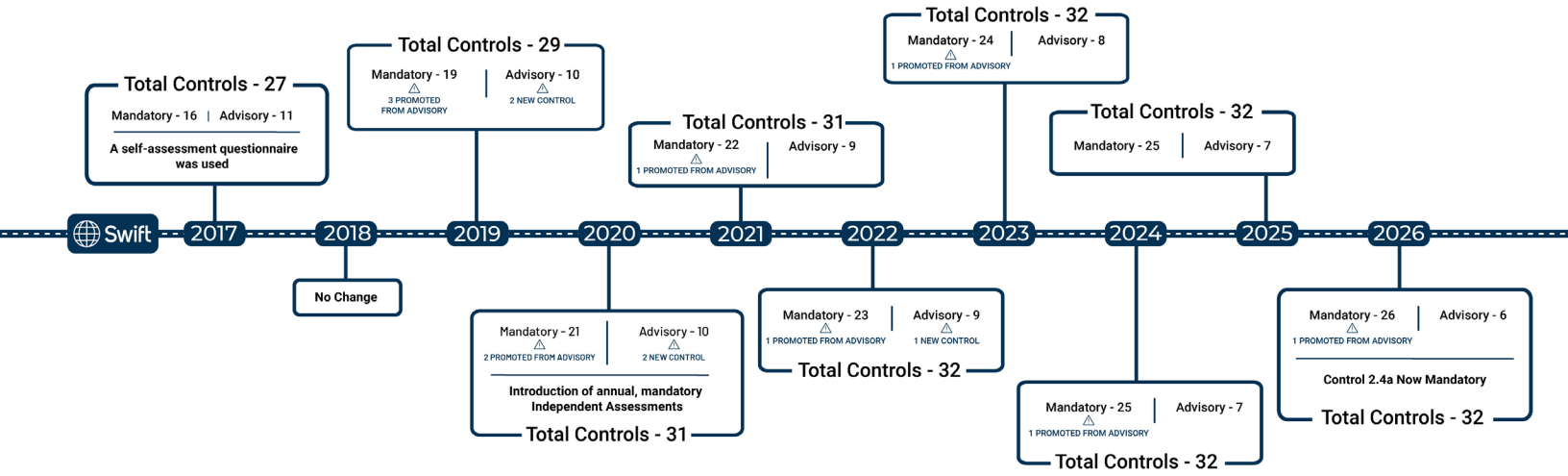
Bottomline

Swift Customer Security Programme (CSP)

CUSTOMER GUIDE

Featuring Guidance for the Customer Security Controls Framework (CSCF) 2026

SWIFT CSP | Key Changes Over Time



Executive Summary

Swift users are obligated to carry out an independent assessment annually when self-attesting to the Customer Security Programme. These can be done through either:

- **Internal assessment** carried out by the company's second- or third- line of defence such as the users' internal compliance, internal risk of internal audit departments (independent from the first line of defence function submitting the attestation);

or

- **External assessment** carried out by an independent external organisation with cyber security assessment experience and individual assessors who have relevant security industry certification.

As a minimum, the 'Community Standard Assessments' must cover all mandatory controls in the latest version of the Customer Security Controls Framework (CSCF) that are applicable based on a user's CSP architecture type and infrastructure. Users that have attested against advisory controls may also consider asking the assessor to include these in the evaluation.

As part of our continuous efforts to support our clients in meeting their obligations, Bottomline has partnered with A Jolly Consulting, to help facilitate the process for our customers.

The purpose of this document is not to explain the CSP, but to provide a simplified summary of what the controls mean, and how we can help you. We strongly encourage your teams read Swift published documentation for full technical descriptions.

Bottomline Summary

We fully support the rationale behind the CSP and welcome the 'raising of the bar' when it comes to payment security. We strongly recommend that you embrace the initiative not as a tick-box exercise but to genuinely ensure your standards are increased.

