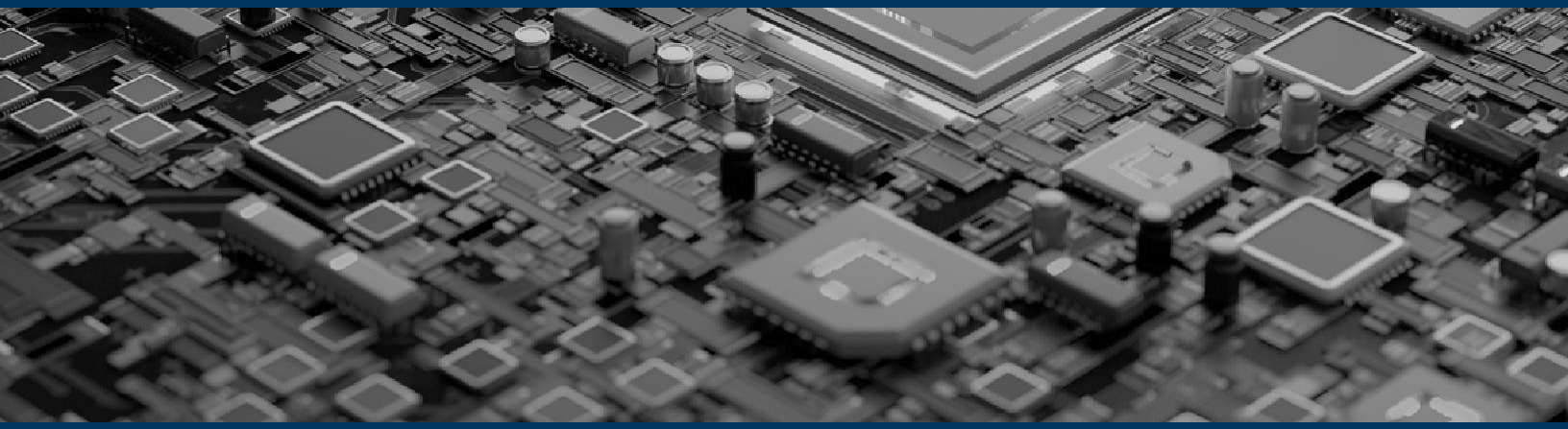
Goldman Sachs



CLIENT SECURITY STATEMENT

Version 12 | October 2025



Table of Contents

Introduction 3

GOVERN
Risk Governance and Oversight 4
Information Security and Cybersecurity Policies and Standards 7

IDENTIFY
Risk Assessment 8
Asset Management 8

PROTECT
Training and Awareness 9
Identity and Access Management 9
Application and Software Security 10
Infrastructure Security 12
End User Device Security 13
Data Protection 14
Physical Security 16
Cloud Security 16
Artificial Intelligence Security 17
Vendor Security 18

DETECT
Continuous Monitoring 19

RESPOND
Incident Management 21
Threat Intelligence 22
Cyber Insurance 22

RECOVER
Business Continuity and Technology Resilience 23
Our Expectations of Client Information Security Practices 25

No part of this material may be (i) copied, photocopied, or duplicated by any means or (ii) redistributed without our prior written consent. This material is for informational purposes only and is not intended to form the basis of any investment decision and should not be considered as a recommendation by Goldman Sachs & Co. LLC, its subsidiaries, or affiliates (collectively, "Goldman Sachs" or "we"). This material does not constitute an offer to provide advisory or other services by Goldman Sachs. Nothing herein is an offer or promise to procure any product or service or to make an investment in any entity.

This document applies to the Goldman Sachs Group Inc. (the "firm"), its affiliates; and its subsidiaries, and supersedes all prior statements, commitments, agreements, and writings with respect to the subject matter hereof and all such have no further force or effect.

Introduction

Goldman Sachs places great importance on information security and cybersecurity, to protect against external threats and insider risks. The firm's cybersecurity strategy emphasizes proactive detection, rapid analysis and response, effective management of cyber risks, and resilience against security incidents.

Goldman Sachs applies a tailored, risk-based approach rather than a one-size-fits all model. Each organization within the firm has both common and unique risks, as well as varying risk appetites and tolerances, specific missions, and objectives to achieve those missions. The firm continuously strives to improve our security practices to align with industry-recognized security practices and apply threat-informed as well as resiliency-focused controls to protect our clients and the firm. The firm's formal cybersecurity program is aligned to the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF).

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 six functions of the NIST CSF: Govern, Identify, Protect, Detect, Respond and Recover.

While cybersecurity measures will evolve over time and carry across our range of services, this document reflects the firm's overarching practices and commitments. 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.

GOVERN

Risk Governance and Oversight

Risk Governance Framework

Goldman Sachs has established an enterprise risk management framework that employs a comprehensive, integrated approach to identifying and managing risks. The framework is built on three core components: governance, processes and people.

- **First Line of Defense**

The firm's revenue-producing units, as well as Treasury, Engineering, Human Capital Management, Operations, and Corporate and Workplace Solutions, form the first line of defense. These units are responsible for managing the risks inherent in first-line activities and ensuring those risks remain within the firm's defined risk appetite.

