CREDIT SUISSE

Global Statement of Information Security 2023

Chief Security Office (CSO)
CISO

Table of contents

Introduction

At Credit Suisse, data confidentiality, data integrity, and system availability are cornerstones of our business. The protection of information and systems is paramount and therefore we continually monitor adherence to industry standards relating to people, process, data, and technology. Ensuring the security of our clients' information is a top priority.

Consistent with industry standards such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework, the International Organization for Standardization ("ISO/IEC") 27002 and the Control Objectives for Information and related Technology ("COBIT"), Credit Suisse's Information Security Program leverages administrative, technical, and physical safeguards to protect the confidentiality, integrity, and availability of information.

Such safeguards are designed to:

- Provide for the security and confidentiality of client, business proprietary, and personal information
- Protect against anticipated threats to the security or integrity of such information
- Protect against unauthorized access or use of information that could result in material harm to any client

Credit Suisse Information Security is aligned to the five NIST Cybersecurity Framework Functions — Identify, Protect, Detect, Respond and Recover. When considered together, these Functions provide a high-level, strategic view of the life cycle of an organization's management of cybersecurity risk.

Information Security Governance

Policy and Standards	Credit Suisse's information security framework of policies and standards aligns to the NIST Cybersecurity Framework, Security and Privacy Controls for Information Systems and Organizations (NIST 800-53) and the International Organization for Standardization ("ISO/IEC") 27002. Credit Suisse has a Global Information Security Policy mandating global information security controls across the organization. Policies and standards cover, but are not limited to information security at Credit Suisse. Policies and standards establish individual controls for user access management (including access control and passwords), privileged access management, change management, security incidents, data protection, handling and destruction, and other security measures.
Policy Review and Refresh	The Information Security at Credit Suisse policy is reviewed at least annually and updated to reflect regulatory or procedural changes affecting information security. Senior management review and approve major policy updates.
Policy Implementation	The Information Security at Credit Suisse Policy is internally available to all personnel on the corporate intranet. Controls are enforced by the first line of defense, and are subject to independent governance, including second line of defense. All Credit Suisse personnel are responsible for compliance and for reporting information security incidents that they become aware of. Governance bodies are in place for escalation of risks to the appropriate level. Credit Suisse requires all personnel to sign and submit an annual acknowledgment of their understanding of the Information Security at Credit Suisse Policy. Procedures are in place for reporting unauthorized non-compliance to the appropriate level of management or committees (non-compliance may lead to disciplinary action up to and including termination of employment).
Personnel	Credit Suisse has a global team dedicated to information security, as well as divisional CISOs responsible for specific divisions and legal entities. Staffing is comprised of experienced, certified information security professionals. A Credit Suisse Cyber Security Incident Response Team (CSIRT) is in place to investigate security incidents. In addition, a 24/7 Security Operations Center (SOC) is in place to detect and respond to suspected security events.
Escalation	Credit Suisse has a formal incident response process, which includes reporting and escalation to the appropriate management teams and committees. Where appropriate, information is escalated to relevant law enforcement, regulators, and impacted clients.
IT Risk Governance Services	Credit Suisse has a dedicated team to perform IT Risk governance services, such as governance committee reporting and metrics, regulatory and external audit management, policy oversight, threat landscape monitoring, IT controls catalog maintenance and client interactions. Risks are reported through a standardized process and are escalated, as appropriate, to senior management.
Three Lines of Defense	Credit Suisse has adopted a Three Lines of Defense model for its Information Security Program. The three lines are: 1) Business, IT and CISO Organisations; 2) Cyber & Technology Risk; 3) Internal Audit.
Management	Credit Suisse has a Chief Information Security Officer (CISO) responsible for overall information security. The CISO sets the strategic information security direction for Credit Suisse, such as the security requirements based on threat landscape, review control effectiveness and management of residual risk. Management committees, including the Board of Directors, are provided with cyber and information reporting on a periodic basis.

