CACEIS GROUP DATA PROTECTION AND INFORMATION SECURITY POLICY

ABOUT THIS DOCUMENT

This is a crucial moment for data protection, a period of unprecedented change, not only in Europe but globally. In this context, CACEIS is delivering its three-year Information Security (IS) Strategic Plan to turn their vision into reality and to identify innovative solutions to address the protection of corporate assets, including personal data and Cyber-Security.

This 2017-2019 Strategic Plan summarises:

a. the major data protection and privacy challenges over the coming years;
b. four strategic objectives and 10 accompanying actions for meeting those challenges;
c. how to deliver the strategy, through effective resource management, clear communication and evaluation of our performance.

This document aims to structure CACEIS response for requests it receives concerning Information Security, in particular Cyber Security, and personal data protection.

CACEIS Requirements:

- Strategy concerning the management of Cyber-Risk, including the definition of roles and responsibilities and processes that cover the 5 following areas: Identification and assessment of potential cyber-risks, Protection against cyber-risk, Detection of cyber-risks, Responding to cyber-attacks, Restoration of operation after a cyber-attack.

- The new European wide General Data Protection regulation that enters into force as of 25th May 2018, has been reviewed and Corporate measures taken to be compliant. CACEIS will ensure that all personally identifiable information (PII) is identified and appropriately protected.

- French Military Programming Law « MPL » that enters into force on 1rst January 2020.

OWNERS: CACEIS Group Chief Information Security Officer (“CISO”) / CACEIS Group Data Protection Officer (“DPO”)
LAST UPDATE: May 2019
Version: 1.4

1.1 Introduction and Background

CACEIS is an asset servicing Group specialising in post-trade functions related to administration and monitoring of all asset classes. With a solid IT infrastructure, we provide execution, clearing, custody, depositary and asset valuation services in markets worldwide to assist institutional and corporate clients in meeting their business development objectives.

It is a regulated company and as such complies with national, European and international legal and regulatory requirements. CACEIS is a 100 % owned subsidiary of Crédit Agricole S.A., as such governance, policies, standards and best practice are inherited from Crédit Agricole Group and adapted to the CACEIS specific business environment and needs.
(On April 27th 2019, Crédit Agricole S.A. and Santander signed a Memorandum of Understanding with a view to combining their institutional custody and asset servicing activities. This merger would bring together CACEIS, Crédit Agricole S.A.'s institutional custody subsidiary, and Santander Securities Services (S3), Santander's subsidiary. The new entity would be 69.5% owned by Crédit Agricole S.A. and 30.5% by Santander.)

Crédit Agricole Group compliance is overseeing the deployment of GDPR around the firm to ensure that all obligations are met in terms of personal data protection (GDPR project management, common standards and best practices, community management, security measures, DPO organisation and accountability, relationship with the lead DPA for CA Group, …)

This is particularly true for Information Technology and Information Security. CAGIP, the Credit Agricole S.A. group's shared Information Technology (IT) production unit, is a skills centre that provides services such as desktop environment (printing, messaging, collaboration tools, office infrastructure, phone and mobile solutions), shared infrastructure services (remote access, Internet), Security Operations and access to common infrastructure (payment services such as Swift). These services are designed and managed to Crédit Agricole Group standards, embedding information protection services against data loss, malware, DDOS.

The Crédit Agricole Group Computer Emergency Response Team leverage state of the art threat monitoring, tracking and identification to deliver best of breed protection for Crédit Agricole Group companies.

CACEIS Information Technology services are primarily focused on building and running the highly automated business information systems. The hosting and lights-out operational management aspects have been outsourced to DXC in Luxembourg since 2007.

The CACEIS Information Security strategy leverages wording from the ISO/IEC 27001 information security standard revised in 2013. Although this standard is not mandatory, it is accepted in most countries as a de facto main framework for information security / cybersecurity implementation. It describes the information security management system, and it places security in the context of the overall management and processes in a company.

Cyber security and Cyber risk is a field of Information Security and traditional security that is concerned with the protection of information assets by addressing threats to information that is processed, stored and transported by internetworked information systems. The rise in internet delivered crime and ransomware, data theft and identity usurpation are but examples of cyber-crime.

1.2 Information Security Strategy

In response to the evolving business context, increasingly demanding legal and regulatory requirements, and the rapid changes to technology the CACEIS Group CISO has elaborated and maintains the following Information Security Strategy to ensure that Information Security threats and vulnerabilities are identified and managed so that Corporate Information assets are appropriately protected.

The strategy is aligned to 5 themes that bring structure and consistency to the underlying objectives:

1. Governance and organisation to ensure key stakeholders are involved in the Information Security decision processes, defining roles and responsibilities, resource allocation and prioritisation,
2. Legal and regulatory compliance so that Information classification and protection measures are delivered,
3. Culture, awareness and training on information and cyber risks,
4. Technology requirements to ensure security processes are efficient,
5. Standards and best practices addressing protection and controls.

Through these themes the Strategy builds and maintains top down awareness of data protection and privacy needs, so that the CACEIS information systems conform to legal and regulatory requirements and is solidly protected against threats. These threats are identified through Information Security risk assessments and monitored to ensure they stay within Corporate risk thresholds. Cyber risk is an important aspect of the threat landscape and fully addressed by the CACEIS Information Security Programme.