- **Second Line of Defense**

The firm's independent risk oversight and control functions form the second line of defense. This group provides independent assessment, oversight and challenge of the risks undertaken by the first line of defense. In addition, the second line of defense also participates in risk committees to improve governance processes. Independent risk oversight and control functions include Compliance, Conflicts Resolution, Controllers, Legal, Risk, and Tax.

- **Third Line of Defense**

Internal Audit serves as the third line of defense, reporting directly to the Audit Committee of the Board and administratively to the Chief Executive Officer. Internal Audit professionals are responsible for validating the effectiveness of controls, including those within the firm's risk management framework. The third line of defense also provides timely reporting to the Audit Committee of the Board, senior management and regulators.

Overall, the three lines of defense model reinforces accountability, ensures effective oversight, and provides a clear structure for managing and challenging risks. Ultimately, each division remains accountable for managing technology risks and safeguarding information system assets.

Governance Committees

The Board of Directors, both directly and through its Risk and Audit Committees, and sub-committees, oversee the firm's risk management policies and practices, including information security, cybersecurity and technology risks.

The firm's Chief Risk Officer (CRO), Chief Information Officer (CIO), and Chief Technology Officer (CTO), among others, regularly brief the Board on operational, technology, and cybersecurity risks, as well as regulatory developments and mitigation strategies. The Board also receives regular briefings from the Chief Information Security Officer (CISO) on a range of security topics, including the firm's Information Security and Cybersecurity Program ("Program"), evolving cybersecurity risks, emerging cybersecurity threats, mitigation strategies and related regulatory engagements. The Board maintains ongoing dialogue and oversight of risk management with senior leadership.

The firm has established several governance committees, steering, and process oversight groups that monitor and implement the firm's cybersecurity risk management strategy and framework. These governance forums provide accountability, and a formal process for risk reporting and escalation. Key Committee and Steering Groups include:

- Firmwide Compliance and Operational Risk Committee (FCORC): The committee oversees global compliance and operational risks and seeks to ensure the firm's business and operational resilience. This Committee is co-chaired by the firm's Chief Compliance Officer, Chief Administrative Officer for EMEA and the global head of Operational Risk Management.

- Firmwide Technology Risk Committee (FTRC): The committee reviews technology design, development, deployment, and usage. In addition, the committee oversees cybersecurity and IT risk management frameworks, methodologies, and their effectiveness. This committee is co-chaired by the CISO and the CTO.

- Digital Risk Office (DRO) Steering Group: The DRO Steering Group is a subordinate group under the FTRC, overseeing Engineering risks. The group provides strategic oversight of the Engineering risk portfolio, streamlines escalation, and coordinates decisions across pillars on key initiatives. This group is chaired by the Chief Digital Risk Officer (CDRO).

Information Security and Cybersecurity Program

The firm's cybersecurity risk management processes are integrated into the overall risk management framework. The Information Security and Cybersecurity Program ("Program"), administered by Technology Risk within Engineering, and overseen by the CISO. The Program is designed to identify, assess, document and mitigate threats; establish and evaluate compliance with information security mandates; adopt and apply the security control framework; and prevent, detect and respond to security incidents. The program is periodically reviewed and updated to address evolving threats and conditions.

A dedicated Operational Risk team, which reports to the Chief Risk Officer, provides oversight and challenge of the Program, independent of Technology Risk, and assesses the operating effectiveness of the Program against industry standard frameworks and Board risk appetite-approved operational risk limits and thresholds.

The firm's approach to managing cybersecurity risks includes the critical components of the risk management framework, as well as the following:

- **Training and Awareness** - Enabling personnel to recognize information and cybersecurity concerns and respond accordingly.

- **Identity and access management** - Covering entitlement management and production access.

- **Application and software security** - Including software change management, open-source software, and backup and recovery processes.

- **Infrastructure security** - Monitoring the network for known vulnerabilities and signs of unauthorized attempts to access firm data and systems.

- **Mobile security** - Covering mobile devices and applications.

- **Data security** - Including cryptography, encryption, database security, data erasure, and media disposal.

- **Cloud computing** - Covering governance and security of cloud applications, as well as software-as-a-service (SaaS) data onboarding.

- **Technology operations** - Encompassing change management, incident management, capacity and resilience.

- **Third-party risk management** - Covering vendor management, governance, cybersecurity and business resiliency on vendor assessments.

