability management, or other areas	CORE+
Asset Inventory - Component	
Statement / Sub-statement	**Exam-level**
The inventory of information assets (software/hardware) includes the following:	CORE+
Accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process sensitive member data	CORE+
Process to track and report on end-of-life and end-of-support information assets	CORE+
Process to detect unauthorized assets	CORE+
Active discovery tools to identify assets connected to the enterprise's network	CORE+
Passive discovery tool to identify assets connected to the enterprise's network	CORE+
Allowlist for Authorized Software	CORE+
Technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, .so, etc., files are allowed to load into a system process	CORE+
Establish a process to ensure software version control across the environment	CORE+
Risk Assessment - Component	

Statement / Sub-statement	Exam-level
The information security risk assessment process includes the following:	CORE+
Use of threat modeling to better understand the nature, frequency, and sophistication of threats	CORE+
Defines inherent and residual risk ratings	CORE+
Measuring risk using qualitative, quantitative, or a hybrid of methods considering lost revenue, data recovery and reconstruction expense, costs of litigation and potential judgments, loss of market share, and increases to premiums or denials of insurance coverage	CORE+
Processes and procedures in place to identify and maintain a catalog of relevant vulnerabilities	CORE+
Mapping threats and vulnerabilities to risk and identifying potential areas for mitigation	CORE+
Updating risk assessments regularly, and as changes occur, to address new technologies, products, services, and connections before deployment	CORE+
Recipients of IT risk reports have the authority and responsibility to act on the reported information	CORE+
Identification of data processing and storage utilizing cloud environments	CORE+
Risk mitigation actions are identified and implemented	CORE+
A risk assessment process to describe and analyze the risks inherent in each line of business	CORE+
Number of risk issues identified for IT activities (updated regularly to reflect new or mitigated issues). This may include information gathered through the threat intelligence and collaboration process.	CORE+
Number of risk acceptance issues approved by the board or designated committee	CORE+

Controls Testing - Component	
Statement / Sub-statement	**Exam-level**
The Independent testing of critical controls includes the following:	CORE+
Establish and maintain a penetration testing program appropriate to the size, complexity, and maturity of the enterprise	CORE+
Testing wireless controls	CORE+
A formal audit plan and schedule for testing critical controls	CORE+
Penetration testing program scope includes network, web application, Application Programming Interface (API), hosted services, and physical premise controls	CORE+
Tracking the total number of current or outstanding (i.e., unresolved) issues identified by the business unit, internal audit, external audit, or regulator	CORE+
Application penetration testing conducted on internally developed applications, or results of testing received from third party developers	CORE+
Corrective Actions - Component	
Statement / Sub-statement	**Exam-level**
The process for tracking formal issues, exceptions, and/or corrective actions includes the following:	CORE+
Number of current and historical events or issues (external and internal events that deviate from the control standards)	CORE+
Penetration testing program characteristics include remediation, such as how findings will be routed internally; and retrospective requirements	CORE+
Issues which are not resolved timely or accepted are documented in the risk assessment	CORE+
_Corrective Actions - Component	
Statement / Sub-statement	**Exam-level**

The information security training program includes the following:	CORE+
Training staff on authentication best practices	CORE+
Member security awareness materials	CORE+
Annual board member training	CORE+
Staff are trained on data leak prevention best practices	CORE+
Staff are trained to recognize and report security incidents	CORE+
Role-specific security awareness and skills training	CORE+
Credit union officials are required to attend security awareness training	CORE+
Incident Response - Component	
Statement / Sub-statement	**Exam-level**
The incident response program includes the following:	CORE+
A response team with assigned roles and responsibilities	CORE+
Incident response plans and capabilities	CORE+
Mechanisms for communicating during incident response	CORE+
Procedures for responding to incidents that occurred at the vendor	CORE+
Procedures to establish and maintain security incident thresholds	CORE+
Data recovery practices sufficient to restore systems to a pre-incident and trusted state	CORE+
Conducting routine incident response exercises	CORE+
Conducting post-incident reviews	CORE+
Tracking action items that come from lessons learned (either from real life incidents or testing)	CORE+
Third-Party Risk Management - Component	
Statement / Sub-statement	**Exam-level**
Third party management process includes the following:	CORE+
Notification of any information security or business continuity incident in a timely manner	CORE+
Frequency, format, and specifications of the service or product to be provided	CORE+
The process for managing and overseeing critical third-party technology service providers	CORE+
Monitoring information security measures at service providers, including reviewing audits, summaries of test results, or other equivalent evaluations	CORE+
Contracts address adequate and measurable service level agreements (SLAs)	CORE+
Third parties comply with all applicable laws, regulations, and regulatory guidance	CORE+
Contracts address insurance coverage to be maintained by the third party	CORE+
Vendor Risk Assessment	CORE+
Review of vendor financial information	CORE+
Contracts address authorization for the institution to monitor and periodically review the third party for compliance with its agreement	CORE+
Contracts address independent validation of security controls	CORE+