Cyber fraud sits in a fast-paced and evolving environment. Securing payments is becoming more critical than ever before. It is our expectation that this programme will continue to evolve as new threats emerge and weaknesses come to light; meaning new controls, and the promotion of advisory to mandatory will likely continue as we have seen before.

Swift customers are responsible for reviewing infrastructure and meeting control standards.

Section 1

Restrict Internet Access and Protect Critical Systems from General IT Environment

1.1 Swift Environment Protection

Mandatory Control

- ○ Bottomline supports CSP compliance
- ✓ Bottomline helps me ask the right questions

What does it mean?

- Segregating Swift related components from non-Swift across the environments.

What can you learn from Bottomline to meet this control?

- As a bureau client, we ensure our corporate infrastructures are completely segregated from Swift related, to ensure compliance. Assurance can be provided by Bottomline through internal audit reports.

What else should you do to meet the control?

- Ask your IT teams to check how you connect, and how Users access the systems. You must ensure you have a separate segregated connection in place into the bureau. e.g. SFTP connection must be separated.

2026 UPDATE

1.2 Operating System Privileged Account Control

Mandatory Control (Advisory for Type B Architecture)

- ○ Bottomline supports CSP compliance
- ✓ Bottomline helps me ask the right questions

What does it mean?

- Limit access and control of operating system level accounts like “Administrator” or “Root”.

What can you learn from Bottomline to meet this control?

- We ensure that usage of OS level privileged accounts is strictly limited and controlled as per Swift guidelines in our bureau infrastructure.
- It remains client responsibility for on-premise deployment.

What else should you do to meet the control?

- Ask your IT teams and check the usage of OS privileged accounts along with supporting policies and procedures.

2026 Update:

- Control 1.2 now includes guidance on break-glass account usage linked to change surrounding Alliance Left Hand and Right Hand Security Officer (LSO/RSO) Accounts

1.3 Virtualisation Platform Protection

Mandatory Control

- ✓ Bottomline supports CSP compliance
- ✓ Bottomline helps me ask the right questions

What does it mean?

- Ensure that virtual machines hosting Swift related components are appropriately protected.

What can you learn from Bottomline to meet this control?

- We ensure that virtual servers are protected to the same level as physical servers and are in line with Swift guidelines for our bureau infrastructure.
- It remains client responsibility for on-premise deployment.

What else should you do to meet the control?

- Ask your IT teams and check the virtual machines hosting Swift related components are protected to at least the same level as physical servers.

1.4 Restriction of Internet Access

Mandatory Control

- Bottomline supports CSP compliance
- Bottomline helps me ask the right questions

What does it mean?

- Limit internet access for all components within the 'secure zone' and PC's connecting to the secure zone.

What can you learn from Bottomline to meet this control?

- We ensure that internet access is restricted on all Swift related components as per Swift guidelines in our bureau infrastructure.
- It remains client responsibility for on-premise deployment.

What else should you do to meet the control?

- Ask your IT teams to restrict access to the internet for all components within the secure zone and those PC's connecting to it.

1.5 Customer Environment Protection

Mandatory Control for Architecture Type A4

- Bottomline supports CSP compliance
- Bottomline helps me ask the right questions

What does it mean?

- Protect via segregation, the customer's connectivity from external risk and other devices within the IT environment.

What can you learn from Bottomline to meet this control?

- We ensure that the connectivity of the customer on all Swift related components is protected as per Swift guidelines for our bureau infrastructure.
- It remains client responsibility for on-premise deployment.

What else should you do to meet the control?

- Ask your IT team to configure your connector server in its own VLAN network, and/or only allow connections from expected devices, blocking all other internal and external connection with a firewall.

Section 2

Reduce Attack Surface and Vulnerabilities

2026 UPDATE

2.1 Internal Data Flow Security

Mandatory Control

- Bottomline supports CSP compliance
- Bottomline helps me ask the right questions

What does it mean?