Within CACEIS people care is a considerable part of the internal culture, management ensure that mentoring and continuous training is widely available to facilitate the development of skills. This includes amongst others management training, product training, and technical training. Specific industry information security experience is driven through awareness programmes or specific industry product related courses but also, by participation in CA Group seminars and workgroups. CACEIS leverage industry standard tools for the delivery of up-to-date content thus enabling staff to self-manage their development throughout their career.

The Strategy focus on the period 2017 to 2019, a 3-year rolling period, for the current period the four strategic objectives are:

a. *Hardening of IT systems*
b. *Reinforce the access management controls*
c. *Improve the monitoring and detection of cyber-attacks*
d. *Improve the IT Continuity planning (ITCP) and recovery*

***The CACEIS Group Information Security strategy for 2017-2019 has been elaborated and adapted to include aspects of the Crédit Agricole Group programme to Reinforce Security (CARS)**.

In terms of Sun Tzu's guiding principles published in 473 BC, *The Art of War*:

"We must know ourselves and our enemies and select a strategy to positively influence the outcome of battle. There is no reason to fear the attack but there is reason to be concerned about our readiness to defend ourselves from the attack and respond appropriately."

1.3 Personal Data Protection and Privacy

In support of its Customer Project, the **Crédit Agricole Group** has chosen to implement a Private Data Charter, which took effect in early 2017.

This charter, which is the result of reflections on the use of private data, is one of the key commitments of the "Ambition Stratégique 2020" Medium Term Plan of Credit Agricole Group. It comes in response to changes in society, as well as in regulations), with the implementation in 2018 of a framework to improve protection for individuals' private data. (under the General Data Protection Regulation – GDPR)

With ever-increasing use of digital technology and data mining, this Charter will differentiate the Group's market positioning through five underlying principles, which will reassure customers and disseminate best practices to employees of the Group's entities, in accordance with our values. CACEIS is adopting this Code of Ethics shared by all Crédit Agricole Group entities. This Code expresses our culture and values, including data protection.

The Code is a reference document containing the principles of action and behaviour which govern on a daily basis, CACEIS's relationships with its clients, staff members and providers. This code will form the basis of all other charters, codes of conduct and internal regulations applicable to Group.

It reflects 12 fundamental principles, some of them place a particular emphasis on our clients. CACEIS's dedication to data protection can be broken down into the following themes:

- *Data Security*: Data security remains our priority and is central to all of our actions. The solutions we use to store or process our clients' data are subject to rigorous validation and certification procedures.
- *Usefulness and Loyalty: We are committed to using data in the interests of our clients in order to provide our clients with tailored products and enhanced quality of service.*
- *Ethics: We are committed to acting ethically and responsibly when handling personal data; such data will only be disclosed to third parties when required pursuant to regulatory obligations or for services provided by third parties that have been subject to CACEIS's rigorous validation and certification procedures.*
- *Transparency and Communication: We are committed to explaining to our clients, in a clear, concise and transparent manner, how client data is used, and to informing our clients of their rights in this area and how to exercise them.*
- *Giving clients control: We are committed to putting our clients in charge of their data and of how it is used.*

This Code is available on CACEIS Corporate Social Responsibility page. It is yet another clear expression of CACEIS's resolve to position itself as a genuine partner to its clients and to maintain its high level of trust.

1.4 General Data Protection Regulation (GDPR)

To ensure compliance with GDPR, CACEIS Group has conducted a comprehensive review of all its processes and databases to (i) clearly understand and document personal data held, processed and transferred - as the case may be, outside of the EU - and (ii) control the flow of data within the organization. The review was based on a 3 steps approach:

- Inventory of personal data and personal data processing (what data is collected, where it is stored, how and who has access to it),
- Risk assessment of such processing,
- Analysis of contractual agreements both with clients and suppliers to determine the legal basis for the collection and use of personal data (consent, contract, legal obligation, vital interests, public task, legitimate interests.)

It should be noted that since the territorial scope of GDPR is extensive, the review also applied to data processing activities performed outside the EU but which related to data subjects residing within the EU.

This review will result in the implementation (or updating) of all principles and policies affected by the application of GDPR. It will also serve to identify and prioritize the Data Protection Impact Assessment ("**DPIAs**") to be conducted. The purpose of DPIAs is to assess the origin, nature, particularity and severity of the risks associated with processing operations, that have the potential to affect the rights and freedoms of individuals.

This also led us to revaluate our access management, to tighten our access controls and tracking, and to review our confidentiality policy. In addition, data protection and privacy principles are now integrated at an early stage of conception of data processing in line with the principle of "*privacy by design"* while "*privacy by default*" will govern existing processes.

CACEIS Group will maintain a written record of processing activities (The Register) that will be made available at any time upon request from DPAs, especially in case where an audit is carried out by a DPA to check whether the organization is compliant with GDPR.

GDPR enshrines existing rights and creates new rights for data subjects, such as the right to erasure, the right to data portability or the right to restriction of data processing. CACEIS Group will thus set up appropriate and clear processes for recording and dealing with such requests.

Management of data breaches is crucial both for individuals and organizations, in particular given the occurrence of cyberattacks which could have serious consequences such as discrimination, identity theft, financial loss, …Therefore, CACEIS Group will have to report certain types of data breaches to the relevant DPAs and, where a breach is likely to result in a high risk to the rights and freedoms of individuals, directly notify those concerned. Our Data Breach Procedure will provide for notification within 72 hours.

