Compliance Brief

Data Security Compliance with the National Credit Union Administration (NCUA) Information Security Requirements

How Thales solutions help with NCUA information security compliance

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

What is the National Credit Union Administration?

Created by the U.S. Congress in 1970, the National Credit Union Administration (NCUA) is an independent federal agency that insures deposits at federally insured credit unions, protects the members who own credit unions, and charters and regulates federal credit unions.

What is the NCUA Examination Program?

The NCUA's primary function is to identify and assess credit union system risks, threats, and vulnerabilities; determine the magnitude of such risks and mitigate unacceptable levels of risk through its examination, supervision, and enforcement programs. As such, NCUA requires all U.S. federally insured credit unions to establish a security program that addresses the privacy and protection of customer records and information.

The NCUA's examination program focuses on the areas that pose the highest risk to the credit union system and the Share Insurance Fund. All federally insured credit unions receive an NCUA examination periodically.

What is the NCUA Information Security Booklet for Credit Unions?

To ensure both compliance with applicable laws and regulations, and safety and soundness, a review of the credit union's information security program is performed at each examination. The **"Information Security" booklet** is an integral part of the Federal Financial Institutions Examination Council (FFIEC) Information Technology Examination Handbook (IT Handbook) and should be read in conjunction with the other booklets in the IT Handbook. This booklet provides guidance to examiners and addresses factors necessary to assess security risks to a financial institution's information systems.

Institutions should maintain effective information security programs commensurate with their operational complexities. Information security programs should have strong board and senior management support, promote integration of security activities and controls throughout the institution's business processes, and establish clear accountability for carrying out security responsibilities.

Which institutions are supervised by the NCUA?

All credit union entities chartered and supervised by the National Credit Union Administration.

How can Thales help Credit Unions comply with the NCUA information security requirements?

Thales helps credit unions comply with the NCUA information security requirements and pass required examinations by addressing key risk mitigation requirements outlined in the NCUA Information Security Booklet.

NCUA Information Security Booklet Section IIC – Risk Mitigation

Management should develop and implement appropriate controls to mitigate identified risks. Controls include risk assessment, data encryption and key management, access management and security intelligence.

Thales helps organizations by:

- **Identifying and classifying sensitive data**
- **Implementing access control**
- **Protecting data in transit**
- **Securing applications, databases, and implementing encryption**
- **Reducing risk of third-party providers**

Section IIC – Risk Mitigation	Requirement	Thales Solutions
5	"Management should inventory and classify assets, including hardware, software, information, and connections."	**CipherTrust Data Discovery and Classification** identifies structured and unstructured sensitive data on-premises and in the cloud. Built-in templates enable rapid identification of regulated data, highlight security risks, and help uncover compliance gaps.
7	"User Security Controls: Establishing and administering a user access program for physical and logical access. Employing segregation of duties..."	**Thales OneWelcome Identity & Access Management** limits the access of internal and external users based on their roles and context with granular access and authorization policies that help ensure that the right user is granted access to the right resource at the right time. **SafeNet Trusted Access** combines single sign-on and scenario-based access policies in a cloud-based access management solution. Multi-factor Authentication with the broadest range of hardware and software methods and form factors. **CipherTrust Transparent Encryption** encrypts sensitive data and enforces granular privileged-user-access management policies that can be applied by user, process, file type, time of day, and other parameters. It provides complete separation of roles enabling only authorized users and processes to view unencrypted data.
13	"... should determine sensitivity of the information to be transmitted, and types of safeguards available to protect information."	**Thales High Speed Encryptors (HSEs)** provide network-independent data-in-motion encryption (layers 2, 3, and 4) ensuring data is secure as it moves from site-to-site, or from on-premises to the cloud and back. Our network encryption solutions allow customers to better protect data, video, voice, and metadata from eavesdropping, surveillance, and overt and covert interception— without performance compromise.
17	"Application Security: Management should use applications that have been developed following secure development practices and that meet a prudent level of security."	**CipherTrust Platform Community Edition** makes it easy for DevSecOps to deploy data protection controls in hybrid and multi-cloud applications. The solution includes licenses for CipherTrust Manager Community Edition, Data Protection Gateway, and CipherTrust Transparent Encryption for Kubernetes. **CipherTrust Secrets Management** is a state-of-the-art secrets management solution, which protects and automates access to secrets across DevOps tools and cloud workloads including secrets, credentials, certificates, API keys, and tokens. **Thales Data Protection on Demand (DPoD)** is a cloud-based marketplace that offers Luna hardware security modules (HSMs) and CipherTrust solutions as a service. This enables in-house teams to leverage these proven and certified data security solutions easily and securely in their own offerings.

