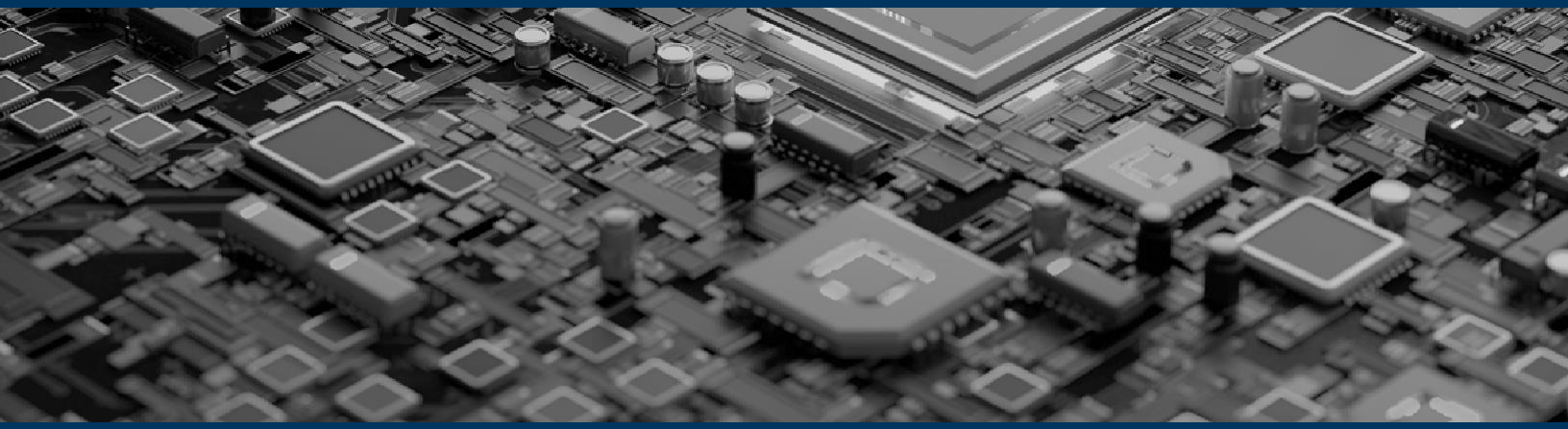
Goldman Sachs



CLIENT SECURITY STATEMENT

Version 10.0 | June 2023

Table of Contents

Introduction

Introduction

Goldman Sachs places great importance on information security, including cybersecurity, to protect against external threats and malicious insiders. The firm's cybersecurity strategy prioritizes detection, analysis and response to known, anticipated or unexpected cyber threats, effective management of cyber risks, and resilience against cyber incidents. The firm continuously strives to meet or exceed the industry's information security best practices and applies controls to protect our clients and the firm. Goldman Sachs maintains a formal cybersecurity program structured around the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and the related Cyber Risk Institute Profile.

This document provides an overview of the firm's approach to information security and cybersecurity, and its practices to secure data, systems and services, which align to the five functions of the NIST CSF: Identify, Protect, Detect, Respond and Recover.

While information security and cybersecurity measures will naturally change over time and may differ across the range of Goldman Sachs' services, this document provides an overview of our security practices. Goldman Sachs does not represent that this document will be appropriate or adequate for your intended purposes.

Please contact your Goldman Sachs representative if you have any additional questions.

IDENTIFY

Risk Governance and Oversight

Risk Governance Framework

The firm employs a risk governance model comprising three lines of defense that promote accountability, oversight and assurance. As the first line of defense, the firmwide Information Security and Cybersecurity Program, administered by Technology Risk and overseen by the Chief Information Security Officer (CISO), establishes information security standards and sets clear expectations for the firm's adherence. The Risk and Compliance Divisions provide independent oversight and challenge functions of the Program as the second line of defense. Finally, the firm's Internal Audit independently evaluates the firm's control environment, as the third line of defense.

Each of the firm's divisions is ultimately accountable for managing technology risks affecting their applications and other information system assets.

Governance Committees

In support of the risk governance framework, the firm has established an overarching committee structure to oversee and hold senior management accountable for implementing the firm's cybersecurity risk management strategy and framework. The committee structure enables formal escalation and reporting of risks to the firm.

The firm's risk committees are globally responsible for the ongoing approval and monitoring of frameworks, policies, and limits which govern the firm's risk management program, including:

- The Risk Committee of the Board of Directors provides oversight of the firm's risk management framework, overseeing and reviewing the firm's risk management practices, as well as establishing the firm's risk tolerance through limits and thresholds, including those relating to operational and information security risks.

- The Audit Committee of the Board of Directors oversees the performance of the firm's internal and external audit functions and the firm's compliance function, including as it relates to information security.

- The Enterprise Risk Committee is responsible for exercising oversight of the firm's financial and non-financial risks (including, but not limited to, the firm's top risks, new risks, and emerging risks). This Committee is co-chaired by the firm's President and Co-Chief Operating Officer and Chief Risk Officer.

- The Firmwide Operational Risk and Resilience Committee is globally responsible for overseeing operational risks and ensuring the business and operational resilience of the firm. This Committee is co-chaired by the firm's Chief Administrative Officer and the head of Operational Risk.