GOVERN

Internal Audit

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

Regulatory Oversight and External Audit

The firm is subject to oversight by regulated authorities across all jurisdictions in which it operates, including (but not limited to):

- **Americas**: The U.S. Federal Reserve System, U.S. Commodity Futures Trading Commission, U.S. Securities and Exchange Commission, U.S. Consumer Financial Protection Bureau, New York State Department of Financial Services.
- **Europe, Middle East, and Africa**: European Central Bank, European Supervisory Authorities, Central Bank of Germany, Dutch Authority for Financial Markets, Swiss Financial Market Supervisory Authority, U.K. Financial Conduct Authority, U.K. Prudential Regulation Authority, Dubai Financial Services Authority, Saudi Arabian Capital Markets Authority, and the South African Reserve Bank.
- **Asia Pacific**: The Monetary Authority of Singapore, the Japan Financial Services Agency, the Australian Securities and Investments Commission, the South Korea Financial Supervisory Service, the Securities and Exchange Board of India, the Reserve Bank of India, the Securities and Futures Commission of Hong Kong and the Hong Kong Monetary Authority

Goldman Sachs maintains a comprehensive external compliance program across revenue-producing units aligning security controls to independent audits and certifications. This process of ongoing evaluation and validation of security controls is designed to ensure our control strategy is relevant, adaptive, and resilient.

As technology evolves our external audit cadence and scope adapt accordingly. These adjustments are intended to maintain independent assurance activities, while supporting the firm's information systems, services and its approach to risk governance and oversight.

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

GOVERN

Industry Engagement

Goldman Sachs actively contributes to key industry initiatives in the United States and globally, reinforcing the firm's role in strengthening the financial sector's resilience to cybersecurity risks.

United States Partnerships: The firm is a founding or active member of groups such as the Financial Services Sector Coordinating Council, the Financial Services – Information Sharing and Analysis Center, the National Cyber-Forensics and Training Alliance, the Cyber Risk Institute, the Analysis and Resilience Center for Systemic Risk, and the Sheltered Harbor initiative.

Government Engagement: The firm engages closely with government agencies in the United States, such as the Federal Bureau of Investigations, the Department of the Treasury, the Department of Homeland Security and the Cybersecurity and Infrastructure Security Agency. In addition, the firm also partners internationally with the UK Financial Sector Cyber Collaboration Centre, the UK Financial Services Information Exchange, and the Computer Emergency Response Team.

Global Industry Associations: The firm participated in financial sector associations including the Securities Industry and Financial Markets Association, Asia Securities Industry and Financial Markets Association, Association for Financial Markets in Europe, Bank Policy Institute, the American Bankers Association and the Australian Financial Markets Association.

Information Security and Cybersecurity Policies and Standards

Policies and Standards

The firm maintains information security and cybersecurity policies and standards that take into consideration information security and cybersecurity, data privacy requirements, digital operational resilience and regulatory obligations across jurisdictions in which the firm operates. The firm maintains comprehensive policies and standards that cover key areas of its operations and risk management framework.

Policies and standards are reviewed and approved by relevant firmwide governance bodies chaired by senior management. The firm's Global Information Security and Cybersecurity Program and Policy are reviewed annually, while other firmwide policies and standards are reviewed at least every three years, in accordance with the firm's periodic review requirements. The firm also conducts additional reviews that may be triggered by changes in the risk environment or regulatory landscape.

A dedicated policy governance group, consisting of representatives from each of the firm's divisions, manages the lifecycle of these policies and standards, which includes development review, update, and decommission.

The firm policies and standards are aligned with recognized industry standards, including those defined by the National Institute of Standards and Technology (NIST). All firm policies and standards are available to personnel through an internal compendium.

IDENTIFY

Risk Assessment

Risk Assessment

Goldman Sachs believes the identification and subsequent assessment of risks and related controls is a critical step in providing the Board and senior management with transparency and insight into the range and materiality of risks facing the firm.

The firm's approach for risk identification and control assessment is comprehensive across all risk types and is both dynamic and forward-looking to reflect and adapt to the changing risk profile and business environment. It leverages subject matter expertise and allows for prioritization of the most critical risks. This approach also encompasses control assessment, for which the second line of defense provides independent oversight and challenge of control design and operating effectiveness ensuring alignment with the firm's strategic objectives. Furthermore, the firm has a data collection process, supported by firmwide policies and procedures which require personnel to report and escalate risk events in a timely manner.

The firm performs risk assessments to gauge the performance of the Global Information Security and Cybersecurity Program, to estimate the firm's risk profile and assess compliance with relevant regulatory requirements. These periodic assessments are conducted either through internal reviews, self-assessments, and/or external independent testing, including external penetration tests and "red team" engagements where third parties test the firm's defenses. The results of these risk assessments, together with control performance findings, are used to establish priorities, allocate resources, and improve the overall control environment.

Asset Management

Technology Asset Inventory

The firm centrally manages its inventory of hardware, software, and virtual assets including cloud. The firm's Technology Asset Inventory function is managed by a firmwide policy, standard and procedures, covering onboarding, attribute management, lifecycle oversight, and periodic reviews of assets. The inventory is reconciled against a secondary source to confirm completeness and accuracy.

PROTECT

Training and Awareness

Training and Education

The firm maintains a cybersecurity training and awareness program, which is designed to help personnel recognize information and cybersecurity concerns and respond accordingly. This program is equipped to assist personnel with the knowledge and skills to prevent, identify, and escalate cybersecurity risks.

