JPMorgan Chase & Co.

Cyber Risk Taxonomy

Prepared by: Arnav Sahai

Course: INAF U6524 – Cybersecurity and Business Risk

Instructors: Prof. Neal A. Pollard and Prof. Matthew Devost

Institution: Columbia University, School of International and Public Affairs (SIPA)

Date: 25 April 2026

Table of Contents

Abstract

JPMorgan Chase & Co. (JPMC) is the largest bank in the United States by assets and one of the world's most systemically important financial institutions (SIFIs), with total assets of $4.0 trillion[1], over 317,000 employees in more than 100 countries, and 2024 net revenues of $177.6 billion[2]. As CEO Jamie Dimon[3] has repeatedly stated, "the threat of cybersecurity may very well be the biggest threat to the U.S. financial system"—a warning he reiterated in his 2026 shareholder letter, naming cyber the single highest risk facing the bank.

JPMC faces an extraordinary threat environment. The firm reports fending off approximately 45 billion[4] daily events processed through its monitoring infrastructure, spends over $15 billion[5] annually on technology (including cybersecurity), and employs 62,000 technologists. Its hybrid multi-cloud architecture spans 32 global data centers and all three major public cloud hyperscalers. The Firm's Kinexys[6] (formerly Onyx) digital assets platform facilitates over $1 billion in daily blockchain-based transactions, while JPM Coin now operates on public blockchain

---

[1] JPMorgan Chase & Co. (2025). JPMorgan Chase & Co. 2024 Form 10-K. U.S. Securities and Exchange Commission. https://www.sec.gov/Archives/edgar/data/19617/000001961725000270/jpm-20241231.htm
[2] JPMorgan Chase & Co. (2025). 2024 annual report. https://www.jpmorganchase.com/content/dam/jpmc/jpmorgan-chase-and-co/investor-relations/documents/annualreport-2024.pdf
[3] Evolution Equity Partners. (2026, March). JPMorganChase CEO warns of rising cyber risk. https://www.linkedin.com/posts/evolution-equity-partners_jamie-dimon-chairman-and-ceo-of-jpmorganchase-activity-7437136166161694
[4] Fanatical Futurist. (2024, March). JPMorgan fights 45 billion hacking attempts each day with $15 billion budget. https://www.fanaticalfuturist.com/2024/03/jpmorgan-fights-45-billion-hacking-attempts-each-day-with-15-billion-budget/
[5] CodeLock. (2024). JPMorgan's $15 billion battle in cybersecurity. https://www.codelock.it/news/jpmorgans-15-billion-battle-in-cybersecurity
[6] JPMorgan Chase & Co. (n.d.). JPM Coin — Kinexys digital payments. https://www.jpmorgan.com/kinexys/digital-payments/jpm-coin

infrastructure[7]—dramatically expanding the attack surface. In October 2025, JPMC launched a $1.5 trillion[8] Security and Resiliency Initiative, committing up to $10 billion in direct equity investments in cybersecurity, quantum computing[9], AI, and critical infrastructure.

[7] MEXC. (2026, April). Inside JPMorgan's plan to take on blockchain rivals. https://www.mexc.com/news/1010105
[8] JPMorgan Chase & Co. (2025). JPMorgan Chase security and resiliency initiative. https://www.jpmorganchase.com/newsroom/press-releases/2025/jpmc-security-resiliency-initiative
[9] J.P. Morgan. (2025, November). Unlocking quantum technology's potential. https://www.jpmorgan.com/insights/technology/unlocking-quantum-technologys-potential

Risk Severity Key

All risks in this taxonomy are assigned a color-coded rating based on the combination of Likelihood and Impact, following the qualitative risk matrix defined in Section III. The four color tiers are:

RED (Critical): High Likelihood x High Impact, Requires immediate escalation to Board Risk Committee and CISO.

ORANGE (High): Any combination yielding High Risk Priority — High Likelihood x Medium Impact, or Medium Likelihood x High Impact. Requires senior leadership review within 30 days.

YELLOW (Medium): Medium Likelihood x Medium Impact, High Likelihood x Low Impact, or Low Likelihood x High Impact. Requires quarterly risk review and monitoring.

GREEN (Low): Low Likelihood x Medium Impact, or Medium Likelihood x Low Impact. Managed through standard controls and annual review.

Minimal Priority: Low Likelihood x Low Impact.

This taxonomy is organized around five primary risk categories — (I) Business Disruption & Operational Resilience, (II) Data Theft & Fraud, (III) Competitive Disadvantage & IP Theft, (IV) Regulatory & Legal Compliance, and (V) Emerging Technology Risks — each analyzed by threat actor, crown jewel assets targeted, scenario, CIA triad impact, qualitative risk rating, controls, and residual risk. A final section addresses interacting risks and risk governance.

