SBS SaaS Security Management Plan Cloud Aws

SBS SaaS Security Management Plan_ (eng)_v28022025

Table of content

1. Presentation of the Security Management Plan

This Security Management Plan (“SMP”) is incorporated to and supplements the Agreement entered into between Customer and SBS. This document describes the security measures, organization and processes put in place by SBS as part of the provision of the Services. This SMP is valid on the Customer’s production and non-production environments operated on the AWS infrastructure. Some security indicators or technical requirements may be adapted according to their criticality and exposure. All capitalized terms not defined in this SMP will have the meaning given to them in other parts of the Agreement.

The document describes the provisions on the availability, the authenticity, the integrity and the confidentiality regarding the protection of information, including Personal Data.

2. Reversibility clause

SBS ensures compliance with the SMP and security levels during the Agreement and reversibility phase. Any data transfer requires prior validation from the SBS ISO and Customer CISO. Specific reversibility requests are subject to a commercial proposal, with SBS maintaining documented reversibility processes.

3. Security Audits

SBS conducts regular security audits, tailored to the specific service line and scope. These audits may include technical assessments, external evaluations, and penetration testing.

The Customer may conduct audits at its own expense, in accordance with the conditions set out in the General Terms and Conditions (GTCs) and Specific Terms and Conditions (STCs).

4. Global Security Clause

SBS is responsible for the security procedures of its subcontractors. Regular checks are put in place by SBS for verification of the security compliance of these subcontractors. (Minimum control: Every year to respect the certification).

5. Security organization

5.1. Information Security Policy (ISP)

SBS’s Information Security Policy (ISP) is managed by the SBS CISO.
SBS’s ISP is available to all employees via the intranet
ISP may be presented during audits carried out by the Customer.

5.2. Security committee

SBS has implemented an internal security committee which takes place on a regular basis. The purpose of the internal security committee is to control the application of the SMP by presenting security KPIs and key information.
Depending on the options/services subscribed by the Customer, a customer security committee will take place at regular periods.

5.3. Customer organization

Customer has the obligation to appoint a security contact in charge of applying Customer’s information security policy. He will be the privileged point of contact for SBS on security matters and the point of contact for security audits, distribution of security documentation or other security topics and security committees. In case of a security incident or threat, she or he will be the contact person for the various exchanges and follow-ups. The contact details of Customer’s security contact and the Data Protection Officer must be shared with SBS.

5.4. SBS Security department organization

Objective. The objective is to define a governance for implementing and verifying the Information Security Policy of SBS (ISP).

SBS CISO. The SBS CISO is appointed by the SBS management.

Information Security Officer of the service line. The Information Security Officer or ISO will be assigned specifically to the service line and specifically to Customer. He or she will be appointed in the SMP as the security officer for Customer on the line named ISO of the service line. The roles of CISO, ISO and PSL (Project Security Leader) are defined in dedicated function sheets validated by the yearly security organization note issued by the SBS CISO.

5.5. Mission of the security department

The security department's organization is reviewed by the SBS CISO on a yearly basis. The result of this review is published internally to inform the different stakeholders of the roles, the mission, and the security objectives to be reached for the current year. The security department's mission is to:

- Ensure the operational application of the Information Security Policy (SBS ISP and to report any discrepancies (in its application or unsuitability to the activities of SBS)
- Manage security risks and initiate actions to prevent crises and make SBS more resilient in case of a crisis
- Help setting up the necessary means at Business Unit (BU) level to achieve the yearly SBS security objectives
- Make employees aware of security issues
- Formalize and deploy the yearly security control plan and support the actions identified following the review
- Tracking the coverage of vulnerabilities in our products and associated remediation plans
- Identify activities needed to be certified (in particular ISO/IEC 27001), and then assist in the implementation of certification projects and their yearly follow-up
- Participate actively to security communities
- Report all incidents and security issues.
- To take part in "external security communities" and thus carry out a security watch necessary for the improvement of the security processes of SBS
- All security roles and functions must be validated by the SBS CISO.

5.6. Risk Management

SBS applies the risk management methodology defined by SBS. This methodology is based on the principles of ISO/IEC 27005 and EBIOS (ANSSI). This analysis is reviewed annually. Security risk assessment criteria within the service line are defined by the ISO. Their main objective is to establish acceptable levels of risk. Residual risks are submitted to and accepted by service line management.
Risk analysis is an integral part of SBS security governance. It is carried out on an ongoing basis between the operational maintenance teams and the ISO. SBS has put in place a risk security exception process that manages deviations from established security policies or specific requirements from services lines.

6. Human activities Security

6.1. Objectives

Make sure that SBS employees are aware of their responsibilities and are suitable for the duties assigned to them according to the regulations in force.
Reduce the risk of theft, fraud, or misuse of computer equipment.
Make sure that SBS employees are aware of threats to information security, to personal or financial data or to other confidential Customer Data.
Reduce the risk of human error or malicious behaviour by applying the four eyes principle.
Verify that the accounts and access rights of leaving employees are effectively deactivated. When an employee leaves the company, all rights are revoked automatically after 45 days maximum.
Ensure that access rights are reviewed on a quarterly basis.