Section IIC – Risk Mitigation	Requirement	Thales Solutions
18	"Database Security: Management should implement effective controls for databases and restrict access appropriately"	**CipherTrust Tokenization** permits the pseudonymization of sensitive information in databases while maintaining the ability to analyze aggregate data, without exposing sensitive data during the analysis or in reports. **CipherTrust Database Protection** provides high-performance, column-level database encryption with an architecture that can provide high-availability to ensure that every database write and read happens at almost the speed of an unprotected database.
19	"Encryption: Management should implement the type and level of encryption commensurate with the sensitivity of the information."	**CipherTrust Data Security Platform** provides multiple capabilities for protecting data at rest in files, volumes, and databases. Among them: • **CipherTrust Transparent Encryption** delivers data-at-rest encryption with centralized key management and privileged user access control. This protects data wherever it resides, on-premises, across multiple clouds, and within big data and container environments. • **CipherTrust Enterprise Key Management** streamlines and strengthens key management in cloud and enterprise environments over a diverse set of use cases. Leveraging FIPS 140-2-compliant virtual or hardware appliances, Thales key management tools and solutions deliver high security to sensitive environments and centralize key management for home-grown encryption, as well as third-party applications. **Thales Luna Hardware Security Modules (HSMs)** protect cryptographic keys and provide a FIPS 140-2 Level 3 hardened, tamper-resistant environment for secure cryptographic processing, key generation and protection, encryption, and more. Luna HSMs are available on-premises, in the cloud as-a-service, and across hybrid environments. • Generates and protects root and certificate authority (CA) keys, providing support for PKIs across a variety of use cases. • Signs application code to ensure software remains secure, unaltered, and authentic. • Creates digital certificates for credentialing and authenticating proprietary electronic devices for IoT applications and other network deployments.

Section IIC – Risk Mitigation	Requirement	Thales Solutions
20	"... Oversight of Third-Party Service Providers: Verification that information and cybersecurity risks are appropriately identified, measured, mitigated, monitored, and reported..."	**CipherTrust Cloud Key Manager** can reduce third-party risks by maintaining on-premises under the full control of the financial institution the keys that protect sensitive data hosted by third party cloud providers. This increases operational efficiency through harmonization and automation. **CipherTrust Transparent Encryption** provides complete separation of administrative roles, so only authorized users and processes can view unencrypted data. Sensitive data stored in a third-party cloud will not be accessible in cleartext to unauthorized users. These could include third-party cloud provider employees, such as support engineers, DB admins, or potentially malicious processes. In addition, the Thales Portfolio of Data Security solutions offers the most comprehensive range of data protection for cloud environments. **Thales Data Protection on Demand (DPoD)** provides built in high availability and backup to its **cloud-based Luna Cloud HSM and CipherTrust Key Management services** and to the **High Speed Encryption** appliances that secure data moving between clouds, to on-premises locations, or to third parties.

About Thales

Today's businesses and governments depend on the cloud, data and software to deliver trusted digital services. That is why the most recognized brands and organizations around the world rely on Thales to help them protect sensitive information and software wherever it is created, stored or accessed – from the cloud and data centers to devices and across networks. As the global leader in data security and software licensing, our solutions enable organizations to move to the cloud securely, achieve compliance with confidence, create more value from their software and deliver seamless digital experiences for millions of consumers every day.