Our Data Protection Officer ("**DPO**"), appointed at Group level, is granted sufficient autonomy and resources, and reports directly to the highest management level (Group Executive Committee). The DPO manages a network of local representatives in each country and entity where CACEIS is conducting business.

A global overreaching data protection compliance program will be implemented and integrated within the internal audit and permanent controls plans.

Caceis will also set up a multi-tiered training plan relevant to the different functions and tasks of its employees, knowing that all staff will have to follow a basic training.

As a company incorporated in France, our lead DPA will be the CNIL (Commission Nationale Informatique et Liberté). However, our DPO and his/her network of representatives will be available to answer any request from local Data Protection Authorities in any place where we are conducting business.

1.5 CACEIS Information Security Governance and Organisation

CACEIS relies significantly on technology to deliver its contractual obligations, and as such Information Security ("IS") is a key aspect supervised by Senior Executives. Building on existing corporate governance practices, a Corporate Information Security policy ("ISP") has been approved by the Executive committee and deployed uniformly across CACEIS, a Chief Information Security Officer ("CISO") has been appointed by Executive management to manage (define, implement, monitor) the CACEIS IS strategy. Governance of the CACEIS IS framework is achieved through the committees listed below (Table 1).

As a CA Group company, CACEIS participates in the CA Group Committees (a) Group Security (CSG), (b) Operational Security (COMOP) and (c) local risk management committees (ITR-C, ISS-C, BCM/DRP-C) and leverages the CA corporate and institutional best practices to ensure that CACEIS IS strategy covers all stakeholder requirements. CACEIS actively contributes to CA Group IS programmes and benefits from the output for continued improvement purposes, sharing intra-group practices and socialising ideas.

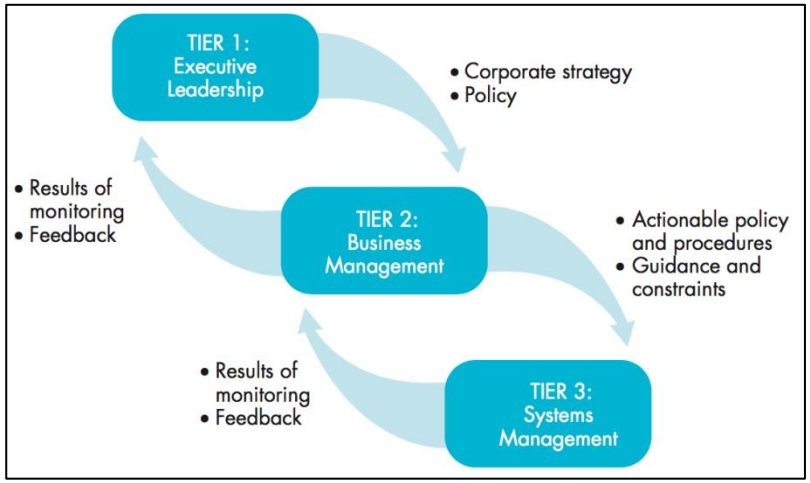
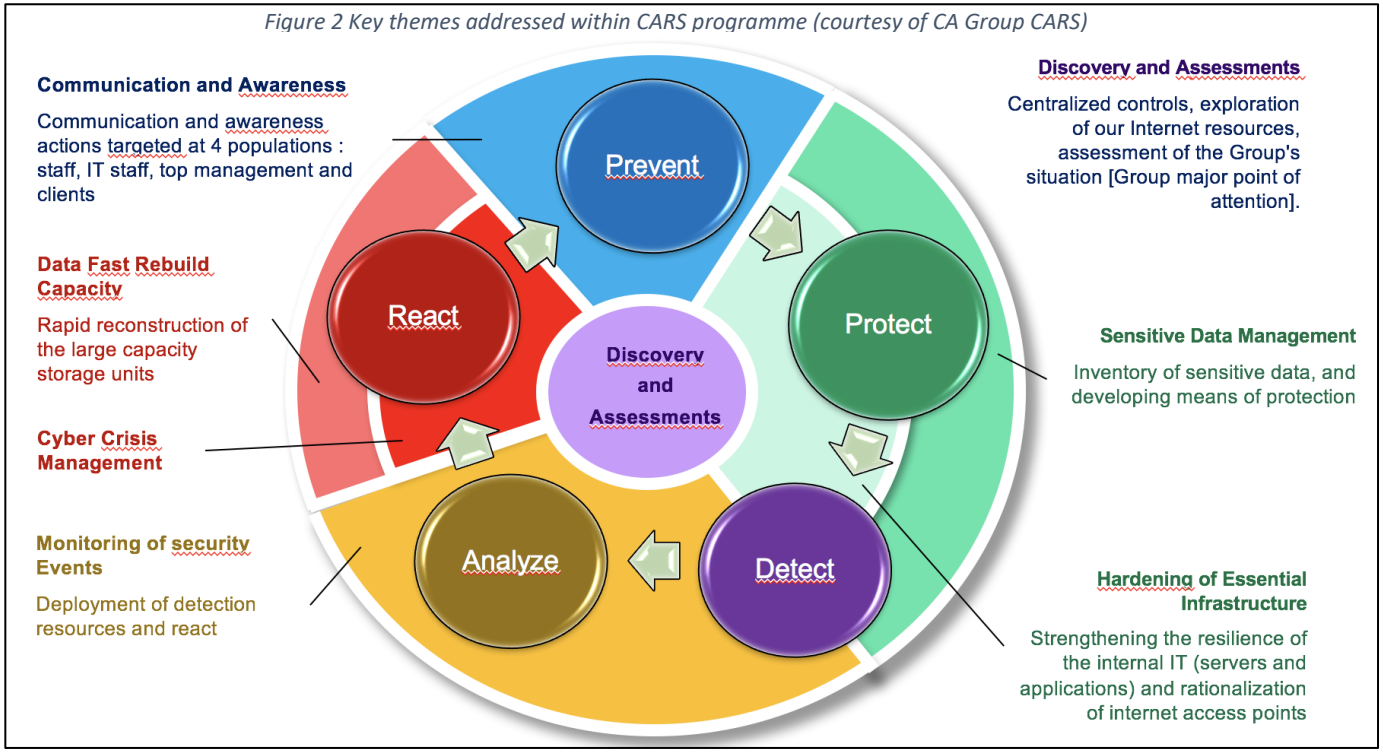