Identify

The “Identify” Function of the NIST Cyber Security Framework assists in developing an organizational understanding to managing cybersecurity risk to systems, people, assets, data, and capabilities. This includes: Asset Management, Risk Assessments, Business Environment and Governance and Risk Management Strategy.

Asset Management	Credit Suisse maintains a global IT Asset inventory. IT resources are categorized based on their criticality, assessed in terms of Confidentiality, Integrity and Availability according to Business Impact Analysis model.
IT Risk Assessments	Credit Suisse has a dedicated team to perform Cyber and IT risk assessments for platforms and applications. IT risk assessments are initiated as a part of Credit Suisse standard processes for new applications periodically based on criticality of assets and through changes to applications. Criticality of applications is assessed in terms of Confidentiality, Integrity and Availability. A risk-based approach has been defined to consider risk across the whole environment while maintaining focus on those IT asset classes considered most critical.
Threat Intelligence	Credit Suisse has a cyber-threat intelligence service which collects and analyzes information from both internal and external sources and disseminates actionable intelligence to enable the Bank to plan proactively for emerging threats and take further action against cyber threats if required.
Risk Management Strategy	Credit Suisse’s Risk Management Strategy is designed to achieve an optimized end-to-end security and risk competence that enables a secure and innovative business environment, aligned with the bank’s risk appetite in order to protect the bank’s clients and assets from cyber and information threats using a risk-based approach and involving people, process, and technology across Credit Suisse.
Third-Party IT Risk Assessments	As part of risk assessments performed on third parties, we ensure that any sub-contractors used as part of services provided to Credit Suisse, undergo a due diligence including periodic assessments on their information security controls, including their governance risk and compliance program and their capabilities to provide a reliable continuity of services. As appropriate, we assess the controls that our third parties have in place to ensure the security of their third parties security posture is commensurate to our own.
Other Third-Party Assessments	Third parties also undergo assessments by other departments within Credit Suisse, depending on the risk exposure, i.e., Legal, Compliance and/or Business Continuity Management.
Subcontractors	Third party information security controls, including oversight of their third parties (i.e., subcontractors), are expected to be consistent with Credit Suisse requirements and policies.

Protect

The “Protect” Function of the NIST Cyber Security Framework outlines appropriate safeguards to ensure delivery of critical infrastructure services. This includes Access Control, Awareness and Training, Data Security, Information Protection Processes and Procedures, Maintenance, and Protective Technology