- Ensure data exchanged between operator and Swift related components is protected for confidentiality, integrity and authenticity.

What can you learn from Bottomline to meet this control?

- A2/A3 – We activate cryptographic algorithms between components

What else should you do to meet the control?

- Ask your IT teams to enforce usage of cryptographic protocols wherever they are available (Web browsers, file transfers, etc.).

2026 Update – Updated Cryptography Enquirements

- Controls 2.1, 2.4, 2.5A, and 2.6 must follow the revised cryptography standards defined in Swift knowledge base article 5.21566. Minimum key sizes now apply.

2.2 Security Updates

Mandatory Control

- Bottomline supports CSP compliance
- Bottomline helps me ask the right questions

What does it mean?

- Reduce the risk of attacks and fix known vulnerabilities by applying security patches.

What can you learn from Bottomline to meet this control?

- Regular deployment of security patches from third-party vendors, compliance with latest security updates from third party components (e.g. database). Automatic deployment of Windows updates.

What else should you do to meet the control?

- Ask your IT for regular deployment of security patches from third-party vendors and upgrade your systems to the versions allowing to apply latest security patches and automatic deployment of Windows updates.

2026 UPDATE

2.3 System Hardening

Mandatory Control

- Bottomline supports CSP compliance
- Bottomline helps me ask the right questions

What does it mean?

- Reduce the risk of attacks by applying best practices and security guidance for systems configuration.

What can you learn from Bottomline to meet this control?

- Bottomline performs system hardening as standard in our bureau environments. Available on request for Bureau services is our SSAE16 / ISAE3402 audit reports.

What else should you do to meet the control?

- Ask your IT to apply industry best practices and Swift recommendations.
  Ensure segregation of duty and "need to know" access. Disable unnecessary services or accounts, remove default passwords.

2026 Update

- Control 2.3 requires that all devices in the Swift secure zone, plus customer connectors and bridging servers outside of the secure zone, are hardened. Hardening typically involves disabling unnecessary features to prevent them from being used in security attacks.
  - The Swift CSCF 2026 change applies to the Windows operating systems on servers and workstations. Two specific
  - Windows -based technologies must be restricted as part of the Windows administration: WMI and PowerShell.

2026 UPDATE

2.4a Back Office Data Flow Security

Mandatory Control

- Bottomline supports CSP compliance
- Bottomline helps me ask the right questions

What does it mean?

- Purpose of control type is to protect confidentiality, integrity and availability of data. The scope has removed any references to customer connector.

What can you learn from Bottomline to meet this control?

- As a bureau, we provide options to interface your applications securely (e.g. MQ over SSL, SFTP file transfer, etc.).
- SAA Customers – can utilise Bottomline's Secure Data in Transit, which will authenticate the file transfer.

Authentication/signature for a FIN message, enabling end to end authentication for a transaction or file using Swift Alliance Access (SAA) or Gateway.

What else should you do to meet the control?

- Speak with your Bottomline Account Manager to confirm Secure Data in Transit service is enabled.
- Ask your IT teams to enforce usage of secure protocols to interface back-office applications.

2026 Update:

- Control 2.4 is now mandatory. In 2025 clients had to document their back-office data flow. In 2026, the inventory must still be shown but three elements now require implementation of and evidence to support secure protection. These are:
  - New direct flows introduced between the organisation's secure zone and the back-office first hop, use an encrypted protocol for data transfer.
  - Any bridging servers themselves, that sit between the organisation's secure zone and the back-office first hop, are protected, by inclusion in the scope of thirteen (13) other Swift mandatory controls namely 1.2, 1.3, 1.4; 2.2, 2.3, 2.6, 2.7; 3.1; 4.1; 5.1; 5.4; 6.1; and 6.4.
  - The data flows from the secure zone to the bridging servers themselves use an encrypted protocol for data transfer.
- Control 2.4 does not apply to Architecture B, as there is no back-office system integration for that architecture. As of
- 2025, Architecture B only applies to GUI application use, where there are no messages or file transfers by any means to or from Swift.