6.2. Security awareness and training

All employees (including the operations team) are regularly trained and made aware on security in their context. They apply for example a 'clean desk policy'. An Information Security awareness program sets out the security

requirements. The management is the sponsor of the implementation of this program. Operators accessing SBS or its customers' data are especially sensitive to: (i) confidentiality of the processed data, (ii) the ethics of the business to which the service relates, (iii) social engineering, and (iv) damage to the image and reputation of SBS or its customers.

6.3. Security measures

Recruitment. During recruitment, the HR department performs controls (screening) depending on the legislation and the rules of the country of the new employee. The following controls are performed: (i) identity control, (ii) proof of "diploma" / certification, (iii) criminal record for new arrivals for the operations team.

Confidentiality clause. SBS undertakes to ensure that a confidentiality clause is systematically included in the employment contract of its employees. The information covered by the confidentiality clause and the prohibition of disclosure mainly concerns: (i) hosted content: the information or functions processed by the system, (ii) information whose disclosure could compromise the security of the system (passwords, encryption keys, documentation on the architecture and security of the system, etc.), (iii) Customer's personal, or confidential information, (iv) exposure of customer's name in unrestricted spaces, (v) depending on the scope of the services, additional clauses may be implemented.

Training and awareness. SBS, including its operations teams are committed to ensure that its employees receive appropriate awareness and regular updates on the security requirements related to the regulations of the services provided, control measures and more specifically on data handling. For SBS employees, SBS implements the SBS security training program. Through its training department, it ensures a basic level of security awareness for all its employees. The training courses can be completed by the Information Security Officer of the different entities. In particular, the participants are informed during their integration process within the project or via the security awareness campaigns planned by SBS. The training courses deal with the following topics: (i) Basics of security for everyone, (ii) Security basics for project managers, (iii) Security in developments (training provided according to the role/function of the employee), (iv) Data protection, (v) Raising awareness about corruption, (vi) Annual phishing prevention test campaign.

Termination or modification of the employment contract. Any SBS employee who ceases to work and who has (or could have) access rights to any system will have all access rights withdrawn. The terms and conditions for restricting access (notably AD) are managed by the IT department following the provisions defined in SBS's ISP. All the modifications done SBS's AD are daily deployed and quarterly reviewed. Specific accesses exercised by the operations teams (and possible administrators), are also neutralized. When an employee or subcontractor leaves the company, their departure date is recorded by their management assistant. His/her account is automatically deactivated when his/her departure date is over. From then on, the employee loses all his/her access authorizations. The account is permanently deleted 45 days after the employee's exit date.

Roles and responsibilities. The procedures applied by the operations teams are documented and describe the roles and responsibilities of the different stakeholders.

7. Assets security

7.1. Objective

Define, implement, and maintain appropriate technical measures to protect information system assets against threats from identified risks.

7.2. SBS requirements

The different configurations of the workstations, which, in function of the service, connect to the information system or to the platform, are described and qualified.
The rules for classifying information (meeting minutes, documents, reference documents, databases, data files, emails, etc.) from SBS or from customers are identified and applied (see chapter Classification of information).
All the equipment that makes up the SBS workstation information system and the infrastructure for the provision of the Services have an up-to-date anti-virus protection software.
The update (recovery and distribution) of the signature bases and anti-virus software is carried out on the workstations and the servers at the time of publication by the editors.
End Point Detection & Response (EDR) protection is enabled on all workstations and the internal IT servers.

7.3. Security measures of the workplace

7.3.1. Laptops

The workstations used by the SBS teams are provided by the IT Department and therefore comply with the patch management policy in terms of “anti-virus” coverage and the application of Windows security patches.
The mastering of workstations is carried out by the IT department, as well as the processes for providing, recycling, and destroying workstations.
The workstations are always in a maintained version of Microsoft Windows and have by default a hard disk encryption tool and USB ports are blocked.
Each employee must:

- Store all classified documents in a locked cabinet.
- Lock screens when they leave a workstation unattended. By default, the screen will lock after a few minutes of inactivity to prevent data theft or loss,

The IT department recommends the following rules for laptops:

- Always secure your laptop with the security cable provided by the IT department when it is not under your direct supervision
- Keep your laptop with you
- Attach your laptop and put it in safety during any absence (evenings, weekends, holidays)
- In public transport, especially on trains or planes, your laptop must remain under your direct and constant surveillance with the confidential screen mode activated (if available).

The use of non-standard resources (BYOD) is not allowed to access our customers' production environments.

7.3.2. Microsoft Office 365

The collaborative tools and messaging used are provided from the Microsoft cloud version, managed by the IT Department. The messaging system has an anti-virus and anti-spam security Solution, which limits the risk of spreading a virus.
Exchanges with customers by email must respect the SBS’s information classification rules and the customer’s rules of use.

SBS allows its employees to have an email access on their professional or personal phone.
Because in all cases, the encryption of the Outlook database is automatic. It is controlled by a MDM (Mobile Device Management) processes.

By default, the SBS messaging gateways use the TLS 1.2 protocol, which enables encryption of transported messages.
If the customer’s gateway does not accept the SBS’s encryption level, no message will be sent until a secure method has been agreed.
Another method is to transfer the compressed and AES 256 encrypted message with password exchange via another way (either by phone or by email).