I. Firm Overview and Critical Asset Inventory ("Crown Jewels")

Business Lines

JPMC operates four principal business lines, each with distinct cyber exposure profiles:

Business Line	2024 Revenue	Key Digital Dependencies
Consumer & Community Banking (CCB)	$71.5B	Mobile/online banking for 84.4M consumers, 57.8M active mobile users, Chase.com, card processing
Commercial & Investment Bank (CIB)	$70.1B	Trading platforms (Fixed Income, Equity Markets), SWIFT, payment rails, prime brokerage, and clearing
Asset & Wealth Management (AWM)	$21.6B	Client portals, $4T AUM data, trading algorithms, custody systems

Corporate / Treasury	$17.4B	Internal IT infrastructure, financial reporting, and regulatory reporting systems

Crown Jewels — Most Valuable Data and System Assets

A "crown jewel" is the data, process, or system whose compromise would cause the most severe harm to JPMC's operations, finances, or reputation. For JPMC, crown jewels span five categories:

1. **Customer Financial Data (PII + Account Data):** Names, Social Security numbers, account numbers, card data, transaction histories, and credit profiles of 84+ million consumer customers and 7+ million small businesses. Compromise triggers immediate regulatory, legal, and reputational consequences.

2. **Proprietary Trading Algorithms and Market Data:** The logic and parameters behind JPMC's market-making, high-frequency trading, and algorithmic execution platforms across Fixed Income ($20B revenue) and Equity Markets ($9.9B revenue). Theft grants competitors — or adversaries — the ability to front-run or destabilize JPMC's market positions.

3. **Payment and Settlement Infrastructure:** Systems supporting $6.4 trillion in annual payment transaction volume, SWIFT connectivity, ACH, FedNow, Fedwire, Kinexys blockchain payment rails, and JPM Coin — the real-time blockchain payment token now processing transactions on public blockchain infrastructure. Disruption halts cross-border settlement globally.

4. **Client Institutional Data and Deal Intelligence:** M&A advisory, underwriting, private equity, and debt/equity capital markets deal data belonging to the bank's global corporate clients. JPMC holds a 9.3% global Investment Banking fee wallet share; leaked deal intelligence would be enormously valuable to competitors and nation-states

5. **Core Banking Technology Infrastructure:** The hybrid multi-cloud ecosystem spanning 32+ global data centers and three hyperscalers, private cloud platforms, and the roughly 17 planned "highly automated" strategic data centers. Failure of this layer cascades across all business lines.[

6. **Authentication and Identity Infrastructure:** Credentials, PKI certificates, and IAM (Identity and Access Management) systems that gate access to all crown jewels above. Compromise of these systems — known as "skeleton keys" — unlocks all other assets simultaneously.

7. **Kinexys / Digital Assets Platform:** Private permissioned blockchain for institutional clients and the emerging JPM Coin on public blockchains, representing JPMC's exposure to the $13 trillion tokenized[10] asset market. Smart contract logic and private key management are uniquely irreversible if compromised.

[10] The Wall Street Journal. (2025, December). JPMorgan steps further into crypto with tokenized money fund. https://www.wsj.com/finance/investing/jpmorgan-steps-further-into-crypto-with-tokenized-money-fund-e3535f13

II. Threat Actor Profiles

JPMC faces a threat actor landscape unlike any other industry. The following four categories represent the most significant adversaries, ordered by sophistication:

Nation-State Actors

The most sophisticated and best-resourced adversaries. Russia, China, Iran, and North Korea are the primary state-level threats to U.S. financial institutions, as confirmed by the Director of National Intelligence. Motivations span financial theft (particularly North Korea's Lazarus Group targeting SWIFT and bank accounts), economic espionage targeting proprietary trading data and deal intelligence, and pre-positioned destructive capabilities intended to cause systemic financial instability as a form of coercive statecraft. JPMC, as the largest U.S. bank and a key node in global payment infrastructure, is a persistent, high-priority intelligence collection target.

Criminal Organizations

Financially motivated criminal syndicates constitute the most frequent day-to-day threat. Their TTPs include ransomware (the finance industry saw a 64% spike in ransomware attacks in recent years), phishing at scale, credential stuffing, BEC (Business Email Compromise), card skimming, and purchase of access credentials on dark-web marketplaces. Criminal groups increasingly operate as organized enterprises — offering "Ransomware-as-a-Service" — and leverage generative AI to produce more convincing phishing lures at a massive scale.