2.5a External Transmission Data Protection

Advisory Control

- ○ Bottomline supports CSP compliance
- ✓ Bottomline helps me ask the right questions

What does it mean?

- Protect data confidentiality when extracted out of the Swift infrastructure for backups or archiving.

What can you learn from Bottomline to meet this control?

- Only backed up data is taken out of the secure zone, and it is encrypted.

What else should you do to meet the control?

- Ask your IT teams to enforce usage of encryption algorithms for all data moving out of the secure zone. Define supervised processes and 'Need to Know' access when extracting data.

2.6 Operator Session Confidentiality and Integrity

Mandatory Control

- ✓ Bottomline supports CSP compliance
- ✓ Bottomline helps me ask the right questions

What does it mean?

- Ensure confidentiality and integrity of user's sessions connecting to the Swift infrastructure.

What can you learn from Bottomline to meet this control?

- Bottomline ensures secure sessions by using SSH protocols for all Swift components access and enable inactivity lock-out of sessions.

What else should you do to meet the control?

- Ask your IT teams to enforce usage of encryption algorithms and session timeout for all user sessions.

2.7 Vulnerability Scanning

Mandatory Control

- ○ Bottomline supports CSP compliance
- ✓ Bottomline helps me ask the right questions

What does it mean?

- Identify known vulnerabilities within the local Swift environment by implementing a regular vulnerability scanning process.

What can you learn from Bottomline to meet this control?

- Covered by Swift SIP accreditation. Bottomline performs regular vulnerability checks and penetration testing internally, or by external auditor that meet the requirements of Swift.

What else should you do to meet the control?

- Ask your IT to advise what regular vulnerability scanning and penetration testing is carried out on Swift components.

2.8 Outsourced Critical Activity Protection

Mandatory Control

- Bottomline supports CSP compliance
- Bottomline helps me ask the right questions

What does it mean?

- Ensure the protection, in line with the CSCF, of the user's Swift infrastructure from risks exposed by the outsourcing of critical activities.

What can you learn from Bottomline to meet this control?

- Bottomline is compliant with the Swift SIP requirements. Bottomline defines an SLA as part of the contract with its customers and undertake annual audit of its bureau services. We undertake annual vendor risk management program for all key/critical vendors.

What else should you do to meet the control?

- Ensure SLA and risk assessment is in place with other third parties, to comply with Bureau SIP / CSP accreditations.

2026 UPDATE

2.9 Transaction Business Controls

Mandatory Control

- Bottomline supports CSP compliance
- Bottomline helps me ask the right questions

What does it mean?

- Ensure that message processing (transactions) are conducted within expected bounds and limits.

What can you learn from Bottomline to meet this control?

- Provide access for RMA housekeeping.
- Transaction anomaly detection is used to identify suspicious payment messages out of expected bounds and limits before sending into the Swift network.
- Message or payment reconciliation.

What else should you do to meet the control?

- Check and review your RMAs and ensure they are still relevant and still current. Remove any redundant agreements.

2026 Update:

- The 2026 CSCF now allows the use of Swift Universal Confirmation data to satisfy this requirement. This service provides real-time status information on payments. For each payment, you can view its status, and the date funds were credited to the account.

2026 UPDATE

2.10 Application Hardening

Mandatory Control

- Bottomline supports CSP compliance
- Bottomline helps me ask the right questions

What does it mean?

- Ensure all applications within the scope of the CSP are appropriately hardened.

What can you learn from Bottomline to meet this control?

- We ensure that all applications within the bureau infrastructure including disabling all non-critical features, capabilities and functions.
- It remains client responsibility for on-premise deployment.

What else should you do to meet the control?

- Ask your IT teams and check that all applications have been hardened including the disabling of all non-critical features/capabilities.

