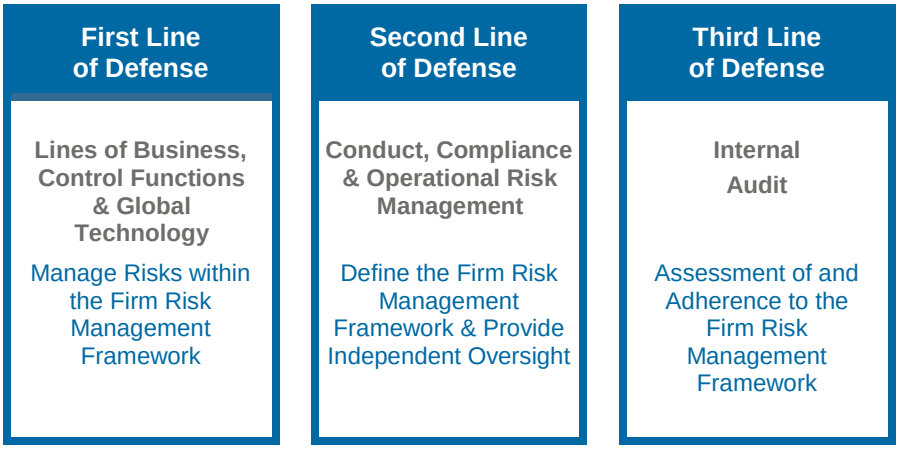
Jason Witty
Managing Director
Global Chief Information Security Officer
Head of Cybersecurity and Technology Controls

Dear Valued Client:

JPMorgan Chase & Co. ("JPMC" or "Firm") maintains a rigorous program to safeguard our clients' information in our care. Our Information & Cybersecurity Program ("Program") is designed to protect the Firm and our clients, support secure delivery of services to our clients, adjust to address the risks presented by an evolving threat landscape, and meet regulatory expectations in the places we operate.

How Our Information & Cybersecurity Program is Designed

Our Program encompasses the governance, policies, processes, assessments, controls, testing, and training efforts required by industry standards and the Firm's regulators. Based on the Financial Services Sector Cybersecurity Profile (FSP), our Risk and Security Policies and Standards provide the Program's foundation and establish the administrative, technical, and physical safeguards for protecting our technology environment, facilities, and client information. Using three lines of defense, the Firm maintains risk assessment and control testing processes to identify, control, measure, monitor, and report information and cybersecurity risks.



Independent Risk Management (i.e. first line of defense), internal auditors (i.e. third line of defense), and external auditors continually review our Program and its processes. Regulators in countries where the Firm operates continually evaluate our Program. As needed, the Firm adjusts the Program based on the following:

- ongoing monitoring of internal and external threats;
- changes in regulations and global standards;
- changes in JPMC business arrangements, client information sensitivity, and information systems;
- results of risk assessments and tests of controls;
- lessons learned from internal and external security and privacy incidents; and,
- information exchange with peers and regulators.