Insider Threats

JPMC defines insider threat[11]s as "the intentional or unintentional misuse of legitimate access to systems, data, or facilities by workforce members, such as employees or contractors". The firm's 317,000+ global employees, many with broad privileged access, represent an unavoidable internal threat surface. Insider incidents include data exfiltration (employees leaving for competitors), fraud enabled by system access, accidental data exposure, and supply chain compromise through disgruntled third-party personnel. The 2014 breach[12] — in which hackers ultimately accessed data from 83 million accounts — exploited inadequately protected credentials, a reminder that access management failures are existential

Hacktivists and Ideological Actors

Groups such as Anonymous, Killnet, and others target financial institutions for political or ideological reasons. Common TTPs are DDoS attacks aimed at disrupting public-facing services, website defacement, and data leaks timed to maximize media impact. Geopolitical events — sanctions, controversial investment decisions, or political statements — increase hacktivist targeting of institutions like JPMC.

[11] JPMorgan Chase & Co. (n.d.). Insider threats: Public guidance document. https://www.jpmorganchase.com/content/dam/jpmorganchase/documents/about/insider-threat-external.pdf
[12] McGrath, M. (2014, October 2). JP Morgan says 76 million households affected by data breach. Forbes. https://www.forbes.com/sites/maggiemcgrath/2014/10/02/jp-morgan-says-76-million-households-affected-by-data-breach/

Third-Party and Supply Chain Actors (Substandard Products and Services)

Not a single adversary but a systemic vulnerability: JPMC operates within an ecosystem of thousands of vendors, cloud providers, fintech integrators, and data processors. Third parties accounted for 30% of data breaches in 2024, a 15% increase from 2023. JPMC CISO Patrick Opet[13] publicly warned that the widespread adoption of SaaS has "eroded traditional security boundaries" and created "compounded risks" from third-party vendors. The SitusAMC[14] breach in 2025 — which exposed mortgage data across JPMC, Citi, and Morgan Stanley — exemplifies this vector.

[13] CEFPro. (2025). JPMorgan CISO urges software vendors to prioritize security over features. https://connect.cefpro.com/article/view/jpmorgan-ciso-urges-software-vendors-to-prioritize-security
[14] CSO Online. (2025, November). JPMorgan, Citi, Morgan Stanley assess fallout from SitusAMC data breach. https://www.csoonline.com/article/4095182/jpmorgan-citi-morgan-stanley-assess-fallout-from-situsamc-data-breach.htm,l

III. Measurement of Risk — Methodology

Qualitative Risk Matrix

Given the inherent difficulty of constructing actuarial-style quantitative models for cyber risk, this taxonomy employs a standardized qualitative approach informed by frameworks from Touhill, NIST CSF 2.0, and the sample taxonomies from Coinbase and DoorDash provided as course materials. Consistent with the Coinbase taxonomy model, the following definitions apply:

Likelihood (probability within a 12-month period):

- **Low:** < 33% chance of occurrence
- **Medium:** 34–66% chance of occurrence
- **High:** > 67% chance of occurrence

Impact (business consequence if event occurs):

- **Low:** Manageable financial loss, no material customer harm, no regulatory breach
- **Medium:** Significant financial cost and/or reputational harm, < 50% of customer data or systems affected; potential regulatory scrutiny
- **High:** Severe financial loss, systemic disruption, > 50% of critical assets affected, major regulatory action or systemic financial stability concern

Risk Priority = Likelihood × Impact, visualized in the heat map below:

	Low Impact	**Medium Impact**	**High Impact**
High Likelihood	Medium Priority	**High Priority**	**Critical Priority**
Medium Likelihood	Low Priority	Medium Priority	**High Priority**
Low Likelihood	Minimal Priority	Low Priority	Medium Priority

Quantitative Supplementation

Where available, annualized loss estimates reference industry benchmarks. The average cost of a financial sector data breach was $6.08 million per incident (IBM Cost of a Data Breach Report 2024). JPMC's 2024 10-K reports $1.4 billion in operating losses — a category that includes cyber incident costs — up from $1.2 billion in 2023. For individual scenario estimates below, expected loss figures are illustrative ranges grounded in industry precedent, not actuarial certainties — reflecting the inherent limitation that "cyber risks have notoriously defied most attempts to quantify and model probabilities."

IV. Risk Category I — Business Disruption & Operational Resilience

These risks threaten the **availability** of JPMC's critical systems and services, affecting the firm's ability to operate, settle transactions, and serve clients.

Risk BD-01: Ransomware Attack on Core Banking Infrastructure

Field	Detail
Risk ID	BD-01
Crown Jewel Targeted	Core banking technology infrastructure; payment settlement systems
Threat Actor	Criminal organizations; nation-state actors (North Korea/Lazarus Group)
CIA Impact	Availability (primary); Integrity (encryption of files)
Likelihood	High
Impact	High

Risk Priority	**Critical**

Scenario: A criminal group or nation-state actor deploys ransomware after achieving initial access via a compromised SaaS vendor or spear-phishing campaign targeting a privileged user. Ransomware encrypts critical files across trading and payment systems, rendering JPMC unable to execute trades, settle transactions through SWIFT, FedNow, or Fedwire, or process card payments. The attack may be paired with a simultaneous DDoS on public-facing customer portals (a "double disruption" tactic). The finance industry saw a 64% spike in ransomware attacks in recent years.

