Security Insurance Plan

reachfive

Version History				
Date	**Author**	**Validator**	**Version**	**Evolution**
01/10/2020	Pierre Bar	Jérémy Dallois	1.0	Creation of document
30/03/2022	Yoann Audon	Pierre Bar	2.0	Global update
23/05/2022	Yoann Audon	Pierre Bar	2.1	Addition of details on encryption, securing of servers, and security incidents

CommuniThink, a simplified joint-stock company with a capital of 114,486.20 euros registered in PARIS Commercial Register under no. 797 606 357 Registered office: 33 rue La Fayette - 75009 PARIS, FRANCE
Phone: +33 1 76 44 06 01 - Website: www.reachfive.com - Email: contact@reachfive.com

Table of Contents

Table of Contents 2

1 Introduction 3

1.1 Purpose of the document 3

1.2 Applicable reference documents 3

1.3 ISS objectives 3

1.4 Risk management 3

2 Organisation of information security 4

3 Information Systems Security Policy 4

4 Security measures implemented by ReachFive 5

4.1 Human resources security 5

4.2 Asset management 5

4.3 Mapping 6

4.4 Qualification of information 6

4.5 Access controls 6

4.6 Mobile devices and homeworking 7

4.7 Cryptography 7

4.8 Physical and environmental security 8

4.9 Operational safety 8

4.10 Communications security 11

4.11 Acquisition, development and maintenance of ISs 12

4.12 Relationship with suppliers 12

4.13 Security incident management 13

4.14 Business continuity management 13

4.15 Compliance management 14

5 Appendix – Glossary and definitions 16

1 Introduction

1.1 Purpose of the document

This document constitutes the Security Insurance Plan (SAP) written by ReachFive as part of the services performed for its clients.

The Security Assurance Plan outlines the provisions ReachFive undertakes to implement to meet the security requirements of its clients. In particular, it defines the organisation that will be put in place, the methodology to be followed to manage the security of the outsourcing project and the technical, organisational and procedural measures that will be implemented.

1.2 Applicable reference documents

- [ISO 27001] ISO/IEC 27001:2013 – Information security management
- [ISO 27002] ISO/IEC 27002:2013 – Information security, cybersecurity and privacy protection — Information security controls
- [ISO 27018] ISO/IEC 27018:2014 – Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

1.3 ISS objectives

- Meet the security needs of the business
- Align with ReachFive's IS strategic issues
- Manage security by risk
- Observe the laws and regulations regarding the protection of the IS

1.4 Risk management

ReachFive's general management wants information security risks that could lead to unacceptable service disruption for clients to be managed on an ongoing basis.

The risk management process is based on the EBIOS (expression of needs and identification of security objectives) method, a methodology that is maintained by the French National Agency for the Security of Information Systems (ANSSI). This process is divided into two sub-processes:

- Under the responsibility of the CISO, risk assessment enables the identification and assessment of security risks related to the ISMS area.
- Under the responsibility of the Management Review Committee, risk management ensures commitment to the selected options (refusal, transfer, reduction or acceptance) and the approval of the residual risks by the management, which then authorises the implementation of the corresponding security measures and the operation of the ISMS.

Risk assessment and management shall be carried out at least once a year. As needed, risks can be reassessed during the year to realign security objectives with the business strategy.

2 Organisation of information security

To respond effectively to the major security challenges of information systems, it is essential to define an ISS organisation meets requirements.

The chief information security officer (CISO)
The CISO guarantees compliance with the Information Systems Security Policy (ISSP). As such, they see to the governance and management of the security of the IS. They are the operational manager of the ISS. In particular, they must:

- Conduct awareness-raising and information activities on information systems security
- Establish an inventory of IS resources of entities and assess the sensitivity of these assets
- Conduct risk analyses for any new sensitive information system or for any major evolution of an existing sensitive information system
- Implement the security provisions laid down by the owners of ISs
- Conduct regular actions to monitor the security level of ISs and implement the necessary corrective actions
- Define and put in place the procedures for responding to alerts, incidents, and emergency situations concerning the information systems security
- Make available the resources necessary for the implementation of the action plans relating to the security of ISs.

The CISO will be able to use technical relays in the various business entities in order to implement the provisions of the ISSP throughout the area.

