DCPLUS

THE ESSENTIAL 2019 COMPLIANCE GUIDE FOR CREDIT UNIONS

TABLE OF CONTENTS

ABOUT CREDIT UNION COMPLIANCE

Congress and Homeland Security hold board members responsible for the security of their consumer information. No financial institution with operations protected by the U.S. government is immune from what seems to be an overwhelming responsibility for IT security governance of risk and compliance. While the threats mount in volume from very sophisticated bad actors, the penalties remain straightforward. Board members and institution officers risk jail, stiff fines and reputational risk from non-compliance.
Many compliance programs can be difficult to justify. However, this is not so for IT security compliance; the benefits of diligent compliance are clear.

- Members and employees reward good stewardship of their sensitive information.
- The Federal Financial Institutions Examination Council (FFIEC) rewards institutions that make competent, good-faith efforts.

While making cybersecurity best practice an embedded function of an organization is possible, it usually requires a system of controls and monitoring typically outside the scope of internal IT staff. Hackers' ever-increasing sophistication requires credit unions to form collaborative partnerships with teams focused on advancing IT security and maintaining up-to-date skills associated with the latest methods and technologies.

This guide provides strategic information and security guidance for credit union executive management. Find the compliance resources you need in one place and learn the tactics necessary for a good strategic play that meets, if not exceeds, federal IT security compliance guidelines. Most importantly, learn IT security best practice for protecting members from cybersecurity threats at the hand of their credit union.

THE RISKS OF GETTING IT WRONG

The Federal Financial Institutions Examination Council (FFIEC) requires institutions to "maintain effective information security programs commensurate with their operational complexities." [1] While data breaches are quite common and widely publicized, FFIEC-compliant institutions are rarely the victims, which testifies to the efficacy and viability of the FFIEC's IT security protocols.

FFIEC requirements – and the means for satisfying those requirements – are publicly available. This resource summarizes regulations and provides best practice suggestions. You may review the full online Bank Secrecy and Anti-Money Laundering (BSA/AML) documentation here. Here are some highlights:

- A written security policy is required of all federally insured credit unions.
- The board of directors is accountable for the IT security policy and its compliance.
- The IT security policy is designed to protect "security and confidentiality of member records, protect against the anticipated threats or hazards to the security or integrity of such records, and protect against unauthorized access to or use of such records that could result in substantial harm or serious inconvenience to a member."
- ·The policy will specify response times and mechanisms.
- The policy will specify that the credit union be able to report incidents of unauthorized access or abuse of member information and assist in identifying their cause and agent.
- The policy will stipulate how to prevent the destruction of vital records.

[1] See Information Security Introduction, FFIEC Information Technology Handbook, September 2016.

RISK ASSESSMENTS

Credit unions are required to perform regular risk assessments. FFIEC examiners also conduct their own risk assessments based on their published guidelines to determine an institution's "level of security risk."

Will your internal risk assessment line-up with the examiner's?

Few credit union executives could claim good-faith compliance without professional, outside assistance, and few responsible board members would permit IT security policy compliance monitoring solely by inside staff. Many credit unions turn to compliance professionals or managed service providers to assist with risk assessments and security compliance.

IT security best practice, as well as third-party managed security assistance, help address such questions as:

- How, without collecting gigabytes of data a second, could an organization monitor and store security audit logs from all applications?
- What mechanism would raise alerts of such activities fast enough to do any good?
- How can such monitoring costs be reduced through policy enforcement that doesn't shut productivity down?

5 STEPS OF IT SECURITY BEST PRACTICE

ESTABLISHING A SECURITY MINDSET

To solidify best practices, management should create an environment that encourages and supports healthy IT security. Most hackers will admit that the easier targets are those that lack a "security mindset."

A healthy security culture is particularly important because of the dynamic nature of the threats as well as its direct impact on the organization's balance sheet and reputation.

Note that high-security environments are especially important when introducing new products or applications.