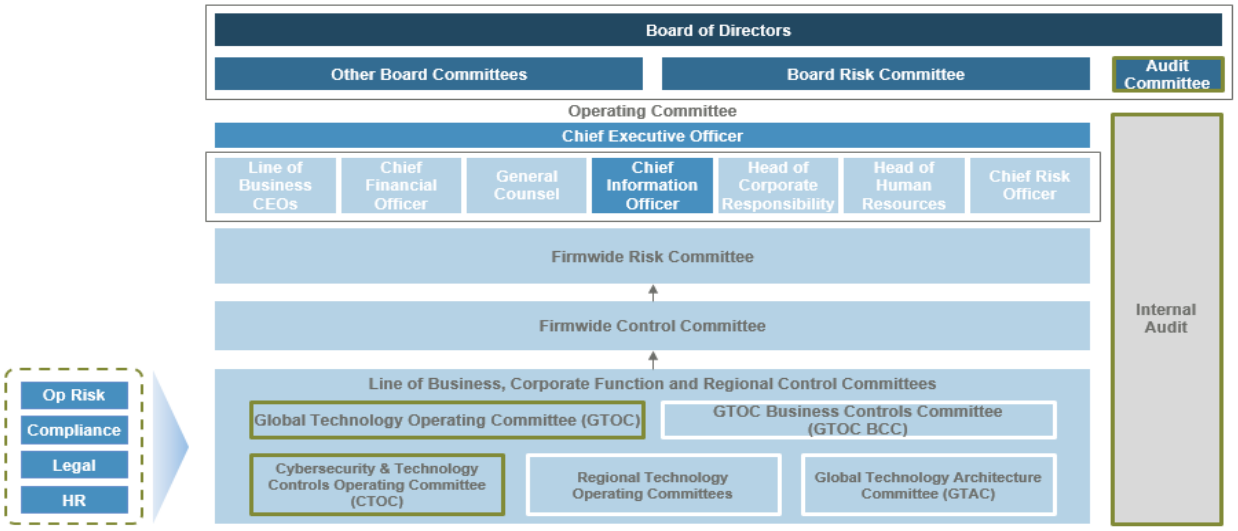
Copyright © 2021 JPMorgan Chase & Co. All rights reserved. This document contains information that is confidential and is the property of JPMorgan Chase & Co. It may not be reproduced, distributed or used, in whole or in part, for any purpose other than as expressly authorized by JPMorgan Chase. All services are subject to applicable laws, regulations and services terms. All trademarks, trade names and service marks appearing herein are the property of their respective owners.

As designed, the Program:

- provides for the security and confidentiality of client and employee information;
- protects against anticipated threats or risks to the availability or integrity of that information;
- safeguards information from unauthorized access;
- supports secure storage, transport, and disposal of client and employee information;
- informs employees about their responsibilities to protect client information and the security of our systems;
- requires our third party service providers adhere to our security policies and standards, as well as applicable regulatory obligations;
- adheres to all customer notification requirements for protecting information; and
- confirms the Firm's resiliency status through regular testing.

How Our Information & Cybersecurity Program is Governed

As illustrated below, JPMC's Board of Directors oversees the Program and leverages the Firm's governance structure to monitor, report, and escalate the status of information and cybersecurity risks. This structure uses key governance forums to disseminate information and monitor Program efforts regularly. Established at multiple levels throughout the Firm, these forums include representatives from each line of business and relevant corporate functions including independent risk management and internal audit. The Board of Directors' Audit Committee reviews and approves the Program semi-annually.



How Our Information & Cybersecurity Program is Implemented

With the accelerating change in technology and an increasingly sophisticated cyber threat landscape, the Program leverages JPMC's Risk Management Framework to systematically and consistently identify, control, assess, measure, treat, and govern information and cybersecurity-related risks. The Program manages existing and emerging risks in a manner consistent with the Firm's risk appetite and tolerance. The Firm implements the Program through the following capabilities, processes, and technology solutions that collectively build, enhance, and sustain strategic information and cybersecurity controls to detect and protect JPMC against information security threats, cyber attacks, and technology failures.

Copyright © 2021 JPMorgan Chase & Co. All rights reserved. This document contains information that is confidential and is the property of JPMorgan Chase & Co. It may not be reproduced, distributed or used, in whole or in part, for any purpose other than as expressly authorized by JPMorgan Chase. All services are subject to applicable laws, regulations and services terms. All trademarks, trade names and service marks appearing herein are the property of their respective owners.

Risk Identification

JPMC maintains a continuous risk identification process to capture and understand significant information and cybersecurity risks and threats to the Firm, clients, and stakeholders through changing business, economic, and operating conditions. As required by Firm Policy, the Program adheres to the JPMC Risk Identification Framework to understand, document, prioritize, and communicate information and cybersecurity-related material risks and how they change over time. The Program's 1st Line of Defense uses business context, threat intelligence, and changes in regulatory requirements to identify risks. These risks are leveraged by Firmwide processes supporting strategic planning, risk appetite management, capital planning, and new business initiative approval.