Security contacts

Here are the persons to contact for all issues to the security of the IS:

NAME	ROLE	CONTACT
Audon Yoann	CISO	yoann.audon@reach5.co
Bar Pierre	CTO	pierre.bar@reach5.co
Security address	Generic address	securite@reach5.co

3 Information Systems Security Policy

To meet its regulatory obligations, improve its processes to continuously integrate the information security aspect, and thus improve the practices of all technical teams, ReachFive has developed an Information Systems Security Policy (ISSP).

To do this, the Information Systems Security Policy:

- Describes internal and external information security issues
- Presents information security governance

- Reiterates the legal and regulatory requirements, which must be met both by the company and individually by each employee
- Defines information security objectives.

The Information Systems Security Policy is reviewed annually, is approved by the president and is distributed to all employees.

4 Security measures implemented by ReachFive

4.1 Human resources security

The company manages all the recruitment and integration processes of employees.

The company carries out screening of candidates for employment. This check makes it possible to verify that the advertised qualifications are in line with the positions concerned.

All employees have signed an NDA in their employment contract.

All employees have read the IT charter, signed it and are committed to respecting and enforcing it. This charter also refers to the confidentiality requirements and defines the rules for the proper use of the computer and digital resources made available.

An official departure management process makes it possible to structure the actions to be taken whenever an employee leaves, and in particular to deactivate and close their accounts and authorisations for the various resources to which they were entitled.

The accounts and authorisations of the outgoing employee are disabled on the day the employee leaves.

The accounts and entitlements of the outgoing employee are disabled within three months.

Employee awareness
Raising awareness and training employees in good safety practices is essential. The CISO conducts security awareness workshops several times a year. These workshops can be in the form of:

- Phishing campaigns (at least once a year)
- eLearning:
  - Reminder of good safety practices via infographics and emergency response cards
  - Reminder of best practices for secure development through the OWASP Top 10
- Communication: Information about a vulnerability that could impact the company.

4.2 Asset management

Inventory of IT resources
The solution JAMF is used to inventory all employees’ desktops.

ReachFive does not have servers in house. All infrastructures are hosted by the following Cloud providers:

- Azure
- GCP
- AWS
- Yandex.

An inventory in Excel format is kept regularly updated for the server fleet. This inventory is a compilation of extracts from hosted infrastructures within cloud providers.

4.3 Mapping

The mapping details the data centres, network architectures (where the hotspots and sensitivity of the information being handled are identified) and qualifies the level of security expected. This mapping is kept up to date and made available to the CISO.

A flow map exists and allows the user to visualise the exchange of information from an application point of view. This mapping is described in the Technical Architecture File (TAF).

4.4 Qualification of information

The sensitivity of any information and assets is assessed.

Our clients' data falls within the domain of personal data and is therefore automatically qualified as sensitive. It therefore benefits from the highest possible level of security.

4.5 Access controls

Google Workspace repository
The user repository is based on Google Workspace and applications are all authenticated using Google SSO.

Applications log all accesses. These logs are kept and analysed in case of abnormal behaviour on access to an account.

Accounts are personal and administrators have specific administration accounts with a secure configuration.

Multi-factor authentication (MFA) is required as soon as the account is created.

The password policy for employees is as follows:

- Minimum number of characters: 12
- Complexity: 1 digit, 1 letter, 1 uppercase letter, 1 lowercase letter and 1 special character minimum
- Blocking: After 10 unsuccessful login attempts
- Unable to save a previously used password
- Renewals every year.

A comprehensive inventory of privileged accounts exists and includes:

- Users with an administrator account (or privileges greater than those of a standard user) on the information system
- Users with privileges high enough to access the working directories of managers or all users.

The CISO carries out reviews of accounts and authorisations every year for employees and every six months for administrators.

Only administrators can connect to the infrastructure of the ReachFive platform.

CIAM Client platform

All instances on GCP have only a private interface with no direct access to the Internet; all outgoing access happens through a Cloud NAT instance. All incoming accesses from all sources are filtered.

ReachFive's CIAM platform allows you to configure:

- Multi-factor authentication (MFA) by text message or email
- A dedicated password policy
- Specific event logs (Audit Logs)
- Rate Limiting
- ReCAPTCHA v3 on user requests
- A policy for blocking suspicious IPs (Identity Fraud Protection)
- Countries authorised to access the platform (ISO code 3166-1).