- The Firmwide Technology Risk Committee (FTRC) reviews matters related to the design, development, deployment, and use of technology. This committee oversees cybersecurity matters as well as technology risk management frameworks and methodologies, and monitors their effectiveness. This Committee is chaired by the firm's Chief Technology Officer.

- The Engineering Risk Steering Group (EngRSG) is a subordinate group under the FTRC, with the mandate to oversee Engineering risk decisions, monitor control performance, review approaches to comply with current and emerging regulation applicable to the Engineering organization, and drive key firmwide priorities in support of the Program. The Chief Information Security Officer (CISO) serves on the FTRC and chairs the EngRSG.

IDENTIFY

Risk Governance and Oversight

Information Security and Cybersecurity Program

The firm maintains an Information Security and Cybersecurity Program (the "Program"), which is centrally managed by Technology Risk. The Program identifies and documents threats, establishes information security mandates, evaluates compliance to these mandates, and detects and responds to security incidents. In addition, the Program consists of security teams embedded within each of the firm's operating divisions that adopt and apply the firm's security control framework. The Program is frequently adjusted to ensure ongoing suitability.

The firm's CISO is responsible for managing and implementing the Program and reports directly to the Chief Information Officer. In addition, the CISO sets firmwide control requirements, assesses adherence to controls, identifies and prioritizes cybersecurity risks, and oversees incident detection and response.

The CISO reports at least annually to the Board of Directors ("Board"), or one of its committees, concerning the overall status of the Program. The written Program is approved by the firm's Board of Directors annually. The Board takes an active interest in information security and cybersecurity matters and sets the firm's risk appetite in these areas, monitors progress, and receives regular updates.

As part of the firm's second line of defense, a dedicated Operational Risk team within the Risk Division provides independent oversight and challenge of the Information Security and Cybersecurity Program and assesses the operating effectiveness of the program against industry standard frameworks and Board Risk Appetite-approved limits and thresholds. In addition, Operational Risk establishes and maintains a firmwide business continuity program to reasonably ensure that technology assets supporting the firm's essential functions can continue to operate in the event of a disruption.

Risk Assessments

Goldman Sachs recognizes the importance of effective risk management, particularly in relation to information security and cybersecurity. In support of the firmwide risk management framework, the firm maintains a standardized risk assessment process that identifies, quantifies and prioritizes risks. The firm performs a number of internal and external risk assessments to gauge the performance of the Program. The purpose of these risk assessments is to accurately estimate the firm's risk profile and adhere to relevant regulatory requirements.

In particular, an annual cybersecurity maturity assessment is administered using the Cyber Risk Institute Profile ("Profile"). Additionally, quarterly assessments of control efficacy and heightened residual risks are conducted through the Risk and Control Self-Assessment ("RCSA") program, administered by Operational Risk.

The firm additionally conducts a variety of technical assessments, including penetration tests and "red team" engagements, and regularly reviews controls using both continuous control monitoring and sample- based testing.

The firm maintains a central inventory of its information security controls and has established a standardized risk treatment framework through which the firm can manage known risks to the firm's systems, applications, data, and business functions.

The results of internal and external risk assessments, together with control performance findings, are used to drive program initiatives and to identify and improve controls.

IDENTIFY

Risk Governance and Oversight

Internal Audit

The firm's Internal Audit division is an independent function that reports to the Audit Committee of the firm's Board of Directors. Internal Audit independently assesses the firm's overall control environment and raises awareness of control risks. Internal Audit also communicates and reports on the effectiveness of the firm's governance, risk management and controls that mitigate current and evolving risks, while monitoring the implementation of management's control measures.

Regulatory Oversight and External Audit

The firm is regulated by numerous authorities in all jurisdictions in which we operate, including (but not limited to):

- **Americas:** The U.S. Federal Reserve System, New York State Department of Financial Services, U.S. Commodity Futures Trading Commission, U.S. Securities and Exchange Commission, U.S. Consumer Financial Protection Bureau;
- **Europe, Middle East and Africa:** The European Central Bank, European Banking Authority, U.K. Financial Conduct Authority, the German Federal Financial Supervisory Authority, the Saudi Arabian Capital Markets Authority, the South African Reserve Bank, the U.A.E. Securities and Commodities Authority;
- **Asia Pacific:** The Monetary Authority of Singapore, the Japan Financial Services Agency, the Australian Securities and Investments Commission, and the Hong Kong Monetary Authority.

PricewaterhouseCoopers LLP (PwC), an external auditor, performs Service Organization Control (SOC) 1 and 2 assessments for select firm businesses and independently tests applicable controls.

Industry Engagement

Goldman Sachs is a founder or leading participant in many relevant industry initiatives both domestically and internationally. In the United States, these partnerships include the Financial Services Sector Coordinating Council (FSSCC), the Financial Services – Information Sharing and Analysis Center (FS-ISAC), the Cyber Risk Institute, the Analysis and Resilience Center (ARC) for Systemic Risk, and the Sheltered Harbor initiative.

The firm maintains direct relationships with government entities globally. In the United States, the firm actively collaborates with the Federal Bureau of Investigations (FBI), the Department of Homeland Security (DHS) and the Cybersecurity and Infrastructure Security Agency (CISA). The firm also engages with international partnerships, such as the Cyber Security Information Sharing Partnership (CiSP – UK) and the Computer Emergency Response Team (CERT - India).