7.3.3. Mobility

Employees may telework according to the provisions implemented by SBS. In this case, they must respect the SBS directives and follow the different security rules defined in the guidelines.
A sanity check is performed to control the compliance of the employee’s workstation (example: antivirus installed and up to date, Windows updates installed, …) before launching the VPN connection to the SBS network.

7.3.4. External media

SBS must ensure the confidentiality of external physical media required for outsourced services and requested by the Customer: paper media, removable storage media. Rules must be issued for the management of these external physical media. As part of an audit, the Customer may ask SBS to forward these rules for checking, in order to validate the level of security of the external media.

7.4. Operations asset database

SBS undertakes to ensure that all IT or other assets (documents, various materials) essential to its activity and delivery of services are protected in accordance with the rules of the Information Security Policy. The assets are managed by product in a manner adapted to the context, and the monitoring of the security of these assets (obsolescence, for example) is ensured by the ISO for the product.

7.5. Classification of information

By default, the rules applied in terms of confidentiality of information are those defined in the Quality System (QS) Documentation Management Guide. This aspect is governed by the "Asset Management" security policy, chapter 4 "Information classification".

Document management rules are applied using associated templates.
The classification levels are as follows:

C1 Public
A record with non-sensitive, non-confidential information is considered unclassified or public

C2 Restricted use
(Limited to need-to-know): default classification for all new documents.

C3 Confidential
Disclosure to an unauthorized internal or external third party may cause harm to SBS, customers and partners or employees

C4 Strictly confidential
Disclosure may cause serious harm to SBS and its customers.

7.6. Protection related to the handling of information

The employees of SBS must apply several internal rules mentioned:

- In the employment contract for compliance with legal and regulatory requirements (GDPR, Labor Agreement, internal policies, IT charter, etc.),
- In the IT department's guides and instructions for network and equipment security,
- In the Documentation Management Guide for document classification,
- In SBS's "Information Classification" policy document, which describes the various use cases,

For assets managed by the IT Department, the integrity of data in the Information Systems access logs is the responsibility of the IT Department administrators,

For assets dedicated to the present Agreement, the integrity of data in access logs is under the responsibility of the operations teams.

Shredding of information:

When information is no longer needed, means are made available to SBS employees to destroy it. This includes the process of managing vulnerabilities or equipment obsolescence:

- Shredder for paper,
- Obsolescence and exception management procedure for infrastructure,
- On AWS, disks are encrypted and destroyed when decommissioned:
  - All AWS EBS volumes used to store data are, in addition to being encrypted with a key managed outside the volume by AWS KMS, zero-wiped before any reuse.
  - Disk decommissioning is described in the white paper "AWS: Overview of Security Processes" section "Storage Device decommissioning" (https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf) which explains that disks at the end of their life are erased and then destroyed according to the NIST 800-88 standard.
- A procedure is deployed by the operations Infrastructure Management (IM) teams for decommissioning.

A Data Loss Protection (DLP) is in place on the SBS workstations and the messaging infrastructure.

8. Logical security

8.1. Security requirements

- All connections to the SBS Information System (IS) on which SBS is providing the Services to its customers, are subject to procedures (editor support activities, third party subcontractors),

- All connections made by Infrastructure administrators (IM) to the SBS Information System (IS) on which SBS is providing the Services to its customers, are tracked, protected, and archived in an integrated manner over a sliding period of at least 6 months,
- In case of a leakage or incident, the generated traces can be investigated for detecting the involved parties and the used resources,
- Logical access rights are subject to a control procedure: any change in status (arrival, departure, omission, etc.) must be considered. The access rights must be modified accordingly,
- Users must be attached to a profile related to their function,
- Users are automatically forced to change their passwords at least every 90 days, including privileged users,
- By default, users are not administrators of their workstation.

8.2. Internal user account management

8.2.1. Rules regarding internal user accounts

For all access to SBS's services, tools or applications, SBS employees follow the SBS request management process (ITSM request management application).
The following SBS rules are applied:

- An SBS employee has a unique and personal identifier,
- It is authenticated against the Active Directory. Its access to the various systems depends directly on the rights contained therein,
- She/he has access only to the applications that are necessary to carry out her/his missions,
- At the start, the employee has at least an MS Office account, an Internet access, a mailbox, password protected,
- Certain employees (admin accounts only) have privileges to carry out administration, maintenance or upgrades to systems and applications. These users must use a strong authentication based on specific Active Directories that are independent of those mentioned above,
- Unused administrator accounts are automatically deactivated after 45 days of inactivity,
- A password management policy is defined and enforced,
- When an employee leaves the company, he/she automatically loses all his/her access rights (see below),
- Passwords must comply with SBS's password policy,
- The IT policy prohibits the employee from disclosing his/her authentication information,
- Access to the system is slowed and then blocked after a certain number of failed authentication attempts, as defined in the ISP,
- Users are logged out after a certain period of inactivity,
- The access rights of employees are not transferable,
- Keep the number of people with administrative privileges to a minimum,
- Avoid generic accounts. If the use of generic accounts cannot be avoided, trace files allow for logging the activities performed by the users by means of these generic accounts,
- Systematically change the accounts provided as standard by manufacturers and editors,
- Generate and store passwords in a secure manner,
- Review privileges at least twice a year,
- Access to information and information systems is done through encrypted channels,
- MFA for SBS users is mandatory to connect to a customer environment.