Figure 1 Organizational Structure and Responsibilities

Committee	Managed by	Frequency	Description of purpose	Participants
ISS-C	Chief Risk Officer, CISO	Quarterly	The Information System Security Committee defines, and reviews IS matters. ISS-C takes full ownership for defining, implementing and oversight of IS policies, processes, procedures, guidelines concerning IT security, physical security and personal safety within CACEIS.	Stakeholders include Executive representation of the businesses and CACEIS entities, legal, human resources, compliance, risk, procurement and technology.
ITR-C	CIO, SECGEN	Quarterly	The committee takes full ownership for Risk management of all IT processes. Ensuring assessments, mapping, setting priorities, …	Stakeholders include local CISO, ITSO, IT, IT security team, owner of.
BCM/DRP-C	RBCM	Every 2 months	The committee manages risks related to BCM and DRP. Plans and oversees all testing.	CIO, DRP processes owners, CISO, RPCA, IG and local representatives.
OES Review	Compliance	2 times a year	Review of the performance of Outsourced Essential Services (OES) to ensure that contractual and financial commitments are being achieved.	Compliance, risk department and permanent control
PROJECT COMMITTEE	CIO	As needed	Control committees supervising portfolio (CODEV and SVC), plus the Management Committees dedicated to each project.	
KEY IS SUPPLIERS	ITSO	2 times a year	Information Security steering committee with key external suppliers (DXC and CA GIP) to manage IS delivery and performance, sharing best practises and a forum for communication and exchange.	CISO, Security officers and Delivery managers of each provider.
NAP	Exec Mngt	As needed	Ensure that all new products or activities are compliant with IT security and data protection policy.	Exec Management, Compliance, risk department and permanent control

The CA Group CARS programme is designed to address specific Cyber Security challenges, the multi-year programme is deployed across the Group and is adapted as appropriate to each entity's specific needs. CACEIS shares in many of the Group initiatives, drawing from Group engineering, best practices, standards and solutions. Figure 1 illustrates the high-level components of the CARS programme.

Figure 2 Key themes addressed within CARS programme (courtesy of CA Group CARS)



CARS embodies Crédit Agricole's strategy for multiple lines of defence against attackers.

Beyond business culture, the CARS programme sets the tone from the top down with regards to risk appreciation and appetite.

CARS is a strategic priority for CACEIS and monitored by the Executive committee and Crédit Agricole Group via the CSG.

Data management initiatives aim to ensure safer access to sensitive Corporate data.

Building and operating security controls.

Monitoring and detecting insider behaviour.

The general 6 Executive Committee components: (a) Security strategy, (b) Policy and budget review, (c) Security leadership, (d) Incident response plan, (e) Ongoing assessment, (f) Internal education.

1.6 CACEIS Information Security Risk management

The Chief Risk Officer and the ISS-C Committee are accountable for oversight of CACEIS Information Risk, the IS risk assessment method, associated procedures and risk treatment. As such, the ISS-C evaluates the level of risk exposure and the resources (technical infrastructure, human resources and services) needed to keep the risk level below the maximum acceptable level of risk.

Information Security risk assessments are overseen by CACEIS Group CISO. The IS risk assessment methodology follows a systematic and pre-defined approach, minimizes the scope of human error, and emphasizes process driven, rather than human driven activities. This structured methodology contributes to achieving consistent results with the identification of threats and vulnerabilities with confidentiality, integrity and availability attributes. This internal CA Group risk assessment method and tools are established based on international best practices.

IS threats and vulnerabilities are assessed based on context, purpose, nature of information, external exposure (internet or clients), characteristics of technology, capacity required. Residual risks and proposed treatment plans are submitted to the ISS-C for final evaluation and approval. An IS risk register keeps track of the IS risks, the approved risk mitigation and treatment, and required controls.

Types of Information Security threat sources (see Figure 3) cover the following:

- Hostile cyber or physical attacks.
- Human errors of omission or commission.
- Structural failures of organization-controlled resources (e.g., hardware, software, and environmental controls).
- Natural and man-made disasters, accidents, and failures beyond the control of the organization.

Specifically concerning Information Security risk management, the following cyber-threats would adversely impact CACEIS ability to serve its customers:

- **Malware (Malicious Code)** —In 2018, external reports indicated that 20 new malware strains were introduced every second during certain periods. Malware has become one of the primary tools used by nefarious actors and organizations to perpetrate infections, data alteration, extortion, fraud, and other negative actions or events.

