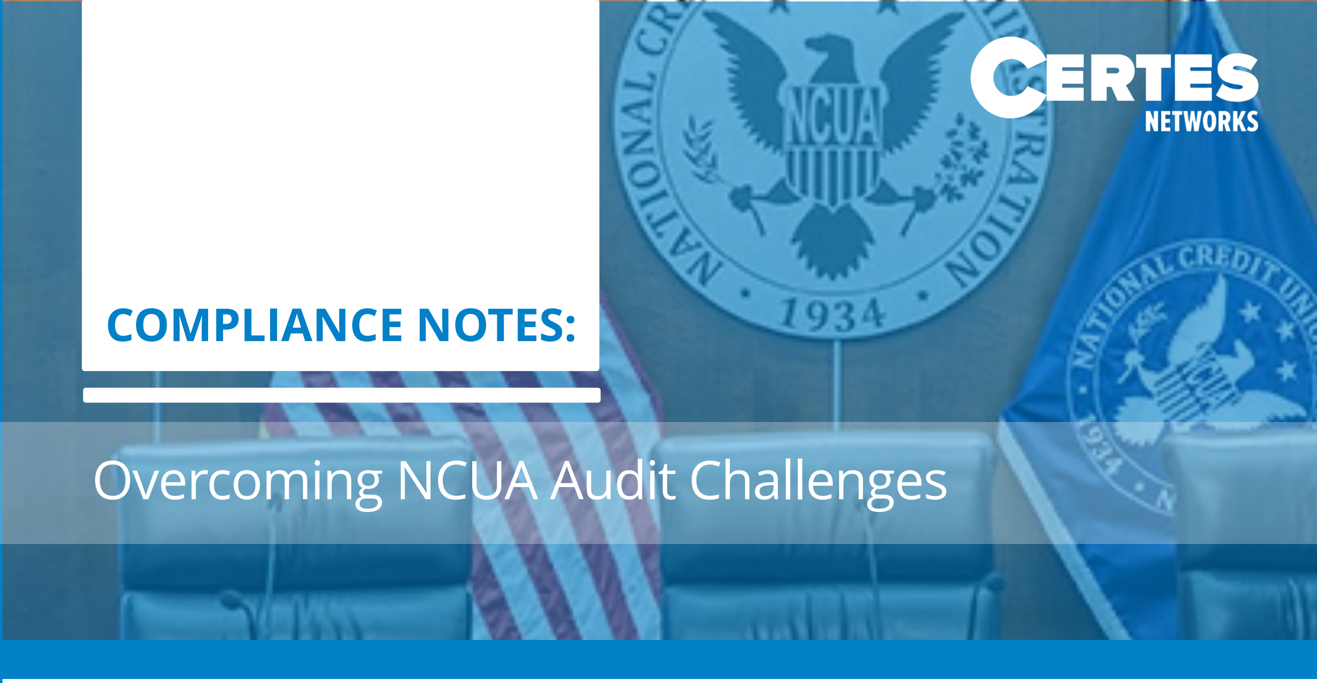

COMPLIANCE NOTES:

Overcoming NCUA Audit Challenges

What is the NCUA's Information Security Examination and Cybersecurity Assessment Program?

The National Credit Union Administration (NCUA) is a federal government agency responsible for insuring deposits at federally-insured credit unions. It regulates, charters and supervises all federal credit unions to protect the credit union system and its members.

One important program that falls under the scope of its regulatory and supervisory responsibilities is the Information Security Examination and Cybersecurity Assessment Program. Within this, the NCUA carries out periodic examinations of all federal credit unions to:

1. Ensure applicable laws and regulations are being complied with (for example, the NCUA 12 CFR Section 748.0: Security Program which requires credit unions to develop and implement a security program to protect the union and its members from various threats).

2. Review federal credit unions' information security plans to determine if technology rates risks have been effectively assessed and monitored. This also covers whether adequate security controls, policies and procedures have been implemented to safeguard member information.

NCUA PRINCIPLES & GUIDELINES

NCUA adopts a risk-based approach to conducting security examinations, but in essence, federal credit unions will need to demonstrate that the security program which they have implemented is adequate to prevent cyberattacks and protect the security of members' information.

As a benchmark for assessment and evaluation, NCUA uses principles and guidelines set out by the Federal Financial Institutions Examination Council (FFIEC) such as its Information Security Booklet. This covers many aspects of data and network security, recommending that a full spectrum of controls be deployed to mitigate various threats and risks to information systems.

CERTES NETWORKS USE CASE

Certes Networks was approached by one of its customers – a federal credit union with over 110,000 members – following an NCUA Security Examination. The examination concluded that adequate controls were not in place to mitigate the risk of sensitive data being disclosed (including PII (Personally Identifiable Information) of members and user credentials) as it was transmitted across an MPLS (Multiprotocol Label Switching) network between various branch locations.

