RIVIAL
DATA SECURITY

# SWIFT Controls Assessment Report

Exclusively prepared for:

## Baxter Credit Union

March 25th, 2024

RIVIAL
SECURED

## Table of Contents

# Executive Summary

## Introduction

Rivial Data Security (Rivial) was contracted by Baxter Credit Union (Baxter) to conduct an assessment that includes a review of security controls compared to the SWIFT security control framework.

Rivial's assessment is designed to express an independent third-party opinion on the suitability of the design and operating effectiveness of the security controls to meet the control objectives in accordance with the SWIFT security control framework. Our assessment was completed by examining evidence to support reasonable assurance that information security controls in place are operating effectively.

The organization is under the Architecture Type B of the Swift framework. No Swift-specific infrastructure components are used within the user environment. To see which controls apply, refer to the table under the Swift Controls Table section. While many controls do not apply to Architecture Type B, all controls were assessed. The controls are good security practices and are noted below.

In our opinion, the information security controls in place at Baxter are adequately designed to provide reasonable assurance that the control objectives are met, and that the controls are operating effectively. Overall, the number of security issues identified during the assessment is ***low*** and Baxter's security posture is ***excellent***.

## Summary of Findings

It is our opinion that:

a) the controls described fairly present Baxter's information security safeguards that were designed and implemented as of March 2024.
b) the controls were designed to provide reasonable assurance that information security control objectives would be achieved if the controls operated effectively throughout the period.

In this report, findings are categorized into four possible areas (high, medium, low, and info) and represented graphically. The chart below depicts the risks found during the SWIFT assessment. There were no findings identified during the SWIFT assessment.


Each finding is ranked as High, Medium, Low or Info. The criticality and a description of risk for these categories are described below:

| | |
|---|---|
| **HIGH** | Should be reviewed and addressed by management immediately. Generally, these items pose a high potential threat to the security or operational viability of the institution. Implementing recommended solutions that are practical and appropriate to the institution as soon as possible will greatly reduce the risk profile of the institution. |
| **MEDIUM** | Should be reviewed and addressed by management in the near future. These items may not pose an immediate threat, but could cause difficulty if not mitigated soon. |
| **LOW** | Should be addressed by management and either resolved, noted for resolution in the future, or documented as an acceptable risk, based on the size and complexity of the system and its associated criticality to business operations. |
| **INFO** | These items do not pose a serious threat to the institution; however, because technologies are continually changing and new threats emerge consistently we recommend the institution maintain a vigilant security posture. |

## Findings and Recommendations

No findings were discovered during the engagement.

## Swift Controls Table

| Mandatory and Advisory Security Controls | Architecture Type | | | | |
|---|---|---|---|---|---|
| | A1 | A2 | A3 | A4 | B |
| **1 Restrict Internet Access and Protect Critical Systems from General IT Environment** | | | | | |
| 1.1 Swift Environment Protection | • | • | • | | |
| 1.2 Operating System Privileged Account Control | • | • | • | • | • |
| 1.3 Virtualisation or Cloud Platform Protection | • | • | • | • | |
| 1.4 Restriction of Internet Access | • | • | • | • | • |
| 1.5 Customer Environment Protection | | | | • | |
| **2 Reduce Attack Surface and Vulnerabilities** | | | | | |
| 2.1 Internal Data Flow Security | • | • | • | | |
| 2.2 Security Updates | • | • | • | • | • |
| 2.3 System Hardening | • | • | • | • | • |
| 2.4A Back Office Data Flow Security | • | • | • | • | • |
| 2.5A External Transmission Data Protection | • | • | • | • | |
| 2.6 Operator Session Confidentiality and Integrity | • | • | • | • | • |
| 2.7 Vulnerability Scanning | • | • | • | • | • |
| 2.8 Outsourced Critical Activity Protection | • | • | • | • | • |
| 2.9 Transaction Business Controls | • | • | • | • | • |
| 2.10 Application Hardening | • | • | • | | |
| 2.11A RMA Business Controls | • | • | • | • | • |
| **3 Physically Secure the Environment** | | | | | |
| 3.1 Physical Security | • | • | • | • | • |
| **4 Prevent Compromise of Credentials** | | | | | |
| 4.1 Password Policy | • | • | • | • | • |
| 4.2 Multi-Factor Authentication | • | • | • | • | • |
| **5 Manage Identities and Separate Privileges** | | | | | |
| 5.1 Logical Access Control | • | • | • | • | • |
| 5.2 Token Management | • | • | • | • | • |
| 5.3A Staff Screening Process | • | • | • | • | • |
| 5.4 Physical and Logical Password Storage Protection | • | • | • | • | • |
| **6 Detect Anomalous Activity to Systems or Transaction Records** | | | | | |
| 6.1 Malware Protection | • | • | • | • | • |
| 6.2 Software Integrity | • | • | • | • | |
| 6.3 Database Integrity | • | • | | • | |
| 6.4 Logging and Monitoring | • | • | • | • | • |
| 6.5A Intrusion Detection | • | • | • | • | |
| **7 Plan for Incident Response and Information Sharing** | | | | | |
| 7.1 Cyber Incident Response Planning | • | • | • | • | • |
| 7.2 Security Training and Awareness | • | • | • | • | • |
| 7.3A Penetration Testing | • | • | • | • | • |
| 7.4A Scenario-based Risk Assessment | • | • | • | • | • |