Business Impact: Halt of $6.4 trillion in annual payment transaction volume operations; trading desk shutdowns; inability to post collateral; cascading disruption to counterparties globally. Direct financial losses (remediation, ransom demand, SLA penalties) in the hundreds of millions. Regulatory scrutiny from OCC, NYDFS, Federal Reserve, and DORA in Europe.

Estimated Loss Range: $250M–$1B+ (remediation, lost revenue, regulatory fines, reputational damage)

Primary Controls:

- Immutable offline backups with tested recovery time objectives (RTO < 4 hours for critical systems)
- Network micro-segmentation to limit lateral movement post-breach
- Privileged Access Management (PAM) to restrict the blast radius of compromised admin credentials

- Zero Trust[15] Architecture (never trust, always verify), which JPMC has adopted firmwide
- AI-powered anomaly detection on network traffic to detect ransomware staging behavior before encryption begins
- Endpoint Detection and Response (EDR) across all enterprise endpoints (now mandated by NYDFS Part 500[16])

Risk Response: Mitigation (primary); Transfer (cyber insurance); Acceptance of residual disruption risk

Risk BD-02: DDoS Attack on Retail Banking and Digital Customer Channels

Field	Detail
Risk ID	BD-02
Crown Jewel Targeted	Consumer digital banking infrastructure (Chase.com, mobile app); 70.8M active digital customers
Threat Actor	Criminal organizations; hacktivists; nation-state actors

[15] CrossClassify. (n.d.). Zero trust architecture and modern AI cybersecurity. https://www.crossclassify.com/resources/articles/zero-trust-architecture-and-modern-AI-cybersecurity/
[16] Beyond Identity. (2025). NYDFS Part 500 in 2025: Key deadlines, new requirements, and compliance strategies. https://www.beyondidentity.com/resource/nydfs-part-500-in-2025-key-deadlines-new-requirements-and-compliance-strategies

CIA Impact	Availability
Likelihood	High
Impact	Medium
Risk Priority	**High**

Scenario: A botnet-powered Distributed Denial of Service (DDoS) attack floods Chase.com and the Chase mobile app with illegitimate traffic, rendering these services inaccessible to 70.8 million active digital customers. Simultaneously, the DDoS serves as a distraction (a "smoke screen") while a separate intrusion attempt targets back-end payment systems or customer data. Hacktivist groups (e.g., Killnet, Anonymous Sudan) have repeatedly targeted major banks using this tactic in response to geopolitical events such as U.S. sanctions.

Business Impact: Customer's inability to access accounts, make payments, or apply for credit. Reputational damage and customer churn. Regulatory notification obligations under NYDFS Part 500 (72-hour notification requirement). Potential downstream fraud as attackers exploit the diversion.

Estimated Loss Range: $10M–$100M per incident (depending on duration; JPMC's card transaction volume alone is $1.8T annually)

Primary Controls:

- Scrubbing centers and Content Delivery Networks (CDNs) to absorb volumetric DDoS traffic

- Partnerships with Cloudflare and cloud hyperscalers to dynamically expand network capacity under attack
- Real-time traffic monitoring with automatic failover to alternate regions across JPMC's multi-cloud infrastructure
- Playbook-tested DDoS response procedures, including customer communication protocols
- Rate limiting, CAPTCHA challenges, and geofencing on high-risk traffic sources

Risk Response: Mitigation (primary); Transfer (third-party DDoS mitigation services)

Risk BD-03: Cloud Provider Concentration Failure / Third-Party Outage

Field	Detail
Risk ID	BD-03
Crown Jewel Targeted	Core banking infrastructure; trading systems; digital banking platforms
Threat Actor	Substandard products/services; natural/physical disasters; nation-state supply chain compromise
CIA Impact	Availability
Likelihood	Medium

Impact	High
Risk Priority	**High**

Scenario: A single cloud hyperscaler (AWS, Azure, or Google Cloud) experiences an extended regional outage — whether from a cyberattack on the provider, a software fault, or physical infrastructure failure — causing cascading failures across JPMC's workloads hosted there. JPMC's CISO and CIO have explicitly flagged concentration risk as a top concern: "If a cloud provider had an outage, the financial services industry cannot be impacted by that — it is critical infrastructure". The EU's Digital Operational Resilience Act (DORA), which applies to JPMC's European operations, mandates specific ICT third-party risk requirements.