Annual information security and cybersecurity training is mandatory for all personnel who access firm technology including full-time and part-time employees, and contractors. New joiners and personnel transferring within the firm receive additional onboarding training. In addition, the firm conducts regular exercises to reinforce awareness of email-based cyber threats and escalations procedures.

The firm incorporates evolving training themes to reflect regulatory guidance, industry standard practices and changes in the risk environment.

The firm also provides technical training for engineering personnel through specialized platforms covering topics such as secure coding principles and updates on emerging security trends.

The firm maintains formalized and automated processes to track, measure and escalate personnel who fail to complete mandatory annual training.

Identity and Access Management

User Identity Management

The firm's access controls follow the principles of no privilege without identity, no privilege without approval, and least privilege access. Entitlements are provisioned in line with role and job responsibilities.

As permitted by local law, firm policy requires background checks to be conducted on employees, consultants and contractors with access to firm systems, non-public information or firm premises. Worker identity is subsequently verified at the start of employment. Prior to joining, firm personnel are required to sign a non-disclosure agreement to protect client information in accordance with firm policy.

Firm personnel are assigned a unique digital identifier and physical access card for entry to firm-managed systems and facilities. Personnel are prohibited from sharing their individual access cards and credential information, including usernames and passwords.

PROTECT

Entitlements Management

The firm maintains security controls that require authentication and authorization before access. Entitlements associated with critical and sensitive applications are required to be reviewed by management at least annually with more frequent reviews for privileged access. Entitlements may also be revoked and/or reviewed when personnel transfer to new roles or departments within the firm.

The firm enforces a Segregation of Duties (SoD) program as a part of its internal control framework. SoD requires that the same individual cannot initiate, approve, and reconcile the same critical transaction or process. An automated system monitors entitlement stores and flags any violation of segregation of duty controls.

When personnel leave the firm, all entitlements including access to facilities and general access to the information systems are revoked.

Access Controls

Passwords must be created at the time of initial login, meet minimum length, password history, alpha-numeric composition standards and do not contain common dictionary words or phrases. In addition, the firm's password controls include mandatory locking of accounts after a set number of failed login attempts, as well as mandatory password expiration and reset if indication of compromise. The firm enforces defined inactivity lock out rules to protect against unauthorized access and conducts ongoing monitoring of these activities.

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

The firm maintains strict controls over access to production environments. This includes access authorizations, logging, and enforcing time-bound limits on access. Segregation of duties (SoD) ensures that any access by technology staff to production systems requires pre-approval. Access is restricted to authorized individuals, subject to logging and periodic review, limited to necessary functions, and regularly monitored. All changes made to production environments are subject to mandatory reviews.

The firm also requires multi-factor authentication (MFA) for personnel accessing its network and internet-facing applications that handle sensitive or non-public information.

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, which determines its regulatory and risk-based requirements. Based on this assessment, applications are assigned one or more risk classifications, each linked to specific required controls and resiliency thresholds.

Risk classifications are required to be reviewed and updated at least on an annual basis. Risks identified during annual and quarterly assessments are recorded in centralized inventory, which serves as the authoritative source for key application risk information.

PROTECT

Software Development Controls

The firm maintains a formal and documented Secure Software Development Lifecycle (S-SDLC) process, which proactively integrates security controls and gates. Application security requirements and associated risk-adjusted assessments are embedded throughout the S-SDLC.

Examples of S-SDLC, and related application security, controls include early-stage threat modelling and design reviews, secure code reviews, and security testing such as penetration testing and Dynamic Application Security Testing (DAST). Proactive and detective measures further encompass Static Application Security Testing (SAST), continuous identification of vulnerable dependencies through Software Composition Analysis (SCA), and infrastructure-as-code scanning to prevent misconfigurations. Firm procedures mandate that production changes undergo security testing and receive authorized approvals prior to deployment.

The firm develops numerous applications internally, and a consistent set of application security standards is applied to these internally developed applications, as well as to open-source software components and third-party software deployed on the firm's infrastructure. This approach validates that all software, regardless of its origin, adheres to the firm's security posture, aligning with best practices for secure software development across the entire software supply chain.

Firm policy requires that sensitive data be masked or protected by other equivalent controls before being utilized in non-production environments. These controls are applied based on the application's risk profile, ensuring adherence to applicable legal, regulatory, and contractual data protection requirements.

Security Testing

The firm maintains a standard for application security that defines assets in scope and the frequency of testing. Prior to deployment, testing is required and periodically thereafter. The testing frequency is determined by the asset's classification. Penetration testing is performed using a combination of internal resources and external consultants. The testing methodology focuses on dynamic testing methods and is based upon Open Worldwide Application Security Project ("OWASP") Top 10.

The firm runs a threat-intelligence-led Red Team Program that utilizes outside vendors, alongside firm penetration testers to execute both Red and Purple Team engagements. The firm employs a risk-based approach to determining how tests are scoped and executed.

The firm maintains a Bug Bounty and responsible disclosure program, covering a majority of the firm's internet facing assets, enabling external researchers to responsibly report vulnerabilities through a dedicated portal.