Contracts include a software escrow clause	CORE+
Review of the contract by legal counsel	CORE+
Obtaining and reviewing reports for periodic independent security reviews, such as System and Organization Control (SOC) reports, for service providers that host sensitive information or critical systems	CORE+
Timely and effectively addressing any material exceptions cited in periodic independent security reviews, such as System and Organization Control (SOC) reports, for service providers that host sensitive information or critical systems	CORE+
Verifying the credit union's performance of complementary user entity controls defined in periodic System and Organization Control (SOC) reports for service providers that host sensitive information or critical systems	CORE+
Business Continuity / Disaster Recovery - Component	
Statement / Sub-statement	**Exam-level**
The Disaster Recovery / Business Continuity program includes the following components:	CORE+
Data centers are redundant and appropriately separated	CORE+
Network equipment, connectivity, and communication needs, including entity-owned and personal mobile devices	CORE+
Prioritization and procedures to recover functions, services, and processes	CORE+
Exercises and tests related to interaction with the core and significant firms/vendors	CORE+
Reciprocal agreements with other businesses/institutions for recovery	CORE+
A risk assessment to determine critical systems	CORE+
A written plan addressing persons with authority to enact the plan, preservation and ability to restore vital records, methods for restoring critical member services, communication methods for employees and members, notification of regulators, training, and testing	CORE+
Internal controls for reviewing the plan at least annually	CORE+
Vulnerability & Patch Management - Component	
Statement / Sub-statement	**Exam-level**
The patch management process includes the following:	CORE+
Patch aging reports that show vulnerability release and remediation date	CORE+
A patch exception practice exists that includes risk assessing and monitoring patch exceptions	CORE+
Credentialed vulnerability scans are conducted internally	CORE+
Reports of missing security patches, including misconfigurations	CORE+
Operating system and application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis	CORE+
Maintaining a documented vulnerability management process	CORE+
Processes for patching databases and monitoring whether the patch level of the production database is up to date	CORE+
Process to ensure firmware is appropriately updated	CORE+
Automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis	CORE+
Automated vulnerability scans of externally exposed enterprise assets	CORE+
Process to remediate detected vulnerabilities in software on a monthly, or more frequent, basis	CORE+
Anti-Virus / Anti-Malware - Component	
Statement / Sub-statement	**Exam-level**
Anti-virus/Anti-Malware controls include the following:	CORE+