## Review of SWIFT Controls

The controls below were provided by SWIFT and attest that an adequate security program is in place.

Testing was performed March 2024.

## SWIFT Control Details

| Control ID | Control Objective | Control Statement | Assessment Notes |
|---|---|---|---|
| **1** | | | |
| **1.1** | Ensure the protection of the user's Swift infrastructure from potentially compromised elements of the general IT environment and external environment. | A separated secure zone safeguards the user's Swift infrastructure from compromises and attacks on the broader enterprise and external environments. | Interviewed Senior Network Engineer: Roam VDI environment is used to access infrastructure - this is the same VDI environment used across the organization. The network is segmented into logical units separated by firewalls. VDI's are scattered across 5 different subnets.<br><br>Interviewed Senior Operations Manager: Test machines are designated for testing but are on the same network.<br><br>Interviewed Senior Network Engineer: FedLine computers are on the general subnet. Laptops are limited to which network resources they can talk to (workstations are not). NAC and 802.1x work together to:<br>1. Prevent unauthorized machines from connecting to the environment<br>2. limit access logically<br><br>Everything processed is through Wells Fargo and is where transactions occur. All done on regular machines. Everyone uses laptops as daily machines. Few desktops in branches, most primarily device. Desktop uses 802.1x. |
| | | a) Overall design for implementing environment segregation (p 28) | |
| | | b) Scope of the secure zone | |
| | | c) Protection of the secure zone | |
| | | d) Access to secure zone systems 1. Local Operator | Interviewed Senior Operations Manager: Users do not have access |

| | | | |
|---|---|---|---|
| | | (end user and administrator) access | at an admin level on either physical or VDI workstations. Users can use personal devices to connect to the Roam environment (VDI). This is insulated from the machine used to access to Roam network. |
| | | d) 2. Remote Operator Access (teleworking, "on-call" duties, or remote administration) | Interviewed Senior Operations Manager: Users do not have remote operator access. |
| | | e) Separation from General Enterprise IT Services | Interviewed Senior Network Engineer: Roam environment is separated from general IT infrastructure through Roam VDI subnets. |
| **1.2** | Restrict and control the allocation and usage of administrator-level operating system accounts. | Access to administrator-level operating system accounts is restricted to the maximum extent possible. Usage is controlled, monitored, and only permitted for relevant activities such as software installation and configuration, maintenance, and emergency activities. At all other times, an account with the least privilege access is used. | Interviewed Senior Manager on Security Team (physical security): There is no local admin access on computers.<br><br>Interviewed Senior Operations Manager: Using a variant of LAPS to control admin permissions (changes password daily). This is accessed through Intune and to use it requires TeamViewer which is RBAC'd. |
| **1.3** | Secure the virtualization or cloud platform and virtual machines (VMs) that host Swift-related components to the same level as physical systems | Secure the virtualization or cloud platform, virtualized machines, and the supporting virtual infrastructure (such as firewalls) to the same level as physical systems. | Interviewed Senior Operations Manager & Director of Member Operations: Roam VDI or Wells Fargo is used for all access. BCU is not hosting any SWIFT related applications. |
| **1.4** | Control/Protect Internet access from operator PCs and systems within the secure zone. | All general-purpose and dedicated operator PCs, as well as systems within the secure zone, have controlled direct internet access in line with business. | Interviewed Senior Operations Manager: Internet access for the VDI environment is controlled through enterprise controls: URL/content filtering.<br><br>Interviewed Senior Manager on Security Team (Ifra/ops/monitoring): URL filtering |
| | | a) Internet access from the secure zone (p 37) | |

