WHITEPAPER

CREDIT UNION COMPLIANCE

IGNYTE ASSURANCE PLATFORM™

7 Steps to Managing Credit Union Cyber Risk

WHAT'S MISSING FROM CREDIT UNIONS' COMPLIANCE PROGRAMS AND PROCESSES?

Cybersecurity is a systemic risk that affects all levels of business and government. It is such a high-risk area for credit unions that the National Credit Union Administration (NCUA), Federal Financial Institutions Examination Council (FFIEC), Consumer Financial Protection Bureau (CFPB) and Payment Card Industry Data Security Standard (PCI DSS) placed cybersecurity as a top focus for assessments and audits.

CREDIT UNIONS AND COMPLIANCE RESEARCH

Reported by CUNA that 85% of the credit unions CUNA surveyed stated they would be likely to use a compliance management platform to help simplify and streamline their daily compliance efforts. 80% of credit unions are seeking a solution that offers compliance procedures and controls and ONLY 17% of credit unions in the U.S. are utilizing compliance technology.

"85% of CUs would be likely to use a compliance management platform to help simplify and streamline their daily compliance efforts."

- CUNA Compliance Management Study

What Needs to be Implemented?
Many credit unions don't have the tools or resources they need to efficiently track and mitigate the risks associated with non-compliance. The most frequently mentioned gaps in credit unions' management capabilities included:

- **Policy Management**
- **Mapping of security controls throughout different frameworks**
- **Advanced Reporting**
- **Controls Management**
- **Advanced Risk Assessments**
- **Training Library**
- **Procedural Documentation**

SEVEN STEPS TO MANAGING CU CYBER RISK

It is estimated that only 17% of U.S. credit unions are currently utilizing compliance management platforms. That means there is significant room for improvement in boosting the effectiveness of compliance management programs. FFIEC has identified seven steps to manage and reduce risk posed in the financial sector. The Ignyte Platform can help in regard to the automation workflow, tracking and reporting on these risk assessments.

1. Conduct ongoing information security risk assessments
A risk assessment program should be implemented, consistently adjusting to respond to new and evolving threats. This includes altering authentication, security systems and controls in response to threats as they manifest and come alive. This also includes performing ongoing due diligence and monitoring of third-party service providers. The security risk assessment depends on which framework you conduct the assessment off of whether it is FFIEC, NCUA, PCI DSS or CFPB the security controls can all be mapped back to each other.

2. **Perform security monitoring, prevention and risk mitigation**
The importance of establishing, maintaining and monitoring cybersecurity controls for intrusion detection and antivirus protection. This could include updating software, conducting penetration testing and regularly reviewing reports of monitoring systems.

3. **Protect against unauthorized access**
Limiting credentials and access privileges, reviewing access rights periodically, and monitoring logs for unusual behavior and the use of out dated data is critical to preventing the use of compromised credentials. There are protocols and controls to put in place like expiration period, multifactor authentication, biometrics, and public-key infrastructure (PKI).

4. Regularly i**mplement and test controls around critical systems**
Adequate monitoring, testing, audits and reporting are necessary to ensure controls are effective and functioning. These should be implemented on the basis of the risk assessed. Limiting the number of sign-on attempts, locking accounts and implementing alerts to ensure that baseline protections are not altered. Active monitoring or implementing a Security Operations Center (SOC) is mandatory for FFIEC, NCUA, CFPB and PCI DSS.

5. **Manage Business Continuity Risk**
Coordinating business continuity development and testing with third parties can assist a credit union in determining whether its planning actually supports to recover and maintain payment processing operations in the event of a potential attack that would affect the network. These capabilities can be managed within the business continuity module in the Ignyte Platform. Implementing a business continuity strategy is mandatory for FFIEC, NCUA, CFPB and PCI DSS