CIAM BackOffice platform

The password policy is as follows:

- Minimum number of characters: 8
- Password strength set to "Good," based on the Dropbox algorithm "zxcvbn" (https://github.com/dropbox/zxcvbn)
- Multi-factor authentication (MFA) in the console is provided for Q4 2022 in the roadmap.

4.6 Mobile devices and homeworking

Remote access to the entity's IS only conducted from company devices that run on the latest versions of MacOS.

4.7 Cryptography

Employee desktop hard drives are encrypted using Apple's FileVault solution.

Managing at-rest data encryption is based on Google's native management. Data is encrypted at storage space level using the AES256 algorithm. The details of Google's encryption at rest are specified here: https://cloud.google.com/docs/security/encryption/default-encryption?hl=fr

Data in transit is HTTPS-encrypted with TLSv1.2 or TLSv1.3 protocols at least. The following cryptographic suites are used:

- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-CHACHA20-POLY1305
- ECDHE-RSA-CHACHA20-POLY1305
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA384
- ECDHE-ECDSA-AES128-SHA256

4.8 Physical and environmental security

The entrance to the building and the ReachFive premises are protected by access badge systems and security guards monitor the entrances and exits.

The entire REACHFIVE IS resides on public clouds. Our hosts have obtained ISO/IEC 27001:2013 certification for the provision and operation of dedicated infrastructures.

Cloud Provider data centre security measures are shown in the links below:

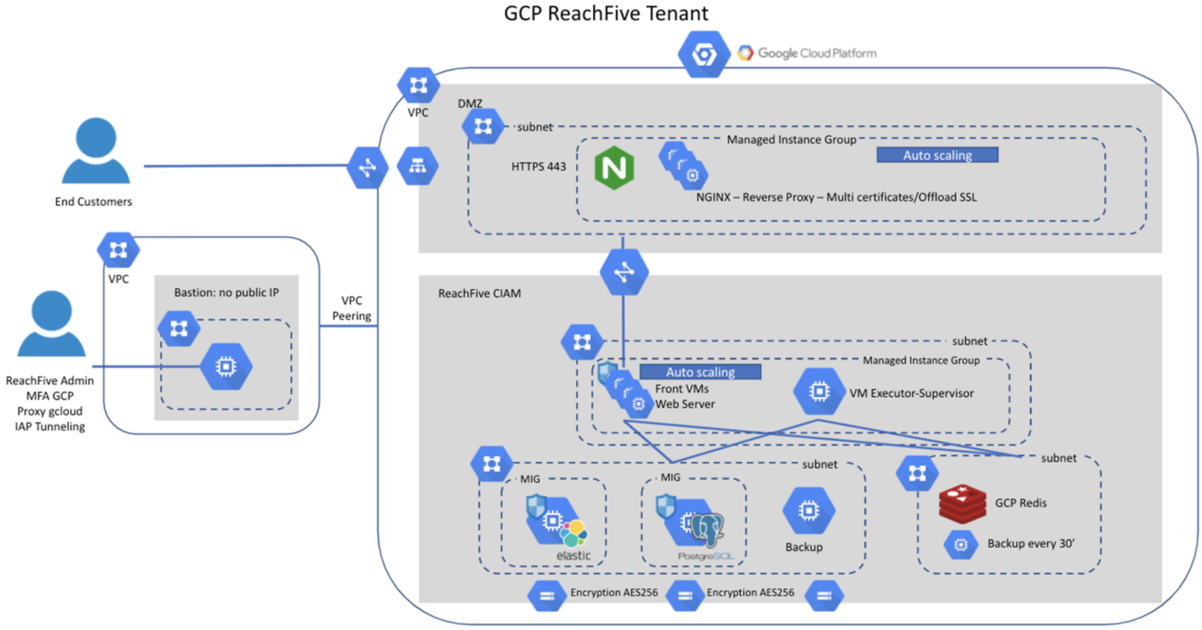
- https://www.google.com/intl/fr/about/datacenters/data-security/
- https://docs.microsoft.com/fr-fr/azure/security/fundamentals/physical-security
- https://aws.amazon.com/fr/compliance/data-center/controls/
- https://cloud.yandex.com/en/docs/overview/security/standarts#physic-sec

4.9 Operational safety

Operating procedure
Any operating procedure is written and integrated into our knowledge base.