| | | | |
|---|---|---|---|
| | | b) Internet access from general-purpose operator PCs | is done through the firewalls (blocks personal email and social media unless exceptions are made). This also pulls threat feeds and blocks anything tagged as malicious.<br>For remote work using NetScope to block content.<br><br>Interviewed Senior Operations Manager & Senior Manager on Security Team (Ifra/ops/monitoring): The wire PC's are locked down GP to whitelist only required sites. |
| | | c) Internet access from other components (middleware servers or the virtualization platform – Advisory) | |
| **1.5** | Ensure the protection of the customer's connectivity infrastructure from external environment and potentially compromised elements of the general IT environment. | A separated secure zone safeguards the customer's infrastructure used for external connectivity from external environments and compromises or attacks on the broader enterprise environment. | Would have to have a set of VDIs to Ops team. Currently are not doing it. Control is not applicable to the organization as they are architecture type B. |
| | | a) Overall design goals for implementing environment separation | |
| | | b) Scope of the secure zone | |
| | | c) Protection of the secure zone | |
| | | d) Access to the secure zone systems.1 Local Operator (end user and administrator) Access | |
| | | d) 2. Remote Operator Access (teleworking, "on-call" duties, or remote administration) | |
| | | e) Separation from General Enterprise IT Services | |
| **2** | | | |
| **2.1** | Ensure the confidentiality, integrity, and authenticity of application data flows between 'user's Swift-related components. | Confidentiality, integrity, and authentication mechanisms are implemented to protect Swift-related component-to-component or system-to-system data flows. | N/A, do not have components, all on website |

| | | | |
|---|---|---|---|
| **2.2** | Minimize the occurrence of known technical vulnerabilities on operator PCs and within the user's Swift infrastructure by ensuring vendor support, applying mandatory software updates, and applying timely security updates aligned to the assessed risk. | All hardware and software inside the secure zone and on operator PCs are within the support life cycle of the vendor, have been upgraded with mandatory software updates, and have had security updates promptly applied. | Inspected vulnerability tracking spreadsheet to find that vulnerabilities are tracked based on criticality and assets affected.<br><br>Interviewed the BCU team to find that scanning is weekly and patches are rolled out depending on priority or on a monthly cycle. The Roam VDI image is scanned for vulnerabilities and patched on the same cadence. |
| **2.3** | Reduce the cyber-attack surface of Swift-related components by performing system hardening. | Security hardening is conducted and maintained on all in-scope components. | Interviewed Senior Manager on Security Team (Ifra/ops/monitoring): Do hardening for VDIs. Hardening GP's are in place to limit PC's to necessary functions only and there is no local admin access for users. Using GP to only allow specific executables (approved browsers, SCCM - this is highly restricted). |
| **2.4A** | Ensure the confidentiality, integrity, and mutual authenticity of data flowing between on-premises or remote Swift infrastructure components and the back-office first hops they connect to. | Confidentiality, integrity, and authentication mechanisms (at system, transport, message or data level) are implemented to protect data flows between Swift infrastructure components and the back-office first hops they connect to. | Interviewed Senior Manager on Security Team: Several authentication controls are in place:<br><br>1. Biometrics & badges are controlling the room with the FedLine computer<br>2. Roam VDI's are access controlled<br>3. FedLine standard RBAC controls<br>4. FedLine Token required for the Wire process |
| **2.5A** | Protect the confidentiality of Swift-related sensitive data transmitted or stored outside of the secure zone as part of operational processes. | Sensitive Swift-related data that leaves the secure zone as a result of operating system/application back-ups for recovery purposes, business transaction data replication for archiving, or extraction for offline processing is protected when stored outside of a secure zone and is encrypted while in transit | Interviewed Senior Operations Manager: Data does not live on the FedLine PC's (is only stored on BCU core or on Fed). N/A to organization. |

