# "Top Ten" IT Exam Scope, Procedures and Recommendations

## Non-Technical Controls

### 1. Does the Credit Union perform required and appropriate risk assessments?

**Description:** Credit unions must have a documented Member Information Security Risk Assessment and Online/Mobile Banking Risk Assessment. (DDoS, Social Media and Technology Specific risk assessments are required by guidance but are not included in this Top Ten list.)

The Member Information Security Risk Assessment must document:

a) Reasonably foreseeable internal and external threats to member information,
b) The controls designed to address the threat, and
c) The impact and likelihood of the threat given the controls and their effectiveness, and
d) A conclusion on the sufficiency of controls.

The Online/Mobile Banking Risk Assessment must document:

e) The capabilities of the online and mobile banking systems (high risk capabilities must be identified)
f) The threats associated with these systems,
g) The controls performed or enforced by the credit union that are designed to address the threats,
h) The controls performed by the member that are designed to address the threats, and
i) A conclusion on the sufficiency of controls.

**Credit Union Size:** Both smaller and larger credit unions must have these risk assessments.

**How to Examine:** **E**ither review a third-party audit report (expert) or perform your own review:

- Review the risk assessments to ensure they include the above described components
- Review the risk assessments to ensure they have been updated as threats and systems have changed over time.
- Ensure basic controls such as anti-virus and strong password requirements are represented in the Member Information Security Risk Assessment.
- Ensure strong authentication practices are required for higher risk capabilities.
- Ask to see evidence that the credit union is communicating any member responsibilities for online/mobile banking security.

**Common Exceptions:** None.

**References:** 12CFR Part 748, Appendix A III.B.1-3., NCUA Letter 05-CU-18, NCUA Letter 11-CU-09, FFIEC IT Examination Handbook

**Proposed Language for Deficiency:** The Credit Union must perform the required risk assessments in a manner that is compliant with guidance and these risk assessments must be kept current and accurate. *Describe deficiency here.*

**Advanced:** The Member Information Security Risk Assessment is intended to identify all the key controls necessary to protect member information. An advanced examination will map the controls identified in the Risk Assessment to the controls tested through IT audits and security assessments. All key controls in the Risk Assessment must be tested to ensure the control is operating as intended. The most robust Risk Assessment's include the frequency of testing, identification of who tested (3rd party, Internal Audit, etc.) and the results of testing. In addition, additional controls to consider are identified and when residual risk has been accepted it denotes at what level of management risk was accepted.

## 2. Does the Credit Union regularly test key controls?

**Description:** Credit unions must test key technical, administrative and physical controls designed to protect member information. These controls are often identified in the credit union's Member Information Security Risk assessment. When this Risk Assessment is deficient, the controls tested can be based upon best practices.

Controls testing must include technical testing such as vulnerability scanning, penetration testing, and employee social engineering. Controls testing must also include a general computer controls review of business continuity planning, vendor management, information security practices, risk assessments, and Board oversight. Many of these controls can only be tested onsite. Testers must be competent and independent.

**Credit Union Size:** Both smaller and larger credit unions must test their key controls. An exam does not fulfill this requirement. The scope and frequency of testing should align with the credit union size and complexity. Generally speaking, any credit union over $100M in assets should perform annual testing. Smaller credit unions could perform testing every other year. When significant changes are made the associated controls should be tested.

**How to Examine:** Review a third-party audit report:

- Verify the scope of testing is appropriate.
- Verify that findings are tracked and the Board ensures reasonable progress toward remediation.

**Common Exceptions:** None.

**References:** 12CFR Part 748, Appendix A III.C.3., FFIEC IT Examination Handbook

**Proposed Language for Deficiency:** The Credit Union must perform regular testing of key technical, administrative and physical security controls. Testing should generally be at least annually and when significant changes occur.

**Advanced:** None

## 3. Does the Credit Union have an effective incident response plan?

**Description:** Credit unions must have an incident response plan that describes the actions to be taken during a computer security incident. The plan should also provide documentation requirements.

Every credit union is likely to have computer security incidents. The credit union must be prepared to respond in a methodical manner that will minimize the impact and duration of the incident.

An incident response plan should document expected practices for incident reporting, initial analysis, triage, response, remediation and communications. Staff and consultants should have defined roles.

The credit union should practice incident response using table-top exercises.

The incident response plan should include specific practices to be performed for malware incidents and reported vendor breach.

**Credit Union Size:** Both smaller and larger credit unions should have an incident response plan.

**How to Examine:** Review a third-party audit report or perform your own review:

- Review a copy of the plan and ensure it contains all components described in 12CFR748 Appendix B.
- Review documentation from past incidents. If no incidents are documented, try and identify incidents that should have been documented.