2026 Update:

- Alliance Left and Right Security Officer (LSO and RSO) accounts are now named as privileged accounts. Control 2.10 must also look at hardening of the account access.
- This control now includes guidance on break-glass account usage.

2.11a RMA Business Controls

Advisory Control

- Bottomline supports CSP compliance
- Bottomline helps me ask the right questions

What does it mean?

- Ensure business transactions are restricted to effective business counterparties.

What can you learn from Bottomline to meet this control?

- Provide Access for RMA.
- Perform regularly due diligence on RMA and ensure obsolete counterparties are removed.
- It remains client responsibility for on-premise deployment.

What else should you do to meet the control?

- Ensure periodic due diligence is performed on all RMA.
- Obsolete RMA's are removed in a timely manner.

Section 3

Physically Secure the Environment

2026 UPDATE

3.1 Physical Security

Mandatory Control

- Bottomline supports CSP compliance
- Bottomline helps me ask the right questions

What does it mean?

- Prevent unauthorised physical access to sensitive equipment, workplace environments, hosting sites, and storage.

What can you learn from Bottomline to meet this control?

- The Bottomline bureau restricts physical access to the Swift infrastructure to authorised personnel or, when absolutely required, to other parties accompanied by authorised personnel as per SIP requirement. Badge and/or biometric access controls is in place.

What else should you do to meet the control?

- Verify physical security access controls are in place for local Swift infrastructure.

2026 Update:

- Luna Backup Device Hardware Security Module (a special type of Hardware Security Module, HSM) device is now included in the scope of Control 3.1, as a valid location for a Password Repository.
- The requirements of this control remain unchanged.

Section 4

Prevent Compromise of Credentials

4.1 Password Policy

Mandatory Control

- Bottomline supports CSP compliance
- Bottomline helps me ask the right questions

What does it mean?

- Implement complex passwords and password policies for Swift components.

What can you learn from Bottomline to meet this control?

- Password policy is in place with enforcement through Active Directory policy and Swift interface password policy for complexity definition.

What else should you do to meet the control?

- Ask your IT to verify this policy is in place.

2026 UPDATE

4.2 Multi-factor Authentication

Mandatory Control

- Bottomline supports CSP compliance
- Bottomline helps me ask the right questions

What does it mean?

- Implement a Multi-Factor Authentication (MFA) solution for all user and administrator access to Swift applications and infrastructure components.

What can you learn from Bottomline to meet this control?

- Bottomline operates a Multi-Factor Authentication solution for both end users & administrators, and for access by Bottomline personnel (see images below).

What else should you do to meet the control?

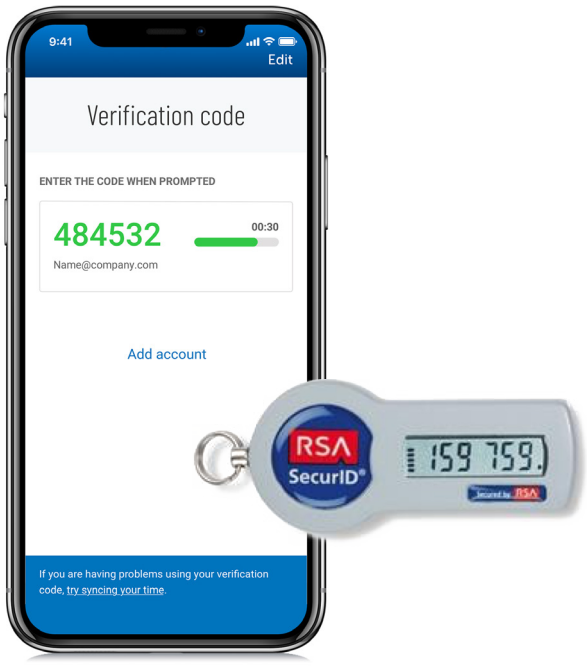
- Speak with your Bottomline Account Manager to confirm Multi-Factor Authentication is enabled for the service bureau.
- Review internal controls with IT & security teams.

