BOMGAR™

Secure Access & SWIFT CUSTOMER SECURITY CONTROLS FRAMEWORK

SWIFT Financial Messaging Services

SWIFT is the world's leading provider of secure financial messaging services. Their services are used and trusted by more than 11,000 financial institutions in more than 200 countries and territories around the world. SWIFT has played a leading role in the standardization that supports global financial messaging and its automation. The use of standardized messages and reference data ensures that data exchanged between institutions is unambiguous and machine friendly, facilitating automation, reducing costs and mitigating risks.

Through SWIFT, banks, custodians, investment institutions, central banks, market infrastructures and corporate clients, can connect with one another exchanging structured electronic messages to perform common business processes, such as making payments or settling trades.

"Our aim in setting out this framework is to support customers by helping to drive awareness and improvements in the industry's overall security."

SWIFT CEO GOTTFRIED LEIBBRANDT

Reinforce the Security of the Global Banking System

Privacy and security has always been a high priority in banking and finance. With the implementation of the SWIFT Customer Security Controls Framework, organizations within this industry using SWIFT are compelled to use extra precaution in handling data and financial systems information.

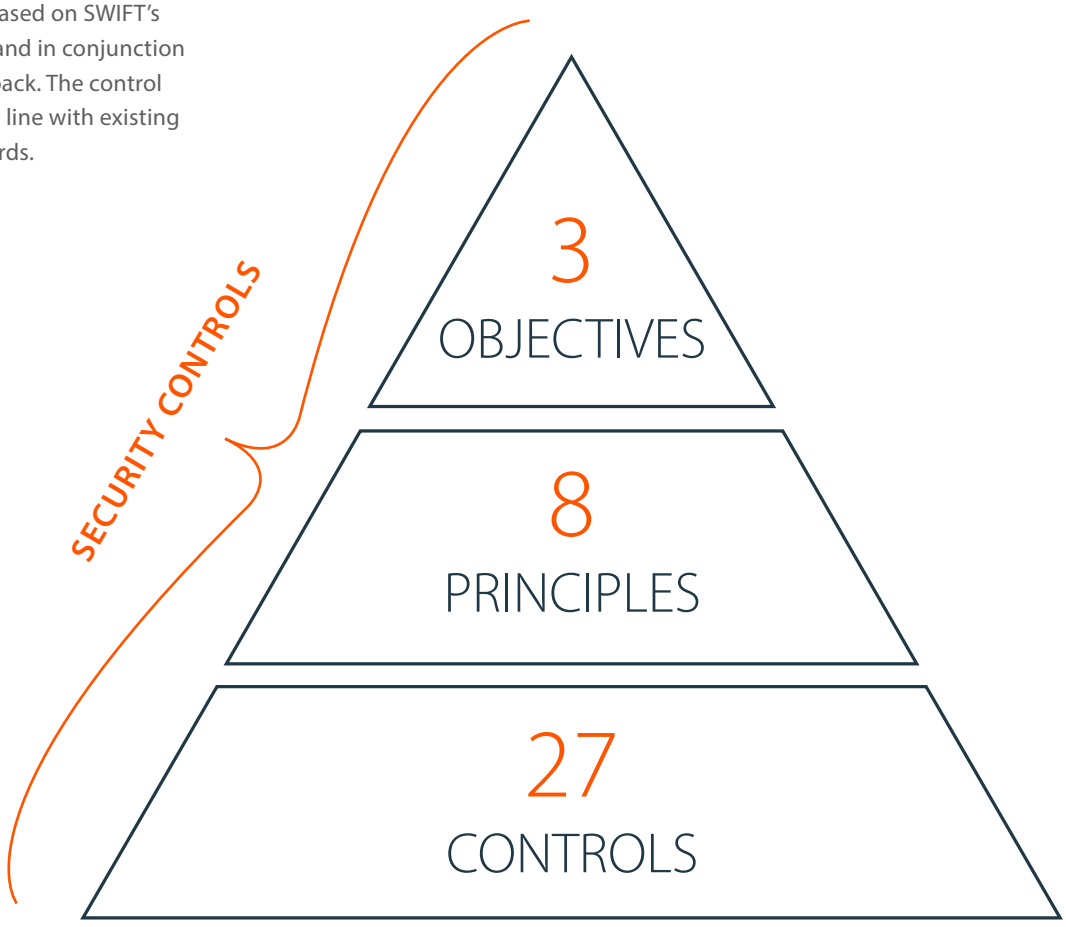
The framework is organized into three main objectives, broken down into 8 principles and 27 controls:

