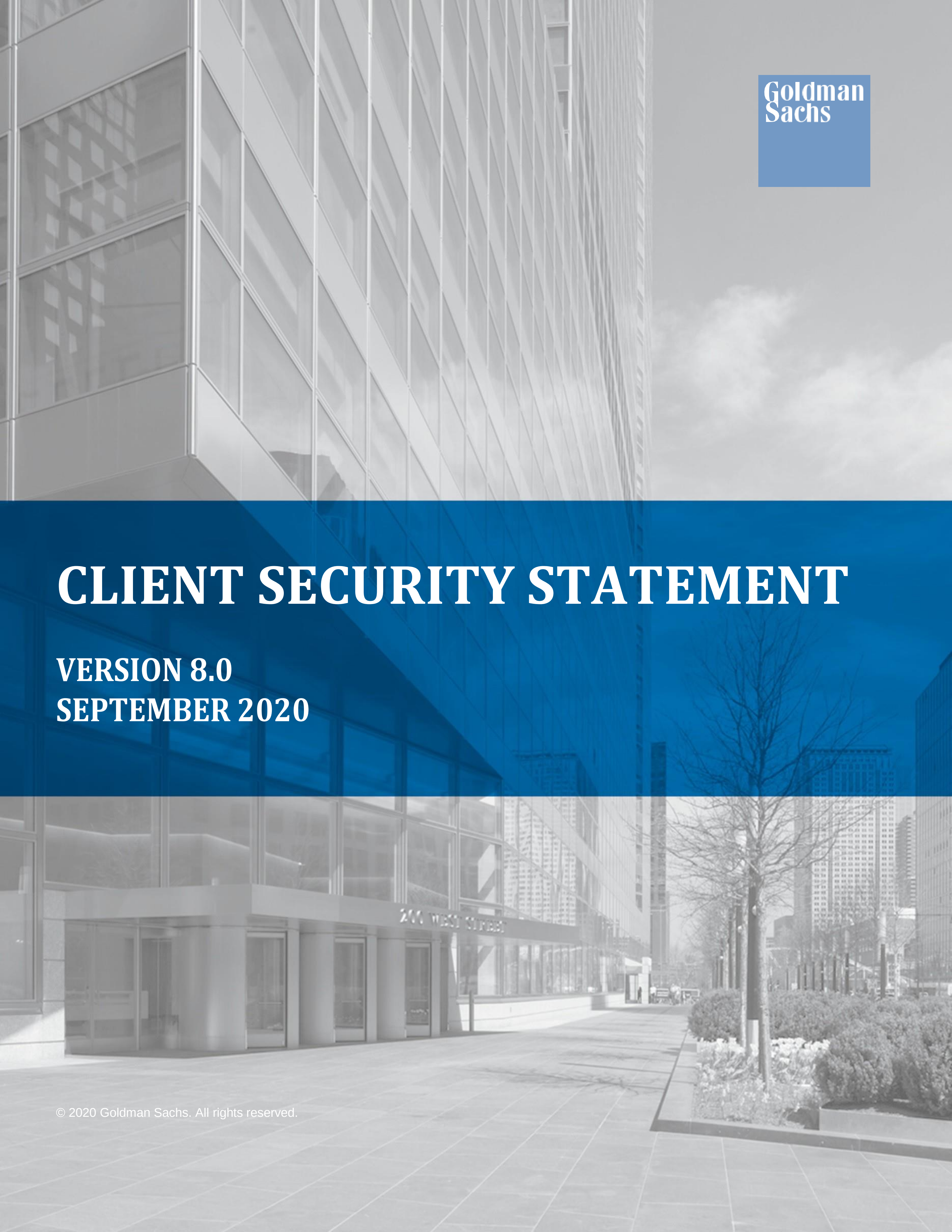

CLIENT SECURITY STATEMENT

VERSION 8.0
SEPTEMBER 2020

Table of Contents

Identify:

Protect:

Detect:

Respond:

Recover:

No part of this material may be (i) copied, photocopied or duplicated in any form 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"). In particular, 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.

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 Financial Sector Cybersecurity Profile.

This document provides an overview of the firm's approach to information security and its practices to secure data, systems and services, similarly aligned around five functions of the NIST CSF:

Identify

- Risk Governance and Regulatory Oversight
  Risk governance and risk management are a function of the firm's management culture, embedded practices and formal oversight. The firm's governance model is achieved by the day-to-day activities of managers and their teams, supported by various working groups and committees.
- Information Security and Cybersecurity Policies and Standards
  The firm maintains a comprehensive set of information security policies and standards to document the firm's approach to compliance with laws, rules, regulations, best practices, and firm management directives.
- Asset Management
  The firm maintains an asset management program to appropriately inventory, classify, and protect applications, data, and hardware.