Centrally manage anti-malware software	CORE+
Behavior-based anti-malware software	CORE+
Anti-exploitation features on enterprise assets and software enabled, where possible	CORE+
Hardware-based roots of trust, which use cryptographic means to verify the integrity of software	CORE+
Application sandboxing	CORE+
Removable media is restricted and scanned for anti-malware upon use	CORE+
Blacklists that disallow code execution based on code fragments, Internet locations, and other factors that correlate with malicious code	CORE+
Systems with antimalware are up to date and checking in at least weekly prior to accessing network resources	CORE+
Endpoint detection and response (EDR) solution that uses software agents or sensors installed on endpoints to capture data, which is sent to a centralized repository for analysis	CORE+
Managed detection and response (MDR) solution that provides endpoint security 'as a service' through a dedicated, experienced security team	CORE+
Extended detection and response (XDR) solution that collects and correlates data from across the infrastructure	CORE+
Restricting the use of administrator accounts to conducting administrator activities	CORE+
Access Controls - Component	
Statement / Sub-statement	**Exam-level**
Limiting access to sensitive information and systems includes the following:	CORE+
Require the use of Multi-Factor Authentication (MFA) for high-risk users and for members accessing high-risk transactions	CORE+
Establish and maintain an inventory of the enterprise's authentication and authorization systems, including those hosted onsite or at a remote service provider	CORE+
Centralize access control for all enterprise assets through a directory service or SSO provider, where supported	CORE+
Restricting administrator privileges to dedicated administrator accounts on enterprise assets	CORE+
Physical and environmental controls	CORE+
Maintaining an inventory of service accounts	CORE+
Procedures are consistently followed for security the virtual environment	CORE+
A formal process to grant and remove access upon hire, role changes, or terminations	CORE+
Network Access Control software	CORE+
Role-based access control is maintained and reviewed periodically based on risk	CORE+
Access control for remote devices includes validating if the device security profile is up to date	CORE+
Requiring MFA for all externally facing applications or documents acceptance of risk	CORE+
Mobile device management solution required for users remotely connecting to the network using personal devices	CORE+
MFA is required for remote users, including vendors	CORE+
Appropriate encryption for remote user access	CORE+
Remote user access activity is appropriately logged and monitored	CORE+
All remove user access is reviewed and approved by appropriate personnel	CORE+
Vendors remote access is disabled when not in use	CORE+
Sharing of remote user accounts is prohibited	CORE+
Network Security - Component	

Statement / Sub-statement	Exam-level
Network defense and perimeter devices include the following:	CORE+
Maintaining accurate network diagrams	CORE+
Maintaining accurate data flow charts	CORE+
A secure boundary, identifying "trusted" and "untrusted" zones	CORE+
Firewall rules are periodically reviewed	CORE+
Tools used to enforce and detect perimeter protection include routers, firewalls, intrusion detection systems (IDS) and intrusion prevention systems, proxies, and gateways	CORE+
Network segregated into internal layers, including production, staging, and development environments	CORE+
Zones with a security policy appropriate to its use, ensuring that zone restrictions are defined by risk, sensitivity of data, user roles, and appropriate access to application systems	CORE+
Use of a network access control (NAC) solution that restricts network access to authorized devices that comply with specified security standards	CORE+
Configuring wireless access points connected to the internal network with professional-grade security controls, such as the use of WPA2-Enterprise (WPA-802.1X) with a RADIUS authentication server	CORE+
Data Leakage Protection - Component	
Statement / Sub-statement	**Exam-level**
Email and internet browser controls include the following:	CORE+
Secure file exchange methods (e.g., encryption, strong authentication)	CORE+
Enforcing restrictions on the use and storage of information on removable media	CORE+
File storage only on trusted servers when controlled by third-party service providers to avoid unauthorized access of the stored files and unapproved copies of the files	CORE+
Files only traverse trusted networks, to avoid unauthorized access (e.g., man-in-the-middle attacks or eavesdropping)	CORE+
Use of only approved and secure file exchange methods	CORE+
Cloud access security brokers (CASBs) for monitoring cloud-based file exchange and sharing capabilities	CORE+
Outbound email messages are screened for sensitive personally identifiable information	CORE+
Web filter prevents access to file sharing sites and web-based email	CORE+
Change & Configuration Management - Component	
Statement / Sub-statement	**Exam-level**
The process for making changes to information assets include the following:	CORE+
Policies, standards, and procedures categorize changes by severity and specify corresponding approval processes	CORE+
Configuration management process to securely maintain the institution's technology by developing expected baselines for tracking, controlling, and managing systems settings	CORE+
A process to remove all nonessential software programs, protocols, services, and utilities from the system	CORE+
Use of standard builds and documented configurations for information systems	CORE+
Defining rollback procedures in the event of unintended or negative consequences with the introduced changes	CORE+
Identified metrics (e.g., implementation time, success rates, and the number of planned versus unplanned changes) to track the efficiency and success of the change management process	CORE+