The firm additionally participates in industry efforts to manage technology risks, including those coordinated by the Securities Industry and Financial Markets Association (SIFMA), Asia Securities Industry and Financial Markets Association (ASIFMA), Association for Financial Markets in Europe (AFME), Bank Policy Institute (BPI), the American Bankers Association (ABA) and the Australian Financial Markets Association (AFMA).

IDENTIFY

Information Security and Cybersecurity Policies and Standards

Policies and Standards

The firm maintains a comprehensive set of information security and cybersecurity policies and standards which take into consideration cybersecurity, data privacy laws and regulations that are applicable to jurisdictions in which the firm operates.

Policies and standards are reviewed and approved by relevant firmwide governance bodies. The firm's Global Information Security and Cybersecurity Program and Policy are reviewed annually. Other firm policies and standards are reviewed at least every three years, in accordance with the firm's review cycle per policy. Additional reviews may be triggered by changes in the risk environment or regulatory landscape.

A dedicated policy group, consisting of representatives from each of the firm's divisions, maintains the process to develop, review, update, and decommission information security policies and standards.

Firm policies and standards are aligned with recognized industry standards, including those defined by the National Institute of Standards and Technology (NIST), the Federal Financial Institutions Examination Council (FFIEC), and the Cyber Risk Institute.

Firm policies and standards are available to all personnel through an internal compendium. These documents cover all aspects of the Information Security and Cybersecurity Program. Topics governed by information and cybersecurity policies and standards include, but are not limited to the following:

- Identity and Access Management, including entitlement management and production access;
- Application and Software Security, including software change management, open source software, and backup and restoration;
- Infrastructure Security, including vulnerability management, and network and wireless security;
- Mobile Security, including Bring Your Own Device (BYOD) and mobile applications;
- Data Security, including cryptography and encryption, database security, data erasure, and media disposal;
- Cloud Computing, including governance and security of cloud applications, and Software-as-a- Service data onboarding;
- Technology Operations, including change management, incident management, capacity and resilience; and
- Third Party Risk Management, including vendor management and governance, and cyber security and business resiliency on vendor assessments.

IDENTIFY

Asset Management

Technology Asset Inventory

The firm maintains asset information for hardware in managed inventories throughout its lifecycle and such inventories are used to track each asset's attributes, components, and operational status through demise.

Inventory management is comprised of manual and automated processes and controls, including the asset's onboarding process, periodic reviews, and is governed by policies and standards.

Each technology asset is assigned an owner. Assets may include hardware, software or virtual assets like virtual machines.

The firm has asset management for software and applications that include classifications based on their inherent risks.

The firm has implemented controls designed to ensure secure data destruction at the end-of-life of a storage device.

PROTECT

Training and Awareness

Training and Education

The firm maintains a cybersecurity training program, which is designed to help personnel recognize information and cybersecurity concerns and respond accordingly. In particular, this program is designed to provide all personnel with the knowledge and skills to prevent, identify, and escalate cybersecurity risks.

Information security and cybersecurity training is required of all firm personnel annually, e.g., full-time and part-time employees, and contractors. Additional training is provided for new joiners and individuals transferring within the firm. The firm conducts regular phishing tests on all personnel to test knowledge on email-based cyber threats and appropriate escalation.

The firm incorporates training themes based on regulatory guidance, industry best practices, and changes in the risk environment.

The firm additionally provides technical training to engineering personnel via specialized platforms. This training includes topics focused on information security, such as secure coding principles and updates on emerging threats.

The firm maintains processes to track, measure and escalate personnel who fail to complete mandatory training, including cybersecurity training.

Identity and Access Management

User Identity Management

The firm's access controls are based on the general principles of no privilege without identity, no privilege without approval, and least privilege access. Entitlements are therefore only provisioned when commensurate with role or job duties.

The firm performs background checks on employees, consultants and contractors. Worker identity is subsequently verified at the initiation of employment via standard human resources processes. Upon joining, the firm's personnel sign a non-disclosure agreement that requires them to abide by the firm's policies to protect client information.

A unique identifier and identification badge is assigned to every worker. Personnel are prohibited from sharing their individual credential information, including usernames and passwords.

Entitlements Management

Firm-approved authentication and entitlement solutions are required for all applications. These solutions are designed to limit access to authorized personnel and enable reporting of user entitlements and management approval.

System entitlements associated with critical and sensitive applications are reviewed by management at least annually. More frequent reviews occur for privileged access. Entitlements are also reviewed when personnel transfer to new roles or departments within the firm.

PROTECT

Identity and Access Management

The firm maintains appropriate segregation of duties as a part of its internal control framework. Segregation of duties requires that the same individual is not in a position to initiate, approve, and reconcile the same critical transaction or process. An automated system is used to continuously monitor entitlement stores and identify violations in segregation of duty requirements.

When a worker leaves the firm, access to the firm's facilities and general access to the information systems are revoked within 24 hours. In special circumstances, access is revoked immediately.