Business Impact: Trading desk disruption, payment processing failure, and customer-facing system downtime. Regulatory penalties under DORA and OCC guidance on operational resilience[17]. Counterparty disputes stemming from failed settlement obligations.

Primary Controls:

- Multi-cloud architecture across three hyperscalers to prevent single-provider lock-in
- On-premise private cloud data centers serving as failover for mission-critical workloads
- Vendor SLA management with contractual uptime guarantees and tested failover procedures
- Regular "game day" exercises simulating cloud provider outages
- DORA-compliant ICT risk management framework for all EU-facing operations

[17] Bank for International Settlements. (2020). Operational and cyber risks in the financial sector (BIS Working Paper No. 840). https://www.bis.org/publ/work840a .pdf

Risk Response: Mitigation (primary); Avoidance (multi-cloud strategy reduces but cannot eliminate concentration risk)

Risk BD-04: Cyberattack on SWIFT / Interbank Settlement Infrastructure

Field	Detail
Risk ID	BD-04
Crown Jewel Targeted	SWIFT connectivity, interbank payment rails, clearing, and settlement systems
Threat Actor	Nation-state actors (highest priority); criminal organizations
CIA Impact	Integrity (fraudulent SWIFT messages); Availability (disruption of settlement)
Likelihood	Low
Impact	High
Risk Priority	**Medium**

Scenario: Following the 2016 Bangladesh Bank SWIFT heist ($81M stolen via fraudulent SWIFT messages), nation-state actors[18] — particularly North Korea's Lazarus Group — have demonstrated the intent and capability to target SWIFT-connected financial institutions. A successful attack would inject fraudulent payment instructions into JPMC's SWIFT network, triggering unauthorized fund transfers or disrupting legitimate settlement operations across global correspondent banking.

Business Impact: Direct financial losses from fraudulent transfers; reputational harm with the global correspondent bank network; systemic risk to international financial stability if JPMC's clearing function is disrupted. Regulatory action across multiple jurisdictions.

Primary Controls:

- SWIFT Customer Security Program (CSP) mandatory controls, including multi-factor authentication for SWIFT operator access
- Real-time anomaly detection on SWIFT message flows (AI-powered pattern recognition)
- Dual-control authorization requirements for large-value or unusual transactions
- Network segmentation isolates the SWIFT infrastructure from the broader enterprise network
- Regular red-team exercises simulating SWIFT-targeted attacks

Risk Response: Mitigation (primary); Risk Transfer (SWIFT cybersecurity insurance)

---

[18] Executive Office of the President. (2018). The cost of malicious cyber activity to the U.S. economy. Trump White House Archives. https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pd.f

V. Risk Category II — Data Theft & Fraud

These risks threaten the **confidentiality** and **integrity** of JPMC's most sensitive data assets, including customer PII, account credentials, and institutional transaction data.

Risk FT-01: Large-Scale Customer PII Data Breach

Field	Detail
Risk ID	FT-01
Crown Jewel Targeted	Customer PII — 84+ million consumer accounts; 7+ million small businesses
Threat Actor	Criminal organizations; nation-state actors; insider threats
CIA Impact	Confidentiality
Likelihood	Medium
Impact	High
Risk Priority	**High**

Scenario: An attacker penetrates JPMC's customer data stores — either via a third-party vendor (as in the SitusAMC mortgage data breach of 2025), a spear-phishing attack on a database administrator, or exploitation of an unpatched vulnerability in a web-facing application — and

exfiltrates the names, Social Security numbers, account credentials, home addresses, and transaction histories of tens of millions of customers. JPMC experienced exactly this in 2014, when hackers accessed data from 76 million households and 7 million businesses by exploiting inadequately protected server credentials. Attackers subsequently used the stolen contact information to launch targeted spear-phishing campaigns against JPMC clients.

Business Impact: Regulatory fines under NYDFS Part 500, GDPR (if EU customer data), and SEC cybersecurity disclosure rules; class-action litigation; customer notification costs; long-term reputational damage, reducing customer acquisition and retention. Industry benchmark: $6.08M average cost per breach in financial services (IBM 2024).

Estimated Loss Range: $100M–$2B+ (at scale, considering litigation, OCC fines, customer remediation, and reputational revenue loss)

Primary Controls:

- Data Loss Prevention (DLP) tools monitor and block unauthorized exfiltration of customer data through email, USB, web, and cloud egress points
- Data encryption at rest and in transit with rigorous key lifecycle management
- Role-based access control (RBAC) limits database access to the minimum required for each job function
- SIEM (Security Information and Event Management) with behavioral analytics to detect anomalous data access patterns

- Regular external penetration testing and red-team exercises targeting database and API layers
- Vendor risk assessments and contractual data security standards for all third-party processors

Risk Response: Mitigation (primary); Transfer (cyber insurance); Acceptance of residual risk from zero-day exploits