Personnel Training	All personnel, including contingent workers, receive mandatory annual trainings on information security policies and procedures and must pass a post-course assessment. An ongoing information security awareness program is also in place to inform personnel of policy updates and application of policies to the workplace. Awareness initiatives include newsletters, speaker series, cybersecurity table-tops, supplementary personal and professional cyber awareness training, and phishing simulation exercises.
Training of Information Security Personnel	Information security professionals within Credit Suisse regularly engage with industry organizations to stay up to date on emerging threats and technologies. Many information security personnel maintain relevant information security certifications, such as Certified Information Systems Security Professional (CISSP) and Certified Information Security Manager (CISM).
Training of Third Parties	Third Parties contractors/consultants with access to Credit Suisse networks receive mandatory annual training on information security policies and procedures. An ongoing information security awareness program is also in place to inform personnel of policy updates and application of policies to the workplace.
Access Management	Credit Suisse provides centralised access management provisioning and governance services that support the principles of least privilege (need-to-know, need-to-have) and segregation of duties. Credit Suisse has systems in place to continuously manage IT entitlements for users and IT Assets. Recertification of access and entitlement rights occurs periodically and requires approval of access for an individual to an application and related data subject to the principal of least privilege. Temporary and emergency processes for access to production systems have been established, including temporary privileged access and/or “Breakglass”. These services and processes are designed to provide an auditable and consistent approach to access management.
Employee Data Access After Termination	Credit Suisse has a fully automated termination process which is automatically triggered when HR Access management is notified of a leaver and it ensures that all access of that user is removed in a timely manner with no residual access to Credit Suisse systems or confidential information whichever its nature.
Remote Access	Procedures are in place to manage secure delivery of remote access. Controls are in place to prevent users copying any Credit Suisse data to personal devices when using remote connectivity. Both direct and remote access to Credit Suisse internal systems requires two-factor authentication leveraging end-user credentials and an asset assigned to the user. Remote access to Credit Suisse internal systems requires two-factor authentication leveraging end-user credentials and an asset assigned to the user. Corporate managed devices for remote access require the Credit Suisse standard VPN client whilst employee personal devices require installation of an approved software suite to enable remote access.
Token Management	Where tokens are in use there are controls in place that are designed to manage and track the use of connected hardware to authentication tokens.
Database Security	Controls are in place that are designed that database administrators receive proper authorization to access data, particularly sensitive data such as Client Identifying Data (CID).
Physical Controls	Credit Suisse policies, including the Global Information Security Policy, outline requirements for the protection and monitoring of every Credit Suisse physical site. Basic controls include: key card access, video surveillance, and security guards.
Data Center Security	Data center entry and exit procedures are in place, and access control is managed under the principles of least privilege. Both on-site and off-site surveillance is maintained 24x7. A periodic review of access rights for restricted areas is undertaken by authorized individuals in order to ensure that appropriate levels of access are maintained. Authorizers are responsible for reviewing the accuracy of the report's content and for the deletion or addition of access rights as appropriate.
Clear Desk / Screen	Personnel must keep their workstations secure, clear of any non-public information, have password protection and remove their Smart Card while they are away from their workstations.
Guest Access	Guests to Credit Suisse locations are required to provide appropriate identification and must be escorted by Credit Suisse personnel at all times.

Principle of Least Privilege	Access to confidential data is granted on a need-to-know/need-to-have basis, as necessary for business functions. For IT personnel that need to have access to sensitive information to support a business area, this access is kept at a minimum using temporary privileged access and/or is monitored. Access rights are reviewed and approved or revoked on a periodic basis.
Network Environment	Credit Suisse hosts and controls its own network environment. We have multitier network architecture through a combination of packet filters, application-level firewalls, and other network layer security controls. Firewalls, intrusion detection and prevention systems, network filters for websites, (e.g. for vulnerabilities, websites and data), endpoint protection at the network, server and workstation level, amongst other controls are in place. A dedicated Network Operations Center (NOC) performs regular network monitoring and operations, and a dedicated Security Operations Center (SOC) manages network security aspects where the findings are analyzed and remediated in a timely manner.
Two-Factor Authentication	Both direct and remote access to Credit Suisse internal systems requires two-factor authentication leveraging end-user credentials and an asset assigned to the user.
Capacity Management	Credit Suisse performs periodic capacity testing and monitors system utilization.
Scheduled Downtime	Credit Suisse has implemented regularly scheduled system downtime to perform critical updates and maintenance.
Maintenance Notification	Credit Suisse provides advance notification to all affected business units prior to performing major system maintenance.
Quality Assurance	Credit Suisse performs tests before applying major system updates or security patches. Plans are put in place to reverse failed or problematic upgrades.
Data Leakage Prevention	Credit Suisse has implemented a diverse set of layered controls (technical, physical, and administrative) designed to restrict information leakage. Credit Suisse policies define requirements for information handling including classification and ownership, access control requirements based on the need-to-know principle, and acceptable use of systems. Technical controls include but are not limited to: data leakage prevention systems, information rights management, website, and email content control systems, restricted and strictly controlled operating systems, application environments and hardware controls such as removable storage blocking and remote printing prevention. Information rights management tools enable the enforcement of classification of documents through warning and blocking mechanisms when emails are sent externally, and for encrypting attachments. Monitoring procedures are in place for the surveillance of email communications.
System Management	Credit Suisse has implemented a System Development Life Cycle (SDLC) for developing and managing Credit Suisse information systems, ensuring that information security principles and controls are implemented, tested, and cannot be circumvented throughout the lifecycle. A baseline configuration is developed and maintained for all information systems, and controls for ensuring adherence to baseline configurations are established and managed. The systems are configured to provide only essential capabilities and functionality.
Change Management Process	Credit Suisse maintains an IT Change Management Policy that defines the overall requirements for the management of changes to IT systems and applications. IT Risk assessments are embedded and triggered during the SDLC process. Program, configuration, and scheduling changes to applications are approved by management prior to implementation.
Software Integrity	Controls are in place designed to ensure software integrity of applications.
Source Code Management	Credit Suisse maintains source code repositories to manage versioning.
Development Environment	The development and testing environment(s) are separate from the production environment.
Testing	Procedures are in place to test changes and updates to production systems before going live.
Change Approval	Program, configuration, and scheduling changes to applications are approved by management prior to implementation.
Distributed Denial of Service (DDoS) Attacks	Credit Suisse has controls on multiple layers designed to detect and mitigate against DDoS attacks, including traffic redirection.
Malware Prevention	Anti-virus and anti-malware software are installed where technically feasible and at multiple layers of the Credit Suisse network.