Access Controls

The firm maintains defined password requirements documented in a formal standard. Password requirements include establishment of a new password at initial login, minimum password length, alphanumeric composition, expiration after a defined period where appropriate, maximum number of unsuccessful login attempts before lockout, a password history and an inactivity lockout.

When required, data segregation is accomplished through logical segregation with data-level access controls. Administrative access to systems that store client data must be approved by authorized managers.

The firm maintains strict controls over access to production environments, including access authorizations, logging, and time limits on access. As part of the firm's segregation of duties, access by technology staff to production systems requires pre-approval before access is granted. In addition, production access is limited to authorized individuals, time-bound, subject to logging and periodic review, limited to necessary functions, and regularly monitored, including keystroke logging. Changes made to production environments are subject to mandatory reviews.

Multi-factor authentication (MFA) is required for any access to Goldman Sachs systems from outside the firm's network.

Application and Software Security

Centralized Inventory and Risk Classification

The firm leverages a centralized inventory to record key information about applications. Each application is required to complete a risk profile to determine regulatory and risk- based requirements. Accordingly, each application is assigned one or more risk classifications, which in turn are associated with specific required controls and resiliency thresholds.

Risk classifications are required to be reviewed and updated for each application on an annual basis. Risks identified through annual and quarterly assessments are recorded in centralized inventories that details key information about applications.

PROTECT

Application and Software Security

Software Development Controls

The firm has a formal Software Development Lifecycle (SDLC) process, which is documented and incorporates appropriate control gates.

Detective and preventative controls make use of: Static Application Security Testing (SAST), identification of vulnerable dependencies, and infrastructure-as-code scanning.

All production changes require successful testing and authorized approvals.

Application security requirements and associated assessments are incorporated throughout the SDLC on a risk-adjusted basis. Examples of SDLC and related application security controls include:

- Design reviews
- Manual code review and automated code scanning
- Periodic penetration testing of externally facing and other high-risk applications using both internal and vendor security experts
- Use of Dynamic Application Security Testing (DAST) scanners and Bug Bounty programs for Internet-facing applications
- Separate development and quality assurance (QA) environments from production environments
- Testing and validation of open source libraries
- Implementation of industry standard security coding practices such as Open Web Application Security Project (OWASP)

Several applications in use throughout the firm are developed internally. Equivalent application security standards are applied to internally developed applications, open source software components, and third- party software deployed on the firm's infrastructure.

The firm maintains a requirement that sensitive data must be masked, or subject to other equivalent controls, prior to being used in non-production environments.

Security Testing

The firm conducts annual penetration tests, red team, joint offensive-defensive team (commonly referred to as "purple team") and hunt team assessments to discover and evaluate the security of applications and infrastructure, focusing on high-priority themes and risks.

Internet-facing applications are continuously scanned using DAST tools.

The firm maintains a Bug Bounty and responsible disclosure program, covering a majority of public Goldman Sachs sites, which allows researchers to report vulnerabilities through a dedicated portal.

PROTECT

Application and Software Security

The penetration testing methodology used by the firm internally and by the firm's vendors is based on several published industry guidelines such as the CREST STAR/CBEST Implementation Guide, NIST SP800-115, and the OWASP Testing Guide. The approach combines manual and automated assessment techniques and the use of proprietary, commercial and open source assessment tools in a consistent and repeatable process. The methodologies typically cover the following activities:

- Pre-test preparation with asset owners
- Threat modeling and triaging
- Automated dynamic / static scans and output verification of scans
- Vulnerability identification and confirmation testing
- Report preparation and delivery with peer and manager review
- Socialization of findings with asset owners
- Tracking and remediation of issues
- Retesting of remediated issues

Infrastructure Security

Configuration Management and Hardening

The firm employs configuration management to validate from a security perspective that firm systems continue to perform consistently and as expected over a period of time.

Firm systems are hardened on a risk-adjusted basis to meet or exceed industry standards and deployed using standard security practices, such as restricted file access permissions and logging.

Hard drives on firm-provided laptops, which are only used for a small number of specific business purposes, are encrypted using industry standard tools.

An inactivity screen lock is enforced by a configuration policy on every endpoint.

PROTECT

Infrastructure Security

Network Security

The firm's network environment is designed to emphasize security and resilience, including through the implementation of multiple network zones separated by firewalls and other controls.

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are deployed at the network perimeter to monitor for and block malicious activity.

Management interfaces on perimeter firewalls, routers and other devices are not accessible from the Internet. firm subscribes to continuous Distributed Denial of Service (DDoS) monitoring and mitigation services from multiple service providers. In addition, the firm hosts its primary Internet web presence on Content Delivery Networks with DDoS mitigation and absorption capacity, which implements network request throttling to limit the number of referrals and requests made by client IP addresses. Alerts generated by DDoS activities are monitored and mitigated as needed.

Wireless access to the firm's infrastructure is only permitted from firm-approved devices, for example firm- issued laptops and registered employee devices.

System Monitoring, Capacity and Vulnerability Management

The firm maintains a capacity management program, which establishes documented process for defining capacity objectives, scope, and requirements for key business services and related dependencies.

