SWIFT Assessment Guidelines
Info sheet

Master the Customer Security Programme assessment methodology

Learning objectives

- Carry out your responsibilities in relation to the Customer Security Programme
- Gain a broader industry perspective
- Ensure you have the necessary technical capabilities
- Review security best practice scenarios and field compliance experience with a SWIFT expert

Audience

- IT Auditors/Assessors
- Compliance Managers and Officers
- Risk and Security Managers
- System Administrators
- Chief Information Security Officers

Our Customer Security Programme sets benchmark security practices, critical to defending against, detecting and recovering from cybercrime. The Independent Assessment Framework, is a significant milestone in our security programme. It reinforces the level of assurance provided by self-attestations by mandating independent assessments by third parties.

Do you perform gap analyses for SWIFT member organisations? Do you help enrich and improve their level of compliance with the Customer Security Controls Framework? Will you be responsible for independent attestations?

If so, you need to understand each of the controls, each of the architecture components in scope, and how to verify evidence for each SWIFT infrastructure type.

SWIFT has designed a new Assessment Guidelines workshop to help you conduct more efficient and robust assessments.

Aimed at auditors, risk managers and IT assessors, the workshop is tailored to the business and technical contexts in which you are operating. It demonstrates how to interpret and comply with mandatory and advisory controls, which evidences are best collected, and how to audit objectively based on security best practices.

The workshop is structured around a blend of theoretical and practical modules.

The theory includes targeted information to help collect and analyse evidence for the design, implementation and operating effectiveness of each control.

The practical elements of the workshop provide unique opportunities to explore real-life case studies and discuss your feedback as a group.

Examples of the topics covered include:

— Application hardening: security parameters settings
— Logical access: profiles, RBAC roles, permissions, segregation of duties and the ‘4 eyes’ principle
— Traceability: actions and event log trails
— Transaction business control: message processing history
— Interface hardening tools: using a “security best practice check” with different outputs
— Cyber incident response: the SWIFT security recovery roadmap

SWIFT Assessment Guidelines Workshop Agenda

Workshop preparation

- Remote kick off to scope the workshop
- SWIFT collects and analyses data relating to your technical environment

Overview of SWIFT

- Context in the financial industry
- Core messaging services
- Secure IP network and connectivity types
- Interface portfolio
- FIN and ISO 20022 messaging standards

The Customer Security Programme

- Customer Security Controls Framework (CSCF)
- Independent Assessment Framework (IAF)

PKI certificates and HSMs

- Public Key Infrastructure (PKI)
- Hardware Security Modules (HSMs)
- SWIFTNet security officers

Connect to Alliance Gateway (or Alliance Remote Gateway)

- Operator access
- Security management
- Operational and auditing profiles

Connect to Alliance Access

- Operator Access
- Security parameters
- Messaging data Flows
- Messaging routing terminology
- Operational and auditing profiles

Connect to FIN and SWIFTNet

- BIC usage and identity importance
- FIN secure login and select (connectivity control)
- SWIFTNet communication channels (InterAct and FileAct profiles)
- Integrity, filtering and other security controls
- Authentication methods and application integrity checks
- Transaction business control (RMA and Payment Controls best practices)
- Confidentiality, availability and integrity of messages
- Reconciliation & integrity of the message flow

Audit trails (financial messages)

- Identification of a message (tracking history)
- Message search and event log (where to see)
- Daily message check report (the what)
- Undelivered message report (why it failed)
- Message delivery monitoring (what is the status)
- Message retrievals (why to retrieve)
- Monitoring event log (for auditing)
- SWIFT.com security and audit trail (who has accessed)

Practical information

The SWIFT Assessment Guidelines workshop can be organised over two or three days. Thanks to its modular structure, each session can be customised to your needs.

The organisation and delivery is managed by a senior subject matter expert.

The workshop can be delivered in various languages.

For more information, please contact your SWIFT account manager.

SWIFT is a member-owned cooperative, providing secure financial messaging services to more than 11,000 organisations, across the financial ecosystem, in almost every country in the world. For nearly five decades we have delivered certainty, continuity and excellence by constantly evolving in an everchanging landscape. In today's fast moving, increasingly connected and challenging world, this approach has never been more relevant.
www.swift.com

57449 - January 2020