- **SECURE YOUR ENVIRONMENT**
  1. Restrict internet access
  2. Protect critical systems from general IT environment
  3. Reduce attack surface and vulnerabilities
  4. Physically secure the environment

- **KNOW & LIMIT ACCESS**
  5. Prevent compromise of credentials
  6. Manage identities and segregate privileges

- **DETECT & RESPOND**
  7. Detect anomalous activity to system or transaction records
  8. Plan for incident response and information sharing

The controls have been developed based on SWIFT's analysis of cyber threat intelligence and in conjunction with industry experts and user feedback. The control definitions are also intended to be in line with existing information security industry standards.



Bomgar and SWIFT: A Perfect Fit

Bomgar Secure Access Solutions enables organizations to address SWIFT security and compliance requirements while contributing to a true defense-in-depth strategy. With a cost-effective licensing model and a secure, robust, architecture capable of supporting up to tens of thousands of critical systems, Bomgar is the ideal choice for large, geographically dispersed environments. Bomgar enables you to:

- **IMPROVE** cybersecurity by closing the door on the #1 attack pathway for hackers
- **REPLACE** multiple ineffective remote access tools with a single, comprehensive solution
- **INCREASE** productivity and security by ditching password spreadsheets and sticky notes for credential management
- **STANDARDIZE** the authentication process by adding MFA, integrating with Smart Cards and identity management systems
- **SECURE** access across hybrid environments to support diverse IT infrastructure components
- **SIMPLIFY** regulatory compliance
- **IMPLEMENT** a solution your users will love

Meeting SWIFT CSCF Compliance

When it comes to remote and secure access, compliance ensures that the organization's data is kept secure and helps mitigate security risks. Bomgar can help you meet a variety of SWIFT Customer Security Controls Framework requirements.

MANDATORY SECURITY CONTROLS:

	CONTROL OBJECTIVE	BOMGAR RESPONSE
1.1 SWIFT Environment Protection	Ensure the protection of the user's local SWIFT infrastructure from potentially compromised elements of the general IT environment and external environment.	Bomgar protects your infrastructure by acting as a secure bastion into the secure zone, limiting activity for privileged users or vendors to specific systems and applications.
1.2 Operating System Privileged Account Control	Restrict and control the allocation and usage of administrator-level operating system accounts.	Bomgar offers granular control over user access and privileges. System administrators can establish granular session permissions and can configure parameters such as access time constraints and areas of access. Access can be approved on an ad hoc basis.
2.1 Internal Data Flow Security	Ensure the confidentiality, integrity, and authenticity of data flows between local SWIFT-related applications and their link to the operator PC.	Bomgar restricts the usage of privileged accounts and controls the access to secure zone systems, and in parallel video records and logs all session activity. All data is encrypted in transit using TLS v1.2. Bomgar provides a range of cipher suites that may be appropriately restricted by authorized system administrators. All access sessions generate a centrally held report and session recording of all activity. This is tamper-proof to prevent any user from editing or deleting their activities. This data can also be held on an encrypted volume to ensure confidentiality at rest.
2.2 Security Updates	Minimize the occurrence of known technical vulnerabilities within the local SWIFT infrastructure by ensuring vendor support, applying mandatory software updates, and applying timely security updates aligned to the assessed risk.	Regular updates to all Bomgar products ensure technical vulnerabilities are patched, and Bomgar's dedicated support team are available to help as needed.
2.3 System Hardening	Reduce the cyber attack surface of SWIFT-related components by performing system hardening.	Bomgar offers a variety of deployment options including a centralized, security-hardened physical or virtual appliance that never passes data through a third-party. All system communications are initiated outbound from the client toward the Bomgar appliance. This provides secure access and an option to reduce the attack surface of systems by shutting down unnecessary services such as RDP or SSH.