2026 Update:

- Alliance Left Hand and Right Hand Security Officer (LSO/RSO) Accounts are now named as privileged accounts.
- MFA must now be applied to administrator external firewall access, to make external access attempts more difficult.

Bottomline Solution

Multi-factor authentication is used for interactive user access to Swift – related applications and operating systems accounts, with choice over MFA solution.



Section 5

Manage Identities and Segregate Privileges

5.1 Logical Access Control

Mandatory Control

- Bottomline supports CSP compliance
- Bottomline helps me ask the right questions

What does it mean?

- The use of industry good practice in the implementation and management of user access controls (access rights, password complexities, expiry, review, audit etc.).

What can you learn from Bottomline to meet this control?

- Bottomline operates a set of good practice controls that provide the required level of user account management, such as: segregation of duties, appropriate privileges allocation, access reviews, reporting on access, 4 eyes. Access is compliant with Bottomline's policies. This is also covered by Bottomline Swift SIP accreditation.

What else should you do to meet the control?

- Check with IT and Operations that internal policies and processes are in place to manage (and review) any user access linked to Swift operations.
- Implement a review process to ensure Service Bureau users have appropriate and required access.

5.2 Token Management

Mandatory Control

- Bottomline supports CSP compliance
- Bottomline helps me ask the right questions

What does it mean?

- Procedures and policies should be in place to manage the tokens and supporting infrastructure, to cover new users, removing a user and auditing the process.

What can you learn from Bottomline to meet this control?

- Bottomline operates a multi factor authentication solution for both end users and all access by Bottomline personnel.

What else should you do to meet the control?

- Speak with your Bottomline Account Manager to confirm Multi-Factor Authentication is enabled.
- Check with IT and Ops that internal polices and processes are in place to manage any user tokens linked to Swift access.

5.3A Staff Screening Process

Advisory Control

- Bottomline supports CSP compliance
- Bottomline helps me ask the right questions

What does it mean?

- Ensure adequate background checks are carried out on staff in key operations areas, these should be done as part of the hiring process and repeated 12/24 months.

What can you learn from Bottomline to meet this control?

- Bottomline ensure that background checks are carried out on staff in key operations areas. Each employee has to renew their chart every year. Also part of Bottomline's Swift SIP accreditation.

What else should you do to meet the control?

- Ask your Security & HR teams to verify the procedure is in place. and processes are in place to manage any user tokens linked to Swift access.

5.4 Physical and Logical Password Storage

Mandatory Control

- ○ Bottomline supports CSP compliance
- ✓ Bottomline helps me ask the right questions

What does it mean?

- Ensure that any recorded passwords are securely stored with formal access control.

What can you learn from Bottomline to meet this control?

- Bottomline operates a set of good practice controls that provide the required secure storage and access controls for such passwords.

What else should you do to meet the control?

- Check with IT and Security Departments to ensure that internal policies and processes are in place to securely store such user and password details.

Section 6

Detect Anomalous Activity to Systems or Transaction Records

2026 UPDATE

6.1 Malware protection

Mandatory Control

- ○ Bottomline supports CSP compliance
- ✓ Bottomline helps me ask the right questions

What does it mean?

- Ensure that suitable anti-malware (anti-virus) software is installed on all Swift related systems. Applicable to Windows machines only.

What can you learn from Bottomline to meet this control?

- Bottomline has deployed anti-malware and anti-virus tools within its corporate and hosted Swift infrastructures, which is routinely updated. Also part of Swift SIP certification.

What else should you do to meet the control?

- Check with IT and Security Departments to obtain details of anti-malware tools/ applications that are deployed within the infrastructure linked to Swift operations.

2026 Update:

- Where possible, non-Windows systems located within a secure zone or hosting a customer client connector must now have anti-malware installed.