Protect

- Identity and Access Management
  The firm has implemented controls to identify, authorize, authenticate and manage individuals' access to the firm's systems and information assets.
- Applications and Software Security
  The firm manages application and software security through its software management process which includes a centralized inventory, secure software development practices, vulnerability testing, control monitoring, and logging.
- Infrastructure Security
  The firm protects its infrastructure through a control framework which includes architecture reviews, vulnerability testing, system hardening, and malware protection.
- Data Protection and Data Privacy
  The firm has implemented controls designed to safeguard firm and client information which covers data classification, secure storage, handling, transmission, and destruction.
- Training and Awareness
  The firm provides all employees with annual cybersecurity awareness training and technical training to engineering personnel.
- Mobile Security
  The firm's mobile solutions allow employees to conduct business activities on their personal devices while protecting firm systems and client data.
- Physical Security
  The firm has implemented physical access controls on all firm facilities including office spaces, near site and far site locations, data centers and storage facilities.

- Vendor Security
  Information security risk management is built into the firm’s vendor management process, which covers vendor selection, onboarding, performance monitoring and risk management.

Detect

- Continuous Monitoring
  The firm maintains detective controls at the network, end-point, and application layers to detect anomalous activity potentially indicative of threat activity. The firm further implements continuous control monitoring to assess the adopting and performance of security controls.

- Anomaly Detection
  The firm ensures that security anomalies and events are detected quickly and their potential impact is understood.

- Enforcing Protective Measures
  The firm tests and confirms all protective security measures to verify the effectiveness and coverage.

Respond

- Incident Management
  The firm’s security incident management program enables effective detection and management of security threats and incidents that have a potential impact on the confidentiality, integrity or availability of the firm’s information and technology environment, including notification to clients as required by applicable laws and regulations.

- Response Planning
  The firm incorporates coordinated response planning processes during and after any security incidents, which include managing communications and analyzing the effectiveness of response activities.

Recover

- Business Continuity and Technology Resilience The firm has a mature and comprehensive global Business Continuity Program for Disaster Recovery (BCP/DR). The program covers both business and technology resilience. The main features of the program include dispersed capabilities, near site recovery, far site recovery and dispersed recovery. The description of the firm’s Business Continuity & Technology Resilience Program for Disaster Recovery is available on the firm’s public website.

While information security 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

Risk Governance Framework

- To ensure appropriate risk governance, the firm employs a three-line-of-defense model to provide accountability, oversight and assurance. The model organizes risk management activities across the firm's business units that own and manage risk (first line), independent risk oversight functions (second line), and internal audit (third line).
- Within the first line, the firm's Technology Risk group establishes information security standards and assesses the firm's adherence thereto. The Risk and Compliance Divisions provide independent oversight and challenge functions as the second line. Finally, as discussed below, the firm's Internal Audit independently evaluates the firm's control environment.
- Each of the firm's divisions is ultimately accountable for managing technology risks affecting their applications and other assets.

Governance Committees

- 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 as related to cybersecurity:
- The Firmwide Technology Risk Committee 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 co-chaired by the firm's Chief Technology Officer and Chief Information Security Officer.
- The Firmwide Operational Risk and Resilience Committee is globally responsible for overseeing operational risk and for ensuring the business and operational resilience of the firm.
- 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).

Technology Risk Program

- The firm maintains a Technology Risk Program and associated organization, which consists of a centralized group to establish information security mandates, evaluate adherence thereto, and detect and response to incidents, along with security teams embedded in each of the firm's operating divisions. The program is frequently adjusted to ensure ongoing suitability.
- The Technology Risk Program regularly assessed the sufficiency of the firm's controls. In particular, the Program administers an annual cybersecurity maturity assessment using the industry-standard Financial Sector Cybersecurity program. The Program additionally coordinates quarterly assessments of control efficacy and heightened residual risks through the Risk and Control Self-Assessment program.
- The firm's Chief Information Security Officer ("CISO") is responsible for managing and implementing the Technology Risk Program and reports directly to the co-Chief Information Security Officers.
- As part of the firm's second line of defense, a dedicated team of operational risk specialists provide independent oversight of the Technology Risk Program and assesses the operating effectiveness of the program against industry standard frameworks.
- The written Technology Risk Program is approved by the firm's Board of Directors annually. The Board of Directors 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.