**Common Exceptions:** None.

**References:** 12CFR Part 748, Appendix B, FFIEC IT Examination Handbook

**Proposed Language for Deficiency:** The Credit Union must have an effective and tested computer security incident response plan. The plan should designate roles, actions and communication expectations.

**Advanced:** None

## 4. Does the Credit Union have an effective business continuity plan?

**Description:** Credit unions must have a business continuity plan that is reasonably certain to allow continued operations despite a continuity event. Business continuity planning includes backups, recovery testing, business impact analysis (determination of critical business processes and systems), strategy, documentation and testing.

Credit unions must be able to reliably restore systems regardless of the time of failure. Timely backups and backup restoration testing is critical. Backups should be encrypted if offsite.

A business impact analysis should be performed at least every 24 months. The analysis identifies critical processes and the systems that support the processes. The BIA documents the maximum acceptable downtime for key systems.

Recovery strategies ensure systems can be reliably restored within the maximum acceptable downtime.

Business continuity plans must be kept up-to-date.

Testing should entail the recovery of key systems, the recovery of key processes and scenario based table-top testing. A testing plan should document a schedule for testing that ensures all critical components are regularly tested.

**Credit Union Size:** Both smaller and larger credit unions must perform business continuity planning. The technologies used typically vary according to the size of the credit union but the requirement for planning is consistent.

**How to Examine:** Review a third-party audit report or perform your own review:

- Obtain a listing of key systems and processes as identified in the business impact analysis.
- Obtain evidence that all key systems are regularly backed up and that recovery has been tested within the last three years.
- Review the BCP testing schedule and recent test results. Test failures are acceptable but actions must be timely to correct failures.

**Common Exceptions:** None; however, if relying upon a 3rd party for contingency purposes the Credit Union must ensure the 3rd party is regularly testing systems. This would fall under appropriate Vendor Management.

**References:** 12CFR Part 749, Appendix B., FFIEC IT Examination Handbook

**Proposed Language for Deficiency:** Business continuity planning and backups must be performed in a manner that ensure reliable recovery from a continuity event. *Cite the deficient condition…*

**Advanced:** None

## 5. Does the Credit Union have an effective vendor management program?

**Description:** Credit unions must ensure vendors protect member information. The key components of a vendor management program are selection, contracting and ongoing monitoring.

Vendor selection should be based, in part, on the vendor's demonstrated record for protecting sensitive information. The ability to protect information is generally represented in an attestation report known as a SSAE16 or SOC2. Vendors systems should meet the credit unions security requirements.

Contracting must require vendors to protect member information in a manner that is consistent with the GLB Act. Breach disclosure should be contractually specified. And vendors should be contractually required to support up-to-date systems.

Ongoing monitoring is generally represented in an attestation report known as a SSAE16 or SOC2. Credit union personnel must ensure the scope of the attestation audit matches credit union requirements and that any noted exceptions are acceptable to the credit union.

**Credit Union Size:** Both smaller and larger credit unions must manage vendors.

**How to Examine:** Review a third-party audit report or perform your own review:

- Obtain a list of vendors with routine custody of member information.
- Review vendor selection documentation for these vendors to ensure security and BCP requirements were evaluated.
- Review contracts to ensure they contain information protection language, breach disclosure provisions, and support for current systems.
- Ensure new attestations are reviewed every 12 to 18 months.

**Common Exceptions:** None.

**References:** 12CFR Part 748, Appendix A III.D.1-3., FFIEC IT Examination Handbook

**Proposed Language for Deficiency:** An effective vendor management program must be in place and must ensure vendors are selected based upon their ability to protect member information, contractually obligated to protect information, and regularly montitored.

**Advanced:** None

## 6. Does the Credit Union Board effectively oversee IT and Information Security?

**Description:** The Board or a designated committee is required to oversee the IT area and the information security program. The Board (or committee) must ensure the following is performed in a manner that is compliant with regulations:

a) A written Information Security Program is present, up-to-date and approved.
b) Specific responsibility for information security is assigned to an individual or committee.
c) IT and Information Security Policies and Standards are appropriate and updated.
d) Security Breaches or attempted breaches are documented and reviewed.
e) The IT Strategic Plan aligns IT with the business objectives of the credit union.
f) All personnel receive appropriate security awareness training.
g) The Member Information Security Risk Assessment is compliant and regularly updated. The controls identified in the risk assessment are tested at least annually.
h) The Business Continuity Plan is reasonably effective and Testing Results demonstrate the ability of the credit union to maintain critical operations despite a continuity event.
i) An Incident Response Plan is appropriate and incidents are consistently documented.
j) Vendor Management is performed in a compliant manner.

The Board or management must also approve policy and standard exceptions. Exceptions should be regularly revisited.