- **Ransomware**—The explosive growth of ransomware and its ever-increasing use has expanded the reach and pervasiveness of cybercriminals everywhere. The fact that variants and families of ransomware have increased from 4 just 3 years ago to more than 350 today shows the extent to which criminals perpetrate digital extortion across virtually every industry.

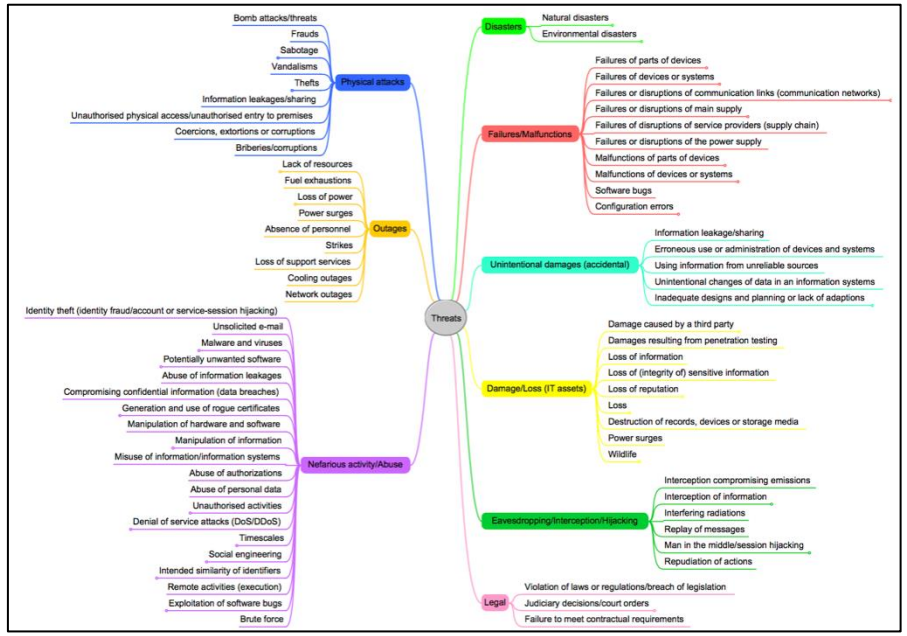


Figure 3 Threat taxonomy (courtesy ENISA)

- **Mobile**—With the advent of the mobile revolution, corporations, organizations, agencies and individuals have used mobile devices to conduct all kinds of business and personal transactions, including highly sensitive financial and personal data exchanges. As a result, the security perimeter of networks is often blurred or outright removed, thereby creating a multitude of security problems and issues around access, authentication and data manipulation.

- **Compromised access control (elevated privileges)**—Administrative/elevated privileges are consistently exploited across virtually every industry, and sometimes result in large data breaches, intelligence exfiltration of sensitive data and major disruption of services for clients and customers. Compromised accounts are still the single biggest cause (81%) of data breaches (Verizon 2018 data breach report).

- **Advanced persistent threat (APT)**—ISACA has defined APTs as parasitic threats across all industries. This problem is limited only by the threat actor's imagination as to methods and means of maintaining a presence on networks and conducting malicious activities in systems and processes for long periods of time.

- **Malicious insider**—Insider threat involves trusted personnel who perform negative activities with often catastrophic consequences for the organization or corporation that employs them. The reasons behind such acts are vast, wide and varied with no single predominate cause, which is why this threat is often considered the most dangerous of them all.

- **Cloud**—The advent of elastic, on-demand services in the cloud has dramatically increased the concerns and exposures for security and IT personnel everywhere in the world. The dynamic nature of the cloud and its currently active variable boundaries provide ever-changing perimeter and network connection issues for corporations. In cloud environments, always encrypt data—no matter where they are—to ensure confidentiality.

- **Third-party Service Providers** As technology becomes more specialized and complex, companies are relying more on outsourcers and vendors to support and maintain systems.

- **Denial of service attacks (DOS and DDOS)** — DDoS attacks typically flood online systems, such as internet banking sites or online trading platforms, with vast amounts of data in order to overload them and take services offline. DDoS attacks are the most common form of attack against financial services businesses, accounting for 32% of all attacks analysed in the report. And Arbor Networks' recent Worldwide Infrastructure Security Report found that 57% of financial institutions have experienced a DDoS attack – the highest of any sector.

- **Eavesdropping, Session interception and hijacking** —refers to a class of actions aiming to listen, interrupt, or seize control of a third-party communication without consent.

- **Code Injection and defacing**— Web defacement is typically done by hackers who break into a web server and replace the hosted website with one of their own, using techniques such as phishing, code injection, cross site scripting etc.

- **Identity usurpation and impersonation**— Generally, to cause harm or gain unfair advantage, identity impersonation occurs when someone uses information identifying another person without this person's authorisation.

Crédit Agricole Group have defined a number of **critical risk cases** that CACEIS apply to develop appropriate mitigating action plans, the following two are specifically related to corporate Cyber-Risks and address many of the threats enumerated above:

A/ IMPT: Massive unavailability of desktops,

B/ LUIS: Logical unavailability of Information systems,

Both scenarios are caused by either (a) unidentified malware attack, (b) an identifiable malware attack, (c) human intentional or accidental actions, or (d) a distributed denial of service (DDOS). They all lead to the Corporate information system being unavailable and potentially to a massive corruption of business data. The most difficult of these to detect are logical bombs.

The conclusions of the risk scenarios and actions plans are then presented to the ISS-C and Executive Committee for approval. The most recent update and action plan dates from 2019.