Identify: Information Security and Cybersecurity Policies and Standards

Internal Audit

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

Regulatory Oversight and External Audit

- The firm is regulated by numerous authorities in all jurisdictions in which we operate, including, in the United States, the Federal Reserve System, New York State Department of Financial Services, Commodity Futures Trading Commission, Securities and Exchange Commission, and the Consumer Financial Protection Bureau. The firm is similarly regulated by prudential and securities regulators in each applicable jurisdiction.
- PricewaterhouseCoopers LLP, the firm's external auditor, independently tests applicable controls as part of their audit of the firm's financial statements, the Service Organization Control (SOC) 1 assessments, and their audit of the firm's Business Continuity Program.

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 Financial Systemic Analysis and Resilience Center (FS-ARC), and the Sheltered Harbor initiative.
- The firm additionally participates in industry efforts to manage technology risks, including as coordinated by the Securities Industry and Financial Markets Authority (SIFMA), Asia Securities Industry and Financial Market Authority (ASIFMA), Association for Financial Markets in Europe (AFME), Bank Policy Institute (BPI), and the American Bankers Association (ABA).

Policies and Standards

- The firm maintains a comprehensive set of information security and cybersecurity policies and standards, which take into consideration 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 policy is reviewed annually.
- 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. These documents are subject to a pre-determined review cycle based on the nature and content of the material. Additionally, reviews may be triggered by changes in the risk environment or regulatory landscape.
- 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 International Organization for Standardization (ISO).

Protect: Training and Awareness

- Firm policies and standards are available to all personnel through an internal compendium. These policies cover all aspects of the Technology Risk Program. Topics governed by information and cybersecurity policies and standards include:
  - Identity and Access Management, for example entitlement management and production access
  - Applications and Software Security, for example software change management, open source software and backup and restoration
  - Infrastructure Security, for example capacity management, vulnerability management, network and wireless security
  - Mobile Security, for example Bring Your Own Device (BYOD) and mobile applications
  - Data Security, for example cryptography and encryption, database security, data erasure and media disposal
  - Cloud computing, including governance and security of cloud applications

Protect: Training and Awareness

Training and Education

- The firm maintains a cybersecurity training program, which is designed to help employees and contractors 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 training is required of all firm personnel annually. Additional training is provided for new joiners and individuals transferring within the firm. The firm conducts regular phishing tests on all employees to test employee knowledge about email-based cyber threats and appropriate escalation. The firm also issues guidance and focused training to employees, as needed, in response to specific events or threats.
- Topics in the Firmwide cybersecurity training curriculum include:
  - Information and Cybersecurity Essentials
  - Bring Your Own Device (BYOD)
  - Social Engineering and Phishing
  - Data Risk Management
  - Insider Threat Awareness and Escalation
  - Application Information Security
  - Managing Application Privileges
  - Email and Other Electronic Communication Security
- The firm incorporates training themes based on regulatory guidance, industry best practices, and changes in the risk environment. This includes ongoing social engineering tests where employees receive simulated phishing emails, to gauge awareness and adherence to firm policy.
- The firm additionally provides technical training to engineering personnel via a specialized platform. This training includes topics focused on information security, such as secure coding principles and updates on emerging threats.

Protect: Application and Software Security

User Identity Management

- The firm's access controls are based on the general principles of no privilege without identity, no privilege without approval, need-to-know, least privilege access, and entitlements commensurate with role or job duties.
- The firm performs background checks on employees, consultants and contractors. Where permissible by applicable law, the background check process includes a credit check and a criminal records check. 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 is assigned to every worker. Employees are prohibited from sharing their individual credential information, including usernames and passwords.
- Staff identification badges are issued to all workers when they join the firm.

Entitlements Management

- The firm has a Segregation of Duties program designed to ensure that different people perform different parts of a critical activity.
- 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.
- System entitlements are reviewed by management at least annually on a risk-adjusted basis. More frequent reviews occur for high-risk entitlements. Entitlements are also reviewed when personnel transfer to new roles or departments within the firm.
- 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 Management

- 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, maximum number of unsuccessful login attempts before lockout, a password history and an inactivity lockout.
- Access to client data and 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, time limits on access, Access by technology staff to production systems is limited to authorized individuals, time bound, subject to logging and periodic review, limited to necessary functions and regularly monitored and keystroke logging. Changes made to production environments are subject to mandatory reviews. Each access session requires pre-approval. Access to source code is restricted to authorized personnel and requires approval.
- Activity performed during the production access period islogged and must be reviewed by an authorized individual. Multi-factor authentication is required for remote access to firm systems and for certain client services.