PROTECT

Infrastructure Security

Change Management

The firm maintains change management processes to protect the integrity and availability of the firm's technology products and services, to minimize change-related incidents and improve operational practices.

Production infrastructure changes are managed using firm-approved change management systems and are recorded. Changes must undergo risk assessments, be tested in non-production environments, and verified prior to applying changes to production systems. Testing results must also be recorded.

Firm standards require that changes are recorded and authorized by designated approvers prior to deployment to the production environment.

Change implementations must be verified to ensure only intended changes have been made. The results of the change verification must be documented and retained in firm-authorized change management systems, per the firm's retention policy.

Configuration Management and Hardening

The firm employs configuration management to validate from a security perspective that systems continue to operate consistently in accordance with the Information Security and Cybersecurity Program.

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

The firm issues laptops to a small population of personnel for specific business purposes. All firm issued laptops are encrypted using industry standard tools.

In addition, an inactive screen lock is enforced through configuration policies on firm-administered endpoints.

Network Security

The firm's network environment is designed to prioritize security and resilience, leveraging a tiered architecture separated by firewalls, Intrusion Detection Systems (IDS) deployed at the network perimeter, and other security controls aligned with industry standard practices.

Management interfaces for perimeter firewalls, routers and other devices are not accessible from the Internet. The firm subscribes to continuous Distributed Denial of Service (DDoS) monitoring and mitigation services from multiple providers. The firm also leverages Content Delivery Networks (CDNs) with DDoS mitigation and absorption capacity, implementing request throttling to limit the referrals and requests from IP addresses. Alerts generated by DDoS activity are actively monitored and mitigated as required.

Access to the firm's IT infrastructure is restricted to authorized users and devices and is enforced through secure network access mechanisms such as secure virtual desktops or virtual private network (VPN) solutions.

PROTECT

System Monitoring, Capacity and Vulnerability Management

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

The firm's vulnerability management program includes regular network vulnerability scans of internal and external network environments using industry standard tools. External third parties are also engaged to scan externally facing infrastructure and provide findings on a recurring basis. Vulnerabilities are addressed on a risk-adjusted basis, in accordance with formal standards.

The firm has a defined process for the treatment of discovered vulnerabilities. Criticality ratings are assigned using industry-standard methods and aligned with remediation plans. Where applicable, 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 may evaluate 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, users access virtual desktops hosted in either a GS data center or cloud infrastructure.

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

The firm's virtualized infrastructure is designed to provide similar levels of controls as the firm's on-premises environment, regardless of the user's geographical location. Non-Virtual Desktop models are permitted only on an exception basis, subject to business functions.

End User Device Security

Secure Remote Access for Personnel

Personnel are permitted to use either issued corporate devices or personal devices (Bring Your Own Device - BYOD) when working remotely to securely access firm resources.

The firm employs Mobile Device Management for data loss protection (DLP) and other security controls to protect data on corporate-issued mobile devices. For BYOD, the firm uses Mobile Application Management (MAM) and Mobile Threat Defense (MTD) strategies. These MAM/MTD security controls safeguard firm data within a secure container, which is accessed by appropriately patched and secure personal devices. 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 are permitted for analytic and/or business-related activities, provided they meet the firm's security standards.

Firm mobile applications incorporate multiple security features, including mobile threat defense, device allow-listing, secured network connections, multi-factor authentication, sandboxing, encryption, mandatory device registration, Operating System (OS) patching, verification of non-jailbroken/non-rooted devices, and remote data wiping.

Personnel may also be issued firm-owned devices for specific business purposes. All data on such devices is encrypted both at rest and in transit to support secure remote access and mobile computing.

PROTECT

Client Mobile Applications

The firm has developed mobile applications for clients to securely access accounts, approve transactions, review market news, and securely communicate with firm personnel. These applications follow industry-standard security practices, including multi-factor authentication, biometric authentication, and encryption of data at rest and in transit.

Data Protection

Data Protection

The firm has an enterprise-wide data governance framework that defines how firm, and client data are managed. This includes controlling data quality at the point of origination, aggregation, and publication. The framework assigns accountability for data quality and establishes the structure needed to confirm data is effectively managed as an asset.

In addition, the firm follows a structured approach to classify and handle data according to its sensitivity and criticality. Information is categorized into defined levels (e.g., public, internal, confidential, restricted) and handling requirements are aligned to these classifications.

Data Loss Protection (DLP) controls are implemented and designed to reduce the risk of sensitive information leaving the firm. These controls include proactive alerts that notify senders if an email to an external recipient contains potentially sensitive information, such as personally identifiable information. In addition, the firm employs continuous monitoring and analytics to detect potential data exfiltration or insider threats, leveraging technology to identify unusual patterns of activity while maintaining compliance with applicable privacy and security requirements.

Access to removable storage media, (e.g., USB flash drives, writable CDs and improved local system functionality) is prohibited by default. Where access is approved for specific business purposes, it is strictly controlled, time-bound, and encrypted for Non-public data.

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

Access to selected websites and categories is restricted or blocked based on regulatory, information security, and internal requirements. This includes social networking sites, file-sharing platforms, and webmail.