The procedures are updated according to technological developments as well as changes in the company’s requirements.

Infrastructure diagram



Separation of environments

ReachFive’s technical teams have dedicated environments for their work (development, acceptance and pre-production) that are totally independent of the ReachFive platform accessed by our users (production environment). The ReachFive platform for users is therefore based on separate servers isolated from other environments.

In addition, we apply the principle of least privilege regardless of the environment.

Anti-malware protection

Employees’ desktops are embedded with the EDR solution SentinelOne. This solution is updated automatically and daily.

Backups and recoveries

CIAM platform data is replicated in real time in active/active mode across different areas of our hosting platforms so that in the event of an incident in an area there is no downtime or data loss. Indeed, the other areas remain fully operational and have all the data available.

In addition, we have many recovery points based on incremental and full backups. This backup is performed daily to allow the data to be recovered to D-1 in the event of an incident.

Backups are kept over 15 calendar days. Within this period, the client may request a copy of the backup, as well as the recovery of the backup of their data in case of an incident that has damaged or led to the total or partial loss of this data. Backups are stored in another third-party data centre.

On GCP, each platform has a dedicated, multi-region GCS bucket limited to Europe. To ensure the operability of backups, data recovery tests are carried out regularly.

Employees are informed that they do not store files locally and should opt for the Google Drive cloud environment.

A logging and monitoring policy is defined

Any access to the machines hosting the services is logged. This access log is replicated and encrypted on our log compilation tool.

All application logs replicated and archived in our log compilation tool can be exported to our clients at their request.

ReachFive is supervised 24/7 in terms of:

- Technical indicators
- Cases of functional uses
- Availability
- Response time
- Security incidents.

As a result, we have rolled out a monitoring solution that:

- Escalates technical hardware, software and storage indicators
- Measures availability and response times via these functional use cases
- Escalate alerts in case of cyber-attacks.

This monitoring aims to anticipate:

- Any technical faults
- Any need for capacity planning
- Cyber-attacks (credential stuffing and compromised accounts, DDoS, blocked IPs etc.)

The tooling that undertakes this monitoring is based on:

- Datadog Agent for process monitoring
- The collection of server metrics (CPU, Mem and IO etc.) via Datadog agents
- The centralisation of all logs generated by the platform
- The commissioning of an APM
- Probes that are scheduled every minute.

Clock synchronisation

The clocks of all information processing systems are synchronised to a single temporal reference source.

Securing of desktops and servers

Securing guides have been officially drawn up for desktops and servers based on the best security practices described in the CIS benchmarks (https://www.cisecurity.org/cis-benchmarks/).

The servers are based on the Ubuntu operating system and the following security measures are implemented (non-exhaustive list):

- Disabling of the Root account

- Personal accounts
- Disabling of standard listening services
- Minimisation of the number of services
- PAM password policy configuration
- Strengthening of configurations of SSH, Cron and logs services.

The desktops are based on the MacOS operating system and security measures are enforced via the solution JAMF allowing policies on the desktops to be monitored and managed. The following rules are configured:

- Locking of the screen in case of inactivity
- Hard drive encryption
- Removal of admin privileges
- Disabling of Apple cloud services (Siri and iCloud etc.)
- Activation of SentinelOne EDR
- Automatic update of OS and applications
- Catalogue of authorised applications.

Desktop updates are monitored and deployed automatically through JAMF MDM. Security patches on Linux servers are applied automatically.

4.10 Communications security

In general, the architecture of the company's networks is designed to meet all the needs of availability, confidentiality, traceability and integrity. The defence-in-depth principle is respected, in particular through the successive implementation of "demilitarised zones" (DMZ), appropriate virtual local area networks (VLANs) and strict filtering of application and administration flows.

To protect the infrastructure of the ReachFive platform, physical and logical isolation is implemented. This partitioning ensures segmentation between the servers that make up the platform and therefore strict separation between three major areas:

- Services exposed publicly on the Internet (web servers, email servers and proxy servers etc.)
- Internal application and data storage services
- Services dedicated to the administration and supervision of ReachFive.

