SECLORE™

Embracing Oman's Cyber Security & Resilience Framework (CS & RF) With Data-Centric Security

Overview

Introduction

Data security is crucial in banking, financial services, and insurance (BFSI), where safeguarding sensitive customer information and financial transactions is a top priority. As technology and digitalization drive the shift towards paperless, cashless, and real-time operations, financial institutions will continue to benefit from increased efficiency.

However, these technological advancements also bring new and complex cybersecurity challenges. The rise in both the frequency and sophistication of cyber incidents highlights the urgent need for robust cybersecurity and resilience frameworks. Implementing a comprehensive approach to data security ensures protection and strengthens competitive advantage, preparing organizations to meet future challenges in the BFSI sector.

Why Does Data Security Matter in BFSI?

Robust data security practices build customer trust, preserve reputations, and prevent financial losses from fraud, identity theft, and other cybersecurity threats. These practices ensure business continuity through robust disaster recovery plans and operational resilience. Advanced threat protection and continuous monitoring are essential to safeguard against sophisticated cyberattacks. Moreover, secure data practices support digital transformation and innovation while effectively managing third-party risks.

Cybersecurity Landscape of Oman

Oman's cybersecurity market is rapidly growing and driven by the nation's digital transformation. As businesses and government bodies adopt cloud computing, IoT devices, and advanced data analytics, secure, interconnected systems are critical. This shift generates vast amounts of sensitive data, making organizations prime targets for cyberattacks and increasing the demand for robust cybersecurity solutions.

Oman Vision 2040 and other government initiatives highlight cybersecurity's importance in building a secure digital landscape, leading to increased investments in cybersecurity infrastructure. The rise of remote work and online services has further amplified the need to secure access and defend against threats like phishing, ransomware, and data breaches. Consequently, organizations are adopting comprehensive cybersecurity strategies, including firewalls, encryption, intrusion detection systems, and employee training programs, driving market growth.

What is the Cyber Security & Resilience Framework (CS&RF)?

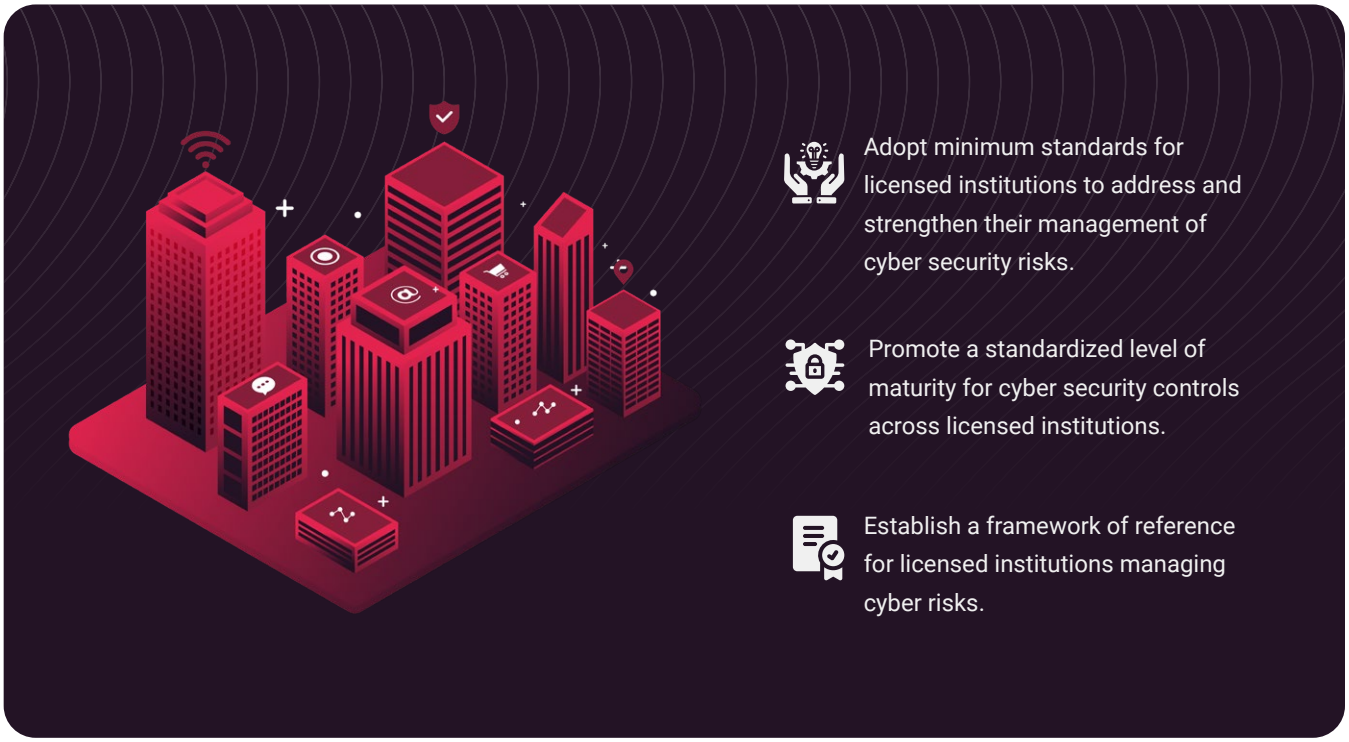
Oman stands out among Persian Gulf nations for its comprehensive cybersecurity strategy, which was initiated in 2010 with the emergence of the Oman Computer Emergency Readiness Team (OCERT). OCERT is responsible for identifying and evaluating cyber threats within the country and enhancing cybersecurity awareness among the populace. The effectiveness of these measures is supported by a significant decrease in attempted cyberattacks, dropping from 880 million in 2017 to just 12 million in 2022.