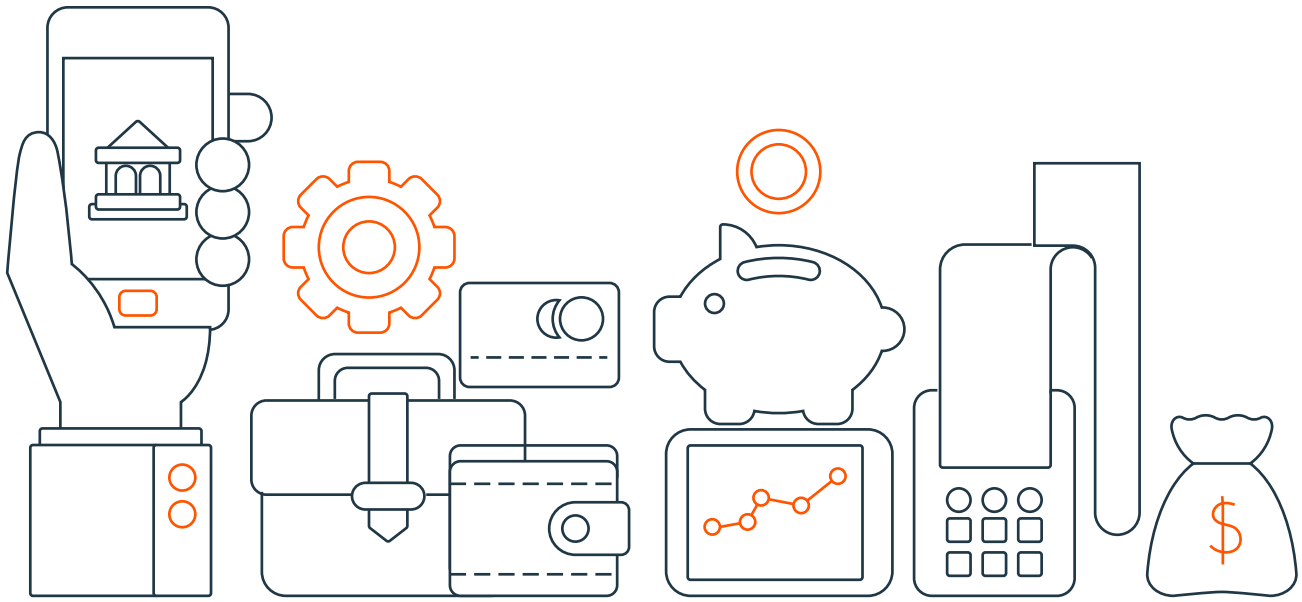
3.1 Physical Security	Prevent unauthorised physical access to sensitive equipment, workplace environments, hosting sites, and storage.	Omit 3.1 – Not relevant to Bomgar
4.1 Password Policy	Ensure passwords are sufficiently resistant against common password attacks by implementing and enforcing an effective password policy.	With Bomgar Vault, privileged credentials can be securely stored, retrieved and managed. Administrators can centrally enforce password requirements, such as length and complexity, and rules for the frequency of password changes. A new password can be automatically generated after each use of the account or on a scheduled basis.
4.2 Multi-factor Authentication	Prevent that a compromise of a single authentication factor allows access into SWIFT systems, by implementing multi-factor authentication.	Bomgar enables secure multifactor authentication via RADIUS, SAML or Smart Cards. Bomgar also includes support for TOTP two factor authentication.
5.1 Logical Access Control	Enforce the security principles of need-to-know access, least privilege, and segregation of duties for operator accounts.	Bomgar offers highly granular control over system access and privileged accounts, ensuring least privileged access to systems and applications on endpoints. Access can also be controlled on a need-to-know basis by following an approval workflow before allowing a session to a system. Bomgar restricts access to privileged accounts, enforcing segregation of duties for your users.
5.2 Token Management	Ensure the proper management, tracking, and use of connected hardware authentication tokens (if tokens are used).	Omit 5.2 – Not relevant to Bomgar
6.1 Malware Protection	Ensure that local SWIFT infrastructure is protected against malware.	Omit 6.1 – Not relevant to Bomgar
6.2 Software Integrity	Ensure the software integrity of the SWIFT-related applications.	Bomgar manages the privileged credentials and access required to make changes to a SWIFT-related application and ensures that the integrity of applications cannot be compromised due to poor privileged access management.
6.3 Database Integrity	Ensure the integrity of the database records for the SWIFT messaging interface.	Omit 6.3 – Not relevant to Bomgar
6.4 Logging and Monitoring	Record security events and detect anomalous actions and operations within the local SWIFT environment.	With Bomgar, session activity is automatically recorded and logged. There are built in capabilities allowing users to generate comprehensive reports for analysis. Bomgar can also integrate with SIEM tools for advanced analysis of audit logs. Alerts can be set for misuse or suspicious activity.