Vulnerability Management	Patches and updates for software, servers, and operating systems are tested and implemented on a regular basis. The timeframe for the implementation depends on the criticality of the patch, with critical patches implemented as soon as reasonably possible.
Data Security & Encryption	Credit Suisse uses industry-standard encryption methods and requires that confidential data is protected in transit and at rest (including back-ups).
Cloud Computing	Cloud computing may be utilized for specific, defined business functions where approved by senior management and as permitted by applicable laws and regulations. Cloud activities are subject to the same risk assessment processes and risk management standards as other technologies at Credit Suisse.
Web Blocking	Web email, Internet chat, data upload/download from untrusted sites, social media, and other potentially malicious sites are controlled and restricted in their use to prevent data leakage and malware intrusion.
Information Sharing	Credit Suisse engages with a variety of information-sharing public- and private-sector bodies, including Financial Services Information Sharing and Analysis Center (FS-ISAC), to remain aware of emerging threats and technologies.
System Maintenance Process	Credit Suisse has a formalized, documented system maintenance process designed to manage consistency across Credit Suisse. Remote maintenance of organizational assets is approved, logged, and performed in a manner intended to prevent unauthorized access.
Log Monitoring	Credit Suisse policy defines the minimum requirements for company-wide computer systems logging. Relevant information pertaining to security-related events must be securely logged and retained. Event logs are required to contain sufficient detail to support incident investigation including failed login attempts. Security relevant log sources are continually monitored by the dedicated Security Operations Center (SOC), with a 24/7 team to analyze and escalate events requiring further investigation (e.g., events that indicate a potential intrusion) to the Cyber Security Incident Response team (CSIRT) for review and action.
Password Management	Credit Suisse enforces industry-standard strong and complex password standards. Minimum character lengths are in place and passwords must include non-repeating alphabetic, numeric, and include special characters where feasible. Additionally, they must be non-trivial (e.g., non-dictionary word). Standard password-only authentication systems have a maximum change period of no longer than 91 days, with other non-standard accounts (e.g., administrator and emergency) requiring changes more frequently. Login credentials (user ID and password) are encrypted during network transit. Sharing of user credentials is prohibited.
Removable Media	Credit Suisse restricts the usage of removable media. Technical controls have been implemented to prevent read/write access to USB storage devices on end-user machines. Exceptions are granted, when there is a demonstrated business need, with a four-eyes review principle for approvals in place. Encryption policies have been implemented on offsite storage media with appropriate physical security measures.
Mobile Devices	Credit Suisse issued laptops are equipped with Credit Suisse standard security controls, including two-factor authentication and encryption of hard drives. Credit Suisse utilizes managed, encrypted, containerized mobile solutions. Procedures are in place designed to prevent data leakage in the case of a lost device.
Bring Your Own Devices (BYOD)	Credit Suisse offers a number of remote access solutions tailored to support hybrid/flexible working models for employees and service providers. In addition to corporate managed devices, Credit Suisse supports BYOD solutions that offer the most flexibility for our staff. Regardless of the remote access solution used, security and protecting customer and corporate data is paramount to Credit Suisse and is the first and foremost principle. Credit Suisse implements and enforces a comprehensive set of industry standard data security and DLP controls on all remote access solutions, including encryption on both corporate and BYOD as well the data itself.
Physical Disposal of Assets	Media containing non-public information is securely disposed of based on approved procedures when no longer needed or defective and non-reparable. Additional technical controls designed to ensure and evidence the integrity of the stored records over their entire retention period is implemented where the information stored qualifies as business records.
Background Checks	Credit Suisse conducts background screening for all regular, full, or part-time new hires. Credit Suisse conducts background screening (e.g., criminal, sanctions screening, depending on local regulation) on employees as part of new hire due diligence. Vendors supplying contingent workers to provide services to Credit Suisse and who have access to Credit Suisse premises, systems, or assets are contractually required to ensure the required background screenings (e.g., education, etc.) occur.
Sanctions Screening (U.S. Only)	Post-engagement, Credit Suisse performs weekly sanctions screening on personnel in the United States.
Security Clearances (U.S. Only)	Members of the Cyber Security Operations Services in the United States team have private sector “Secret” security clearance sponsored through the U.S. Department of Homeland Security.