The following are the primary elements of a reliable IT security policy based on the FFIEC examination framework.

1. QUANTIFY IT SECURITY RISKS

Threats may represent internal or external operational risk as well as the failure of processes, people or systems. Most risks arise from human error, usually driven by a lack of training or insufficient knowledge. It is therefore imperative to systematically and thoroughly inspect every aspect of the institution's computers and network.

Business operational processes may also expose the institution to unnecessary risk. One common example is for management to assume wire transfer validation occurs prior to the transfer, while in practice, the manual process takes place afterwards. Management should take initiative and demand the support necessary to strengthen institution health and security. This includes:

- ·Ensuring that processes and procedures comprehensively identify threats. Consider reinforcing this step with a trusted third-party audit.
- Maintaining a documented catalog of vulnerability.
- Documenting any decisions to act or not act in response to known vulnerabilities.

Several resources are available to aid institutions in identifying risks.

- The FFIEC issues a voluntary cybersecurity assessment tool.
- The National Institute of Standards and Technology (NIST) publishes a cybersecurity framework.
- The U.S. Computer Emergency Response Team provides a national cyber awareness system (US-CERT NCAS).

While these standard templates are useful, they require specialized skills to perform the various assessments, deployment, and maintenance recommendations. Further, risks should be reviewed and categorized. Here are common areas to inspect:

- **Inter-connectivity -** Data is often shared with other institutions and vendors. Connections, network activity and the volume and type of data must be reviewed.
- **User security -** Access to data should be controlled by both physical and virtual access to the network and offices. Note that administrative users pose special risks. In addition to the risk of access, there is the risk of adverse user actions such as data alteration, deletion and distribution. Extortion and disruption must also be factored into the risk evaluation. Security screening should be well defined and systematic.
- **Physical security -** Account for paper documents, computers, mobile devices, doors and restricted spaces, cash and other physical assets. Also review all security measures for physical assets, such as security cameras, door locks, alarm systems and other methods.
- **Network security -** Networks should have built-in security measures and be consistently monitored for suspicious activity and threats.
- **Change management -** Application and system changes should be vetted prior to production rollout.
- **End of life -** Important functioning elements of the institution's network may be nearing the end of qualified support and maintenance, and therefore open to attack.
- **Third-party vendors -** All vendors and supply chain links, especially IT vendors, must hold to a high standard for IT security, as well as abide by the institution's requirements.

MEASURING RISK

To manage threats, a security professional should rank the risk of identified threats by potential, prevalence and other variables. The ranking factors should correlate with the institution's reputation and capital. There are many different methodologies for identifying the threat pathways and their relative effects on other technologies and use-cases within the institution.

2. MITIGATE INFORMATION TECHNOLOGY RISKS

The extent and control of the institution's assets must be disclosed by the IT security policy to inform the scope of the risk mitigation plan. The mitigation plan should also incorporate up-to-date threat intelligence and response mechanisms to respond to the dynamic nature of cyber threats.

A proper mitigation strategy includes these primary functions:

1. Policies to control and maintain IT security.
2. IT security architecture.
3. Operational controls (preventative, corrective, detective, technical and others).
4. Control implementation, such as triggers and authorities.

The institution's policy should require the collection and encryption of event logs. These files contain details about data usage and should be protected from tampering.

SECURITY AUDITS

Security audits are the foundation of a reliable IT security operation. However, security audits are voluminous, and are often in different formats and vary in information depth.

Meaningful IT security audits, therefore, require robust systems with professionally developed and managed system architecture. In some instances, analyzing endpoint logs is more critical and easier to perform in smaller institutions. Larger institutions, by contrast, must carefully balance the risk and effort of such endpoint log collection.

3. MONITOR THREATS TO SECURITY

Institutions should track information about their risk profile and identify gaps in their mitigation efforts. This can be difficult when cybersecurity threats change rapidly. However, there are tools and resources that help diligent institutions remain current with software and hardware updates that address known threats.