8.2.2. Access rights management for internal users

Assigning / changing access rights:

- Requests to create or modify access rights to specific applications and services are subject to validation by the line manager (or application manager),
- Logical access rights are granted according to the needs of the employee and his/her function. The granting of these rights is systematically tracked.

8.2.3. Withdrawal of access rights for people at the end of their contract

As soon as an employee leaves the company, internal company procedures are applied and all access rights to company applications are removed. The default offboarding process is launched on: D+1 (more precisely the same day at midnight).

8.2.4. Review of access rights

Access reviews are determined according to the scope (administrators, users, etc.) and described in technical documentation of each product.

8.3. Management of Customer's user accounts

8.3.1. Management of access rights of the Customer's users

In the case where the application allows access to features by the Customer's users, the management of the Customer's users and their level of rights are the responsibility of the Customer.
On request the list of accesses can be provided to the Customer.
The management (creation/modification/deletion) must be done through a request to SBS.
The Customer user account and its password are communicated by SBS in a secure way.

8.4. Ticketing tool

8.4.1. Authorizations

The ticketing tool has an authorization management system that allows each user to be assigned a profile. This profile will define the actions that can be performed on the tool (consultation of documentation, consultation of tickets, creation of tickets, administration, etc.).
Customer users only have access to the tickets of the site to which they are attached (a site can correspond to several subsidiaries).

8.4.2. Authentication and password

Authentication for SBS users is based on active directory rules.
On request, it will be possible to provide the rules to date on the management of passwords. The access modalities can evolve according to the needs expressed by SBS.

8.4.3. Assigning / changing access rights

When a new employee arrives, an account is created, and a profile is assigned to him or her that matches the position. An access rights review is executed on a regular basis.

8.4.4. Withdrawal of access rights for people at the end of their contract

Blocking the AD will block access to the ticketing tool.

9. Physical security

9.1. Physical Security on SBS premises

The Group organization in charge of management of the premises ensures that the services required in terms of general services (electricity, air conditioning, etc.), fire safety and anti-intrusion services comply with the standards and security requirements imposed by local regulations, insurance companies and the ISP:

- By default, Group sites use the centralized badge access control system recommended by the Group. This system is used to restrict access to Group premises to authorized persons only,
- If necessary, the premises are divided into zones to control access,
- Computer rooms (or technical rooms) have restricted access,
- The site's internal regulations describe the security instructions on the sites and are accessible to all site employees (via on-site posting),
- The electrical emergency systems and air conditioning systems are sized according to the site and its criticality,

- The site can have remote surveillance for the critical infrastructure of the site (e.g., access doors to the premises, windows on the ground floor, machine room doors, etc.),
- Physical access management is the responsibility of the Real Estate & Purchasing Department or its equivalent in other countries,
- The responsibility for people and assets is entrusted to the Site Director who is supported by a site manager,
- The Site Infrastructure Security Document ("SISD") summarizes these requirements for each of the Group's sites.

9.1.1. Objective

- Prevent unauthorized physical access, damage, or intrusion into the premises.
- Prevent loss, damage, theft or compromise of assets and disruption of SBS operations.

9.1.2. The Site Infrastructure Security Document ("SISD") of the sites

The SBS sites are managed by the Group (or SBS by exception).

A site manager is assigned to each site, his/her role is to implement the security measures of the site in accordance with the Information Security Policy.
A SISD (site infrastructure security document) is present at each site, under the responsibility of site managers and general services.
The actions identified in the SISD, and the requirements taken by the service include:

- Prevent unauthorized physical access, damage or intrusion to the Service's premises and information
- Prevent loss, damage, theft or compromise of property and disruption of Service operations

9.2. Datacenter site

Amazon Web Services has received various certifications from third-party organizations. The reports and certificates are available to all customers of AWS under NDA via their AWS Artifacts service.
These certifications include SOC 1, SOC 2, SOC 3, ISO 27001, HIPAA, and HITECH. These documents can be consulted via https://us-east-1.console.aws.amazon.com/artifact/reports/aws (requires AWS account).
In accordance with the AWS privacy policy, it is not possible for SBS to share these reports. However, any person or organization with their own AWS subscription can view these documents.
Additional information about AWS compliance and security policy is available on their site.
The following table provides links to some resources on this topic:

Title	Origin	Link
AWS Cloud Security	AWS	security
AWS Datacenter security	AWS	compliance/data-center/controls
AWS Whitepapers	AWS	whitepapers
AWS Compliance	AWS	compliance
AWS Artifacts	AWS	artifact

Complement: Unless specified differently into the Agreement, a change of datacenter location with the same level of security is possible upon decision of SBS: in this case, an information will be provided to the Customer. The new location will remain compliant with the Customer's obligations and local regulation.
Customer's Data is stored in datacenters located in the European Union.

10. Security incident management

10.1. Objectives

Make sure that information security incident reporting procedures allow for early corrective action.

Implement consistent and effective policy and processes for managing information security incidents.
Make sure that timely reporting of all information security events through appropriate reporting channels is in place.