Risk FT-02: Business Email Compromise (BEC) and Wire Fraud at Scale

Field	Detail
Risk ID	FT-02
Crown Jewel Targeted	Payment authorization systems; corporate treasury wire transfer infrastructure
Threat Actor	Criminal organizations (AI-augmented BEC syndicates)
CIA Impact	Integrity (unauthorized transactions); Confidentiality (financial instructions)
Likelihood	High
Impact	Medium
Risk Priority	**High**

Scenario: Criminals use generative AI to craft highly convincing impersonation emails mimicking JPMC's CFO, a corporate client's CEO, or a known vendor — requesting urgent wire transfers to attacker-controlled accounts. Jamie Dimon has warned that AI is making JPMC "more vulnerable" before it ultimately helps defense, noting that threat actors are "using generative AI to automate and scale attacks, lowering the barrier to entry and increasing attack sophistication". AI-generated voice deepfakes are an additional vector, with attackers impersonating executives in phone calls to treasury staff.

Business Impact: Direct financial losses from unauthorized transfers; reputational damage if client funds are misdirected; regulatory reporting obligations; potential contractual liability to corporate clients.

Primary Controls:

- AI-powered email security with deepfake and impersonation detection
- Multi-person authorization requirements for wire transfers above the defined thresholds
- Out-of-band confirmation protocols (callback on verified numbers) for unusual or urgent transfer requests
- Employee security awareness training with a specific focus on BEC and AI-generated social engineering

- AI Threat Modeling Co-Pilot[19] (AITMC) — JPMC's proprietary tool that has improved threat identification efficiency by 20% and identifies nine more threats on average than human analysts alone

Risk Response: Mitigation (primary); Transfer (cyber insurance with social engineering coverage)

Risk FT-03: Insider Fraud — Unauthorized Access to Client Trading Data or Account Funds

Field	Detail
Risk ID	FT-03
Crown Jewel Targeted	Client investment accounts (AWM, CIB); proprietary trading positions
Threat Actor	Malicious insiders; insiders coerced or recruited by criminal organizations or nation-states
CIA Impact	Confidentiality; Integrity
Likelihood	Medium
Impact	High
Risk Priority	**High**

[19] JPMorgan Chase & Co. (n.d.). Revolutionizing threat modeling with AI: The threat modeling co-pilot (AITMC). https://www.jpmorganchase.com/about/technology/blog/aitmc

Scenario: A JPMC employee or contractor with privileged access to client account systems — motivated by financial gain, personal grievance, or external coercion — manipulates account balances, executes unauthorized trades, or exfiltrates institutional client data before departing for a competitor. JPMC's own published Insider Threat guidance explicitly identifies data exfiltration, supply chain compromise, and collusion with external actors as the primary intentional insider threat vectors. The sheer scale — 317,233 employees globally — makes this an unavoidable threat surface.

Business Impact: Direct client financial losses; regulatory enforcement (OCC, FINRA, SEC); potential criminal prosecution of the firm for failure to supervise; reputational damage impacting high-net-worth and institutional client relationships.

Primary Controls:

- Principle of least privilege: access limited strictly to job function requirements
- User and Entity Behavior Analytics (UEBA) detects anomalous data access, unusual download volumes, or off-hours activity.
- Robust off-boarding procedures, including immediate access revocation upon departure notification
- Insider Risk Program with a dedicated detection, escalation, and investigation team
- Separation of duties for high-risk financial functions (no single person can initiate and approve large transactions)

- Regular access audits and PAM (Privileged Access Management) for system administrators

Interacting Risk Note: Insider threat risk is inversely correlated with availability controls. Resilience strategies that provide many people access to critical systems (to ensure redundancy) increase the potential insider threat pool. This is the classic tension: "How an approach to resilience, with many people having access to key systems, is a trade-off against insider threats."

Risk Response: Mitigation (primary); Acceptance (residual risk from sufficiently motivated or sophisticated insiders with legitimate access)

Risk FT-04: Payment Card Fraud and Credential Theft at Scale

Field	Detail
Risk ID	FT-04
Crown Jewel Targeted	Chase credit and debit card data; card processing infrastructure ($1.8T annual card transaction volume)
Threat Actor	Criminal organizations; dark web marketplaces
CIA Impact	Confidentiality (card credential theft); Integrity (fraudulent transactions)

Likelihood	High
Impact	Medium
Risk Priority	**High**

Scenario: Attackers compromise a third-party merchant's point-of-sale systems or a card-not-present e-commerce platform to skim Chase card credentials at scale, subsequently selling these on dark web marketplaces. Alternatively, malicious scripts injected into e-commerce checkout flows ("Magecart attacks") harvest card data in real-time. Stolen credentials are monetized through card-present fraud using counterfeit physical cards or card-not-present online fraud.