1.7 Protection against cyber-risks

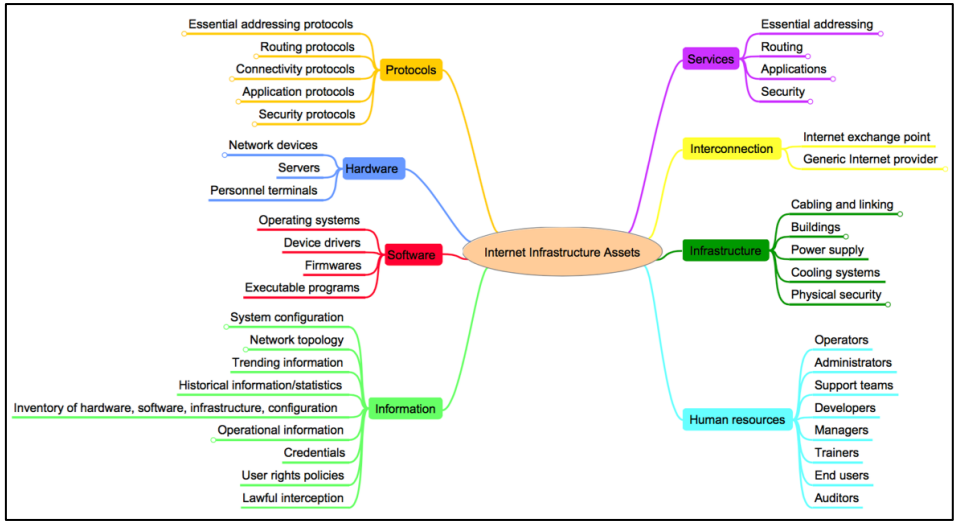


Figure 4 illustration of infrastructure assets (courtesy of ENISA)

As any financial sector company, we have recognised for a long time that we are the targets of cyber-attacks. Business lines are formerly responsible for defining their security risk profile and implementing the solutions needed. A Local ISC or delegate supports the Business units in applying the corporate methodologies.

Global shared infrastructure naturally integrates security, to which Business lines contribute financially according to a well-defined repartition grid.

Protection measures for information, applications and infrastructures are applied based on classification using the standard Information Security criteria:

- Confidentiality
- Integrity
- Availability

Corporate Policy II.2 defines Information classification to be applied.

Infrastructure as illustrated in Figure 4 is protected at different levels of the architecture and using many different means. Table 2 on the following page is a high-level summary of the principal protection measures used within CACEIS. It is aligned in the broadest sense with the Information Security IEC/ISO 27001:2013 control objectives and can be mapped with SANS and NIST frameworks.

Part of the mid-term Information Security action plan aims to progressively improve protection, detection and discovery measures, in particular the following are core to Cyber Security defences:

- Backup and restore solutions that implementing journaling that allows a roll back line by line,
- Addition of journaling functions at the application level for the batch jobs and the interactive operations,
- Vulnerability management, to minimise the exposure to threats and increase the availability of the platforms,
- Management of privileged access and accounts with improved audit logs and monitoring,
- Network security management, targeting the efficiency and effectiveness of the systems,
- The prevention against logic bombs relies also on the hardening of systems and the analysis of security events.

No	Risks	ype of Measur	Measures	Risks Process
1	Malware (malicious code)	technical	Malwares defences (Antivirus on workstation & Servers)	Malware
2	Ransomware	technical	Malwares defences (Sentinel One -End point solution) + Data recovery capability	Malware + backup/restore management
3	Mobile	technical	Secure configurations for hardware & software on mobile devices	Vulnerability management
4	Compromised access control (elevated privileges)	technical	Controlled use of administration priviliges	Privilege access right
5	Advanced persistent threat (APT)	technical	Maintenance, monitoring and analysis of audit logs, Analysis of events correlation and us	Security Incident management
6	Malicious insider	technical	inventory of authorised devices (NAC control)	Access to the network Malware
7	Cloud	organisational	Cloud methodology (Group CA). Risk Analysis and Confidentiality of Data is ensured thru ciphering of data at rest and in transit	Protection of sensitive data
8	Third Party Services provider	organisational Technical	Questionnaire on security everery 2 years.Audit of providers. Analysis of external audit reports (ISAE 3402, SSAE 16 type II)	Management of Provider
9	Denial of service attacks (DOS/DDOS)	technical	Account monitoring and control (SOC alert thru detection analysis, limitation of login attemps) Secure (long & complex) password and 2FA	Network security Password management
10	Eavesdropping, Session interception and hijacking	technical	Application software security Intrusion testing & External Vulnerability scans	Secure Development policy Vulnerability management
11	Code Injection and defacing	technical	Application software security Intrusion testing & External Vulnerability scans	Secure Development policy Vulnerability management
12	Identify usurpation and impersonation	technical	Application software security Intrusion testing & External Vulnerability scans	Secure Development policy Vulnerability management