Security monitoring should go beyond system updates and patch management; it must also monitor external threats and attacks. Security information and event monitoring (SIEM) solutions are now available to more than just large commercial and governmental enterprise networks. They allow even small organizations to configure network monitoring and identify events that align with highly ranked risk assessment threats.

Credit Union IT security monitoring best practice includes:

- Fast, accurate response to standard and ad hoc security threats.
- Priority alerts based on IT security policy.
- IT security KPIs and benchmarks.

4. RESPOND INTELLIGENTLY AND QUICKLY

To minimize attack damage, a credit unions should implement an IT security incident response program that ensures prompt action with a robust alert system and the means to communicate information to stakeholders quickly. The IT security system must be able to provide sufficient details about any incidents, so that a thorough analysis may be provided to authorities and network administrators.

In addition, there should be clear and well-known escalation protocols, roles and authorities. Who is empowered to declare an incident? What steps is that person expected to take, and by what means? Credit union IT security response best practice includes guidance for how to react to a security incident. Here is a partial list;

- Who is on the Security Incident Response Team (SIRT), what is their collective and individual role and their limit of authority?
- ·When to involve outside experts, and how to qualify those experts.
- How to balance concerns regarding confidentiality, integrity, and availability of data and devices.
- When and under what circumstances to invoke an incident response, and the proper notification channel(s).
- ·Roles and authorities. Who has the authority call the regulators? Who has the authority to take action with or against network components? Who decides on discontinuation and restoration of services?
- What "after the event" actions should happen? Who will present a "lessons learned" report to management or the board?

5. RINSE AND REPEAT

For IT security to do its job, it must be routinely curated and refined. Most organizations routinely test their IT security by auditing their network and processes. The FFIEC requires management to ensure that information security programs remain viable through testing.

Security is never complete. It is a continuous process of searching for improvements and deploying them. Therefore, every aspect of a credit union's information security system must undergo routine inspection and maintenance. Credit unions' best practice for continuous IT security improvement helps management successfully protect members and the organization.

These practices may be summarized as follows:

1. **Test and evaluate.** Confidential self-assessments and audits should be of sufficient independence, scope and competence.
2. **Align IT security with personnel skills and business needs.**
3. **Create an IT security documentation and education process** and embed it into the culture of the institution.

The size of the institution will determine the scope and type of tests and audits. However, **standard methodologies such as penetration (PEN) tests and vulnerability assessments should be conducted quarterly.**

SOURCING EXPERTS

Most organizations choose outside organizations to help with some or all of IT security best practices. This allows management to minimize or eliminate bias as well as access expanded capabilities and threat intelligence. Independence lends credibility to the results.

GOOD DATA STEWARDS DELIVER BEST FINANCIAL STABILITY FOR MEMBERS

Members' success largely depends on the credit union's ability to continually serve their interest. Only by protecting itself against cyber threats will an institution endure as a steward of their most vital information and financial assets.

In the past, a lender served the market by managing only the real-estate assets on its balance sheet. Now lenders must also protect real digital assets unrecorded on the balance sheet. Credit unions that take IT security seriously, and back it up with policy best practices, position themselves to meet members' current and future financial stability needs, earning their trust and continued business.

ABOUT THE AUTHOR

DC Plus is a recognized leader in information technology security. Founded to support the growing needs of global manufacturing firms, the company offers advanced technology support and counsel to small to mid-sized credit unions and enterprises.

The company offers certified IT and services for credit unions, including risk assessments, scheduled network security audits, patch management, PEN tests, vulnerability assessments and employee training. DC Plus also offers managed services for malware and anti-virus, firewall security, content filtering and many others.

DC Plus' credit union IT security specialists may be reached at CU@dcplus.net.

Click below to continue the conversation with DC Plus

CONTACT US NOW

DC Plus makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. DC Plus does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

https://www.DCPlus.net

Email: support@DCPlus.net