7.1 Cyber Incident Response Planning	Ensure a consistent and effective approach for the management of cyber incidents.	Bomgar audit logs and session data can be leveraged for a forensic investigation in the case of a cyber incident.
7.2 Security Training and Awareness	Ensure all staff are aware of and fulfil their security responsibilities by performing regular security training and awareness activities.	Omit 7.2 – Not relevant to Bomgar

ADVISORY SECURITY CONTROLS:

	CONTROL OBJECTIVE	BOMGAR RESPONSE
2.4 A Back Office Data Flow Security	Ensure the confidentiality, integrity, and mutual authenticity of data flows between back office (or middleware) applications and connecting SWIFT infrastructure components.	Bomgar Vault supports Application-to-Application password management. This allows for the secure injection of credentials from Bomgar Vault into a back-office application or script, without storing credentials in plain text.
2.5 A External Transmission Data Protection	Protect the confidentiality of SWIFT-related data transmitted and residing outside of the secure zone.	Bomgar works through your firewall without VPN tunneling, so your perimeter security can remain intact. Extend remote connection protocols beyond the LAN without compromising security by using a Layer 7 (Application) approach that incorporates much tighter controls than those available with a traditional VPN.
2.6 A Operator Session Confidentiality and Integrity	Protect the confidentiality and integrity of interactive operator sessions connecting to the local SWIFT infrastructure.	Bomgar provides confidential and secure access to systems, and creates a tamper proof report of all session activity. Bomgar also controls the privileged credentials used to access to applications, scripts, and systems, without revealing these to the operator ensuring confidentiality.
2.7 A Vulnerability Scanning	Identify known vulnerabilities within the local SWIFT environment by implementing a regular vulnerability scanning process.	Omit 2.7 – Not relevant to Bomgar
2.8 A Critical Activity Outsourcing	Ensure protection of the local SWIFT infrastructure from risks exposed by the outsourcing of critical activities.	Provide third-party vendors with secure, reliable connections to access your network externally, maintaining segregation and can give temporary elevated access, limited to certain timeframes. All session activity is recorded in a tamper-proof report and video recording.

2.9 A Transaction Business Controls	Restrict transaction activity to validated and approved counterparties and within the expected bounds of normal business.	Omit 2.9 – Not relevant to Bomgar
5.3 A Personnel Vetting Process	Ensure the trustworthiness of staff operating the local SWIFT environment by performing personnel vetting.	Omit 5.3 – Not relevant to Bomgar
5.4 A Physical and Logical Password Storage	Protect physically and logically recorded passwords.	Manage, rotate, and randomize credentials for privileged accounts, used by both people and systems including service accounts, cloud services, SSH keys, and app to app access. Inject credentials directly into privileged sessions without exposing plain text passwords with Bomgar Vault.
6.5 A Intrusion Detection	Detect and prevent anomalous network activity into and within the local SWIFT environment.	Omit 6.5 – Not relevant to Bomgar
7.3 A Penetration Testing	Validate the operational security configuration and identify security gaps by performing penetration testing.	Omit 7.3 – Not relevant to Bomgar
7.4 A Scenario Risk Assessment	Evaluate the risk and readiness of the organization based on plausible cyber attack scenarios.	Omit 7.4 – Not relevant to Bomgar



Make Least Privilege Productive – Quickly

Bomgar helps security and IT support professionals be compliant with SWIFT CSCF regulations and improve business performance by enabling secure, controlled access to nearly any device or system, anywhere in the world.

REMOTE SUPPORT

Super-fast, all-inclusive remote support for IT service desks and customer tech support

PRIVILEGED ACCESS

Manage and monitor privileged access to critical systems... without VPN

PASSWORD VAULT

Store and manage shared passwords and credentials for privileged users

Start securing access and accounts from day one without lengthy implementations and gain back valuable time to spend on your business instead of getting dragged down by process. With features such as seamless credential injection, unattended access, remote control and screen sharing, your technicians and vendors can quickly and securely attend to remote devices and servers across any OS.

ABOUT BOMGAR

Bomgar is the leader in Secure Access solutions that empower businesses. Bomgar's leading remote support, privileged access management, and identity management solutions help support and security professionals improve productivity and security by enabling secure, controlled connections to any system or device, anywhere in the world. More than 12,000 organizations across 80 countries use Bomgar to deliver superior support services and reduce threats to valuable data and systems. Bomgar is privately held with offices in Atlanta, Jackson, Washington D.C., Frankfurt, London, Paris, and Singapore. Connect with Bomgar at www.bomgar.com.

CONTACT | INFO@BOMGAR.COM | 866-205-3650 (U.S.) | +44 (0)1628-480-210 (U.K./EMEA) | BOMGAR.COM