Only the flows essential to the service are publicly accessible online. Similarly, only flows required between servers are accepted; any other flows are blocked.

The only possible incoming flow on the CIAM platform is port 443 on the load balancer.
The minimum TLS version supported is 1.2.

Outgoing flows are not subject to filtering. Here are the flows used:

- Identity management APIs of different providers (Facebook, Google and Twitter etc.)

- Sending emails to:
  - Mailjet where use cases of the control centre are used
  - The SMTP servers of clients who have configured it in their account.
- Webhooks for clients who have configured it in their account
- Datadog Agent that sends logs as well as metrics.

For any communication or exchange of data with our clients, we may set up suitable and secure exchange protocols that are specific to the characteristics and requirements of our clients.

4.11 Acquisition, development and maintenance of ISs

Any IS must be subject to a security validation decision before it is put into operation under the defined conditions of use.

Validation involves the CISO or their representative formally attesting that the information system is protected in accordance with the set security objectives.

This decision is based on a risk analysis adapted to the challenges of the system in question, and specifies the conditions of employment.

The security of IS must be considered and documented in all phases of IT projects, under the control of the CISO, from the design and specification of the system to its withdrawal from service.

Test data are not copies of production data.

Any new versions are subject to prior testing and validation before implementation. A backtracking phase is planned if the slightest malfunction is detected following an update.

The solution Veracode performs continuous code audits on development environments.

Employees develop on a private Github repository protected by strong authentication with MFA and accessible only to developers.

4.12 Relationship with suppliers

The ISS risk associated with a third party’s access to the company’s IS is identified and assessed, and the security measures needed to reduce it are implemented before granting such access.

Where the company’s IT infrastructure needs to be interconnected with that of an external company or another group entity, a formal risk analysis is carried out.
Any service in the field of IS is governed by security clauses. These clauses specify the ISS measures that the provider needs to comply with in the course of its activities, and the associated service levels (including non-disclosure of information).

4.13 Security incident management

Incidents are reported and recorded systematically following the established procedure. This procedure describes the escalations and people to be alerted depending on the severity of the incident.

Internal security incidents
Employees are aware of the importance of reporting any incident. The CISO is informed promptly by the IS operational chains of any security incidents.

In case of infection (worms, viruses or Trojan horses etc.), security flaws or security incidents found or suspected on a desktop, a reaction procedure known to all users is implemented.

CIAM security incident
At the client's request, the security events detected by ReachFive give rise to automatic communication with the client by email.

ReachFive will communicate all available information and will be available to the client to conduct further investigations.

The following is a non-exhaustive list of security incidents that can be escalated to clients:

- Compromised client accounts
- Attacks received on the platform corresponding to the number of error requests (400, 401, 403 and 429) reaching a defined threshold for a determined period of time
- Denial-of-service attacks.

Appropriate information regarding ReachFive's relationship with the authorities is passed on to clients. Any request from the authorities is forwarded to the clients.

An incident of the type of personal data breach complies with the obligations related to the GDPR and can be notified to the CNIL depending on the case.