Documents that the change performs as intended, identifies any flaws (e.g., integrity issues), and verifies that the change integrates with other systems	CORE+
Perform a post-implementation review to verify that the change was implemented successfully and achieved performance objectives	CORE+
Monitoring - Component	
Statement / Sub-statement	**Exam-level**
Anomalous activity monitoring includes the following components:	CORE+
Monitoring Incoming network traffic	CORE+
Monitoring Outgoing network traffic	CORE+
Monitoring for Insider malicious activity	CORE+
Logs collected from key systems	CORE+
Logs are analyzed	CORE+
Centralized security event alerting and logging across enterprise assets for log correlation and analysis using tools such as Security Information and Event Management (SIEM)	CORE+
Tuning security event alerting thresholds monthly, or more frequently	CORE+
Port monitoring to identify unauthorized network connections	CORE+
Appropriate controls over wired and wireless networks	CORE+
A host-based intrusion detection solution on enterprise assets	CORE+
Traffic filtering between network segments, where appropriate	CORE+
Application layer filtering via a proxy, application layer firewall, or gateway	CORE+
Encryption on Wireless networks is appropriate	CORE+
Wireless networks are properly segmented between guest and internal network access	CORE+
Appropriate authentication standards for wireless networks are used (passwords, 802.1x)	CORE+
Logging - Component	
Statement / Sub-statement	**Exam-level**
Security logging and monitoring activities include the following components:	CORE+
Third-party vendor monitors log activity	CORE+
An audit log management process that defines the enterprise's logging requirements	CORE+
Configuring detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation	CORE+
Collect URL request, DNS query, and command-line audit logs on enterprise assets, where appropriate and supported	CORE+
Collect service provider logs, where supported	CORE+
Data Governance - Component	
Statement / Sub-statement	**Exam-Level**
Controls to identify, classify, securely handle, retain, and dispose of data include the following components:	CORE+
Policy or program established to maintain a data governance process	CORE+
Data Inventory established	CORE+
Data access list established	CORE+

Data retention enforced	CORE+
Data disposed of in accordance with its sensitivity	CORE+
Data is encrypted on end-user devices containing member sensitive data	CORE+
Sensitive data is encrypted at rest and in transit	CORE+
Remote wipe process in place on company or personal-owned portable devices	CORE+
Data management controls for safeguarding data in physical and digital form	CORE+
Documenting the types of data maintained, data owners and users, and purpose for reports	CORE+
Processes for controlling non-masked data in non-production environments	CORE+
Defined processes to remove or destroy data when no longer used in the data analytics tools	CORE+
Identifying data analytics processes used by the entity to comply with applicable laws and regulations (e.g., Bank Secrecy Act)	CORE+
Data oversight committee contain board and management representations from across the organization	CORE+
Oversight committee regularly reviews metrics which demonstrates the information security program is operating as intended	CORE+
Conversion - Component	
Statement / Sub-statement	**Exam-level**
The process to effectively manage and maintain a critical services core conversion includes:	CORE+
Formal project plan for converting the core system(s)	CORE+
Vendor/Third party maintaining formal project minutes and notes during conversion planning	CORE+
Formal post-conversion minutes/notes	CORE+
Tracking any outstanding material items or concerns post-conversion	CORE+
Adequate training by the vendor or management on the new systems and applications	CORE+
Formal project plan for converting the core system(s) to include testing timeframes	CORE+
Assigning appropriate skills and resources to the program based on the credit union's size and complexity	CORE+
Conversion plans include timelines for key processes and milestones such as data cleanup, data mapping, deconversion processes, integrated testing, mock conversions, reconciling control totals, mirrored transaction processing, and user acceptance testing	CORE+
Adequate resources are assigned to the conversion, including dedicated project managers and subject matter experts	CORE+
Where warranted, contract with third party experts for deconversion and conversion management or support	CORE+
Software Development Process - Component	
Statement / Sub-statement	**Exam-level**
A defined systems/software development life cycle process that includes:	CORE+
Establish and maintain a documented secure application development process	CORE+
A secure code repository and controls for checking code in and out	CORE+
Appropriate segregation of duties	CORE+
A process for root cause analysis evaluating underlying issues that create vulnerabilities in code	CORE+
An updated inventory of third-party components used in development	CORE+
Separate environments for production and non-production systems	CORE+
All software development personnel receive training in writing secure code for their specific development environment and responsibilities	CORE+