In September 2023, the Central Bank of Oman (CBO) issued a new regulatory framework for cybersecurity and resilience. This new regulation mandates banks, financing and leasing companies, payment service providers, and money exchange companies meet minimum requirements to build a resilient financial industry against cybersecurity risks.

CS&RF Objectives

The CS&RF aims to support and regulate the implementation of appropriate cybersecurity governance, strengthen system security, and implement necessary preventative controls for institutions licensed in Oman. The regulation aims to help these institutions achieve high resilience against cyber threats and ensure they can effectively respond to and mitigate cyber-attacks. The framework aligns with international standards such as ISO/IEC 27001, PCI DSS, BASEL, and NIST and complies with Oman's local laws and regulations.

The objectives of the framework can be summarized as follows:



CS&RF Intended Audience

The primary audience for this framework includes:

- Board of Directors
- Chief Information Security Directors (CISD)
- Senior Management
- Other stakeholders who are responsible for defining, implementing, and reviewing cybersecurity controls and processes.

CS&RF Applicability and Enforcement

The CS&RF applies to all institutions licensed by the Central Bank of Oman (CBO), which include:

- All banks operating in the Sultanate of Oman, as well as their foreign branches.
- All Finance and Leasing Companies (FLCs) operating in the Sultanate of Oman.
- All Money Exchange Companies operating in the Sultanate of Oman.
- All Payment Service Providers operating in the Sultanate of Oman.

Institutions must comply with the framework unless they no longer engage in regulated activities or operations. Foreign banks operating under their parent organizations' country-specific cybersecurity and governance frameworks must provide a letter of comfort to CBO to ensure compliance.

The framework is enforced by the Central Bank of Oman, which has the authority to periodically review and update guidelines to address emerging cybersecurity risks and threats. Licensed institutions must implement the mandated controls by July 31, 2024, and any institution unable to implement specific controls must provide justification and demonstrate substitute controls to the CBO for approval. Compliance is mandatory, and non-compliance could result in severe regulatory action.

Introduction to Data-Centric Security

Many organizations are looking at how to build a data-centric security infrastructure to efficiently eliminate security gaps, especially in light of new regulations. Regulations, such as ITAR/EAR, NIST, SDAIA, NIAP, GDPR, and CCPA, require sensitive data to remain protected, whether that data is in the custody of an organization or their authorized third party. Unfortunately, data security tools often work in isolation (e.g., data loss prevention, rights management, and data classification) and only partially meet the security requirements of these regulations.

Comprehensive data-centric security solutions empower organizations to know, protect, and control their most valuable information, safeguarding it from unauthorized access and breaches. Some of the tools that perform these functions include Data Loss Prevention (DLP), Data Discovery, Data Classification, Enterprise Digital Rights Management (EDRM), and Security Information and Event Management (SIEM) systems.

This whitepaper explains how Seclore's data-centric security platform helps BFSI institutions meet CS&RF requirements to ensure robust data protection, compliance, and operational resilience.

With data-centric security, organizations can:

- **Know** which assets are sensitive and what their locations are.
- **Protect** and classify the data with labels, watermarks, or encryption.
- **Track** activity related to sensitive digital assets.
- **Control** who can access this information and for how long.