10.2. Security Event

A security event is an event that attracts attention because it is potentially compromising the security of a system and its data.

10.3. Security Incident

After analysis, an event may be requalified as a security incident when the integrity, confidentiality or availability of information is potentially compromised in an undesirable or unauthorized manner.
A security incident may require corrective actions, crisis management, incident reporting and post-incident evaluation.

10.4. Procedures

SBS applies the security incident management policy defined in the SBS ISP. The latter specifies the escalation process, the people to be contacted and kept informed, and the formation of the crisis unit that will be activated in case of a major security incident. Given the nature of the information contained in this procedure, this document is confidential.
The security incident and escalation process involves three levels:

- The local level, as soon as the incident is detected at run level,
- The entity and site level, after escalation,
- The SBS level after escalation.

In the SBS context, the management of security incidents is described in the SBS security incident procedure.
The process of follow-up of an incident is as follows: Report, Collection of evidence; Analysis, Possible escalation, Processing, Communication, Post-incident analysis.

10.5. Declaration and follow-up.

The ISO of the service line is notified by the service line teams of each security incident. Security incidents will be presented to the Customer according to what has been agreed in the Contract.
All information security incidents affecting SBS and/or the outsourced services subscribed by the Customer must be notified to the Customer within the regulatory timeframe (maximum 24 hours) following the ISO's qualification of these incidents.
A procedure exists and is shared on request. The procedure contains information regarding the notification, descriptions, remediations and lessons learned.
Security events (not yet officially declared as incidents) may be sent to the Customer's CISO if the information is sufficient to set up a direct communication.

It is possible to declare a security incident via the ticketing tool as well, if the security incident is considered as critical by SBS then it will be treated as a “burning” or critical production incident (P1).
Timeframes regarding treatment of incidents are indicated in the Contract.
In other cases, it will be handled by the service line's ISO as soon as possible.

In case of a security incident, SBS will apply all means for collaborating with the Customer’s CISO, assuring a transparent communication and by actively participating in providing evidence required for the analysis and remediation of the security incident.
To contact SBS, a specific email address is provided: security.incident@soprabanking.com

Also, the analysis of the origin of reoccurring security incidents, the identification and implementation of the measures of the final resolution of security problems makes part of the generic problem management (for all kind of incidents) put in place by SBS.

10.6. Personal data incidents (GDPR)

The security incident process includes the management of personal data breaches.
Incidents are reported to the data controller as soon as possible and follows the regulatory requirements.
If the incident involves personal data, additional information must be communicated to the Customer's DPO and the SBS DPO. The email address of the SBS DPO is GDPR.ACCESS@soprabanking.com

10.7. Report

All employees and contractors should report such problems to the point of contact as soon as possible to avoid information security incidents. The reporting mechanism should be as simple, accessible, and available as possible. Therefore, security incident reporting is done via the IT Service Management application, which has a dedicated process for security incidents.

11. Business Continuity Management

SBS has the organizational and technical means to ensure the continuity of activities of the Services.

SBS shall endeavour to maintain the level of service as defined in the Agreement and to protect critical business processes from the effects of an information system failure or disaster, and to ensure the recovery of these processes as soon as possible.
In the case of an incident affecting the availability of the service, SBS undertakes to restore the Service as defined in the Agreement.
SBS maintains a document describing the measures of its Disaster Recovery Plan.

11.1. Business Continuity Plan (BCP) test

By answering to criteria of identified risk scenarios, operations teams carry out a yearly test of their Business Continuity Plan.
The results of this exercise and the associated documentation can be made available on request. The tests are carried out on operations team level.
(Example scenario: Unavailability of the main site).

11.2. Disaster Recovery Plan (DRP) test of environments

To ensure the resilience of the Solution and to enable the efficiency of the back-up Solution of the infrastructure made available to the Customer, an exercise is carried out yearly. The DRP test is planned and organized by the teams in charge of Solution.
Depending on the nature of the Solution, the DRP tests can be carried out on a control environment.
The results of this exercise and the associated documentation can be provided annually on request.

12. Encryption & Secret Management

12.1. Objective

Ensure the correct use of encryption to protect the confidentiality, authenticity and/or integrity of information.

12.2. Requirements

A policy for using cryptographic measures to protect information has been developed and implemented by SBS.

12.3. Encryption at rest

Company Laptop
All SBS workstations are encrypted at rest (the deployed Solution by internal IT currently is Bitlocker).
SBS undertakes to use robust encryption protocols with no known vulnerabilities.

AWS Servers and services
By default, the data on the servers is encrypted using AWS processes (AES-256 encryption is used, more details are described in the internal product documentation).

12.4. Encryption of data in transit

By default, the implementation of any transfer protocol must be encrypted for data exchanges between VPCs (Virtual Private Cloud) and for data exchanges between SBS's VPC and customers.
By default, all network flows are encrypted within the VPC service (Virtual Private Cloud). Except in case of an exceptional technical reason. In such case a security exception is raised by the ISO of the service line.

Protocol

By default, only encrypted protocols (sFTP, HTTPS, ...) are allowed between the different VPCs.
This measure is mandatory when Customer Data is present in the environment. For encrypted communication flows, the TLS 1.2 protocol is applied, or a higher TLS version as soon as this is validated by SBS R&D.