The firm has a comprehensive vulnerability management program that includes frequent network- vulnerability scans of internal and external network environments using an industry standard scanner. The firm also engages third-parties to scan its externally facing infrastructure and provide findings on a regular basis. Vulnerabilities are resolved on a risk-adjusted basis, as required by a formal standard.

The firm has a defined treatment process for discovered vulnerabilities. Each vulnerability is assigned a criticality rating based upon industry-standard processes and aligned with a remediation plan. The timeframes for systems patching are documented in a formal standard. In cases where a vulnerability is identified for which a patch is not yet available, the firm evaluates the adoption of appropriate compensating controls to minimize the likelihood of unauthorized access.

Virtual Desktop Solution

The firm uses Virtual Desktop Infrastructure for desktop computing. In this model, all users use a thin client to access their virtual desktop hosted in a GS data center.

Remote access from outside the firm's premises is enabled through a secure connection to a user's virtual desktop using multi-factor authentication.

The firm's virtualized infrastructure is designed to provide the equivalent level of control as the firm's on- premise infrastructure, regardless of the geographical location it is accessed.

Non-Virtual Desktop computing models are conducted on an exception basis, when required by business functions.

PROTECT

End User Device Security

Secure Remote Access for Personnel

Personnel are permitted to use their personal devices when working remotely through the firm's Bring Your Own Device (BYOD) Program to securely access firm resources.

Personal devices can only connect to the firm's systems through firm-approved mobile applications. Any storage of firm or client information on personal devices, outside of firm-approved applications, is strictly prohibited.

Remote access to the firm's network provides the same controls as on-premise access. There are two primary mechanisms for personnel to remotely access the firm: (i) secure applications for use on personal mobile phones or tablets, which can be used to access select services, and (ii) through the firm's remote access solution that enables access to a virtual desktop.

The firm-approved mobile applications allow personnel to securely send and receive emails and access internal websites and documents. A limited set of third-party applications allow personnel to conduct analytic and/or business-related activity only if such applications meet the firm's security criteria.

Mobile applications used by the firm generally utilize a range of security features, including:

- mobile threat defense
- device allow-listing
- secured network connections
- multi-factor authentication
- sandboxing
- encryption
- required device registration
- required operating system (OS) patching
- verification of non-jailbroken OS
- remote data wiping

Personnel may be issued a firm device for specific business purposes. All data on firm-issued devices is encrypted at rest and in transit for remote access and mobile computing.

Client Mobile Applications

The firm has developed mobile applications for clients to access their accounts, perform and approve transactions, access market news and securely communicate with Goldman Sachs personnel. Client mobile applications employ additional industry-standard security controls including multi-factor authentication (MFA), biometric authentication, and encryption of data at rest and in transit.

PROTECT

Data Protection

Data Governance

Data governance at the firm encompasses the people, processes, and information technology required to create a consistent and proper handling of firm and client data across all businesses. The firm's data management practices provide the necessary structure to ensure data is managed as an asset and transformed into useful information.

The program supports data security programs across the firm, defines and verifies the requirements for data distribution practices, and designates accountability for information quality.

Data Protection

Data Loss Prevention (DLP) controls are designed and implemented to prevent content from leaving the firm that is not intended for external use and distribution. These controls include proactive alerts to notify a sender if an email to an external recipient contains potentially sensitive information, such as personally identifiable information (PII).

The firm additionally maintains various surveillances to identify potential incidences of data exfiltration or insider threats, including using big data techniques.

Access to removable media, such as USB flash drives, writable CDs and local administrative and enhanced system functionality, is prohibited by default. When access to removable media is approved for specific business purposes, such access is strictly controlled and time-bound. Non-public data stored on removable media is encrypted.

Firm personnel are prohibited from using third-party systems and functions, such as webmail or unapproved analytics tools, for business purposes. In addition, firm personnel may not use firm resources to access such systems for personal use.

Staff access to selected websites and site categories is blocked or limited based on regulatory, information security, and internal control requirements. This includes social networks, file sharing and webmail.

Global Compliance oversees the firm's electronic communications monitoring and surveillance program, including the review of alerts potentially indicative of a variety of risks resulting in potential non-adherence to regulatory requirements and/or firm policy.

Encryption

The firm encrypts sensitive personal information in transit and at rest. Other types of data are encrypted and/or protected with compensating controls based upon particular regulatory, security, and contractual considerations.

The firm uses strong industry standard encryption methods. We regularly review the strength of all encryption protocols.

Firm-standard solutions are available for file encryption transferred between the firm and third-parties.

Opportunistic email encryption, such as Transport Layer Security (TLS), is enabled with all clients where business requirements dictate. Mandatory email encryption is supported and enabled by mutual agreements.

PROTECT

Data Protection

Key generation and management occur in firm-standard key management solutions that are backed by hardware encryption modules. Access to encryption keys is pre-approved, limited to authorized individuals, subject to logging, and is regularly monitored.

Data Security

The firm has a formal, structured data privacy security program that includes mandatory controls and processes for all applications and assets storing or processing personally identifiable information, including end-user computing tools. This program is continuously updated in accordance with applicable laws and regulations, and with the firm's internal standards.

The firm has clean desk guidelines which instruct personnel to keep the workspace clear of paper containing sensitive data.

The firm has implemented controls which lock user workstations after a defined idle period. Personnel are advised to lock workstations when away from their desk.