Control

The Program leverages Firmwide capabilities to ensure the appropriate policies, standards and control procedures are established and maintained. Information and Cybersecurity Program controls and objectives are identified and defined in Firm Policy and its supporting Standards and Control Procedures. Collectively, these policies provide requirements for key elements of the design, build, and operations of the Program's capabilities. The Policy, Standards, and Procedures are informed by threat intelligence, regulatory requirements, industry frameworks, and lessons learned. Firm Policy and Standards are reviewed and approved annually. The following table summarizes Program capabilities:

CAPABILITY	DESCRIPTION
Physical Security	The Firm maintains physical security controls designed to protect employees, clients and our assets from external and internal threats. These include controls to restrict physical access and conduct surveillance monitoring at JPMC locations including data centers and computer facilities that contain critical systems and confidential information.
Asset Management	The Firm maintains an inventory of all assets that contain consumer and client non-public information, including policies to govern the inventory and classification of assets both at inception and throughout their life cycle, and wherever the assets store, transmit, or process data. Technical assets are reviewed as part of the Application Risk Classification process to classify the sensitivity and criticality of applications.
Security Configuration	Leveraging industry security standards, the Firm's Security Configuration capability establishes controls for securing technology assets by defining secure configurations, or baselines, and associated deployment patterns (e.g., segregation of systems, environments, network zones). This capability enables security controls to detect and prevent malware and malicious activity on endpoints within the JPMC network.
Vulnerability Management	JPMC Vulnerability Management capability establishes controls for the prevention, detection, and remediation of vulnerabilities through assessments and exercises. The Vulnerability Management and Assessments Team (VM&A) determines exposure to current cyber threats by identifying and providing remediation oversight of vulnerabilities found throughout JPMC's Technology estate. The goal for the VM&A Team is to ensure vulnerabilities are identified and addressed quickly and efficiently, using a risk-based approach, to help maintain the security of our network, applications, and data for the Firm and our clients.
Workforce Screening & Investigations	JPMC understands that threats can originate from inside the Firm too. To address insider threats, the Firm's employee and new hire screening process include fingerprinting and background checks on all U.S. based employees as well as those who are responsible for, or have access to, JPMC client information, premises, or systems. Additionally, the Firm's Global Security group examines internal and external fraud incidents that include employee wrongdoing, to identify not only root causes and impact but also corresponding remediation solutions.

Copyright © 2021 JPMorgan Chase & Co. All rights reserved. This document contains information that is confidential and is the property of JPMorgan Chase & Co. It may not be reproduced, distributed or used, in whole or in part, for any purpose other than as expressly authorized by JPMorgan Chase. All services are subject to applicable laws, regulations and services terms. All trademarks, trade names and service marks appearing herein are the property of their respective owners.