6.2 Software Integrity

Mandatory Control

- Bottomline supports CSP compliance
- Bottomline helps me ask the right questions

What does it mean?

- A check needs to be performed on all Swift related applications to ensure they have not been tampered with.

What can you learn from Bottomline to meet this control?

- Bottomline utilises technologies built into the messaging interfaces (SAA) to ensure no code change or manipulation, also using anti-malware to detect software changes and identify events that would indicate the manipulation of the infrastructure.

What else should you do to meet the control?

- Check with IT and Security Departments to obtain details of any software integrity tools (+ supporting policies & processes) that are deployed within the infrastructure linked to Swift operations.

6.3 Database Integrity

Mandatory Control

- Bottomline supports CSP compliance
- Bottomline helps me ask the right questions

What does it mean?

- A check needs to be performed on the database of the Swift messaging interface to ensure that it has not been tampered with.

What can you learn from Bottomline to meet this control?

- Bottomline utilises technologies built into the messaging interfaces and supporting databases, to identify events that would indicate the manipulation of the database.

What else should you do to meet the control?

- Check with IT and Security Departments to obtain details of any software integrity tools (+ supporting policies & processes) that are deployed within the infrastructure linked to Swift operations.

6.4 Logging and Monitoring

Mandatory Control

- Bottomline supports CSP compliance
- Bottomline helps me ask the right questions

What does it mean?

- Monitoring and alerting capabilities are needed to detect anomalous actions and operations within the local Swift environment.

What can you learn from Bottomline to meet this control?

- Monitoring of systems and infrastructure is routinely carried out.
- Pro-active Transaction and Behaviour anomaly detection is used to identify suspicious payment messages and stop them before sending into the Swift network.

What else should you do to meet the control?

- Connect with your Bottomline Account Manager to explore tailored solutions that can support compliance.
- Check with IT and Security Teams to obtain details of any additional security monitoring and alerting tools deployed within your infrastructure linked to Swift operations.

6.5a Intrusion Detection

Advisory Control

- Bottomline supports CSP compliance
- Bottomline helps me ask the right questions

What does it mean?

- Monitor network traffic and access to detect and contain unusual or unauthorised traffic/ access, with supporting policies and procedures.

What can you learn from Bottomline to meet this control?

- Bottomline operates a range intrusion detection and prevention technology, on application servers and within the network infrastructures. Also covered by Swift SIP accreditation.

What else should you do to meet the control?

- Check with IT and Security Departments to obtain details of existing technology (+ supporting policies and processes) deployed within the infrastructure linked to Swift operations.

Section 7

Plan for Incident Response and Information Sharing

7.1 Cyber Incident Response Planning

Mandatory Control

- Bottomline supports CSP compliance
- Bottomline helps me ask the right questions

What does it mean?

- To ensure a customer is prepared to respond to a cyber incident, it should include the real life scenarios already published and cover (as a minimum) the key steps/ elements that Swift have identified.

What can you learn from Bottomline to meet this control?

- Bottomline operates its own cyber incident response plan as part of its corporate operations.
- Help provide forensic copy of suspicious activity for evidence of fraud through Replay functionality or reports.

What else should you do to meet the control?

- Connect with your Bottomline Account Manager to explore tailored solutions that can support compliance.
- Contact your IT, Security and Business Continuity teams to advice on current plans and the mandated requirement from Swift.

2026 UPDATE

7.2 Security Training and Awareness

Mandatory Control

- Bottomline supports CSP compliance
- Bottomline helps me ask the right questions

What does it mean?

- All staff should be aware of and fulfill their security responsibilities, both new and existing. Perform regular awareness activities and maintain security knowledge through additional training and learning activities

What can you learn from Bottomline to meet this control?

- Bottomline already operates a programme of security training as part of the staff induction process and annual refresher training.

What else should you do to meet the control?

