DC PLUS

FOR CREDIT UNIONS

The Essential Compliance Guide

Strategic information and IT security guidance for credit union executive management.

CONTENTS

What's inside

COMPLIANCE · 01

About Credit Union Compliance

NCUA examiners and FFIEC guidance hold credit union boards accountable for the security of member information. As threats grow in volume and sophistication, regulators expect institutions to maintain strong, documented IT security programs and to demonstrate good-faith effort year over year. Lapses can result in regulatory findings, supervisory actions, civil penalties, and reputational damage that's hard to undo.

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.

Building cybersecurity into the fabric of a credit union takes controls, monitoring, and current expertise to keep pace with increasingly sophisticated attackers — more than most in-house teams can sustain on their own. Many smaller credit unions, particularly those under $50 million in assets, have no dedicated IT resource at all. Larger institutions with established IT teams benefit from a co-managed partner that adds specialized security capability alongside the work their team already handles. Either way, the right outside partnership extends what's possible without stretching the institution thin.

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 the IT security best practices that protect members from cybersecurity threats targeting their credit union.

> **Diligent compliance isn't a tax on the business — it's a quiet competitive advantage.**

COMPLIANCE · 02

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." Data breaches are common and widely publicized — but institutions that follow FFIEC guidance are better positioned to prevent, detect, limit, mitigate, and recover from attacks, which testifies to the practical value of the FFIEC's IT security protocols.

FFIEC requirements — and the means for satisfying those requirements — are publicly available through the FFIEC IT Examination Handbook. This guide summarizes those regulations and offers best-practice suggestions. 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 board must receive at least an annual report on the information security program.
- The policy must identify risk-assessment requirements and frequency.
- The policy must protect member records and prevent unauthorized access that could harm a member.
- The policy must specify incident response times and mechanisms.
- The policy must enable incident reporting and help identify cause and agent.
- The policy must stipulate how to prevent the destruction of vital records.
- A formal, tested disaster recovery plan must be maintained.
- A written third-party oversight program must cover due diligence, contracts, and ongoing monitoring — especially for the core processor, card processor, and ACH provider.

SPOTLIGHT · RECENT RULE

The NCUA 72-Hour Rule

Effective September 1, 2023, federally insured credit unions must notify the NCUA within 72 hours of a reportable cyber incident — including those originating at a third-party vendor. Roughly 70% of first-year incidents traced back to vendors.

…and others. This guide is a primer — your full Part 748 obligations are broader. Happy to walk through where your credit union stands.

Will your assessment line up with the examiner's?

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."

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 — together with managed security assistance — answers questions in-house teams struggle with:

- Are you collecting and correlating security events from your firewalls, network appliances, servers, and desktops in one place?
- Is that monitoring backed by a SIEM platform and a SOC team that can detect and respond around the clock — not just during business hours?
- Can alerts be tuned by policy so they surface true threats without drowning your team in noise or shutting down productivity?

BEST PRACTICE · 03

5 Steps of IT Security Best Practice

5

Establishing a Security Mindset

To solidify best practices, management should create an environment that encourages and supports healthy IT security. Most hackers will admit 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 — and its direct impact on the organization's balance sheet and reputation.

> **High-security environments are especially important when introducing new products or applications.**

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

STEP ONE

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: management assumes 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 vulnerabilities.
- Documenting any decisions to act — or not act — in response to known vulnerabilities.

STEP ONE · RESOURCES

Resources to Aid Institutions

Several authoritative resources are available to help credit unions identify and quantify cybersecurity risks. These references are current as of 2026:

FFIEC IT Examination Handbook & CISA Cybersecurity Performance Goals (CPGs)

The FFIEC's IT Examination Handbook remains the authoritative guidance for financial institutions. The FFIEC Cybersecurity Assessment Tool (CAT) was retired in August 2025; institutions now align with CISA's CPGs and the broader frameworks below.

ithandbook.ffiec.gov →

NIST Cybersecurity Framework (CSF 2.0)

The National Institute of Standards and Technology published CSF 2.0 in 2024. It is the current, widely-adopted framework for managing and reducing cybersecurity risk across organizations of every size.

nist.gov/cyberframework →

CISA Cybersecurity Advisories

The Cybersecurity and Infrastructure Security Agency (CISA) now provides the consolidated national cyber awareness function previously delivered through US-CERT and NCAS. CISA's advisories alert institutions to active threats and vulnerabilities.

cisa.gov/news-events/cybersecurity-advisories →

These frameworks are useful, but they require specialized skills to perform the assessments, deployment, and maintenance they recommend.

STEP TWO

2 Mitigate IT 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 plan should also incorporate up-to-date threat intelligence and response mechanisms to keep pace with the dynamic nature of cyber threats.