| | | | |
|---|---|---|---|
| | | to the first storage location. | |
| **2.6** | Protect the confidentiality and integrity of interactive operator sessions that connect to the on premises or remote (operated by a service provider or outsourcing agent) Swift infrastructure or to a service provider or outsourcing agent Swift-related applications. | The confidentiality and integrity of interactive operator sessions that connect to service provider or outsourcing agent Swift-related applications or into the user's secure zone are safeguarded. | Interviewed Senior Operations Manager: No service providers with access, only internal IT team. Remote sessions require positive affirmation on the other side. All done on website.<br><br>Interviewed Senior Manager on Security Team (physical security) & Senior Manager on Security Team (Ifra/ops/monitoring): The only exception would be for backend access for CrowdStrike (CMD only, not application). This connection would require supervision. |
| **2.7** | Identify known vulnerabilities within the user's Swift environment by implementing a regular vulnerability scanning process and act upon results. | Secure zone (including dedicated operator PC) systems are scanned for vulnerabilities using an up-to-date, reputable scanning tool and results are considered for appropriate resolving actions. | Interviewed Senior Operations Manager: Computers are managed through the vulnerability program. Weekly vulnerability scans done internally. Everything is in scope of penetration testing. |
| **2.8** | Ensure the protection, in line with the CSCF, of the user's Swift infrastructure from risks exposed by the outsourcing of critical activities. | Critical outsourced activities are protected, at a minimum, to the same standard of care as if operated within the originating organization. | Interviewed Director of Business Resiliency: There are no vendors who provide critical services or interact with the SWIFT system.<br><br>No exceptional vendor management process for Swift related vendors.<br><br>Wells Fargo is the vendor providing the SWIFT infrastructure. They went through the standard vendor review process to review the SOC report and other sources and they also go through an annual review process. |
| **2.9** | Ensure outbound transaction activity within the expected bounds of normal business. | Implement transaction detection, prevention, or validation controls, or a combination of them to ensure outbound transaction activity within the expected bounds of normal business. | Interviewed Director of Member Operations: Any transactions submitted outside of normal hours would wait as pending until the next batch time. The wire process uses separation of duties/dual controls. Only time using Swift is for international wires which is minimal. |

| | | | |
|---|---|---|---|
| | | 1) Limiting traffic outside of business hours | Process is the same logging into wells, etc. They then submit and it goes to Wells directly and is on the Wells website. |
| | | 2) limiting traffic beyond normal business amount ranges | |
| | | 3) Performing end-of-day and (possibly) intra-day validations or reconciliations through any or a combination of the following | Interviewed Director of Member Operations: Batches are sent 3 times a day and has a built-in process for validation |
| | | 4) Performing central checks on payments to spot potential abnormal behavior | Interviewed Director of Member Operations: All wire transactions through FedLine go through BSA/fraud monitoring. Accounting department and operations and director of accounting will go through process of transfer or problems within Wells Fargo. |
| | | 5) performing independent reconciliation with transaction data securely obtained from a secondary source (either internal or external, such as reports from service providers) or verifying that the transaction is genuine with the emitter or the recipient (or both) | |
| **2.10** | Reduce the attack surface of Swift-related components by performing application hardening on the Swift-compatible messaging and communication interfaces, the Swift connector and related applications. | All messaging interfaces and communication interfaces products within the Swift secure zone are Swift compatible. Application security hardening is conducted and maintained on all in-scope components. | Interviewed Senior Manager on Security Team (Ifra/ops/monitoring): Hardening GP's are in place to limit FedLine PC's to necessary functions only and there is no local admin access for users. Using GP to only allow specific executables (approved browsers, SCCM - this is highly restricted). N/A to organization. |
| **2.11 A** | Restrict transaction activity to validated and approved business counterparties. | Implement RMA controls to restrict transaction activity with effective business counterparties. | N/A |
| **3** | | | |
| **3.1** | Prevent unauthorized physical access to sensitive equipment, | Physical security controls are in place to protect access to sensitive | Interviewed Director of Member Operations: The environment is access controlled using biometrics. The Roam environment is hosted in |

| | | | |
|---|---|---|---|
| | workplace environments, hosting sites, and storage. | equipment, hosting sites, and storage. | Azure. Backup FedLine computer is in a data center with comparable physical security controls. |
| | | Security of removable equipment | Interviewed Senior Manager on Security Team (physical security): CrowdStrike policy disallows USB usage outside of keyboard/mouse and the FedLine token. |
| | | Security of the Workplace Environment | Interviewed Senior Manager on Security Team (physical security): Using card access for the building, visitors are escorted, video cameras are monitoring the room with physical computers. Video camera feed is maintained for 90 days. |
| | | Security for Remote Workers | Interviewed Senior Manager on Security Team (physical security): There is policy language at BCU to cover physical protection of assets. Employees are also required to attend annual awareness training which includes topics of physical security from remote work. There is also quarterly training on select topics including physical security from time to time. New hire training as well for tailgating, and other physical training aspects. |
| | | Security of the Server Environment | Interviewed Senior Manager on Security Team (physical security): The server environment is secured with badged access control which uses an access request process and is monitored by video cameras. IDF closets are provisioned to network/service desk teams only. All other access has to be requested and approved. |
| | | Equipment Disposal | Standard equipment disposal in place. Nothing specific to Swift as use Wells Fargo for Swift. |
| | | Physical Access Logging and Review | Interviewed Senior Manager on Security Team (physical security): Badge system includes auditing controls. Abnormalities in access logs don't have a method of active |