Detect

The “Detect” function of the NIST Cyber Security Framework defines the appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables timely discovery of cybersecurity events. This includes such categories as Anomalies and Events, Security Continuous Monitoring, and Detection Processes.

Baseline Configuration	Credit Suisse has a Solutions Delivery Framework designed to manage correct implementation of new systems and major changes to existing systems. This is supported by standard baseline system configurations which are monitored and maintained. Baseline configurations are documented, formally reviewed and agreed-upon sets of specifications for systems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, and/or changes to systems. Baseline configurations include information about system components, network topology, and the logical placement of those components within the system architecture. Maintaining baseline configurations requires creating new baselines as organizational systems change over time. Regular baseline compliance scans are to identify noncompliance to agreed baseline configurations and are performed using appropriately configured and Credit Suisse approved tools.
Intrusion Detection/ Prevention	Credit Suisse has industry-standard IDS/IPS systems installed throughout the enterprise to identify, log, and alert on and block known attacks.
Detection Processes	Credit Suisse monitors for unauthorized devices and software. Detection processes are tested. Credit Suisse employs an in-depth defense strategy with a number of technical controls supported by comprehensive processes designed to detect and prevent unauthorised activity. These controls undergo regular reviews and testing designed to monitor continued coverage and continued effectiveness.
Vulnerability Scanning	Regular vulnerability scans to identify patching levels and those components with vulnerabilities are performed using appropriately configured and Credit Suisse approved tools. Scheduling of vulnerability scans is performed outside of business hours (to reduce the likelihood of system outage) and the frequency is based on the location of the assets within the Credit Suisse network. Additional ad hoc vulnerability scans may be requested by the business to determine the extent of new top severity rated vulnerabilities or to confirm status of existing vulnerabilities.
Penetration Testing	Periodic, controlled penetration testing is performed on internet-facing applications by selected independent third parties, and findings are reviewed and addressed to mitigate associated risks. An internal application security testing program is in place to run similar tests on selected internal applications.
Video Surveillance	Credit Suisse records and maintains images in accordance with local laws and connects digital video recorders (DVRs) or other recording media to the Credit Suisse centrally managed system whenever possible. In some offices with specific client zones, CCTV operational use may be limited by time in order to comply with client identity protection requirements.
Building & Keycard Access	All Credit Suisse facilities require access with a Credit Suisse ID card or Keycard access. Credit Suisse maintains records of Credit Suisse ID Card and Keycard use.
Guest Access	Guests to Credit Suisse locations are required to provide appropriate identification and must be escorted by Credit Suisse personnel at all times.