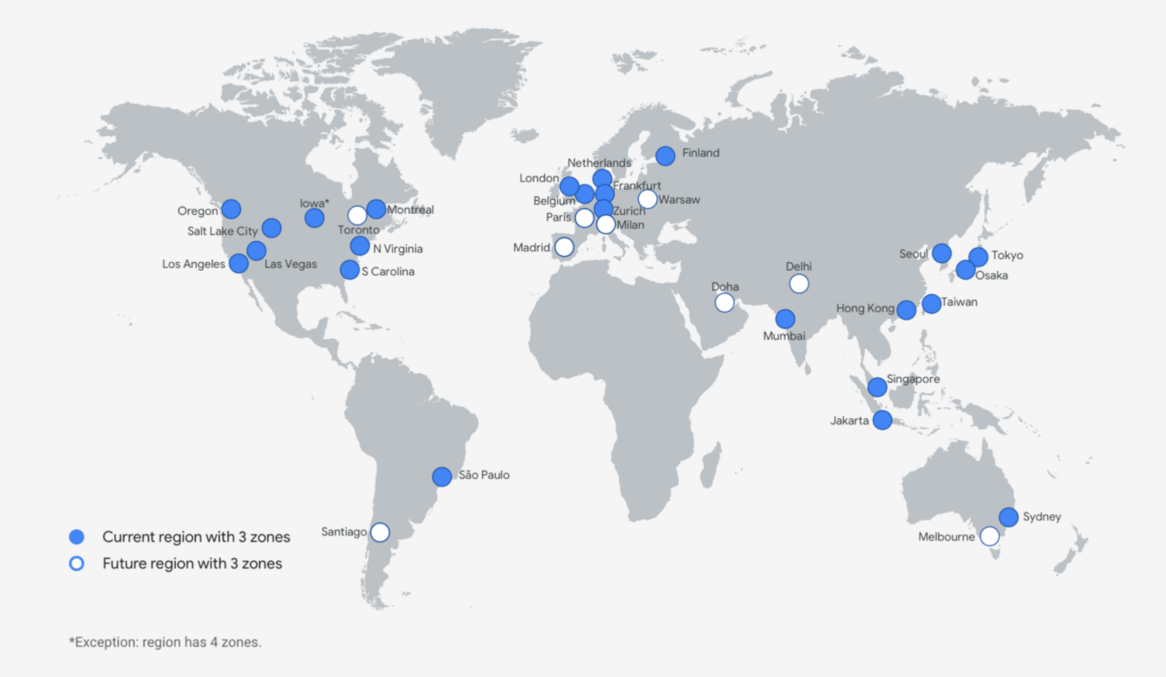
Crisis management
In the event of a crisis on ReachFive's IS system, an alert will be issued for the attention of the clients concerned. ReachFive undertakes to communicate to these clients as frequently as possible the progress of the work being done to resolve the crisis and the detailed action plan implemented. ReachFive reserves the right to employ an external company specialising in the resolution of cyber incidents according to the crisis in question.

4.14 Business continuity management

The business continuity plan has been formally established and applied. It is tested regularly during exercises to confirm its effectiveness.

Clients' ReachFive licensees benefit from a highly available service thanks to the redundancy of all software and hardware components

In the interests of high availability, CIAM bodies on GCP are deployed in at least three availability zones. Here are the areas available for GCP:



The management of backups and recoveries is described in the "Operational Security" chapter in the "Backups and Recoveries" section.

4.15 Compliance management

Technical audits

A Security Maintenance Procedure (SMP) procedure exists to address vulnerabilities identified during the various audits.

For any vulnerabilities discovered, a ticket is issued and a correction time set according to the criticality of the vulnerability:

- Low/Minor vulnerability: No time limit set or on the next release
- Medium vulnerability: 2 months maximum
- High/Major vulnerability: 1 week maximum
- Critical vulnerability: 2 days maximum

In the case of a vulnerability with high or critical criticality, the ticket is added to the so-called "Fast Lane" backlog for immediate processing. Current activities are then put on hold to process this ticket. Once the fix is developed, it is embedded to be delivered immediately in a hotfix release.

Technical audit: vulnerability scans

Infrastructure and application vulnerability scans are scheduled monthly on the CIAM platform. Reachfive is based on the solution Qualys Cloud Platform. Vulnerability scan reports can be requested by signing an NDA.

Technical audit: intrusion tests

ReachFive organises an intrusion test at least once a year. The scope of the tests encompasses the entire CIAM infrastructure. Test reports can be requested by signing an NDA.

Technical audit: code audits

Reachfive uses the solution Veracode to perform code scans. Code audits are integrated into the development chain and performed daily.

Personal data

The legal, regulatory and contractual requirements in force for the protection of personal data and the approach taken by the company to meet these requirements are identified, documented and met.