| | | | |
|---|---|---|---|
| | | | alerting however there is a monthly review of access logs. |
| **4** | | | |
| **4.1** | Ensure passwords are sufficiently resistant against common password attacks by implementing and enforcing an effective password policy. | All application and operating system accounts enforce passwords with appropriate parameters such as length, complexity, validity, and the number of failed login attempts. Similarly, personal tokens and mobile devices enforce passwords or a Personal Identification Number (PIN) with appropriate parameters. | Interviewed Senior Manager on Security Team (physical security): BCU uses password standards set in AD: 14 char, U/L/#/*. Also using Azure password protection which compares passwords to a known-bad password list maintained by Microsoft (also includes a custom list Baxter has developed). Wells Fargo sets parameters to 8-14 minimum, 1 letter, 1 number, and 1 special character. |
| **4.2** | Prevent that a compromise of a single authentication factor allows access into Swift-related systems or applications by implementing multi-factor authentication. | Multi-factor authentication is used for interactive user access to Swift-related components or applications and operating system accounts. | Interviewed Senior Manager on Security Team (physical security): The ROAM environment requires MFA. For Swift, access to the Wells Fargo site requires MFA from every user. |
| **5** | | | |
| **5.1** | Enforce the security principles of need-to-know access, least privilege, and separation of duties for operator accounts | Accounts are defined according to the security principles of need-to-know access, least privilege, and separation of duties. | Interviewed Senior Manager on Security Team (physical security): Baxter is currently implementing RBA through IdentityNow. Access to FedLine room is assigned only to approved personnel.<br><br>Interviewed Senior Operations Manager: They are limited by being in locked rooms and RTP being controlled.<br><br>Interviewed Senior Operations Manager: Active Directory access to the FedLine machine is not currently limited to approved personnel but it would also be further limited by not having a fed token.<br><br>Least privilege would be applied to Swift environment as well. |

| | | | |
|---|---|---|---|
| | | Need-to-know | There are specific GPO's for the Manager of Systems Engineering: FedLine computers, these are highly restrictive.<br>Swift access is granted on need-to-know basis. |
| | | Least privilege | Interviewed Manager of Systems Engineering: FedLine computers are highly restricted using GPO's.<br>Least privilege in place for Swift. |
| | | Separation of Duties and Four-Eyes | Interviewed Director of Member Operations: FedLine is set up to use separation of duties to limit who can submit and approve transfers. Swift environment in place as well. |
| | | Account Review and Revocation | Interviewed Director of Member Operations: Logical and physical access to the Swift system is reviewed and adjusted appropriately. |
| | | An emergency procedure to access privileged accounts is documented for use when authorized people are unavailable due to unexpected circumstances | |
| **5.2** | Ensure the proper management, tracking, and use of connected and disconnected hardware authentication or personal and software tokens (when tokens are used). | Connected and disconnected hardware authentication or personal tokens are managed appropriately during their assignment, distribution, revocation, use, and storage. | Interviewed Director of Member Operations: EAUC's and users with access to Swift are highly controlled. |
| **5.3A** | To the extent permitted and practicable, ensure the trustworthiness of staff operating the user's Swift environment by performing regular staff screening. | Staff operating the user's Swift infrastructure are screened prior to initial appointment in that role and periodically thereafter | Inspected the background check sample to find that initial background checks are performed on new employees.<br><br>Interviewed Security Analyst to find that employees reviews are also done at least once every five years. |
| **5.4** | Protect physically and logically the repository of recorded passwords. | Recorded passwords are stored in a protected physical or logical location, with access restricted on a need-to-know basis. | N/A |
| **6** | | | |