Global Compliance oversees the firm's electronic communications monitoring and surveillance program, including the review of alerts that may indicate risks such as regulatory non-compliance or breaches of firm policy.

PROTECT

Encryption

The firm's policies and standards establish security principles regarding encrypting sensitive and personal information as well as material non-public information (MNPI). These policies and standards require that sensitive data is encrypted in transit over public networks and, at rest within the firm's environment. Other types of data are encrypted or protected with compensating controls, based on regulatory, security, and contractual requirements/considerations.

The firm mandates the use of industry standard encryption mechanisms, which are documented in formal policy and standard and are reviewed and refreshed on a periodic basis. Firm-standard solutions are available for file encryption between the firm and third parties.

Opportunistic email encryption, such as Transport Layer Security (TLS), is enabled with clients by default. Mandatory email encryption is supported and activated/enabled through mutual agreements.

Key generation and management are handled through firm-standard solutions backed by hardware encryption modules where required by Firm policy. The firm policy requires that access to encryption keys be pre-approved, restricted to authorized personnel. Access is logged and monitored.

Data Security

The firm maintains formal, structured data privacy and security programs that include mandatory controls and processes for applications and assets that store or process sensitive and personally identifiable information. This program is regularly updated to align with applicable laws, regulations, and the firm's internal standards.

The firm enforces clean desk guidelines requiring personnel to maintain clear workspaces free of paper containing sensitive data. The firm has implemented controls to lock user workstations after a defined idle period and personnel are instructed to lock workstations when away from their desks.

The firm maintains controls to securely perform data destruction at the end-of-life systems. The firm has a defined process to identify end-of-life systems, prioritize upgrades or decommissioning, and helps ensure data is destroyed according to defined procedures.

Firm policy requires that retired media are sanitized using a standard set of tools, and that physical media destruction is performed according to pre-defined procedures. Asset decommissioning is managed through defined workflows, including inventory, tracking, and scanning processes.

The firm retains records for various periods to comply with applicable laws, regulations, and internal retention policies.

PROTECT

Physical Security

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 a need-to-have basis, aligned with firmwide access controls, and must be approved by designated access approvers. Access rights are reviewed periodically. Separation of teams and offices is maintained to meet business and regulatory requirements. All entry to data centers and offices is electronically logged via access cards or biometric systems.

Firm procedures require that visitors 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 for monitoring and audit purposes.

Critical data centers are geographically dispersed and on diverse utility and power infrastructure. Security personnel are on duty 24/7, and access is restricted to essential support staff.

Facilities supporting Goldman Sachs businesses are protected from environmental hazards and power outages by the following controls, where applicable: Uninterruptible Power Supply (UPS), surge protection and power conditioning, generators with fuel reserves, HVAC equipment, fire detection and suppression systems, environmental monitoring and alerting (e.g., water detection systems, earthquake-resistant construction and seismic design features).

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

Cloud Security

Cloud Governance

The firm leverages public, private, and hybrid cloud-based solutions where appropriate for compute, storage, and business purposes. A governance process and control framework for cloud-based solutions is maintained and documented in firm standards.

Risk governance is embedded in the firm's global cloud governance framework to support the sustainable deployment and migration of cloud systems, applications, and data across 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 oversight forums responsible for managing processes related to the deployment and implementation of cloud technologies.

PROTECT

Cloud Controls and Assessments

The firm has established controls for cloud solutions, including encryption, strict authentication & role-based access requirements, centralized logging, network segmentation, and auditing. Continuous control monitoring and automated control enforcement gates are leveraged to detect misconfigurations. External compliance activities, such as reviewing SOC reports, are conducted by revenue-producing units to independently assess cloud controls.

Firm policy requires that cloud hosted solutions undergo a risk assessment and architecture review on a risk-adjusted basis using a centralized control inventory. New solutions are required to complete a risk profile to determine regulatory and risk-based requirements.

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

Cloud service providers are subject to vendor management reviews, covering secure service delivery, audit provisions, and adhering to the firm's public cloud control requirements.

Artificial Intelligence Security

Artificial Intelligence Security

Given technological developments in Generative Artificial Intelligence (GenAI) and Large Language Models (LLMs), the firm is carefully assessing its approach to Artificial Intelligence (AI) as it or its third-party vendors, clients or counterparties may develop or incorporate AI technology in certain business processes, services or products.

As such, the firm has a documented policy and a standard governing the use of AI across the firm. The framework leverages a federated model for AI use case development to facilitate synergies between business segments with commercial expertise and platform teams with GenAI expertise.

Formal firmwide and divisional governance and oversight ensures risk mitigation and alignment with business goals, regulatory requirements, firm policies, and investment considerations. Access to external LLMs is intentionally restricted by the firm and cannot be accessed from firm systems or used for business purposes without prior approval.

Enterprise-wide training has been established to educate our people on responsible AI usage and associated risks, including as part of the firmwide Information Security and Cybersecurity annual training. In addition, tailored training is introduced for relevant personnel based on their roles and responsibilities.