**Credit Union Size:** Both smaller and larger credit unions must have effective Board oversight.

**How to Examine:** Review a third-party audit report or perform your own review:

- Review Board or Committee meeting minutes to ensure all of the above is performed in a manner that represents Board or committee oversight.
- Attend a Board or committee meeting if possible. Ensure IT oversight receives adequate attention.

**Common Exceptions:** None.

**References:** 12CFR Part 748, Appendix A III.A.1., FFIEC IT Examination Handbook

**Proposed Language for Deficiency:** The Credit Union Board or a designated committee must effectively oversee the IT area and the information security program. *Cite the specific deficiency.*

**Advanced:** None

## Technical Controls

### 7. Does the Credit Union have a properly configured Firewall(s)?

**Description:** A firewall is the primary defensive mechanism separating the internal network from other networks. Firewall(s) should be in place between the internal network and all external networks. Firewalls are generally configured by default to block all traffic. Rules are then added to the firewall configuration to allow only the traffic that is necessary. Management should be able to provide evidence that the firewall is properly configured.

**Credit Union Size:** Both smaller and larger credit unions have firewalls. A smaller credit union may have only one. Larger credit unions will have several, some designed to provide protection from Internet based traffic and some designed to provide protection from vendor networks.

**How to Examine:** Either review a third-party audit report (expert) or perform your own review:

- Ask to be physically shown the firewall
- Ask to see evidence of professional configuration of the firewall rules

**Common Exceptions:** Sometimes Core Banking System Providers will not allow a firewall between the internal network and the provider's network. Smaller credit unions will not be able to force a vendor to allow a firewall.

**References:** 12CFR Part 748, Appendix A III.C.1., FFIEC IT Examination Handbook

**Proposed Language for Deficiency:** Firewall(s) must be present to protect the internal network from unauthorized access that would originate from any external network. Firewalls must be configured by default to block all traffic and must have specific rules to allow only the traffic that is necessary. Firewall logging must be enabled and logs should be kept for 180 days.

**Advanced:** Firewalls must have rules defined that permit traffic based upon the source/destination of the traffic and its type. For example, email traffic should be permitted by a rule to come from anywhere (Any) to the email server. Specific rules are much better than generic rules. Specific firewall rules help prevent the unintended transmission of sensitive information. For example, adding a rule that allows files to be transferred to specific approved destinations is much better than adding a rule that allows file transfers to any destination.

Firewalls should also write log records for access changes, file transfers and other activities deemed higher risk.

An advanced examination will review the firewall rules to be sure they are as specific as possible and that there is a justified business case for the rules that permit traffic.

## 8. Does the Credit Union keep Systems up-to-date and resilient to attack?

**Description:** Systems must be kept updated with patches/updates to be sure they operate as efficiently and effectively as possible. Missing updates can lead to compromise of the system. Generally speaking, updates should be applied within 30 to 45 days from release by the vendor.

Once a vendor deems a system as 'end-of-life' the vendor will no longer provide updates. Examples of end-of-life systems include those running Windows XP or Windows NT.

Systems categories include laptops/workstations, servers, mainframes, routers, switches, firewalls and mobile devices. Each vendor will supply the updates for the systems they sell.

Workstations/laptops and servers will have both operating system patches/updates and application patches/updates. Application patches address Java, Adobe Reader and similar applications.

**Credit Union Size:** Both smaller and larger credit unions must apply updates/patches. Larger credit unions will have more complex change requirements and testing procedures.

**How to Examine:** Either review a third-party audit report (expert) or perform your own review:

- Ask to be shown reports listing all patches/updates that are not yet applied to each category of system. Include laptops/workstations, servers, routers and firewalls in your examination.
- Exclude those patches released in the last 45 days.
- Ask for written documentation explaining why updates/patches older than 45 days are not applied.
- Ask to see a report from an internal vulnerability scan. Reconcile the scan results showing missing patches to ensure management is addressing updates identified by vulnerability scanners. Note, vulnerability scanners (when run with admin access) generally produce more accurate reporting than other systems tools.

**Common Exceptions:** Some patches/updates can cause compatibility issues. If patches are excluded for this reason they should be well documented and regularly revisited.

**References:** 12CFR Part 748, Appendix A III.C.1., FFIEC IT Examination Handbook

**Proposed Language for Deficiency:** All systems must be updated and patched to the latest version that is supported by the vendor. This helps to ensure that security vulnerabilities are addressed. If a system is at "end-of-life" should be replaced.

**Advanced:** None; however, those that are most successful have transitioned from patch management to vulnerability management which includes reconciliation between the patching console and vulnerability scan results.

## 9. Does the Credit Union configure systems to generate log records and provide timely reports showing concerning activities?