| | | | |
|---|---|---|---|
| **6.1** | Ensure that the user's Swift infrastructure is protected against malware and act upon results. | Anti-malware software from a reputable vendor is installed, kept up-to-date on all systems, and results are considered for appropriate resolving actions. | Interviewed Senior Manager on Security Team (Ifra/ops/monitoring): CrowdStrike is updating definitions and scanning automatically and alerted through the SOC. |
| **6.2** | Ensure the software integrity of the Swift-related components and act upon results | A software integrity check is performed at regular intervals on messaging interface, communication interface, and other Swift-related components and results are considered for appropriate resolving actions. Origin and integrity of the software is ensured at download and at deployment time. | Interviewed Senior Manager on Security Team (Ifra/ops/monitoring): CrowdStrike inherently monitors file integrity values as part of the malware detection process. |
| **6.3** | Ensure the integrity of the database records for the Swift messaging interface or the customer connector and act upon results. | A database integrity check is performed at regular intervals on databases that record Swift transactions and results are considered for appropriate resolving actions. | Interviewed CISO: Org is an Architecture B so this does not apply. Wells Fargo hosts all infrastructure. |
| **6.4** | Record security events, detect and respond to anomalous actions and operations within the user's Swift environment. | Capabilities to detect anomalous activity are implemented, and a process or tool is in place to keep and review logs. | Interviewed Senior Manager on Security Team (Ifra/ops/monitoring): Arctic Wolf is the SIEM tool and the FedLine computers are integrated with it. CrowdStrike, firewalls, and AD are the only monitoring/reporting tools to report on malicious software/AD object level changes. These changes are notified through the SOC. |
| | | Overall goals for logging and monitoring | |
| | | Logging | Interviewed Senior Manager on Security Team (physical security) & Senior Manager on Security Team (Ifra/ops/monitoring): CrowdStrike records are maintained for 45 days and firewall logs are kept for 90. |
| | | Monitoring | Interviewed Senior Manager on Security Team (Ifra/ops/monitoring): Arctic Wolf is the SIEM tool and the FedLine |

| | | | |
|---|---|---|---|
| | | | computers are integrated with it. CrowdStrike, firewalls, and AD are the only monitoring/reporting tools to report on malicious software/AD object level changes. These changes are notified through the SOC. |
| | | Log retention | Interviewed Senior Manager on Security Team (physical security) & Senior Manager on Security Team (Ifra/ops/monitoring): CrowdStrike records are maintained for 45 days and firewall logs are kept for 90. |
| **6.5A** | Detect and contain anomalous network activity into the on-premises or remote Swift environment. | Intrusion detection is implemented to detect unauthorized network access and anomalous activity. | Interviewed Senior Manager on Security Team (Ifra/ops/monitoring): The firewalls have IDS built in, using SecureWorks as a network level IPS. |
| **7** | | | |
| **7.1** | Ensure a consistent and effective approach for the management of cyber incidents. | The user has a defined and tested cyber incident response plan. | Interviewed Senior Manager on Security Team (Ifra/ops/monitoring): Organization maintains an incident response plan. The IRP is updated at least annually and when regs change or testing provides input for improvement. |
| **7.2** | Ensure all staff are aware of and fulfil their security responsibilities by performing regular awareness activities, and maintain security knowledge of staff with privileged access. | Annual security awareness sessions are conducted for all staff members with access to Swift-related systems. All staff with privileged access maintain knowledge through specific training or learning activities when relevant or appropriate (at management's discretion). | Interviewed the Security Analyst to find that this is in place. There is quarterly training for all users in the company with training categories covering specific training categories. Semi-annual training is done to users with elevated roles and responsibilities. If a big incident occurs, training will also be done over incident. New hire training is done as well. Nothing specific for Swift, member operations may provide additional training for users who use system. |
| **7.3A** | Validate the operational security configuration and identify security gaps by performing penetration testing. | Application, system and network penetration testing is conducted towards the secure zone and the operator PCs or, when used, the jump server. | Interviewed Senior Manager on Security Team (Ifra/ops/monitoring): The FedLine PC's are included in weekly vulnerability scanning in their own unique group (for unique reporting). Penetration tests are done annually: FedLine PC's are included in the |

| | | | |
|---|---|---|---|
| | | | range of targets and tested at the testers discretion. Everything is in scope of penetration tests. Vulnerability scans are done weekly internally. |
| **7.4A** | Evaluate the risk and readiness of the organization based on plausible cyber-attack scenarios. | Scenario-based risk assessments are conducted regularly to improve incident response preparedness and to increase the maturity of the organization's security program. | Interviewed Director of Business Resiliency: There is an annual IRP tabletop and each year the scenario changes based on identified risks or outputs of various audit processes (other security assessments) or other real-life incidents relevant to BCU. |