Figure 5 Mapping between risks and protection measures

Table 2: Protection Measures deployed and maintained by CACEIS

Protection Measure	Description of measure
Inventory of authorised devices	A complete inventory of all authorised corporate equipment (servers, desktop, mobile, network equipment, …) is maintained within the CMDB.
Inventory of authorised software	Inventory of authorised corporate applications and software. SCCM is used for the desktop, CMDB is used for servers (SGBD, Applications).
Secure configurations for hardware and software on mobile devices, laptops, workstations, and servers	The configurations leverage the Crédit Agricole standards and best practices for desktops and the policies are available. Air watch is used to control mobile devices. A secure hardening guide describes servers. Laptops are encrypted.
Continuous vulnerability assessment and remediation	QUALYS is used to regularly perform scans of the network and identify the equipment attached, the software in use and any vulnerability. The resulting high-priority items are identified, and remediation action plans assigned. Skybox (threat intelligence solution) is used to evaluate and analyse the risk level in order to prior the action of technical teams
Malware defences	Malware defences are deployed on servers, desktops, and strategic ingress points to provide monitoring, protection, and quarantining against known malware. These systems are auto updated, monitored by the ITSO, and reporting performed to the ISS-C.
Application software security	Each application is subject to risk assessments that map the appropriate security controls and security measures (C.I.A). Application software is subject to internal SECAPI architecture and development standard, is maintained, tested and reviewed prior to Change Control permitting promotion to production environments.
Wireless access control	Based on Crédit Agricole standards and best practices. Corporate access requires a corporate certificate on the machine to be authenticated.
Data Recovery capability	Data recovery is structured around the Backup Policy that defines the standards and practices for recovery All systems and data are saved daily and maintained securely. Restoration tests are performed regularly.

Protection Measure	Description of measure
Secure configurations for network devices such as firewalls, routers and switches	These follow the Corporate Crédit Agricole design and standards provide by CANOES. Operational management is outsourced to either CA GIP (for desktop services) or DXC (for data centres). Skybox is used for network equipment.
Limitation and control of network ports, protocols and services	Firewalls, IDS, IPS and WAF are implemented. A CAB dedicated to network flows, protocols and services. Skybox is used to monitor the compliance with the agreed technical policies.
Controlled use of administrative privileges	All administrative and privileged access to data centre and network systems are closely monitored and logged through a dedicated tool. Active Directory administrator accounts are subject to review and limited. Desktop privileges are subject to authorisation and reviewed yearly.
Boundary defence	Internet and remote access connectivity is designed, monitored and supervised by Crédit Agricole (CA). The CA CERT monitor 24x7. CACEIS apply CA standard ING 08v2 to the data centre Internet access for applications.
Maintenance, monitoring and analysis of audit logs	All the activity is logged and collected, however a SIEM solution is being designed to improve efficiency. A SOC has been recently selected and is being deployed.
Controlled access based on the need to know	A corporate identity management system to manage and provision access and attribution of rights based on business profiles. This follows the internal Access Control policy and Procedure. Regular reviews and reconciliation are performed to ensure access is on a need to know basis.
Account monitoring and control	Active directory accounts are monitored. Failed attempts are identified and acted upon by the SOC based on CA rules and policy.

1.8 Detection of Cyber attacks

As part of Crédit Agricole Group, CACEIS benefits from the Crédit Agricole Security Operations Centre (SOC). The SOC is a fully qualified CERT (Computer Emergency Response Team), a certification and recognition delivered by Carnegie Mellon University. The team actively participates in, and receives regular information about incidents, vulnerability analysis, network situational awareness, and digital intelligence including information from Europol, state authorities, national security institutions, and other qualified CERTs.

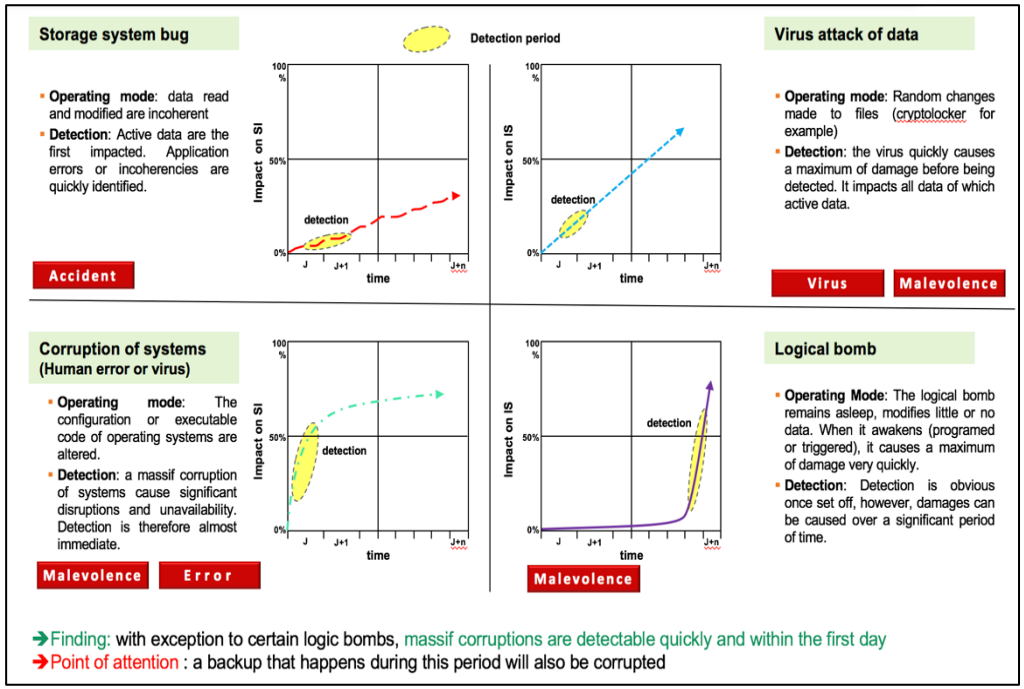


Figure 6: overview of major cyber threats

Firewalls, IDS, IPS, Air watch, Malware, Varonis, Skybox, are tools implemented by CACEIS to detect cyberattacks. The SOC monitors and responds to alerts identified through these tools.

