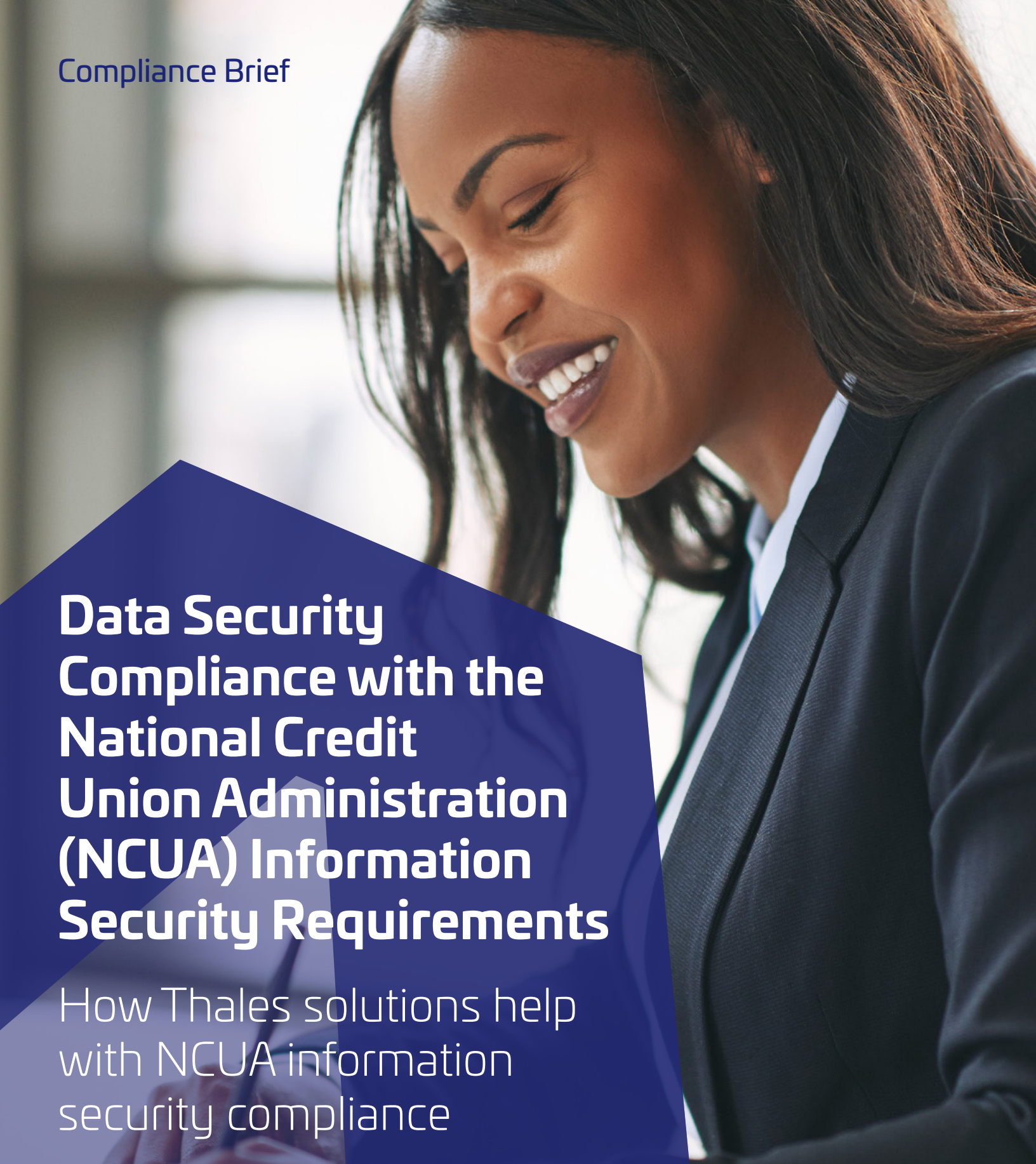
Compliance Brief



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 Thales Helps with NCUA Compliance

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.

We provide comprehensive cyber security solutions in three key areas of cybersecurity: Application Security, Data Security, and Identity & Access Management.

- **Application Security:** Protect applications and APIs at scale in the cloud, on-premises, or in a hybrid model. Our market leading product suite includes Web Application Firewall (WAF) protection against Distributed Denial of Service (DDoS) and malicious BOT attacks, security for APIs, a secure Content Delivery Network (CDN), and Runtime Application Self-Protection (RASP).
- **Data Security:** Discover and classify sensitive data across hybrid IT and automatically protect it anywhere, whether at rest, in motion, or in use, using encryption, tokenization, and key management. Thales solutions also identify, evaluate, and prioritize potential risks for accurate risk assessment. They also identify anomalous behaviour and monitor activity to identify potential threats and verify compliance, allowing organizations to prioritize where to allocate their efforts.
- **Identity & Access Management:** Provide seamless, secure, and trusted access to applications and digital services for customers, employees, and partners. Our solutions limit the access of internal and external users based on their roles and context with granular access policies and multi-factor authentication that help ensure that the right user is granted access to the right resource at the right time.