Data-centric security platforms help organizations safeguard sensitive data by defining and implementing access policies based on user roles. This ensures that only authorized individuals can access the data. Implementing data-centric security controls helps organizations reduce cybersecurity risks, enable seamless collaboration, and adopt innovative technologies without worrying about security.

How Seclore Can Help You Comply with CS&RF

Seclore helps BFSI companies comply with the Cyber Security & Resilience Framework (CS&RF) by enabling them to:

Know

By accurately classifying, tracking, and providing complete visibility for protected digital assets, banks can ensure they know where their sensitive data resides and who has access to it.

Protect

By protecting digital assets with symmetric and asymmetric encryption, including AES256 and RSA2048 bit encryption, Seclore's data is protected at rest, in transit, and in use, ensuring that sensitive information is safe regardless of how it's shared or where it's stored.

Control

Giving BFSI companies complete control over who can access, edit, and share sensitive data, in addition to real-time activity information for protected digital assets, helps ensure they're compliant with CS&RF guidelines.

Cybersecurity in Technology and Operations

As digital transformation accelerates, cybersecurity has become essential to technology and operations in Oman's financial sector. The Cyber Security & Resilience Framework tackles the complex challenges of protecting digital assets.

This framework mandates robust cybersecurity measures to safeguard sensitive information, ensure operational resilience, and maintain the integrity of financial transactions. Given the evolving nature of cyber threats, the CS&RF requires stringent controls and continuous monitoring to mitigate risks, enhance incident response capabilities, and ensure regulatory compliance.

By prioritizing cybersecurity, Oman's financial institutions can build a resilient infrastructure that withstands cyber-attacks and maintains trust in their services.

Requirements

3.3.4 Cryptography

- A process of cryptographic security measures should be defined, approved, implemented, and periodically reviewed and updated.
- Cryptographic mechanisms and algorithms must comply with data privacy and protection policy requirements and industry best practices.
- The Cryptographic security measures should include:
  - » Selection of cryptographic controls (Do not use weak or broken algorithms).
  - » Cryptographic key management.
  - » The key length used for encryption is as per the latest security standards.
  - » Utilization of true pseudo-random number generators.

How Seclore Helps

Seclore employs highly secure encryption algorithms, including AES 256 and RSA 2048, to protect digital assets regardless of how many times they're copied, or the transfer mode—whether via email, USB, shared folder, or another method.

Seclore also supports multi-layered encryption, utilizing various dimensions and parameters, including custom or proprietary encryption methods. This robust approach ensures comprehensive data protection across all environments.

Requirements	How Seclore Helps
3.3.5 Data Loss Prevention (DLP) Solution • The DLP procedure should include: » Data classification	Seclore integrates seamlessly with popular DLP solutions like Broadcom (Symantec®), Forcepoint, McAfee/Trellix, and Skyhigh, so your security investments go further. It also lets users classify and automatically protect assets before sharing them, strengthening email and network DLP systems. Seclore addresses vulnerabilities in the DLP re-scanning process by decrypting data for scanning and re-encrypting it before it leaves the organization. It also integrates with data discovery and classification tools to apply protection and usage controls based on existing labels.
3.3.6 Bring Your Own Device (BYOD) The BYOD procedure should ensure the coverage of the following: • Governance processes include the security of BYOD within information security to minimize risks when users connect devices to systems. • Security controls around the introduction of BYOD to avoid an impact on confidentiality, integrity, and data availability should deploy reasonable security controls, including acceptable usage, encryption, disposal, audit logging, etc. • Implementation and compliance requirements.	Seclore's data-centric security platform protects sensitive digital assets with persistent encryption and granular usage controls, meaning that data is safe on a personal device, company network, or public cloud. Seclore-protected files are also protected by dynamic yet persistent access and rights management controls that can be adjusted remotely. Information owners can also revoke access to any protected file at any time.
3.3.10 Access Control Management • The principles of "segregation of duties," "need-to-have," and "least privileges" should be applied when granting access to the users, and access rights and privileges should be granted according to the roles and responsibilities of the staff, contractors, and third-party vendors.	Seclore rights management enables information owners to apply strict access controls, including time-based and location-based restrictions. Its Digital Rights Management (DRM) capabilities provide fine-grained control over who can access, view, edit, and share sensitive information. Seclore's granular usage controls and remote enforcement of data governance policies allow organizations to safely share protected digital assets with staff, contractors, and third-party vendors while maintaining stringent data security standards. Organizations can instantly revoke access to any protected digital asset when access is no longer needed or unauthorized activity is detected.