Protect: 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.

Software Development Controls

- The firm has a formal software development lifecycle (SDLC) process documented in written standards and incorporating appropriate control gates.
- 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
  - 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)
- Most applications in use throughout the firm are developed internally. Some applications leverage open source libraries and source code. The same application security standards are applied to internally developed applications, open source software components and third-party software.

Protect: Application and Software Security

Security Testing

- The firm conducts penetration tests, red team, “purple team,” and hunt team assessments to evaluate the security of applications and infrastructure.
- 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 Open Web Application Security Project (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

Protect: Infrastructure Security

Hardware Inventory

- The firm maintains asset information for hardware in managed inventories, which are used to track each asset's attributes and operational status. Each hardware asset is assigned an owner. Inventory management is comprised of manual and automated processes and controls, including periodic reviews, and is governed by policies and procedures.

Configuration Hardening

- The firm has established hardened builds to ensure adoption of standard configuration baselines. All 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.

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.
- Separate Domain Name Service (DNS) servers are deployed for internal and external DNS resolution. The firm's internal DNS namespace is distinct from the external namespace.
- Management interfaces on perimeter firewalls, routers and other devices are not accessible from the Internet. Access to these network infrastructure devices is limited to dedicated management zones.
- The firm subscribes to 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 GS issued laptops and registered employee devices. The firm's guest wireless network does not permit access to the firm's network.

Protect: Infrastructure Security

System Monitoring and Vulnerability Management

- 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 regular basis. Vulnerabilities are resolved on a risk-adjusted basis, as required by a formal standard.
- The firm maintains a bug bounty and responsible disclosure program, which allows researchers to report vulnerabilities in the firm's websites and mobile applications through a dedicated portal.
- 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 timeframe, which are accordingly defined in a firm standard.

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 is enabled through a secure connection to a user's virtual desktop using multi-factor authentication.

Cloud Infrastructure

- 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.
- All utilized of public cloud is required to be approved by a senior governance body.
- Access to the firm's public cloud environments is strictly limited to authorized users.
- The firm has established defined controls for cloud applications, including encryption of data at rest and in transit, firm-controlled authentication, centralized logging, auditing and role-based access to resources.
- Cloud providers are subject to an enhanced vendor management review covering the secure delivery of services, audit provisions, and satisfying the firm's public cloud control requirements.

Protect: Mobile Security

Secure Mobile Access for Employees

- In general, employees use their personnel devices for remote access and mobile computing. Personal devices can only connect to the firm's systems through firm-approved mobile applications. These applications store firm information in secure containers which are segregated from personal information on the devices and encrypted. Any other storage of firm or client information on personal devices is prohibited.
- The firm approved mobile applications allow employees to securely send and receive emails and access internal websites and documents. A limited set of third-party applications allow employees to conduct analytic and/or business-related activity only if they meet the firm's security criteria.
- The firm approved mobile applications utilize a range of security features include:
  - device allow-listing and block-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 when triggered for loss of device or theft

Client Mobile Applications

- The firm has developed mobile applications for clients to access their portfolio data information and market news and to securely communicate with Goldman Sachs employees. Client mobile applications employ additional industry-standard security controls including prohibited local storage and cache clearing.

Protect: Data Protection and Privacy

Data Leakage 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 leakage 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.

Encryption

- The firm encrypts sensitive privacy information in transit and at rest. Other types of data are encrypted or protected with compensating controls based upon particular regulatory, security, and contractual considerations.
- All data stored in the public cloud is encrypted at rest and in transit.
- We use strong industry standard encryption methods and products. 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 possible. Mandatory email encryption is supported and enabled by mutual agreements.
- Access to encryption keys is pre-approved, limited to authorized individuals, time-bound, subject to logging, and is regularly monitored.

Data Security

- The firm has clean desk guidelines which instruct employees to keep the workspace clear of paper containing sensitive data. These guidelines prohibit employees from leaving documents containing sensitive data visible, unlocked or unattended.
- The firm has implemented controls which lock user workstations after a defined idle period. Employees are advised to lock workstations when away from their desk.
- The firm has implemented controls to ensure secure data destruction at the end-of-life of a storage device. Retired media are sanitized using a standard set of tools. Physical media destruction is performed according to pre-defined procedures.

