Governance

- A governance structure is in place to enable SWIFT to meet its security commitments to its customers, supported by policies and procedures and the organisational management structure;
- Responsibilities and accountabilities between SWIFT and its customers are contractually defined, agreed and monitored;
- Responsibilities and accountabilities between SWIFT and its suppliers are contractually defined, agreed and monitored.
- Processes and procedures are in place to protect personal data processed by SWIFT on behalf of customers in its provision of the SWIFTNet and FIN messaging services.

Confidentiality

- Cryptographic methods are designed and used to protect the confidentiality of customers' messages;
- Logical access to the messaging service infrastructure is restricted;
- Physical access to premises, computer equipment and resources is restricted.

Integrity

- SWIFT has mechanisms in place such that:
  - Only authorised customers can access messaging services;
  - Messages are delivered to the authorised recipients only.
- Mechanisms are in place to protect against unauthorised changes to the messaging service infrastructure, and to detect corruption of messages;
- SWIFT validates messages, and only validated messages are processed and delivered.

Availability

- The messaging service infrastructure is designed and tested to meet quality objectives;
- The messaging service infrastructure is designed and tested to meet recovery time objectives;
- The messaging service infrastructure is monitored against availability targets;
- Processes and procedures are in place to detect and react to problems;
- Customers can report problems and obtain the status of problems and the messaging service infrastructure.

Change Management

- Changes to the messaging service infrastructure are planned, validated, monitored and implemented in a controlled manner;
- Changes to customer configurations are planned, validated, monitored and implemented in a controlled manner.