CACEIS and CA performs regular penetration tests and reviews on their critical infrastructure, which confirms the strength, the performance and water tightness of the security systems in place. There are mainly two key findings from such tests (a) that, although global tightness is correct, it is sometimes necessary to improve the partitioning of system users, and (b) we regret that many software products available on the market place, for which we do not master the development, carry vulnerabilities that demand special security correctives.

Known threats and attacks are identified and managed through the internal security teams (including SOCs), and the CERT, leveraging the industry best practices and the processes in place within CA. However, as within any organisation, identifying “unknown” attacks are an on-going challenge.

To this end, information is shared with internal and external partners to ensure as early detection as is possible.
The CARS Programme is driving the implementation of additional tools such as SIEM to improve the efficiency of the implemented measures.

1.9 Response to Cyber attacks

Regardless of the attack CACEIS and Crédit Agricole maintain a strict crisis management process, best practices that contribute to efficient and effective response. Regardless of the nature of the incident CACEIS Group will coordinate and communicate through the Crisis management function and work to stop propagation as quickly as possible.

The response plan is a critical element of the crisis management strategy—not because it provides a prescriptive, detailed list of action items, but because it has been refined and practiced through table top drills. The CARS program structures the roles and responsibilities, the organisation and activities for Cyber-attack response within the CA Group:

- Identify the internal incident response team,
- Identify who will lead the incident response team,
- Categorization of the incident,
- Response protocol. Provide a flexible frame- work for executing the eight key steps of incident response: (1) preparation, (2) identification, (3) assessment, (4) communication, (5) containment, (6) eradication, (7) recovery, and (8) post-incident,
- Third parties. Identify key third parties that will assist the company, including external privacy counsel, forensics, crisis communications, mail and call centre.

Once compromises have been detected and verified, CACEIS Crisis management assembles cross-functional response teams to act quickly, to investigate and remediate the breach while preserving all electronic evidence. Ascertaining what data were lost, destroyed, or stolen is paramount to enable CACEIS to determine risk exposure and potential liability.

Disaster recovery plans are tested and retested to ensure that all systems and management processes are operational and actualised. Performed at least yearly, the Business Continuity Management team reports to the ISS-C, and tracks the results of tests, and the lessons learned.

Rapid Rebuild: The ability to restore and resynchronise massively within a very short time frame (several hours) is part of the Information systems data architecture and one of the key means of response to a LUIS scenario.

Logic Bombs: The possible corruption operated during the sleep phase of the logic bomb is not massive. We can suppose that this is bearable because often go undetected by modern protection mechanisms. After the activation of a logic bomb, a rapid restore would allow to return to the stable situation that existed prior to activation.

1.10 Recovering from Cyber attacks

Steps to return to normal operations and limit damage to the organization and its stakeholders continue after the incident or crisis. Post-event steps include assessments of the causes and of the management of the incident or crisis, and promulgation of lessons learned

Lessons learned—containment and eradication

- Investigate incident more thoroughly;
- Report incident to relevant stakeholders;
- Carry out a post incident review;
- Communicate and build on lessons learned;
- Update key information, controls and processes;
- Perform trend analysis.

Recovering from Cyberattacks is part of CACEIS business continuity planning, under the control of head of BCP, the management of security incidents and cyber crisis management comply with the policies and procedures of the CA Group.

2 Appendix

Internal References

CACEIS Information Security Policy

Crédit Agricole Personnel data charter

External References

CACEIS Web site
http://www.caceis.com/fr/media-room/actualites/a-la-une/article/gdpr-caceis-is-committed-to-data-protection/detail.html

The International Organization for Standardization (ISO), the information security series,
http://www.iso.org/iso/home/search.htm?qt=information+security&published=on&active_tab=standards&sort_by=rel

National Institute of Standards and Technology (NIST) Special Publication 800 (SP-800) series and Federal Information Processing Standards (FIPS),
http://csrc.nist.gov/publications/index.html

European Data protection Rules for the protection of personal data inside and outside the EU.
https://ec.europa.eu/info/law/law-topic/data-protection_en

French Data Protection Authority "CNIL"
https://www.cnil.fr/fr/comprendre-le-reglement-europeen

European Banking Authority (EBA) Final Report on EBA Guidelines on outsourcing arrangement (EBA/GL/2019/02 - 25 February 2019)
https://eba.europa.eu/documents/10180/2551996/EBA+revised+Guidelines+on+outsourcing+arrangements

European Banking Authority (EBA) Recommendations on Cloud Outsourcing and the forthcoming Guidelines on Outsourcing Arrangements (London, 17 October 2018)
https://eba.europa.eu/documents/10180/2422294/Session+4+-+NY+and+DB+-+EBA+Recs+on+cloud+and+Outsourcing+GLs+-+17+Oct+18.pdf

National Institute of Standards and Technology (NIST) Special Publication 600-145 "The NIST Definition of Cloud Computing"
https://csrc.nist.gov/publications/detail/sp/800-145/final

ACRP – "The risks associated with cloud computing"
https://acpr.banque-france.fr/sites/default/files/201307-risques-associes-au-cloud-computing.pdf