PROTECT

Vendor Security

Vendor Security

The Firmwide Vendor Management Policy and Program Lifecycle establishes a risk-based framework for managing third-party and vendor relationships consistent with regulatory guidance and firm policy. Information security risk management is integrated into the vendor management process, covering vendor selection, onboarding, performance monitoring and risk management. Vendors are expected to design, implement, and maintain information security controls that align with the firm's security policies and standards.

Firm policy requires that third parties and vendors accessing Goldman Sachs' sensitive data are required to undergo an initial risk adjusted assessment. Subsequently, the firm conducts re-certifications at a breadth and frequency determined by each vendor's information security rating, per the firm's vendor asset inventory, which is calculated based on several factors, including the type of data stored and processed by a particular vendor.

Assessments may also include the use of external market scoring products to evaluate vendors' internet-facing security posture. Assessments consider the maturity of the vendor's information security, and cybersecurity practices. Gaps identified during due diligence assessments are assigned a risk rating, recorded and remediated in line with the firm's standards.

The firm conducts ongoing oversight of vendors based on the criticality of each vendor's services provided to the firm and the results of the initial risk assessment. Critical vendors receive enhanced focus and due diligence. Changes in the services provided by a particular vendor are identified and reviewed as part of a standard oversight process and may trigger an updated risk assessment before additional services are onboarded. Any vendor material service changes involving classified sensitive data require an updated risk assessment.

Firm policy requires vendors to sign standard contractual provisions before receiving sensitive firm information from the firm. Dedicated teams across the firm are responsible for regular assessments and reporting on vendor information security controls. Periodic reporting of key vendor risk management metrics is provided to business management.

DETECT

Continuous Monitoring

Logging

The firm enables logging in accordance with security standards, including failed logins, administrative activity and change activity. Logs are maintained in accordance with firm policy on records retention and legal and regulatory requirements.

Log file management follows the principle of least privilege. Only application processes have "write" access to log files, System accounts only have "read" access to log files. The firm has controls in place to prevent logs from containing sensitive information such as personally identifiable information (PII), authentication credentials or encryption keys. Security event logging supports system forensic analysis and Technology Risk surveillance. Logs are protected against unauthorized access, modification, or accidental and deliberate overwriting.

Malware Protection

Industry-standard anti-malware software is installed on Windows, Mac, and Linux endpoints as well as on the firm's email infrastructure. Anti-malware alerts are monitored by the firm's staff; when detected, the malware is remediated and if needed, affected systems are rebuilt. Malware signature files are updated on a regular basis regularly through automated system requests.

Runtime checks are performed on specific executables designed to detect and block potential malware. Application allow-listing is deployed to detect, report and prevent the execution of malware.

The firm utilizes an email protection system which is designed to block spam, phishing, and viruses from reaching personnel inboxes. The firm subscribes to an email pre-filtering solution to reduce the amount of malware reaching the firm's email gateway.

The firm mitigates spoofing using 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/review.

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 generate alerts, which are classified, prioritized and assigned to appropriate personnel for timely remediation based on business criticality.

DETECT

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 the firm's control posture. Additionally, the Hunt Team also collects threat intelligence to actively identify potential indications of threat activity across the network.

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

The firm conducts periodic cyber-attack simulations, micro-drills, quarterly drills, and tabletop exercises 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 in place to detect and prevent any unauthorized access to critical systems by third-party service providers.

The firm performs threat intelligence collection to analyze threat actor tactics, techniques, and procedures, supporting the tuning of controls to mitigate emerging threats. In addition, the firm also shares threat intelligence with peer firms to maintain collective risk mitigation and strengthen the security of external connections.

Insider Threat

The firm has an established insider threat program designed to detect and respond to malicious and unintentional or unauthorized activities.

The firm leverages a variety of telemetric, detective and preventive controls including endpoint monitoring and entitlements management to address insider threats.

RESPOND

Incident Management

Security Incident and Problem Management

The Global Cyber Defense and Intelligence (GCDI) team is a firmwide function that is responsible for detecting, investigating, and responding to information security threats and incidents that may impact the confidentiality, integrity, or availability of the firm's information and technology environment.

GCDI maintains procedures to identify and respond to specific information security incidents and collaborates with teams across the firm to contain, mitigate and remediate potential issues. GCDI maintains escalation protocols for appropriately notifying clients, regulators or other parties of security incidents and operates a threat management center 24/7.

The firm maintains an incident and problem management policy and procedures to mitigate risks and protect the firm's production environments, while minimizing business disruption. Standardized procedures are established to support incident management, notification, and post-mortem governance. Security events and information management (SEIM) technology is used to aggregate and correlate platforms, application and infrastructure logging across the firm to track and manage user-reported security events.

Through the global security incident preparedness program, the Technology Risk Division conducts business-focused tabletop exercises with business units and regional teams to assess their processes and readiness, with oversight from the Operational Risk Division. Externally, the firm participates in financial sector and public–private sector cybersecurity exercises and information sharing with other institutions, financial markets and relevant government agencies.