12.5. Secrets management

SBS is committed to ensure that secrets (e.g. passwords, access keys, cryptographic keys, certificates, encryption keys, etc.) are properly protected.

By default, we apply the following rules:

- secrets must not be hard-coded
- secrets must not be stored in plain text files
- secrets must never be shared unprotected (encrypted)
- secrets must expire (usually annually).

Several technical means can be put in place to ensure that an approved Key Management System (KMS) or vault is implemented to store and manage secrets. Access to the KMS or vault is protected and restricted to a limited number of authorized users.
Expiration times are defined according to the criticality of the secrets.

13. Security of service operations

13.1. Operating procedures and responsibilities

13.1.1. Documented operating procedures

Operating procedures should be documented and made available to all relevant users.
These procedures are not shared with the Customer but may be presented during an audit.

13.1.2. Competences

The staff is trained and made aware of the different SBS processes and standards that allow them to understand the business and operational processes (e.g., ITIL).

13.2. Backups

The Supplier undertakes to backup, in accordance with the rules defined by default in this Appendix, all Customer's Data transmitted, uploaded or stored on or to the Infrastructure and the Supplier shall be responsible for restoring, by using the last backup completed, all lost or modified data, files or information.

13.2.1. Standard policy

As part of the Services agreed with its customers, SBS describes all the backup and recovery services implemented for its customer services. It specifies the scope, means, general principles, types of backup and associated services. These backup and recovery services are based on AWS services dedicated to providing this functionality to all AWS subscriptions using the same services. SBS is responsible for the correct configuration and implementation of these AWS services. Therefore, the backup of assets providing the customer services (software/infrastructure/database) are placed under the responsibility of SBS.

Any data (example: database instances, files, virtual machines, …) necessary for the operation of the Solution in function of the services must be backed up according to the standard backup policy.
SBS ensures that backups of Customer Data are secured and protected against physical destruction.
Backups are stored in a secure manner using robust encryption techniques.

For production environments the standard policy is:

Frequency	Retention	Type
Daily	7 days	Complete backup
Weekly	4 weeks	Complete backup
Monthly	12 months	Complete backup

(*) no incremental backup on AWS, this can be considered as complete backup.

In specific cases the service line can decide to deviate from this standard policy when the backup of an asset has no added value to the operated Solution.

13.2.2. Exceptions

Several AWS services deviate from this standard because they are relying on following versioning principles:

Databases

In operated Solutions using one or more database instances not containing any Customer Data. The service line can decide to adapt the frequency and retention.

Virtual machines

The backup policy is not applicable for virtual machines based on images (AMI) or microservices containers (example docker container) containing no persistent data.

AWS S3

There is a possibility to store data on cold storage using AWS S3 (Glacier). This data is stored on S3 via objects. By using the S3 versioning on these objects, data can be preserved, retrieved, and restored. A retention policy can be defined to meet compliance obligations.

13.2.3. Restore test

Every year, SBS performs a restoration test on a reference environment. This test makes part of the yearly Disaster Recovery Test Report.

13.2.4. Archiving

By default, archived data concerns the Solution's production resources and is managed in AWS. If required by regulations, an optional archiving process may be provided, and this must be specified in the Agreement.

13.3. Change management

For any change impacting security, the ISO will be informed. The operations carried out on the Customer's environments are under the responsibility of SBS operations teams in terms of management and deployment.
In case of a planned maintenance that requires service interruption, the Customer is notified in advance, as described in the Quality Assurance Plan. Any intervention in production is tested in an acceptance and/or test environment beforehand.

13.4. Separation of environments

Production and non-production environments (PROD, UAT, test …) are segregated to reduce the risk of unauthorized access or changes in the production environment.
Unless explicitly requested by the Customer, production data must not be copied to non-production environments.
In case there is a copy to the non-production environment, this environment must have equivalent security measures as the production system.
The partitioning by different security zones, especially for the administration, is necessary to limit the propagation of attacks.
Regarding the segregation mechanisms of Customer's Data in AWS environments, SBS has implemented strong security controls to ensure isolation between the corporate network and the management interfaces and Customer's environments.

The security measures implemented, monitored, and reviewed are as follows:

- Administration and operation activities are performed by authenticated SBS users.

- Administration and operation activities are only possible by employees authorized by the Delivery Manager.
- Workstations, which are subject of a regular sanity check (OS patches, AV signatures, …), are used to connect to the AWS environments.
- SBS infrastructures build in AWS use AWS VPC to provide the necessary network and segmentation restrictions.
- Some product connection interfaces may be subject to mTLS, direct connect, leased line, VPN or IP Whitelisting...
- Administration activities are recorded and monitored.

The R&D environments are not managed by the operations teams, but directly by the R&D department. SBS ensures that R&D environments do not contain Customer's Data unless explicitly requested by the Customer.