Business Impact: Fraud losses charged back to JPMC; customer notification and remediation costs; card reissuance expenses; reputational damage to the Chase brand; regulatory scrutiny from card network rules (Visa/Mastercard) and CFPB.

Primary Controls:

- EMV chip technology and tokenization minimize the value of static card data
- AI-powered real-time fraud scoring on all card transactions (JPMC processes millions of transactions per second)
- Behavioral analytics flagging unusual transaction patterns (geography, velocity, merchant category)

- PCI-DSS compliance requirements are enforced across all merchant and acquiring relationships
- Dark web monitoring for the emergence of JPMC-branded card data in criminal forums

Risk Response: Mitigation (primary); Transfer (fraud insurance; chargebacks to merchants)

VI. Risk Category III — Competitive Disadvantage & IP Theft

These risks threaten JPMC's **confidentiality** of proprietary intelligence and strategic advantage, enabling competitors or hostile actors to replicate or undermine the firm's competitive positioning.

Risk CD-01: Theft of Proprietary Trading Algorithms and Market Intelligence

Field	Detail
Risk ID	CD-01
Crown Jewel Targeted	Quantitative trading models, algorithmic execution logic, Fixed Income and Equity Markets platforms
Threat Actor	Nation-state actors (China, Russia); criminal organizations acting as mercenaries; malicious insiders
CIA Impact	Confidentiality
Likelihood	Low

Impact	High
Risk Priority	**Medium**

Scenario: A nation-state actor — leveraging a supply chain compromise of a software vendor used in JPMC's trading infrastructure, or a spear-phishing attack targeting a quantitative analyst — exfiltrates the source code and parameters for JPMC's proprietary trading algorithms. China, which "will continue actively targeting US companies for cyber espionage", would regard JPMC's trading intelligence as a high-value intelligence collection target. An insider leaving for a competing hedge fund or a state-linked financial institution constitutes a lower-tech threat vector.

Business Impact: Competitor replication of trading strategies eroding alpha generation; potential market manipulation using stolen knowledge of JPMC's order flow logic; revenue loss from Fixed Income ($20B) and Equity Markets ($9.9B) businesses.

Primary Controls:

- Strict compartmentalization and need-to-know access controls for trading algorithm codebases
- Source code repository monitoring with DLP rules blocking bulk code downloads
- Enhanced due diligence before acquiring companies or technology solutions with proprietary integration potential
- Background screening and enhanced monitoring of employees with access to the most sensitive trading systems

- Network segmentation, isolating trading infrastructure from general corporate IT

Risk Response: Mitigation (primary); Avoidance (some algorithms are not documented in single repositories)

Risk CD-02: Exfiltration of M&A Deal Intelligence and Client Confidential Information

Field	Detail
Risk ID	CD-02
Crown Jewel Targeted	CIB deal intelligence (M&A, IPO, debt issuance), client advisory documents
Threat Actor	Nation-state actors; criminal organizations (insider trading motivation); malicious insiders
CIA Impact	Confidentiality
Likelihood	Medium
Impact	High
Risk Priority	**High**

Scenario: An attacker — whether a nation-state intelligence service or a criminal organization selling information to hedge funds — compromises a JPMC investment banker's email or document management system and extracts confidential M&A advisory materials. These could include non-public acquisition targets, deal pricing, corporate restructuring plans, or sovereign debt negotiation positions. The OCC's 2024 enforcement action against JPMC — resulting in a $250M civil money penalty — for failing to adequately surveil trading activity illustrates how inadequate data controls around market-sensitive information can itself constitute regulatory liability.

Business Impact: Client breach of confidentiality; SEC insider trading investigation; loss of client trust and mandates; reputational damage across the global I-banking franchise, generating $9.1B in IB fees.

Primary Controls:

- Information barriers ("Chinese walls") between advisory and trading businesses, enforced by access controls
- Email DLP is preventing forwarding of deal-sensitive documents to external accounts.
- Digital Rights Management (DRM) on deal documents restricts printing, copying, and forwarding
- Audit logging of all access to deal rooms and M&A document repositories
- Regular OCC and SEC trade surveillance program coverage — a specific regulatory requirement highlighted by JPMC's 2024 enforcement action

Risk Response: Mitigation (primary); Transfer (professional liability insurance)

VII. Risk Category IV — Regulatory & Legal Compliance

These risks threaten JPMC's **compliance posture** and **license to operate**, generating financial penalties, reputational harm, and operational constraints.