Protect: Data Protection and Privacy

- Asset decommissioning is internally managed through workflow, inventory and scanning processes.
- The firm retains records for various periods as needed to comply with applicable law and regulation and to conform to its internal retention policies.

Data Privacy

- The firm has a formal, structured data privacy 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.

Protect: Physical Security

Physical Security

- The firm has standardized physical security measures in its data centers and offices, including card 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. All data center and office facilities access is electronically logged by card access systems.
- 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 electronically. In addition, enhanced screening of carry-in materials is performed as needed based on the assessment of the existing risk conditions.
- The firm's critical data centers are geographically dispersed and on diverse utility and power infrastructure with no direct dependencies. These facilities have security personnel on duty 24 hours a day.
- The firm's facilities are protected from environmental hazards and power outages by the following controls:
  - Uninterruptible Power Supply (UPS)
  - Generators
  - Air conditioning units
  - Fire detection and suppression systems
  - Water detection systems
  - Earthquake resistant facilities and seismic designs, where applicable
- The firm applies the same physical security standards to all offices globally, including business recovery site locations.

Protect: Vendor Security

Vendor Security

- Third parties are viewed as an extension of the firm. As such, third parties are expected to design and implement controls consistent with the firm's security policies and standards. To understand the extent to which third parties have implemented controls consistent with the firm's requirements, all vendors that handle Goldman Sachs information are required to undergo an initial assessment. Subsequently, the firm conducts periodic assessments based on 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.
- These assessments determine the maturity of vendors' information security and business continuity practices. Gaps found during these due diligence assessments are recorded and tracked to resolution.
- The firm conducts ongoing oversight of vendors based upon 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.
- The firm leverages several types of assessment based upon the criticality of a given vendor, including on-site assessments and the use of third-party services to review vendors' Internet-facing security posture.
- Firm policy requires vendors to sign non-disclosure agreements before receiving sensitive information from the firm. All vendors that store or process sensitive information on behalf of the firm are required to adopt standard contractual provisions with specific information security control requirements.
- A dedicated team is responsible for regular assessment and reporting on vendor information security controls. Vendor information is stored in a central database
- Monthly reporting of vendor risks and vendor review activity are 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.
- Logs do not contain 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 all Windows 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 employee inboxes. The firm maintains a “hunt team” to actively identify potential indications of threat activity across our network.
- 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.

Respond: Security Incident

Security Incident Management

- The firm has a dedicated Security Incident Response Team (SIRT) 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. SIRT 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, SIRT 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.

- SIRT further maintains a dedicated threat management center that operates 24/7. Security intelligence and threat information are obtained from third party intelligence service providers, industry consortia, internal monitoring, as well as public and government sources. “Hunt team” missions are regularly conducted across the firm’s infrastructure to proactively identify any indications of malicious activity.

- The firm recognizes that cyber threat actors target the firm’s networks, vendors, suppliers, and its employees, 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 SIRT 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.

- The firm has implemented a global security incident preparedness program to support security incident management. The program conducts business focused table top exercises with business units and regional teams to assess their processes, understanding and readiness. Externally, the program coordinates firm participation in financial sector and public–private sector cybersecurity exercises to ensure that the firm is well prepared to integrate and coordinate with other institutions, financial markets and relevant government agencies.

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.

Recover: Business Continuity and Technology Resilience

Business Continuity

- The firm's Business Continuity Planning/Disaster Recovery Program comprises six 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 Continuity & Technology Resilience Program for Disaster Recovery is available on the firm's public website.
- Each business unit has a specific Business Continuity Plan (BCP) and assigned BCP coordinator for each operating region. The BCP plans are reviewed and certified quarterly to ensure compliance with firm standards.
- 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.
- The firm conducts periodic resilience impact analyses. Business managers are asked to verify the criticality, recovery time objective, dependencies and recovery strategies of their core processes. These processes determine the type of assurance needed to record completeness; for example: people recovery tests, application failover tests, training, table top drills, etc.
- The firm's business continuity risk mitigation strategy includes near site, far site 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.
- 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

- 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 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
  - 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.

Our Expectations of Your Information Security Practices

Client Information Security Practices

- Information security is everyone's shared responsibility and often involves cooperation between financial institutions and their clients. While we seek to provide as much assurance as possible for the services offered, we do rely on your adoption of standard information security control 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 username and password, 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, identity 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.
  - Consider commissioning "red team" tests from an independent third party to evaluate security controls and incident response processes.