- Contact your Security team to obtain details of current security training within your organisation and to advise of the Swift mandated requirement.

2026 Update:

- Awareness training must now include Deepfake technology, as an example of AI-based threats. This should complement existing training requirements, such as phishing and safe browsing.

2026 UPDATE

7.3a Penetration Training

Advisory Control

- ○ Bottomline supports CSP compliance
- ✓ Bottomline helps me ask the right questions

What does it mean?

- Carry out testing of the Swift related infrastructure, at least annually, to check for vulnerabilities.

What can you learn from Bottomline to meet this control?

- Bottomline regularly undertakes internal vulnerability tests or external penetration tests. The results are then assessed and addressed. As part of our continuous improvement programme and in-line with good-practice and Swift mandates we are working with our customers to increase the levels of security, encryption and authentication.

What else should you do to meet the control?

- Check with IT and Security Departments to obtain details of any such testing program that is currently being used, along with existing policies and processes (linked to Swift operations).

2026 Update:

- Reference is made to Knowledge Base article 5021823 – CSP Common Questions. This provides guidance on the scope and testing scenarios of your penetration tests which should be conducted at least annually. All scenarios must be covered within a three-year penetration testing cycle. Swift suggests that penetration testing is conducted using three approaches:
  1. An unauthorised external user
  2. A valid, authorised internal or external user
  3. A malicious insider (employee or other

7.4a Scenario Risk Assessment

Advisory Control

- ○ Bottomline supports CSP compliance
- ✓ Bottomline helps me ask the right questions

What does it mean?

- The Swift related and Ops should be risk assessed, to identify risks, potential impact, likelihood and identify mitigating actions.

What can you learn from Bottomline to meet this control?

- Bottomline's operations and infrastructure are regularly risk assessed by the operational business lines, with the oversight of our global CISO organisation and our corporate Risk, Governance, Security, and Compliance Committee. This is being expanded to include specific Swift Scenario Risk Assessments in line with the controls framework.

What else should you do to meet the control?

- Advise your Security and Risk Department(s) to advise them of this Swift advisory and review current Risk Assessments in line with the program.

Should you have any questions about this document, please contact your Bottomline Representative.

Get Started

Recommended Next Steps

1. Review the Swift CSP documentation, understand any operational gaps your organisation may have. If you require assistance with this review, please let Bottomline know and we may be able to guide you further with our 'CSP Attestation Review'.
2. Implement any changes to process and update technology as needed to ensure compliance with all mandatory controls. Contact your Bottomline Representative to discuss enablement of any solutions to support your compliance, such as Bottomline Risk Solutions including MFA and Secure Data Transfer, and how else we can help you.
3. Schedule your CSP Independent Assessment via your Bottomline Representative.
4. Complete Swift CSP Self-Attestation online and advise Swift and your counterparties that you meet all mandatory controls by 31st December 2026.

Bottomline

About Bottomline

Bottomline helps businesses transform the way they pay and get paid. A global leader in business payments and cash management, Bottomline's secure, comprehensive solutions modernize payments for businesses and financial institutions globally. With over 35 years of experience, moving more than $16 trillion in payments annually, Bottomline is committed to driving impactful results for customers by reimagining business payments and delivering solutions that add to the bottom line. Bottomline is a portfolio company of Thoma Bravo, one of the largest software private equity firms in the world, with more than $184 billion in assets under management.

For more information, visit www.bottomline.com

REV US060226KG

Corporate Headquarters
100 International Drive, Suite 200
Portsmouth, NH 03801
United States of America

Phone: +1-603-436-0700
Toll-free: +1-800-243-2528
info@bottomline.com

Europe, Middle East, Africa Headquarters
1600 Arlington Business Park
Theale, Reading, Berkshire RG7 4SA
United Kingdom

Tel (Local): 0870-081-8250
Tel (Int): +44-118-925-8250
emea-info@bottomline.com