CAPABILITY	DESCRIPTION
Identity & Access Management	The Global Identity & Access Management Program implements access standards and controls across our infrastructure and applications, including those that contain client information. These controls are designed to authenticate users, ensure authorized access, enforce consistent administration procedures, maintain segregation of duties, and ensure timely changes through on-boarding, transfer, and termination processes for Firmwide information systems. Controls include dual approvals for privileged access and separation of approval and fulfilment for the same access request.
Data Protection	The Data Protection Program establishes controls to protect firm data including client and employee personal information. The Program is responsible for designing and governing controls to ensure confidentiality, integrity, and availability of data throughout its lifecycle from collection to disposal. Through these efforts, the Program helps prevent the unauthorized disclosure or loss of this data and supports data integrity needs.
Security Operations	The JPMC Cybersecurity Operations function is a combined Intelligence, Operations, and Assessment organization. The team is dedicated to identifying and protecting against cyber-related threats as well as anticipating and responding to cybersecurity incidents, while complying with the Firm's information security requirements. The team provides follow-the-sun coverage with seamless integration across the New York, London and Singapore Cybersecurity Operations Centers, and various other locations globally.
Technology Development	The Technology Development capabilities establish controls for maintaining the technology architecture including the secure design, build, test, and deployment activities of the Software Development Lifecycle.
Technology Operations	Technology Operations establishes controls for technology change management, request fulfilment, capacity management, service level management, operational backup, standard operating procedures, and support of JPMC technology resources. This capability supports JPMC Data Center management requirements. It focuses on consistent, reliable technology quality of service while minimizing adverse impact to business operations and maximizing the productivity of JPMC resources.
Records Management & Disposal	The Firm's Centralized Records Management Program controls retention and destruction of the Firm's records and data based on regulatory and legal requirements. The Program governs adherence to these requirements by lines of business and corporate functions.
Business Resiliency	The Firmwide Business Resiliency Program supports an integrated, risk-based approach to safeguard delivery of services to clients and partners in line with their requirements and the Firm's business strategy and principles. Our resiliency capabilities incorporate crisis management processes to support responses to global, regional, and local crises across all hazards. In partnership with senior leaders and teams from the lines of business and corporate functions, the Technology Resiliency Program supports Firmwide resiliency efforts by providing governance and oversight of the Firm's application and data center resiliency status that is confirmed through a test strategy that includes scenario-based testing. In all regions, JPMC participates in externally-led sector-wide cybersecurity exercises with other public and private sector entities. Lessons learned from test activities are provided to management with root cause analysis and recommendations to improve overall resiliency.
Incident Management	The Firm maintains a centralized Incident Management process for information and cybersecurity incidents that require external engagement. The process focuses on institutionalizing coordination, communication, and escalation activities for internal and external stakeholders to ensure effective and timely issue resolution. Our process covers internal and external engagements with our line of business partners including regulatory, compliance, privacy, and media communications.

Copyright © 2021 JPMorgan Chase & Co. All rights reserved. This document contains information that is confidential and is the property of JPMorgan Chase & Co. It may not be reproduced, distributed or used, in whole or in part, for any purpose other than as expressly authorized by JPMorgan Chase. All services are subject to applicable laws, regulations and services terms. All trademarks, trade names and service marks appearing herein are the property of their respective owners.

CAPABILITY	DESCRIPTION
Third Party Oversight	The Firm's Corporate Third Party Oversight (CTPO) function identifies, controls, assesses, measures, treats, and governs risk from third-party suppliers. An Initial Supplier Control Assessment is required at onboarding for new critical, high, and medium risk engagements and aligned supplier-hosted applications. The resulting control effectiveness rating provides a view of the supplier's control environment to help make an informed decision regarding supplier selection and use of the standard Master Service Agreement. Subsequent periodic supplier control assessments, executed based on inherent risk rating, provide a view into instances where control effectiveness may have changed. The function leverages the Firm's Global Technology Standards for Technical Assessments and additional cybersecurity monitoring is executed in partnership with Security Operations where appropriate. The Firm's threat intelligence capabilities include continuous monitoring and intelligence collection for our most critical third parties in order to assess cyber threats posed to the Firm through these engagements.
Training & Awareness	The Firm maintains formal Training and Awareness Programs focused on privacy and information and cybersecurity tenets of maintaining data confidentiality, integrity, and availability. These Programs include training that reinforces the Firm's Policies and Standards including responding to unauthorized access to or use of information. Additionally, they offer live, virtual, and computer-based training on how to identify potential information and cybersecurity risks and protect the Firm's resources and information. This training is mandatory for all employees globally on a periodic basis, and it is supplemented by Firmwide testing initiatives, including regular phishing tests.

Assess & Measure Risk

The Firm assesses and evaluates the adequacy and effectiveness of Program controls via manual or automated processes. Processes, risk, and controls are defined in alignment with firm taxonomies and recorded in approved systems of record. Program control objectives are evaluated by the Firm's risk assessment processes and tests of controls in accordance with their risk-based methodologies and frequencies. Metrics are maintained to measure material risks and the effectiveness of key controls in accordance with Firm Standards for Operational Risk Metrics.