Requirements

3.3.16 Secure Disposal of Information Assets

- The licensed institutions should define, approve, and implement a secure disposal standard and procedure.
- The licensed institution should ensure compliance with the secure disposal process and periodically evaluate the effectiveness of the secure disposal of Information Assets.
- Disposal procedures should be proportional to the information asset's classification level, as the higher the classification, the greater the assurance that information cannot be retrieved after disposal. Shredding (cross-cut), incineration, secure wiping, and overwriting are good practices.
- Information assets should be disposed of per regulatory and legal requirements when no longer required.

How Seclore Helps

Information owners can remotely revoke access to digital assets when they need to dispose of sensitive data shared with agencies, partners, or contractors. This eliminates the need for third parties to dispose of information independently and creates a verifiable and secure disposal mechanism for organizations to manage third-party risk effectively.

Cybersecurity in Third-Party Supply Chain Management

Because an organization must share sensitive data with contractors, partners, auditors, and other third parties, a robust cybersecurity strategy must prioritize third-party risk management. BFSI Organizations operating in Oman should include a comprehensive program for addressing cybersecurity risks associated with third-party relationships as part of their overall risk management strategy.

These programs should identify, evaluate, quantify, monitor, predict, and mitigate cybersecurity risks from third-party engagements such as contracts, vendor management, outsourcing, and cloud computing service providers (CCSP).

An effective third-party cybersecurity risk management program includes four key elements:

Assessing Risks
Conduct thorough risk assessments.

Performing Due Diligence
Vet third parties to ensure they meet cybersecurity standards.

Structuring and Reviewing Contracts
Include precise cybersecurity requirements in contracts.

Providing Oversight
Maintain continuous oversight to ensure compliance.

By integrating these components, institutions can enhance their cybersecurity posture and manage third-party risk.

Requirements

3.4.2 Cloud Computing

- Review the cloud policy periodically to ensure compliance with cyber security measures and requirements and that these requirements adequately support cyber security resilience.
- Document the agreements entered into with cloud service providers (CSPs) and ensure the following security requirements, at a minimum:
  - » End-to-end encryption of all sensitive data while double encryption may be considered based on the risk assessment.
  - » Establish control over encryption processes, robust cryptographic key management policy, standards, and procedures covering key generation, distribution, installation, renewal, revocation, recovery, and expiry.
  - » CSPs are to notify the licensed institutions of any data breach/compromise, including the remedial actions taken by CSPs.

How Seclore Helps

Seclore's data-centric security platform offers precise usage controls (view, edit, print, share, and copy) for sensitive digital assets across various platforms, such as email, cloud storage, FTP, or USB drives. It protects data in cloud repositories like SharePoint, OneDrive, and Google Drive, even when shared externally, ensuring that only authorized users can access protected files.

With persistent encryption and granular usage controls, Seclore ensures data security regardless of the network, storage, or device. It provides end-to-end encryption, including double encryption based on risk assessment, for data in transit and at rest.

Seclore securely manages cryptographic keys and supports multi-layered encryption, including custom methods. The Seclore Enterprise Digital Rights Management (EDRM) utilizes AES 256 and RSA 2048 encryption algorithms and can notify stakeholders when unusual or unauthorized activity is detected.