13.5. Protection against malware

Antivirus management is valid only for Windows operating systems (servers & laptop) (cf. this point is described in each product of the Solution).
Antivirus and EDR are deployed on all SBS employees' workstations (current software is Microsoft Defender).
Antivirus and EDR are deployed at a minimum on all the Solution's Windows operating systems, and some Linux environments (current software is Trend Micro Cloud One).
Antivirus monitoring is conducted by the Cloud Ops teams and presented to the SBS security committee in case of a failure or in case the security committee requires information (operating deviation, etc.).

13.6. Logging and Tracking

13.6.1. NTP clock synchronization

Correct clock settings are essential to ensure accurate audit logs that can be used in investigations or as evidence in court cases or disciplinary proceedings. Inaccurate audit logs can hinder investigations and undermine the credibility of evidence. For logging systems, a master clock connected to a time signal broadcasted by a national atomic clock can be used.
The NTP protocol ensures that all servers are synchronized with the master clock. There can be several time servers depending on the use (firewall / servers).

13.6.2. Tracking of operations on AWS.

All operations performed on AWS are logged according to the needs of the various teams, including the operations teams.

13.6.3. Application logs

Application logs are logs generated by the applications of the Solution. The logs are essential for analysis in the event of an incident, but the level of detail and volume in production must not be a constraint to the proper functioning of the Solution.

13.7. Skill management for software operation

All operations affecting the systems are performed by trained and qualified operators regarding the change process. The operator is clearly identified and undergoes regular training to upgrade his/her knowledge.

13.8. Patch Management

13.8.1. Patch Management of the workstations & servers managed by the IT dep.

Security patch management is applied to both workstations and servers managed by the IT department.
Within the context of the implementation of security measures, the management of security patches on the administrator workstations and on the servers providing services to customers, is under the responsibility of SBS.

13.8.2. Patch Management of SBS's Customer environment infrastructure

Patch Management is ensured by the different technical teams and documented.

By default, the security rule is weekly automatic updates for security patches in our operating systems with a manual patching capability in case of emergency. Depending on the application and its prerequisites, these updates can be organized differently.

13.8.3. Patch management of the applications

Concerning the SBS Offerings, this is indicated in the QAP (Quality Assurance Plan).

13.9. Vulnerability management

13.9.1. Criticality and CVSS scoring

Vulnerability handling is analyzed and reported, with an assessment based on raw CVSS 3 scoring:

The impact of vulnerabilities can vary, it can be recalculated automatically or manually depending on certain parameters such as the exposure of the concerned asset, its environment, ...
Vulnerabilities considered as Critical (contextualized CVSS ≥9) and proven are considered like a P1 incident and addressed immediately.

13.9.2. Vulnerability watch

The vulnerability watch service is organized in SBS and relies mainly on:

- CERT bulletins from the Sopra Steria Group's cyber security unit
- A subscription with a private French CERT

The management of the CERT alerts is based only on alerts indicated as High or Critical.
The impact of vulnerabilities can vary depending on several parameters, such as the exposure of the asset concerned and its environment. The service line ISO is responsible for assessing and recalculating the vulnerability score and defining priorities from P1 to P4.
Only vulnerabilities classified as P1 and P2 are managed directly, with a processing time established from internal confirmation of the alert (following the CERT publication date). If the deadline is not met, the ISO must be consulted.

The CERT alert reports are analyzed by the ISO of the service line. All P1 and P4 CERT alerts are reviewed and presented in the security committee or COMSEC.

Category	Processing delay
P1 - Critical	Processing delay: 1 week
P2 - High	Processing delay: 3 weeks for exposed services Processing delay: 6 weeks for a non-exposed service (example: VPN) If the asset is not considered at risk, the delay is 26 weeks.
P3 - Medium	Managed by the standard processes (business as usual)
P4 - Low	Managed by the standard processes (business as usual)

13.9.3. Vulnerability scanning by operations teams

The vulnerability monitoring service provides for:
Vulnerability scans periodically performed on the assets identified in the Customer service (perimeter frequency adapted to each line, at least every month (with an internal report and presented by the ISO during the security committee)). Tools used: AWS Inspector, CyberWatch, or Qualys or equivalent.

Optionally, a monthly report, dedicated to the Customer, can be provided.

The impact of vulnerabilities may vary. Depending on certain parameters such as the exposure of the concerned asset, its environment, … The ISO of the service line could re-evaluate or recalculate the CVSS score or internal score of the scan tool and define a priority/category P1 to P4.

Category	Processing delay
P1 – Critical	Processing delay: 1 week
P2 – High	Processing delay: 3 weeks for exposed services Processing delay: 6 weeks for a non-exposed service (example: VPN) Processing delay: 26 weeks if the asset is not considered at risk.
P3 – Medium	Processing delay: 26 weeks
P4 – Low	Deadline: to be agreed with the service line according to the cost complexity, risk. Often integrated into the version update. Actions considered long-term are security exceptions.

A security exception is raised if the timeline defined below is not or cannot be respected.
As a reminder, if the software package is not at the latest version, vulnerability management makes it possible to determine if components have become obsolete or vulnerable.

13.10. Connections to Customer's environments

Connection from SBS
SBS has a procedure for managing connections. The procedures can be presented during an audit. Each user has its own security key or personal credentials secured with a Multi Factor Authentication and based on the AWS session manager.
All access to the system is only possible through this session manager that centralizes all connections. Multiple sources of logs and events are collected and stored securely to constitute a reliable audit trail that tracks connections done on the platform. These trails could be used for audits, for reviews or for analyzing behaviours on the platform.