It was determined that encryption should be applied as a security measure to protect the transmission of such sensitive data. Encryption is referenced as a control in the Risk Mitigation section of the Information Security Booklet (11.C.19):

Institution management should employ encryption strength sufficient to protect information from disclosure. Encryption methods should be reviewed periodically to ensure that the types and methods of encryption are still secure as technology and threats evolve.

The Information Security Booklet also sets out standards to be adopted regarding key management:

Key management is crucial to the effective use of encryption. Effective key management systems rely on an agreed set of standards, procedures, and secure methods that address the following:

- Generating keys for different cryptographic systems and different applications.
- Distributing keys to intended users, including how keys should be activated when received.
- Storing keys, including how authorized users obtain access to keys.
- Changing or updating keys, including rules on when and how keys should be changed.
- Logging the auditing of key management-related activities.
- Instituting defined activation and deactivation dates, and limiting the usage period of keys.

CREDIT UNION SOLUTION REQUIREMENTS

The team at Certes worked with two main decision makers – the credit union's Information Security Officer (ISO) and Network Administrator - who each expressed different concerns and objectives regarding potential solutions.

The Network Administrator's requirements focused on two key areas:

Ease of Implementation and Management: Taking responsibility for the overall management of a complex network environment with several critical projects in flight, it was important for the Administrator that the solution could be implemented with minimal network changes being undertaken. Ongoing management was a concern as the network team lacked sufficient resources to learn how to manage an encryption product. Therefore, ease-of-use was a priority when choosing a solution.

Maintaining Network Visibility: It was also important that network visibility was not impacted when running the encryption. The Administrator was concerned that the encryption of data would cause a loss of visibility when packet header information is encrypted and QoS markings are lost, which would disrupt daily operations.

The Information Security Officer highlighted additional requirements:

Effective Key Management: The credit union's ISO wanted to ensure that the specific standards and methods for effective key management set out in the Information Security Booklet were met. Standard encryption solutions operating at Layer 2 or Layer 3 were a concern because administration and ownership of encryption keys would fall under the responsibility of a third-party administrator, therefore, potentially conflicting requirements set out in other areas of the Information Security Handbook, such as segregation of duties (Section 11. 7 (c)).

CERTES NETWORKS' SOLUTION

Certes Networks' patented Layer 4 Encryption Solution secures data in transit independently from the underlying network, therefore, segregating the functions of security and networking.

This enables security teams to retain total control of administration and ownership of security protocols without impacting the duties of the network team.

Certes' patented Layer-4 encryption solution enables secure encryption of only the data (payload), providing transparent deployment that operates independently with zero changes to routers, switches, and firewalls. Network visibility and operational functionality are fully maintained with zero impact on performance.

This allows for a simple and scalable, end-to-end encryption management that is network agnostic, which easily integrates into any network infrastructure physically or virtually, and is fully interoperable with the existing security stack – with zero impact on performance.

The specific requirements of the credit union referred to in this Compliance Overview were met as follows:

NETWORK ADMINISTRATOR REQUIREMENTS

Quick and easy implementation.

Deployment across 20 sites was completed within a day. No changes were needed to existing network architecture. Unique encryption keys at a per policy workflow, application or network level.

Ease of ongoing use of platform.

No additional resources were needed due to the 'Plug and Play' nature of Certes' platform and automated key rotation.

Maintaining network visibility.

Payload only encryption ensured network traffic could be identified and prioritized and network tools functioned the same after the deployment as before.

INFORMATION SECURITY OFFICER REQUIREMENTS

Generating keys for different cryptographic systems and different applications.

Certes' solution ensures unique encryption keys at a per policy workflow, application or network level

Distributing keys to intended users, including how keys should be activated when received.

Certes' solution allows for automated key generation and distribution between components of the Certes solution.

Storing keys, including how authorized users obtain access to keys.

Encryption keys are stored within Certes' Enforcement Points, providing segregation of duties and only accessible to authorized users of platform.

Changing or updating keys, including rules on when and how keys should be changed.

Certes' solution allows for automated 'fail safe' key refresh at customizable intervals with no oversight required.

Logging the auditing of key management-related activities.

Robust auditing and logging capabilities track key management activities including rotation as well user activities within platform.

Instituting defined activation and deactivation dates, and limiting the usage period of keys.

Certes' solution allows for per policy workflow key rotation at intervals that are fully customizable and refreshed at a minimum of every hour.

Segregating duties and enabling encryption to be deployed without network teams having access to encryption keys means that additional requirements set out in the Information Security Booklet can be easily met.

CERTES NETWORKS

Contact Certes Networks

300 Corporate Center Drive, Suite 140
Pittsburgh, PA 15108

Tel: 1 (888) 833-1142
Fax: 1(412) 262-2574

info@certesnetworks.com
sales@certesnetworks.com