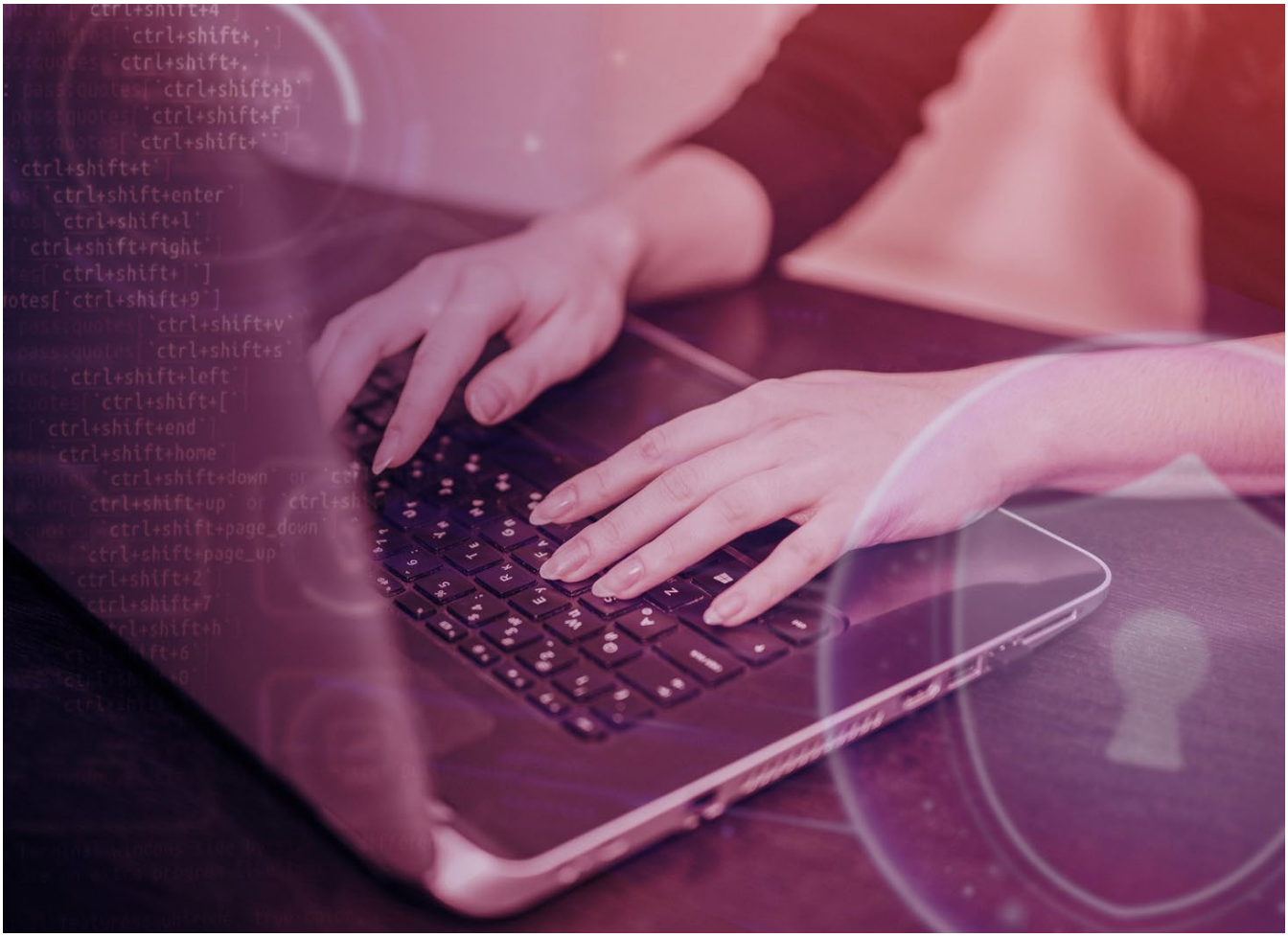
Protect Your Sensitive Data Anywhere

Seclore's data-centric security solution has been proven to:

Help organizations protect their confidential information.

Reduce data leakage and theft.

Improve compliance and reporting capabilities.



The introduction of the Cyber Security & Resilience Framework (CS&RF) by the Central Bank of Oman is a significant milestone in the nation's commitment to strengthening the cybersecurity posture of its financial sector. It sets a high standard for data security practices among BFSI institutions.

In navigating digital transformation, frameworks like CS&RF enhance cybersecurity. The shift to data-centric security, seen in solutions like Seclore, highlights shifting priorities and the need for organizations to adopt modern cybersecurity defense strategies. The ability to continuously adapt to local, regional, and international compliance standards is crucial for safeguarding our digital economy. Oman sets an excellent example for cybersecurity governance in the financial industry and beyond.

SECLORE™

About Seclore

Our mission is to safeguard sensitive information worldwide, regardless of its location. Seclore offers persistent protection and visibility for digital assets to help organizations remain secure and compliant. Our data-centric security approach ensures that only authorized individuals can access protected digital assets. With Seclore, organizations can specify who can access their data, what actions are permitted, and how long that access lasts. Join industry leaders like American Express in choosing Seclore for superior digital asset protection without sacrificing seamless collaboration and sharing.

Visit **seclore.com** for more information.

5201 Great America Parkway
Suite 440
Santa Clara, CA 95054