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, data governance, access management, application security and security intelligence.

Thales helps organizations by:

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

NCUA	Thales Capabilities	Thales Solutions
5: Inventory and Classification of Assets and Information	• Identify structured and unstructured sensitive data at risk across Hybrid IT. • Identify current state of compliance and documenting gaps. • Discover and classify potential risk for all public, private and shadow APIs.	**Application Security** API Security **Data Security** Data Discovery & Classification Data Risk Analytics Vulnerability Management
7: User Security Controls and Segregation of Duties	• Limit access to systems and data based on roles and context with policies. • Apply contextual security measures based on risk scoring. • Centralize access policies and enforcement to multiple hybrid environments in a single pane of glass. • Provide customers secure access to their information in company's systems.	**Identity & Access Management** Workforce Access Management Customer Identity & Access Management **Data Security** Transparent Encryption
13, b: Protection for Data in Transit	• Protect data in motion with high-speed encryption. • Certified FIPS 140-2 L3, Common Criteria, NATO, UC APL	**Data Security** High Speed Encryption
13, c: Appropriate disposal procedures for electronic information.	• Locate structured and unstructured regulated data across hybrid IT and prioritize remediation. • Remove keys from CipherTrust Manager can ensure secure deletion, digitally shredding all instances of the data.	**Data Security** Data Discovery & Classification Encryption & Key Management
15: Remote Access by Employees	• Enable secure remote access for employees to all company resources on-premises or in the cloud with seamless user experience. • Enable MFA with the broadest range of hardware and software methods. • Build and deploy adaptive authentication policies.	**Identity & Access Management** Workforce Access Management Multi-Factor Authentication Risk-Based Authentication
16: Remote Access by Customers	• Provide customers secure access and seamless experience. • Enable MFA with the broadest range of hardware and software methods. • Enable customers to manage data privacy with consent and privacy management.	**Identity & Access Management** Customer Identity & Access Management Multi-Factor Authentication Consent & Privacy Management

NCUA	Thales Capabilities	Thales Solutions
17: Application Security	• Protect apps from runtime exploitation, while integrating with tools in the CI/CD pipeline. • Detect and prevent cyber threats with web application firewall, ensuring seamless operations and peace of mind. • Safeguard critical network assets from DDoS attacks and Bad Bots while continuing to allow legitimate traffic. • Deploy data protection controls in hybrid and multi-cloud applications to protect DevSecOps. • Protect and automate access to secrets across DevOps tools. • Easily access data security solutions through online marketplaces.	**Application Security** Runtime Protection Web Application Firewall DDoS Protection Bot Protection API Security **Data Security** Community Edition Secrets Management DPOD Marketplace
18: Database Security	• Transparent column-level encryption of structured, sensitive data in databases with centralized key management. • Pseudonymize sensitive information in databases.	**Data Security** Transparent Encryption Tokenization
19: Encryption commensurate with the sensitivity of the information	• Encrypt data at rest on-premises, across clouds, and in big data or container environments. • Protect cryptographic keys in a FIPS 140-2 Level 3 environment. • Pseudonymize sensitive information in databases. • Protect data in use by leveraging confidential computing. • Gain full sensitive data activity visibility, track who has access, audit what they are doing and document. • Security products designed for post-quantum upgrade to maintain crypto-agility.	**Data Security** Transparent Encryption Tokenization Key & Secrets Management High Speed Encryption Hardware Security Modules Confidential Computing Data Governance Data Activity Monitoring
20: Oversight of Third-Party Service Providers	• Reduce third party risk by maintaining on-premises control over encryption keys protecting data hosted by in the cloud. • Enforce separation of roles between cloud provider admins and your organization, restrict access to sensitive data. • Monitor and alert anomalies to detect and prevent unwanted activities from disrupting supply chain activities. • Enable relationship management with suppliers, partners or any third-party user; with clear delegation of access rights. • Minimize privileges by using relationship-based fine-grained authorization.	**Data Security** Cloud Key Management Transparent Encryption Data Activity Monitoring User Rights Management Discovery and Classification **Identity & Access Management** Workforce Access Management Third-party Access Control Delegated User Management Externalized Authorization

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.

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us