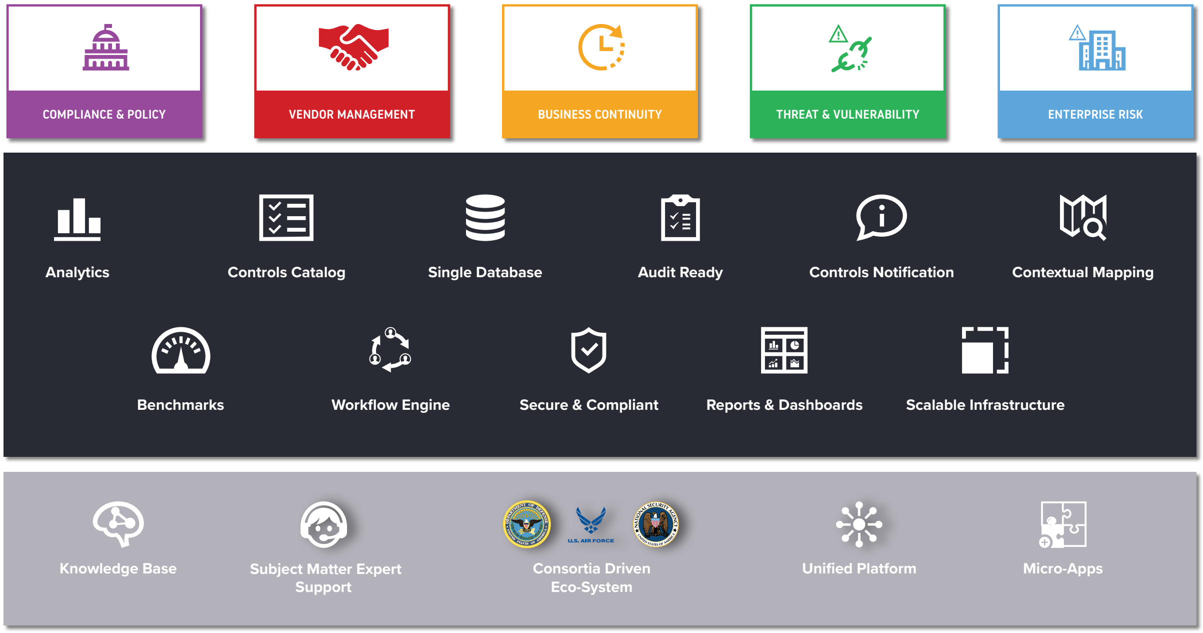
6. **Enhance information security awareness and training programs**
Recommend regular, mandatory training for employees, which is tailored to their function, and covers the identification and prevention of phishing attempts or other efforts to compromise credentials. Implementing a security awareness and training program is mandatory for FFIEC, NCUA, CFPB and PCI DSS.

7. **Participate in industry information-sharing forums**
Due to the nature and threat of attacks changing so rapidly, participating in information sharing regarding threats and incidents can assist a credit union to stay well-informed of the newest information and how to identify, prevent and mitigate these advanced attacks. Suggested alerts and reporting vulnerabilities to US-CERT.

HOW CAN IGNYTE HELP?

Ignyte can holistically help automated workflows for every stage of the compliance process allowing credit unions to save time and devote more resources to serving their members. Key areas of automation include:

- **FFEIC CAT Automation**
- **NCUA Automated Cybersecurity Examination Tool (ACET)**
- **Current maturity level & target state reporting**



COMPLIANCE & POLICY

VENDOR MANAGEMENT

BUSINESS CONTINUITY

THREAT & VULNERABILITY

ENTERPRISE RISK

Analytics

Controls Catalog

Single Database

Audit Ready

Controls Notification

Contextual Mapping

Benchmarks

Workflow Engine

Secure & Compliant

Reports & Dashboards

Scalable Infrastructure

Knowledge Base

Subject Matter Expert Support

Consortia Driven Eco-System

Unified Platform

Micro-Apps

GET STARTED NOW!

Give us a call to setup a demo today at https://ignyteplatform.com/request-a-demo/

FOR MORE INFORMATION

To learn more about how Ignyte can help solve your business and IT challenges, contact your local representative or authorized reseller - or visit us at ignyteplatform.com If you are an existing Ignyte Platform customer and have questions or require additional information about licensing, please contact Ignyte at support@ignyteplatform.com or call 1.833.IGNYTE1, (937) 789.4216.