RESPOND

Threat Intelligence

The firm recognizes that cyber threat actors target the firm's networks, vendors, suppliers and personnel, along with the broader financial sector, for a variety of reasons, including conducting fraud, stealing 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 works to protect 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 and business units to reduce or mitigate risks.

Threat intelligence and related cybersecurity trends are sourced from third-party intelligence service providers, industry consortia, internal monitoring, as well as public and government sources.

The identified risks are recorded in a centralized risk register, which captures details such as risk description, potential impact and assigned ownership. The register is periodically reviewed and updated to confirm risks are tracked, prioritized, and managed in line with the firm's risk appetite.

Cyber Insurance

Goldman Sachs maintains a cybersecurity insurance policy that covers the firm's direct costs from a covered security incident including customer notifications and credit monitoring services where necessary. The policy also provides coverage for Business Interruption. The insurance is serviced by consortium providers.

RECOVER

Business Continuity and Technology Resilience

Business Continuity

Goldman Sachs has established a global, structured Business Continuity Planning (BCP) framework to coordinate the firm's response 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 and 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 (BCPs) to address operational disruptions. Each plan must have identified BCP Coordinator(s) responsible for developing and maintaining the plan and ensuring testing requirements are met including return to operation (RTO) and recovery point objectives (RPO), as applicable. BCPs must be reviewed and updated by BCP Coordinators and certified by BCP Owners at the frequency required by firm standards. Under each BCP, the business unit identifies its critical activities, the dependent assets (people, facilities, systems, and third parties), and the potential impact of disruptions.

As part of this process, BCP Coordinators conduct Business Impact Analysis (BIA) to define criticality, recovery objectives, dependencies and recovery strategies of their core processes. These processes determine the type of assurance needed to record completeness through recovery exercises, application failover tests, training and tabletop drills.

The firm's business continuity risk mitigation strategy includes resilience capabilities such as near site, far site, work from home, and dispersed recovery facilities to reduce regional risks. The firm's far site recovery facilities reside on different power and utility grids from primary office locations.

The firm conducts regular preparedness testing, including technology failover, people recovery facilities, and regional handoffs. The firm also participates in industry-level tests with securities exchanges, government agencies, and local authorities. In addition, the firm's also conducts activities including command center drills and automatic notification testing and micro-drills at the division level.

Crisis Management Centers operate 24/7 in every region, monitoring the environment and executing pre-established response protocols in coordination with business units and stakeholders.

Data Backup and Recovery

The firm's data backup and recovery processes are executed using an industry-standard enterprise system. Procedures are in place to identify, escalate and remediate exceptions as needed. Data backups are written on an immutable, disk-based platform for recovery purposes, and periodically data is encrypted and written to tape media for secure off-site storage.

The firm regularly tests the capability of applications to failover to alternative locations as part of the digital resilience testing program. User recovery requests are managed through a streamlined ticketing system and recovery attempts of backed-up data are logged.

In addition, the firm's cloud solutions utilize the backup services provided by their respective vendors to ensure both operational continuity and adherence to regulatory mandates.

RECOVER

Technology Resilience

The firm maintains a technology resilience program to assess whether internal applications and supporting infrastructure demonstrate an appropriate level of resiliency and recovery based on business criticality. Key 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 (aligned with recovery time objectives);
- Inclusion of technology dependencies in applicable business unit plans; and
- Resilience testing.

Based on business requirements, critical applications are deployed and tested across multiple data centers designed to ensure continuous operation in the event of disruption.

The firm also participates in financial industry test initiatives, in jurisdictions where they are offered, to exercise alternative connectivity capabilities and to demonstrate its ability to operate in the event of disruption.

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

Client Information Security Practices

Information security is a shared responsibility that requires cooperation and clear commitments between financial institutions and their clients. While the firm maintains safeguards and provides assurance for the services offered, effective protection also depends on each party adopting industry recognized information security practices in their use of shared data and systems, 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, AICPA SOC reports and ISO 27001;
- Ensuring that only authorized users and systems have access to the firm's data;
- Protecting authentication credentials, e.g., usernames and passwords of users authorized to access the firm's data;
- Protecting computer equipment used in interactions with the firm through anti-malware software, a firewall and up-to-date operating systems;
- Notifying the firm promptly in the event of any actual or suspected compromise of its data or system;
- Establishing a designated person to sponsor and drive information security, ideally from the executive leadership team with the authority to make risk decisions across lines of business and effect change;
- Establishing a governance/oversight process through which the leadership team can determine risk management priorities;
- Retaining a third-party to test security and determine its resistance to common attacks (e.g., perimeter intrusion, malware infections, leakage of sensitive data, social engineering, ransomware). As part of this essential practice, identify internal owners, external partners, law enforcement and other key contacts best positioned to help during a security incident;
- Prioritizing risk mitigations based on criticality;
- Considering the use of managed services to expand security capabilities, including security monitoring, vulnerability scanning, vendor assessments and incident response; and
- Considering commissioning "red team" tests by an independent third-party to evaluate security controls and incident response process