The firm maintains controls to ensure secure data destruction at the end-of-life of a storage device. The firm has implemented a program to identify end of life systems, prioritize upgrades or demise of these systems based upon the criticality of supported services.

Retired media are sanitized using a standard set of tools. Physical media destruction is performed according to pre-defined procedures.

Asset decommissioning is internally managed through workflow, inventory, and scanning processes.

The firm retains records for various periods as needed to comply with applicable laws and regulations and to conform to its internal retention policies.

Physical Security

Physical security measures are deployed to protect data centers and offices. These measures include card access, biometric access, video surveillance, on-site security staff, environmental controls, and visitor management.

Physical access is granted based on need, aligned with firmwide access controls, approved by designated access approvers, and reviewed periodically. Physical separation of teams and offices is in place based on business and regulatory requirements. Access to data centers and offices is electronically logged by access card or biometric technology.

All visitors must present photo identification and have a confirmed host before being granted access to the firm's offices or data center facilities. Visitor logs are maintained.

Critical data centers are geographically dispersed and on diverse utility and power infrastructure. These facilities have security personnel on duty 24 hours a day and access is limited to only essential support personnel.

PROTECT

Physical Security

All facilities supporting Goldman Sachs business are protected from environmental hazards and power outages by the following controls, where applicable:

- Uninterruptible Power Supply (UPS)
- Generators
- Air conditioning units
- Fire detection and suppression systems
- Water detection systems
- Earthquake resistant facilities and seismic designs

Physical security standards are applied consistently to all offices globally, including business recovery site locations.

Cloud Security

Cloud Governance

The firm leverages public, private, and hybrid cloud-based solutions where appropriate for certain compute, storage, and business purposes. The firm maintains a formal governance process and control framework for all cloud-based applications, which are documented in formal standards.

Risk governance is embedded in the firm's global cloud governance framework to ensure the sustainable deployment and migration of the firm's cloud systems, applications and data on public cloud environments. Formal standards apply to cloud resources that are scoped to multiple offerings, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

The firm's public cloud environments are governed by committees responsible for overseeing the processes relevant to deploying and implementing cloud technology. In addition to the Firmwide Technology Risk Committee and Engineering Risk Steering Group previously mentioned, the following groups have oversight over cloud security:

- The Public Cloud Governance Steering Group ensures compliance with the Firmwide Standard on Global Cloud Governance and oversees end-to-end governance of cloud adoption.
- The Third Party Risk Steering Group manages the vendor risk review process, including risk acceptance and remediation plans for cloud vendors.

Cloud Controls and Assessments

The firm has established defined controls for cloud applications, including encryption and compensating controls, strict authentication, role-based access, centralized logging, network segmentation, and auditing. Continuous control monitoring and automated control enforcement gates are leveraged for cloud-based resources to detect any misconfiguration.

PROTECT

Cloud Security

Cloud hosted applications undergo a formal risk assessment and architecture review on a risk-adjusted basis using a control inventory. Each application is required to complete a risk profile to determine regulatory and risk-based requirements.

Risk classifications are required to be reviewed and updated for each application on an annual basis. Risks identified through assessments are recorded in centralized inventories that detail key information about applications and findings.

The firm has established procedures, review processes, and control gates for onboarding data to cloud-hosted software platforms.

Cloud service providers are subject to an enhanced vendor management review covering the secure delivery of services and audit provisions, and must satisfy the firm's public cloud control requirements.

Vendor Security

Vendor Security

Vendors are viewed as an extension of the firm. As such, the firm has a comprehensive Firmwide Vendor Management Policy and Program that documents a risk-based framework for managing third party vendor relationships consistent with regulatory guidance and firm policy. Information security risk management is built into the firm's vendor management process, which covers vendor selection, onboarding, performance monitoring and risk management. Vendors are expected to design, implement, and maintain information security controls consistent with the firm's security policies and standards.

Vendors that access Goldman Sachs information are required to undergo an initial assessment on a risk adjusted basis. Subsequently, the firm conducts re-certifications at a breadth and frequency determined by each vendor's information security rating, which is calculated based on a number of factors, including the type of data stored and processed by a particular vendor.

Such assessments may also include the use of third-party market scoring products to review vendors' internet-facing security posture. All assessments determine the maturity of the vendor's information security, cybersecurity and business continuity practices. Gaps found during these due diligence assessments are ranked by risk, recorded, and addressed per the firm's standards.

The firm conducts ongoing oversight of vendors based on the criticality of each vendor's particular service to the firm and the results of the initial risk assessment. Critical vendors receive enhanced focus and due diligence. Changes in the service provided by a particular vendor are identified as part of a standard oversight process and may trigger an updated risk assessment prior to the firm onboarding additional services.

Firm policy requires vendors to sign standard contractual provisions before receiving sensitive information from the firm. These provisions have specific information security control requirements, which are negotiated with vendors that store, access, transmit, or otherwise process sensitive information on behalf of the firm during onboarding or contract renewals, as applicable.

Dedicated teams across the firm are responsible for regular assessment and reporting on vendor information security controls. Periodic reporting of key vendor risk management metrics is provided to business management

DETECT

Logging and Continuous Monitoring

Logging

The firm has enabled logging for key events including failed logins, administrative activity, and change activity.