The data protection officer guarantees ReachFive's compliance with its obligations. They can be reached at: dpo@reach5.co

5 Appendix – Glossary and definitions

ISP	Integration of security into projects
OW	Owner
PM	Project manager
BCP	Business continuity plan
PCI-DSS	Payment Card Industry Security Standards Council /
ISSP	Information Systems Security Policy
CISO	Chief information security officer
IS	Information system
SIEM	Security information and event management
ISS	Information systems security
IS administration	All the actions ensuring the functioning and operation of one or more of the company's hardware or software elements (tools, networks, databases and messaging etc.). The IS administration thus ensures the consistency, accessibility and security of information.
Audit	An operation to analyse actions taken on data or assets or to measure the deviation from a benchmark (e.g. ISSP) or from the current state of the art.
Authentication / Identification	A process designed to verify the identity of an entity (natural persons or IT resources). Typically, authentication is preceded by identification allowing this entity to be recognised from the system by an element given to it. In short, identification involves communicating your identity, and authentication involves providing proof of your identity.
IS security requirements	The expression of required needs in terms of availability, integrity, confidentiality, traceability of an item information, a function or an IS.
Electronic certificate	An electronic identity card signed by a trusted third party, used to authenticate a natural person or an IT resource and to encrypt exchanges.
Encryption	A cryptographic method for rendering a document unintelligible to anyone who does not have the (de)encryption key.
ISS risk mapping	All ISS risks identified and assessed (in terms of occurrence, severity and control) for an entity (a department or subsidiary etc.).
Classification of IS or data	The evaluation of the criticality of an IS or data in terms of availability, integrity, confidentiality and traceability.
Partitioning	The principle of confining information system assets to specific security zones (or a network segment) and controlling communications between assets located in separate security zones.

Confidentiality	This guarantees that information is only accessible to authorised entities under predefined conditions.
Access control	The ability to restrict access to information or a resource to legitimate computer users or resources through appropriate controls. These means of control can be physical (e.g. swipe cards to access sensitive areas) or logical (e.g. login/password combinations).
Security patches	Updates to apply to IS assets to eliminate their known vulnerabilities.
Availability	This guarantees that information and related systems are accessible and usable by authorised entities when needed.
Right of access	Authorisation given to a user to perform a certain number of actions (e.g. accessing, creating, viewing, amending or deleting data) on a specific company resource (e.g. a printer, computer or computer room).
Securing of resources	Processes to reduce vulnerabilities in IT resources and limit their exposure to operational risks.
EDR	A tool to detect and block known and unknown threats on devices based on behavioural analysis, machine learning and event correlation.
ISS risk management	An iterative management process, aimed at identifying, assessing and treating ISS risks.
Authorisation	Granting a user access rights (physical or logical) to resources by an authorised entity.
User ID	Non-confidential information to identify a person (e.g. the public key for a certificate, login or client reference).
Security incident	One or more adverse or unexpected information security events with a high probability of compromising operations related to the organisation's business and jeopardising information security.
Integrity	This guarantees the accuracy and completeness of data, systems and processing methods.
Inventory	A detailed description of the assets (identification, owner, geographical location and versions etc.) of the company.
Threat	An event or action that may lead to the occurrence of a risk. A threat can be intentional (carried out by an aggressor with motivations) or accidental (occurring as a result of an error or a natural phenomenon).
Security measure	A technical or organisational means of hedging a risk.
Business continuity plan	The business continuity plan brings together all responsibilities, processes, operations and contributing resources, in the event of a major incident, to ensure the continuity of the company's vital business activities and to guarantee a return to normal operation.
ISS risk management plan	A set of actions to be implemented to improve the level of control of one or more ISS risks until the residual risk achieved corresponds to the level acceptable to the entity and company.

ISSP	An official set of strategic elements, directives, procedures, codes of conduct, and organisational and technical rules, designed to protect the company's information system(s).
Mobile equipment	Any technological equipment allowing access to a company's information or information systems, while on the move (e.g. a mobile desktop, smartphone or tablet).
Privileges	Permissions to perform actions that normal users cannot perform (e.g. administrative privileges).
Risk	Any "feared" event with negative consequences on the achievement of objectives at department, subsidiary or group level.
Information systems security	All technical and organisational protection measures enabling an information system to withstand events that could compromise the availability, integrity or confidentiality of data.
Information system	An organised set of resources (data, procedures, hardware, software and staff etc.) to acquire, process, store, disseminate or destroy the information used by entities in their professions, regardless of the medium of the information (digital, paper or oral etc.).
Traceability (or evidence)	Assets ensuring that events, activities or information, suffered or triggered by an entity (a natural person or computer resource), can be uniquely and unequivocally associated with that entity.
Vulnerability	A weakness in an information resource that can be exploited by one or more threats.