A proper mitigation strategy includes these primary functions:

- Policies to control and maintain IT security.
- IT security architecture.
- Operational controls — preventative, corrective, detective, technical, and others.
- Control implementation, including triggers and authorities.

SECURITY AUDITS

Security audits are the foundation of a reliable IT security operation, but they are voluminous, often in different formats, and vary in information depth. Meaningful audits require robust systems with professionally developed system architecture. In smaller institutions, analyzing endpoint logs is often more critical and easier to perform; larger institutions must carefully balance the risk and effort of endpoint log collection.

MEASURING RISK

To manage threats, a security professional should rank identified threats by potential, prevalence, and other variables. The ranking factors should correlate with the institution's reputation and capital.

3

STEP THREE

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. Fortunately, tools and resources exist to help diligent institutions stay 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 — once the realm of large enterprise — are now accessible to even small organizations, enabling network monitoring tuned to high-priority risk-assessment threats.

CREDIT UNION SECURITY MONITORING — BEST PRACTICE

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

4

STEP FOUR

Respond Intelligently & Quickly

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

There should be clear, 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? Best-practice guidance includes:

- Who is on the Security Incident Response Team (SIRT)? What is their collective and individual role and limit of authority?
- When to involve outside experts, and how to qualify those experts.
- How to balance confidentiality, integrity, and availability of data and devices.
- Under what circumstances to invoke an incident response, and the proper notification channels.
- Roles and authorities: who has the authority to call regulators? Who can 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

STEP FIVE

Rinse & Repeat

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

> **Security is never complete. It is a continuous process of searching for improvements — and deploying them.**

Every aspect of a credit union's information security system must undergo routine inspection and maintenance. Best-practice continuous improvement helps management successfully protect members and the organization.

SUMMARY

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

Standard methodologies such as penetration tests and vulnerability assessments should be conducted at least quarterly. The size of the institution determines the scope and type of tests and audits.

CHOOSING A PARTNER · 04

Sourcing Experts

GOOD DATA STEWARDS DELIVER FINANCIAL STABILITY FOR MEMBERS

Most organizations choose outside partners to help with some — or all — of IT security best practices. This allows management to minimize bias, expand capability, and access threat intelligence that's hard to develop internally. Independence lends credibility to the results.

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.

> **Independence lends credibility. The right outside partner makes good faith visible.**

CHOOSING A PARTNER · 04

What a Credit Union MSP Should Deliver

A managed service provider (MSP) is more than a vendor that answers helpdesk tickets. The right MSP becomes an embedded extension of your leadership team — strategically engaged, accountable, and present in the moments that matter most. Here's what to look for:

vCIO — Strategic Technology Leadership

Acts as your virtual Chief Information Officer: setting technology direction, planning budgets and roadmaps, and helping leadership make sound IT investment decisions.

Designated Incident Response Lead

A named, accountable role in your incident response plan — not a phone number you hope picks up. Coordinates containment, recovery, forensics, and member-impact communication when something goes wrong.

Technical Liaison to Core, ACH & Key Vendors

Acts as the technical interface to your core software provider, ACH processor, card processor, and other critical third parties — translating between vendor requirements and your environment so projects don't stall.

NCUA & Examination Support

Guides you through NCUA examinations and IT audits: preparing documentation, responding to examiner questions, and helping close findings with credible remediation plans.

IT Policy & Procedure Maintenance

Keeps your IT policy handbook current as regulations, technology, and the threat landscape evolve — so the document on the shelf actually reflects what's running on the network.

Threat & Technology Intelligence

Keeps you informed of changes in security threats and evolving technology — not as a newsletter, but as actionable guidance tailored to your environment, risk profile, and member base.

Disaster Recovery Stakeholder

An active stakeholder in your business continuity and disaster recovery planning, testing, and execution — not a spectator who shows up after the outage.

ABOUT · 05

About DC Plus

DC PLUS

DC Plus is a veteran-owned managed IT and cybersecurity company serving small businesses, credit unions, and manufacturers across Kentucky and Southern Indiana. With more than 25 years of industry experience, we help institutions protect what matters and stay examination-ready.

Our credit union practice includes risk assessments, scheduled network security audits, patch management, penetration tests, vulnerability assessments, end-user awareness training, managed firewalls, and endpoint protection.

TALK TO OUR CREDIT UNION TEAM

DC Plus · 120 Ball Park Rd, Hardinsburg, KY 40143

(270) 215-2626 · info@dcplus.net · dcplus.net

Proudly Veteran-Owned · 25+ Years Serving Kentucky

DCPLUS

Let's continue the conversation.

A 30-minute conversation is the easiest way to find out whether your credit union's IT security program is examination-ready.

SCHEDULE A FREE ASSESSMENT

info@dcplus.net · (270) 215-2626 · dcplus.net