**Description:** Systems of all types are capable of generating activity logs. These activity logs can be used to generate alerts following certain activity or for investigation purposes. This system that records and analyzed log data is generally known as a Security Information and Event Management (SIEM) system. Log records can be analyzed with or without a commercial SIEM product.

The log records that tend to be most useful include successful or unsuccessful login, access failure, access administration, admin account activity, disabling of controls, installation of software, connection of hardware to the network, and file transfers of any type.

Suspicious activity should result in an alert. The following events should result in an alert to management within 30 to 60 minutes:

a. Installation of unauthorized software.
b. Connection of unknown hardware to the network.
c. File transfer to an external destination.
d. Admin account creation or modification and Admin activity performed from non-IT systems.
e. Consecutive unsuccessful logins from the same account at more than one location.
f. Disabling of controls such as anti-virus, firewalls, logging.

**Credit Union Size:** Both smaller and larger credit unions must generate log records as recommended. Smaller credit unions generally retain just 90 days of logs and have less sophisticated alerts and reports. Larger credit unions should aggregate log records to a central and more secure server, aka a log aggregation server, and should retain 365 days of log records.

**How to Examine:** Either review a third-party audit report (expert) or perform your own review:

- Select a sample of systems (3 to 20) and ask to see the configuration settings on the system that defines the log records created, the forwarding of the log records to a SIEM, and the retention period for log records.
- Ask to see a list of the alerts and reports that are generated out of the SIEM.
- Ask to see proof that each of the events noted above would result in an alert.
- With permission and cooperation from the credit union, ask staff to login with an admin account on a branch network and observe the corresponding alert.

**Common Exceptions:** None

**References:** 12CFR Part 748, Appendix A III.C.1., FFIEC IT Examination Handbook

**Proposed Language for Deficiency:** Systems must generate log records for activities that could be considered suspicious. The log records must be retained for a reasonable period of time, 90 days for smaller credit unions and 365 days for larger credit unions. Log records must be analyzed for suspicious activities and timely alerts must be generated when suspicious activity occurs.

**Advanced:** A SIEM should not be confused with an Intrusion Prevention System (IPS). IPS is a complementary control that monitors a network for patterns of network traffic that are associated with known attacks. IPS does not rely on system logs and does not provide the same capability. Larger credit unions tend to have SIEM systems and IPS systems.

An advanced examination will verify that IPS systems are reliably alerting management to attack patterns. The best way to examine this is to review the alerting that occurred during the last penetration test.

## 10. Does the Credit Union protect administrative accounts?

**Description:** In a Windows environment there are two types of administrative accounts; domain administrator and local administrator. Domain administrators can control all windows systems while local administrators can only control the one system they are associated with.

IT personnel are often granted domain administrator privileges on one account and regular 'user' privileges on another account. In this situation, IT personnel should only use their admin account when necessary. Regular work activity that does not require admin privileges should be performed with the user account.

The total number of domain admin accounts should be as limited as feasible. Domain admin accounts must have complex and lengthy passwords (15+ characters).

Each system has a local admin account. This account is generally used to make changes when a domain admin account is not working. Many organizations share a common password for all local admin accounts. But if one is compromised all systems are compromised. Organizations that find it necessary to use common passwords should do so by system type. In other words, laptops should share a common password, workstations should share another, external servers should share a third and internal servers a fourth. Etc.

Users should not be granted local admin privileges.

**Credit Union Size:** Both smaller and larger credit unions must protect admin accounts. Smaller credit unions typically have 3 to 5 domain admin accounts. Larger credit unions may have 5 to 20 depending on the number of IT staff and 'service' accounts (accounts that are not assigned to a human but perform automated management tasks).

**How to Examine:** Either review a third-party audit (expert) or perform your own review:

- Review a report listing all Domain Admin accounts. Verify that all accounts are either assigned to a current IT staff member OR are assigned to a documented service account.
- Verify domain admin accounts must have 15+ character passwords.
- Inquire about common local admin passwords and ask if they are unique per category of system.
- Inquire about users with local administrative privileges. Review documentation describing why this is necessary.

**Common Exceptions:** Some Core systems require that users be defined as local administrators. This is a terrible exception that puts a credit union at highly elevated risk. Credit unions should aggressively manage vendors to reduce the need for users to be admins.

**References:** 12CFR Part 748, Appendix A III.C.1., FFIEC IT Examination Handbook

**Proposed Language for Deficiency:** Admin accounts must be protected. Domain admin privileges must be restricted to the minimum necessary and must be protected with complex and lengthy (15+ character) passwords. Documentation should thoroughly describe why Local admin account privileges are granted to regular users. Common local admin passwords must be unique per category of system.

**Advanced:** None.