Applying static and dynamic analysis tools within the application life cycle to verify that secure coding practices are being followed	CORE+
A process to accept and address reports of software vulnerabilities, including providing a means for external entities to report	CORE+
Internal Audit Program - Component	
Statement / Sub-statement	**Exam-level**
The Internal Audit Program includes the following:	CORE+
An audit plan detailing internal audit's planning processes	
Audit work programs that set out for each audit area the required scope and resources	CORE+
Written audit reports informing the board and management of individual department or division compliance with policies and procedures	CORE+
Requirements for audit work paper documentation to ensure clear support for all audit findings and work performed	CORE+
Follow-up processes that require internal auditors to determine the disposition of any agreed-upon actions to correct significant deficiencies	CORE+
Professional development programs to be in place for the institution's audit staff to maintain the necessary technical expertise	CORE+
Due Diligence - Component	
Statement / Sub-statement	**Exam-level**
Managing third-party relationships in a sound manner	CORE+
The credit union's vendor risk assessment considers the factors identified under the Planning/Risk Assessment Section of the Job Aid: Third-Party Relationships	CORE+
The credit union evaluated the costs of monitoring and providing support to the third party program (i.e., staffing, capital expenditures, communications, and technological investment)	CORE+
The credit union's strategic business plan includes measurable and achievable goals, and clearly defines levels of authority and responsibility related to the third party arrangement	CORE+
The credit union performed and documented a cost-benefit financial analysis to determine if it is receiving sufficient reward for the risk associated with the proposed relationship	CORE+
The credit union considered more than one third party before entering into a relationship	CORE+
The credit union considered the third party's experience or legal concerns with providing the proposed service or program	CORE+
The third party relationship(s) compliment the credit union's overall mission and philosophy	CORE+
The credit union understands the third party's business model	CORE+
The credit union understands the vendor's sources of income and expense and considered any conflicts of interest that may exist between the third party and the credit union	CORE+
The credit union's analysis of the financial statements of the third party and its affiliates provides reasonable assurance that the third party has the ability to fulfill the contractual commitments proposed	CORE+
The credit union's third-party contract(s) address the Due Diligence – Contract Issues and Legal Review areas in the Job Aid: Third-Party Relationships	CORE+
The credit union obtained an independent legal opinion about any services provided by the third party under the arrangement	CORE+
The credit union verified the third party's compliance with state and federal laws and regulations and is contractually bound to comply with applicable laws (i.e., Regulation B, Regulation Z, HMDA, Bank Secrecy Act/Anti-Money Laundering (BSA/AML), etc.)	CORE+

The credit union has an adequate accounting infrastructure to appropriately track, identify, and classify transactions in accordance with GAAP	CORE+
Reports are prepared on a monthly basis; adequately reflect the activity with the third party, and provide sufficient information to properly monitor the activities	CORE+
Senior management or the board of directors receives informative risk summary reports on the third-party or firms providing the outsourced services	CORE+
Appropriate credit union staff assigned to oversee the third-party relationship to monitor performance and compliance with contracts	CORE+
If the third party originates member transactions, the credit union verifies the transactions with the member	CORE+
When the third party services member accounts, the credit union receive periodic reports on that activity	CORE+
The credit union controls the issuance and receipt of all member account verifications	CORE+
The credit union verifies third party's reports are accurate	CORE+
When the third party services loans, the credit union verifies that member payments are remitted to the credit union in compliance with the contract	CORE+
The credit union has the infrastructure (staffing, equipment, technology, etc.) in place to sufficiently monitor the third-party arrangement	CORE+
The credit union established appropriate internal controls to ensure internal staff is following policy guidance for third-party relationships	CORE+
The credit union's policies appropriately address the third-party relationship	CORE+
Credit union policies place limits on the activity of the third parties	CORE+
The credit union maintains an established list of approved parties	CORE+
The credit union transmits member data between themselves and the third party in a secure manner (encrypted email, secure fax, via encrypted tapes, virtual private network with secured files, etc.)	CORE+
CISA Ransomware Readiness Assessment (RRA)	
Statement / Sub-statement	**Exam-Level**
CISA RRA (BASIC Practices)	CORE+
Are important systems and data backed up daily to an offsite location with the ability to restore multiple versions back at least 30 days?	CORE+
Are data backups tested annually?	CORE+
Is malicious web content being blocked using DNS filtering via methods like DNS resolvers and DNS firewalls?	CORE+
Are web browser security settings managed?	CORE+
Are annual tabletop exercises that include phishing response scenarios conducted?	CORE+
Are users trained to recognize cyber threats like phishing?	CORE+
Is email filtered to protect against malicious content?	CORE+
Is perimeter network traffic monitored?	CORE+
Have the organization's hardware and software assets been inventoried and is the inventory managed?	CORE+
Has the organization removed all unsupported hardware and software from its operating environment?	CORE+
Are documented and approved secure configurations used to manage the organization's hardware and software assets?	CORE+
Is all public-facing software patched for vulnerabilities within 15 days for vulnerabilities rated as "Critical" and 30 days for vulnerabilities rated as "High"?	CORE+