Respond and Recover

In the event of a Cybersecurity incident, Credit Suisse follows its Cyber Security Incident Response Plan which supports its Business Continuity Management's standard, IT and Global Incident Management processes. The threat will be addressed via established escalation procedures, roles, responsibilities, and communication.

Incident Simulation Exercises	Credit Suisse participates in internally organized and performed, and externally organized (regulatory, exchanges and industry bodies) exercises to test the effectiveness of its incident response program and communication procedures with external parties
Backups	Full backups are performed prior to major system updates or security patches, as well on a nightly/weekly basis depending on information requirements. Backups are encrypted and stored at an alternative secure off-site facility.

Compliance and Audit

Regulatory Compliance	As a global financial services company, Credit Suisse's information security controls are reviewed by government agencies and self-regulatory organizations, which include but are not limited to: the Swiss Financial Market Supervisory Authority, and the Financial Institution Regulatory Authority, the Federal Reserve Bank of New York, the Securities and Exchange Commission, the Prudential Regulation Authority, the Monetary Authority of Singapore, the Securities and Futures Commission of Hong Kong, and Hong Kong Monetary Authority and Sarbanes-Oxley Certificate.
Internal Audit	Internal Audit's Audit Plan is created on the basis of a solid risk assessment framework where the Group's global system of internal controls and governance processes are assessed. As a result, Credit Suisse's internal auditors assess the effectiveness of the information security program on a periodic basis.
External Audit	Credit Suisse engages external auditors to assess the effectiveness of the information security program as part of both recurring regulatory audits and focused cyber security assessments.
Internal Controls Testing	IT has standard processes and methods in place providing control assurance during development and for operational assets. Additionally, IT Assets are regularly assessed on an agreed frequency basis, depending on the criticality of the assets. Numerous independent assessments are done by the SOX group, Internal Audit, regulators, and other external, independent auditors.

Miscellaneous

Insurance	Credit Suisse maintains cybersecurity insurance structured to mitigate financial loss associated with information security incidents.
Electronic Fraud	Credit Suisse takes measures to protect the integrity of client transactional information. These measures include authentication mechanisms and systems for the purpose of preventing, detecting, and responding to fraudulent activities.
Client Data Protection	Credit Suisse classifies Client data as confidential. Credit Suisse has controls in place designed to ensure that Client Identifying Data (CID) are available or disclosed to authorized individuals and through secure systems and services only.
Privacy	Credit Suisse is committed to maintaining the confidentiality of current, former, and prospective customers in accordance with applicable laws and regulations. One of the regulations is General Data Protection Regulation (GDPR) on data protection and privacy for all individual citizens of the European Union (EU) and the European Economic Area (EEA). Credit Suisse recognizes that customers may entrust important personal information and Credit Suisse has implemented technical and organizational measures to secure personal data per applicable laws and regulations
Know Your Customer (KYC)/Anti-Money Laundering (AML)	Credit Suisse has internal Know Your Customer (KYC) and Anti-Money Laundering (AML) processes that are in compliance with applicable AML laws and regulations.
Recordkeeping	The Records and Information Management (RIM) department within Credit Suisse manages services to support the businesses in order to comply with Credit Suisse Records Management Policies. RIM Compliance develops and maintains policies and a retention schedule with different record categories to manage related risks, apply adequate levels of control, and meet business needs as well as regulatory requirements, in collaboration with General Counsel.
Business Continuity Management	Credit Suisse maintains a separate Business Continuity Management Overview letter, which can be provided upon request.

Glossary

AML	Anti-Money Laundering
BAU	Business as Usual
CID	Client-Identifying Information
CISO	Chief Information Security Office
DLP	Data Leakage Prevention
FS-ISAC	Financial Services Information Sharing and Analysis Center
NOC	Network Operation Center
RIM	Records and Information Management
SDLC	Systems Development Lifecycle
SOC	Security Operations Center
VPN	Virtual Private Network

Credit Suisse Services AG
One Cabot Square
London E14 4QJ
credit-suisse.com