Log file management follows the principle of least privileges. Only application processes have "write" access to log files. System accounts only have "read" access to log files.

Logs are maintained in accordance with firm policy on records retention and legal and regulatory requirements. At a minimum, logs are retained for 30 days.

The firm has controls designed to prevent logs from containing sensitive information such as personally identifiable information (PII), authentication credentials or encryption keys.

Security event logging is enabled to allow for system forensic analysis and Technology Risk surveillance analytics. Security event logs are protected from unauthorized access, modification and accidental or deliberate overwriting.

Malware Protection

Industry-standard anti-malware software is installed on Windows and Linux endpoints and servers and on the firm's email infrastructure.

Anti-malware alerts are monitored by the firm's staff. Malware is remediated and, if need be, systems are rebuilt.

Malware signature files are updated on a regular basis, at a minimum daily, by way of automatic requests from systems on the firm's network.

Runtime checks are performed on specific executables to reduce the possibility of exploit via malware. Application allow-listing is deployed to detect, report and prevent the execution of malware.

The firm subscribes to an email pre-filtering solution to reduce the amount of malware received by the firm's email gateway.

The firm utilizes an email protection system that is designed to block spam, phishing and viruses from reaching personnel inboxes.

The firm actively mitigates spoofing through the use of an email authentication policy and protocol to prevent spoofing of emails between the firm and its clients. The firm also assigns an imposter score to each email and flags emails above a threshold score for quarantine to assess potential email spoofing.

The firm has established key metrics to establish a baseline for continuously monitoring system state and anomaly detection in the firm's production environment. Pre-determined criteria are applied to security events to generate alerts. Monitoring tools are in place to notify appropriate personnel of security issues. Alerts are classified, prioritized and actioned by appropriate personnel for timely remediation based on business criticality.

DETECT

Logging and Continuous Monitoring

Security Monitoring and Intrusion Detection

The firm maintains a Hunt Team with dedicated experts focused on proactively identifying previously undetected malicious activity and opportunities to continuously improve Goldman Sachs' control posture. Additionally, the Hunt Team collects threat intelligence to actively identify potential indications of threat activity across the firm's network.

The firm maintains monitoring processes to detect anomalous activity in a timely manner. The firm collects, analyzes, and correlates events data across the organization to perform real-time central aggregation to detect and prevent multifaceted cyber attacks, leveraging a variety of sensors distributed across the firm's environment.

The firm conducts periodic cyber-attack simulations, micro-drills, monthly drills, and tabletop exercise to detect control gaps in personnel behavior, policies, procedures, and resources.

The firm authorizes and monitors third-party connections and continuously collects and retains relevant information. The firm has automated alerts to monitor and prevent any unauthorized access to a critical system by a third-party service provider.

The firm performs threat intelligence collection to analyze threat actor tactics, techniques, and procedures, which results in the tuning of controls to mitigate emerging adversary threats. The firm also shares threat intelligence with peer firms as an approach to actively maintain collective risk mitigation and improve security of external connections.

Insider Threat

The firm has an established insider threat program to detect and prevent malicious and unintentional unauthorized activity carried out by firm personnel.

The firm leverages a variety of telemetric, detective and preventive controls to address insider threats, including but not limited to, user endpoint monitoring and entitlements management.

RESPOND

Security Incident

Security Incident Management

The firm has a dedicated Global Cyber Defense and Intelligence Team (GCDI) responsible for detecting, investigating, and responding to information security threats and incidents that have a potential impact on the confidentiality, integrity, or availability of the firm's information and technology environment.

GCDI maintains procedures for identifying and responding to specific information security incidents and works with other areas within the firm to contain, mitigate and remediate potential incidents. In addition, GCDI maintains escalation protocols to ensure that clients, regulators, or other parties are appropriately notified of any security incidents, where required by applicable law, contract, or regulation. GCDI further maintains a dedicated threat management center that operates 24/7.

The firm has implemented a global security incident preparedness program to support security incident management. Technology Risk conducts business-focused table top exercises with business units and regional teams to assess their processes, understanding and readiness, with oversight from the Operational Risk Division. Externally, the program covers firm participation in financial sector and public–private sector cybersecurity exercises to ensure the firm's preparedness to coordinate with other institutions, financial markets and relevant government agencies.

Threat Intelligence

The firm recognizes that cyber threat actors target the firm's networks, vendors, suppliers, and its personnel, along with the broader financial sector, in order to conduct fraud, steal proprietary information, and/or disrupt the firm's ability to conduct business and support its clients and customers.

The GCDI Cyber Threat Analysis (CTA) team is responsible for protecting the firm from external adversaries by proactively identifying relevant cyber threats, evaluating the risk these threats pose to the firm's assets, and working with personnel in the Engineering Division and affected business units to proactively reduce or mitigate risk to the firm.

Security intelligence and threat information are obtained from third-party intelligence service providers, industry consortia, internal monitoring, as well as public and government sources.

Cyber Insurance

The firm maintains a cybersecurity insurance policy that covers the firm's direct costs from a covered security incident along with applicable customer notifications and credit monitoring services where necessary. The policy also includes coverage for Business Interruption issues. The firm's cybersecurity policy is serviced by a consortium of insurance providers.