Are all internal-facing software and firewalls patched for vulnerabilities within 30 days for both vulnerabilities rated as “Critical” and for vulnerabilities rated as “High”?	CORE+
Are strong and unique passwords implemented throughout the entire organization?	CORE+
Is the principle of least privilege enforced through policies and procedures?	CORE+
Is there a list of known bad software (a “Blocklist”), and is the software on that list being blocked?	CORE+
Has the organization developed an incident response plan?	CORE+
Does the organization conduct annual incident response tabletop exercises that include ransomware response scenarios?	CORE+
CISA Ransomware Readiness Assessment (RRA)	
Statement / Sub-statement	**Exam-level**
CISA RRA (INTERMEDIATE Practices)	CORE+
Are important systems and data backed up daily to an offsite location with the ability to restore multiple versions back at least 30 days?	CORE+
Are data backups tested annually?	CORE+
Is malicious web content being blocked using DNS filtering via methods like DNS resolvers and DNS firewalls?	CORE+
Are web browser security settings managed?	CORE+
Are annual tabletop exercises that include phishing response scenarios conducted?	CORE+
Are users trained to recognize cyber threats like phishing?	CORE+
Is email filtered to protect against malicious content?	CORE+
Is perimeter network traffic monitored?	CORE+
Is internal network traffic monitored?	CORE+
Are networks segmented to protect mission critical assets?	CORE+
Have the organization’s hardware and software assets been inventoried and is the inventory managed?	CORE+
Has the organization removed all unsupported hardware and software from its operating environment?	CORE+
Are documented and approved secure configurations used to manage the organization’s hardware and software assets?	CORE+
Does the organization detect rogue hardware and alert key stakeholders?	CORE+
Are standard baseline images used to control hardware and software configurations?	CORE+
Is all public-facing software patched for vulnerabilities within 15 days for vulnerabilities rated as “Critical” and 30 days for vulnerabilities rated as “High”?	CORE+
Are all internal-facing software and firewalls patched for vulnerabilities within 30 days for both vulnerabilities rated as “Critical” and for vulnerabilities rated as “High”?	CORE+
Are all software and firewalls patched for vulnerabilities within 15 days for vulnerabilities rated as “Critical” and 30 days for vulnerabilities rated as “High”?	CORE+
Are strong and unique passwords implemented throughout the entire organization?	CORE+
Is the principle of least privilege enforced through policies and procedures?	CORE+
Is least privilege enforced through technical (technology based) restrictions?	CORE+
Are audit logs maintained for all privileged (e.g. system administrator) accounts?	CORE+
Is two-factor authentication implemented for all privileged (e.g. system administrators) and remote users	CORE+
Is rogue hardware being detected?	CORE+
Is there a list of known bad software (a “Blocklist”), and is the software on that list being blocked?	CORE+
Has the organization documented a list of known approved software (an “Allowlist”)?	CORE+
Is the Allowlist organized by software publisher, and is that list used to allow only approved software to run on organizational systems?	CORE+

Has the organization developed an incident response plan?	CORE+
Does the organization conduct annual incident response tabletop exercises that include ransomware response scenarios?	CORE+
Are cybersecurity incidents reported and escalated to the appropriate stakeholders?	CORE+
Have disaster recovery procedures been developed?	CORE+
Are incident response tabletop exercises performed at least twice a year?	CORE+
Is a physical incident response exercise performed at least once a year?	CORE+
Has the organization implemented redundant systems where appropriate for the purpose of resiliency?	CORE+
Does the organization perform business impact assessments?	CORE+