14. Development security

14.1. Secure Software Development Lifecycle

The software developed by SBS is subject to the rules of the Editor Security Management Plan (e-SMP). The latter defines security requirements for the development activities and mainly the following points:

- Good practices on security and secure development
- Integration and review of frameworks
- Considering the OWASP TOP 10 guidelines

The processing of recommendations following audits carried out by SBS and the SECAPP SBS auditors.

The goal is to ensure, through regular checks, that SBS Offerings deployed do not contain any critical vulnerabilities.
In addition to these controls, intrusion tests can be carried out by Sopra Steria's cyber security unit to ensure that no critical vulnerabilities are present in the environment. This service can be provided on request and will be subject to a quotation.

14.2. Open-Source Management

The management of open-sources software integrated into our software is monitored directly by our R&D department, following the guidelines of a "License Rules Book", documentation which defines the rules governing the use of GPL2-type licenses, for example, and the management of vulnerabilities and debt detected by our SBOM control tools.

Controls are carried out within the framework of SBS KPI's and in the monitoring of version upgrades by Security Officers.

15. Relations with suppliers

Critical suppliers are identified according the EBA guidelines. The follow-up of the suppliers is performed by the service line and operations team.
The list of the critical suppliers depends on the provided Solution.

Supplier	Product Name or Function	Domain	Description
TINK	TINK	Market Place	DSP2 Use case; PSD2 Bank Act as TPP API PSD2 Bank Act as TPP
KOBIL	KOBIL	Market Place	Use Case; Secure Digital Identities and Business Communications
AWS	AWS	Technical	Cloud Technical services
MongoDB	ATLAS	Technical	Database managed on AWS
IBM	Safer Payment	Soft	Fraud detection

16. Compliance

16.1. Objectives

To avoid any breach of legal, regulatory, or contractual obligations and security requirements.
Ensure compliance of systems with SBS security policies and standards.

16.2. Measures

The measures in place must be proven to be effective. Security performance is measured within operations by the formalization of objectives and associated indicators that are reported by the SBS CISO to the General Management.

The operations department monitors the following to comply with the requirements:

- Follow-up by the monthly security committee dedicated to the service line for all customers.
- Follow-up in the IAM risk committees.
- Monitoring through the yearly SBS Information Security compliance plan. Indicators include monitoring of vulnerability scan plans, continuity, audits, training, and monitoring of P1s identified in audits, these indicators are reviewed on a yearly basis.
- Weekly monitoring of the service line for any alerts or security events.

In the event that the Agreement between SBS and the Customer includes the latter's right to audit, and subject to the signing of a specific confidentiality commitment or Audit Agreement, the various documents may be presented to the auditors.

16.3. Security Management and Security Performance Indicators

Depending on the scope, security indicators are established and monitored by the ISO of the service line. KPIs are periodically reported to the SBS's CISO.

16.4. Certification

SBS is currently certified ISO\IEC 27001:2017 for the cloud native perimeter. During the next reviews an extension of the scope will take place.

16.5. Continuous Improvement

Regularly feedback from compliance teams, auditors, and employees is collected and analyzed to continuously improve security measures and compliance efforts.

17. Reference documents

- The SBS Information Security Policy including the SBS security incident management policy
- Charter for the use of IT equipment
- Account management policy (administrator and service accounts, password policy, etc.)
- Yearly internal memo on the organization of Information Security
- Site SISD for each premises

18. Abbreviations and acronyms

Abbreviation	Definition
SMT / ITSM	SBS support services management tool, allowing the management of incidents, changes, problems, releases. This tool is used to capture and track incidents and requests.
DRP	Disaster Recovery Plan
SMP	Security Management Plan
ISP	Information Security Policy
CISO	Chief Information Security Officer
ANSSI	French National Agency for the Security of Information Systems
CAB	Change Approval Board
CERT	Computer Emergency Response Team
CNIL	French National Commission for Information Technology and Liberty
COMSEC	Security Committee
COPIL	Steering Committee
MM	Meeting Minutes
PD	Personal Data
GM	General Management Executive Officer
DI	Industrial Department
DID	Industrial Department Director
DOD	Director of Operations Department
DPO	Data Protection Officer
IT Dep	Information Technology Department
F2F	Face2Face - Corporate Intranet
I/O	Input/Output
ITIL	Information Technology Infrastructure Library
RACI	Responsible-Accountable-Consulted- Informed Matrix
ISO	Information Security Officer
DSIS / SISD	Dossier de sécurité infrastructure site or in English Site Infrastructure Security Document File, is a document describing physical security of the premises.
IAM	Internal Approbation Meeting. An Iteration Assessment Report (IAR) is presented during this meeting
Run manager	Responsible for the Agreement and operations for the Customer
Vulnerability	A weakness of an asset or group of assets that can be exploited by one or more threats
SBS	SBS Software a subsidiary of 74 Software Group (hereafter “the Group”)
Customer	The customer who subscribed for the provisioning of the Solution as stipulated in the Agreement
Solution	Refers to the combination of (i) the SBS Offerings; and (ii) the infrastructure