RECOVER

Business Continuity and Technology Resilience

Business Continuity

Goldman Sachs has established a global, structured Business Continuity Planning (BCP) framework to ensure it is prepared in the event of an operational disruption.

The firm's Business Resilience Program comprises the following key elements: Crisis Management, Business Continuity Requirements, Technology Resilience, Business Recovery Solutions, Assurance and Process Improvement / Continual Assessment. The description of the firm's Business Resilience Program (including Disaster Recovery) is available on the firm's public website.

The firm has developed Business Continuity Plans (BCP) to address operational disruptions. Plans must have identified BCP Coordinator(s) who develop and maintain the assigned BCP and ensure testing requirements. BCPs must be reviewed and updated by BCP Coordinators and certified by BCP Owners at the frequency required by firm standards. Each business unit identifies its critical activities, the dependent assets (people, facilities, systems, and third parties) that support those activities and the impact that a disruption to these dependent assets would have on the business unit's activities.

As part of the BCP, the business unit must complete business impact analysis. BCP Coordinators identify the criticality, recovery time objectives, dependencies and recovery strategies of their core processes. These processes determine the type of assurance needed to record completeness, *e.g.*, people recovery tests, application failover tests, training, table top drills.

The firm's business continuity risk mitigation strategy includes resilience capabilities such as, near site, far site, work from home, and dispersed recovery capabilities where appropriate in order to mitigate risks and address threats to the region. The firm's far site recovery facilities reside on different power and utility grids from primary office locations.

The firm conducts extensive business continuity preparedness testing, including tests of technology failover, people recovery facilities, work from home, and regional handoff. The firm also participates in industry-level tests with major securities exchanges, government agencies, and local authorities. The firm's divisions perform micro-drills, as well as chain of command and automatic notification testing.

Crisis Management Centers that operate 24/7 in every region allow the firm to monitor its environment, execute pre-established crisis management procedures, and coordinate responses to incidents worldwide.

Data Backup and Recovery

Data backups are written to an immutable, continuously-available, disk-based platform for recovery purposes. Periodically, data is written to encrypted tape media and shipped to off-site locations for storage.

The firm's record keeping, data backup and recovery processes are executed using an industry-standard enterprise system. Processes are in place to identify, escalate, and remediate exceptions as appropriate.

The firm regularly tests the capability of applications to failover to alternate data centers as part of the BCP testing program.

User-driven recovery requests are streamlined through a ticketing system. Recovery attempts of backed up data are logged.

RECOVER

Business Continuity and Technology Resilience

Technology Resilience

The firm has a robust technology resilience program to ensure internal applications and dependent infrastructure components demonstrate the appropriate level of resiliency and recovery based on business criticality. Such controls include:

- Processing dispersion (reducing dependency on any one location)
- Network, telecom, and remote access resilience (multiple points of redundancy and resilience)
- Regional technology operating independently of critical market applications
- Business application inventory and tiering (recovery time objectives)
- Inclusion of technology dependencies in all applicable business unit plans
- Semi-annual testing

Based on business requirements, many critical applications are deployed and tested across multiple data centers to ensure seamless operation should a data center experience a disruption.

The firm participates in financial industry test initiatives, in jurisdictions where they are offered, to exercise alternative connectivity capabilities and to demonstrate an ability to operate through a significant business continuity and/or disaster event using backup sites and alternate recovery facilities.

The firm maintains a documented framework and recovery program to identify and mitigate cyber-destruction incidents like ransomware, including coordination among internal stakeholders and collaboration with external parties, such as law enforcement and regulators.

RECOVER

Our Expectations of Your Information Security Practices

Client Information Security Practices

Information security is a shared responsibility which often involves cooperation between financial institutions and their clients. While Goldman Sachs seeks to provide as much assurance as possible for the services offered, the firm relies on your adoption of standard information security controls for the use of data and systems shared between you and the firm, for example:

- Aligning your information security and cybersecurity controls to international standards, such as the NIST Cybersecurity Framework, Center of Internet Security (CIS) Critical Controls, and ISO 27001;
- Ensuring that only authorized users have access to the firm's data;
- Protecting authentication credentials, such as usernames and passwords, of users authorized to access the firm's data;
- Protecting computer equipment used in interactions with the firm with such tools as anti-malware software, a firewall and up-to-date operating system;
- Notifying the firm promptly in case of any actual or suspected compromise of its data or system;
- Establish a designated person to sponsor and drive information security, ideally from the executive leadership team who has the authority to make the right risk decisions across all lines of business and can effect change;
- Establish a governance/oversight process where the leadership team can decide on risk management priorities;
- Retain a third-party to test your security and determine if it is resistant to common attacks such as perimeter intrusion, malware infections, leakage of sensitive data, or ransomware. As part of this exercise, identify internal owners, external partners, law enforcement, and other key contacts who are best positioned to help during a security incident;
- Prioritize risk mitigations based on criticality;
- Consider leveraging managed services to expand your security capabilities, including for security monitoring, vulnerability scanning, vendor assessments, and incident response; and
- Consider commissioning "red team" tests from an independent third-party to evaluate security controls and incident response processes.