Risk Treatment

The Program monitors and manages risk exposure through prioritized remediation efforts. As required by Firm Policy, issues resulting from a control gap or weakness identified by the 1st Line of Defense, Independent Risk Management, Internal Audit, and Regulators are recorded in the Firm's approved system of record. Risk Treatment Plans to remediate or accept the risk are approved and monitored regularly for completion with significant delivery issues escalated for senior management attention.

Our Evolving Technology Landscape

JPMC employs approximately 50,000 technologists globally and invests more than $12 billion annually in technology to better serve our clients. This investment reinforces our Firmwide strategy to leverage emerging technologies to drive innovation and accelerate time to market for new products and services while continually advancing our cyber defenses to remain ahead of the threat and support business resiliency needs. These emerging technologies include Artificial Intelligence, Machine Learning, Blockchain and Distributed Ledger Technology (DLT), Intelligent Automation, and Robotics.

At JPMC, we are executing a multi-cloud approach, working with Amazon, Google, and Microsoft in addition to running our private cloud. Security of the cloud and security in the cloud are foundational tenets for our Cloud Strategy. An application hosted in the cloud – whether public or private – needs to meet all the

Copyright © 2021 JPMorgan Chase & Co. All rights reserved. This document contains information that is confidential and is the property of JPMorgan Chase & Co. It may not be reproduced, distributed or used, in whole or in part, for any purpose other than as expressly authorized by JPMorgan Chase. All services are subject to applicable laws, regulations and services terms. All trademarks, trade names and service marks appearing herein are the property of their respective owners.

security and regulatory standards required of an application hosted on premise in addition to controls required to manage the cloud. The Firm has implemented a comprehensive governance structure to manage the migration of applications to the public cloud. This includes rigorously building and testing our security and resiliency controls before migration.

We Are an Industry Leader

The Firm continues to devote significant resources to collaborate with peers and innovators, strengthen our partnerships with appropriate government and law enforcement agencies, and drive public-private initiatives in order to understand the full spectrum of cybersecurity risks in the operating environment, enhance defenses, and improve resiliency against cybersecurity threats. The Firm partners with law enforcement, government officials, and peer and industry groups to address cybersecurity risks. We are a leader in the Financial Services Information Sharing & Analysis Center (FS-ISAC), which is an intelligence-sharing cooperative for the financial services sector. Our firm also helped drive the creation of the Analysis and Resilience Center (ARC) for Systemic Risk. Formerly known as the Financial Systemic Analysis and Resilience Center (FSARC), ARC is an industry-funded nonprofit whose mission is to increase the resilience of the systems that underpin the U.S. financial services sector. JPMC is also a leader in the Cyber Risk Institute (CRI), which is non-profit industry coalition that promotes enhancing cybersecurity and resiliency through standardization. CRI maintains the Financial Services Sector Cybersecurity Profile (FSP) tool used by firms to benchmark their cybersecurity and resiliency capabilities. The FSP is curated from the intersection of global regulations and cyber standards, such as those maintained by the International Standards Organization (ISO) and the US National Institute of Standards & Technology (NIST).

Information and Cybersecurity is a Shared Responsibility

At JPMC, we take seriously our role in protecting our clients' data and implementing the Program's capabilities, processes, controls, and technology solutions to safeguard it. However, even the best security measures can only be effective to ensure data security if our clients are also vigilant about employing the necessary safeguards to protect their information – a shared responsibility we look forward to advancing together.

Thank you for your continued confidence in JPMorgan Chase & Co. We appreciate the partnership with you.

Jason Witty
Managing Director
Global Chief Information Security Officer
Head of Cybersecurity and Technology Controls

Copyright © 2021 JPMorgan Chase & Co. All rights reserved. This document contains information that is confidential and is the property of JPMorgan Chase & Co. It may not be reproduced, distributed or used, in whole or in part, for any purpose other than as expressly authorized by JPMorgan Chase. All services are subject to applicable laws, regulations and services terms. All trademarks, trade names and service marks appearing herein are the property of their respective owners.