Risk RL-01: Violation of NYDFS Part 500 Cybersecurity Regulations

Field	Detail
Risk ID	RL-01
Crown Jewel Targeted	License to operate in New York (JPMC's home state and primary market); regulatory standing
Threat Actor	Substandard products/services; insider negligence triggering compliance failures
CIA Impact	All three (the regulation covers the entire cybersecurity program)
Likelihood	Medium

Impact	High
Risk Priority	**High**

Scenario: JPMC fails to meet one or more of the phased requirements of the NYDFS Second Amendment to Part 500. The November 2025 final deadline introduced universal MFA requirements, personal CEO/CISO liability through dual-signature certifications, mandatory PAM solutions for Class A companies, and EDR deployment across all enterprise endpoints. A cyber incident that reveals a compliance gap — such as an MFA implementation failure or inadequate third-party risk assessment — triggers NYDFS enforcement. Penalties have reached $30M in prior cases.

Business Impact: Civil money penalties up to $30M per violation; personal legal liability for the CISO and CEO under dual-certification requirements; OCC and Federal Reserve scrutiny triggering broader supervisory actions.

Primary Controls:

- Dedicated compliance function tracking NYDFS Part 500 phased deadlines
- Annual CISO cybersecurity report to the Board of Directors
- 72-hour cyber incident notification protocol per Section 500.17(a)

- Third-party vendor risk assessments and contractual MCR (Minimum Control[20] Requirements) compliance
- Regular penetration testing and vulnerability assessments per NYDFS requirements

Risk RL-02: Non-Compliance with DORA (Digital Operational Resilience Act) — European Operations

Field	Detail
Risk ID	RL-02
Crown Jewel Targeted	JPMC's European franchise (CIB operations across the EU, with a major hub at 25 Bank Street, London)
Threat Actor	Third-party ICT providers; operational failures
CIA Impact	Availability; Compliance
Likelihood	Medium
Impact	Medium
Risk Priority	**Medium**

[20] JPMorgan Chase & Co. (2025). Supplier minimum control requirements: 2025 updates. https://www.jpmorganchase.com/content/dam/jpmorganchase/documents/updates-to-minimum-control-requirements-2024.pdf

Scenario: JPMC's European operations fail to meet DORA's requirements for ICT third-party risk management, incident reporting, or digital resilience testing. DORA, referenced explicitly in JPMC's 2024 10-K, requires financial entities to conduct TLPT (Threat-Led Penetration Testing), maintain ICT risk frameworks, and report major incidents to European regulators within defined timeframes.

Business Impact: Regulatory sanctions from European supervisory authorities; restrictions on ICT vendor relationships; reputational damage in European institutional client markets.

Primary Controls:

- DORA-compliant ICT risk management framework covering all EU-facing technology systems
- Contractual provisions with ICT third-party providers aligned to DORA standards
- TLPT exercises conducted with designated EU testing authorities
- Centralized incident response protocol covering both US (NYDFS) and EU (DORA) simultaneous reporting

Risk RL-03: SEC Cybersecurity Disclosure[21] Rule Non-Compliance

Field	Detail

[21] U.S. Securities and Exchange Commission. (2022). Cybersecurity risk management (Release No. 33-11028). https://www.sec.gov/rules/proposed/2022/33-11028.pdf

Risk ID	RL-03
Crown Jewel Targeted	JPMC's regulatory standing with the SEC, investor confidence
Threat Actor	Internal governance failures; cybersecurity incidents exceeding the materiality threshold
CIA Impact	Confidentiality; Availability
Likelihood	Medium
Impact	Medium
Risk Priority	**Medium**

Scenario: JPMC experiences a cyber incident that meets the SEC's materiality threshold but fails to disclose it on Form 8-K within the required four-business-day window, or makes materially misleading statements in its annual cybersecurity risk disclosures. Given JPMC's status as a public company and systemically important financial institution, SEC enforcement of cybersecurity disclosure failures carries both financial penalties and profound reputational consequences.

Primary Controls:

- Pre-established materiality assessment framework for cyber incidents tied to disclosure workflow
- Legal and compliance review integrated into the incident response process

- Board-level cyber risk oversight protocols with quarterly cybersecurity updates to the Audit Committee
- Cross-functional incident response team including Legal, Compliance, IR (Investor Relations), and Communications

VIII. Risk Category V — Emerging Technology Risks

These risks reflect JPMC's exposure to cutting-edge technology vectors that do not yet have settled control frameworks, requiring forward-looking risk management.

Risk ET-01: AI-Augmented Attacks and Adversarial AI

Field	Detail
Risk ID	ET-01
Crown Jewel Targeted	All crown jewels (AI lowers the barrier to attack across all categories)
Threat Actor	Criminal organizations; nation-state actors; hacktivists (all categories now AI-empowered)
CIA Impact	All three (AI augments attacks on Confidentiality, Integrity, and Availability)
Likelihood	High
Impact	High

Risk Priority	**Critical**

Scenario: Generative AI dramatically lowers the cost and skill threshold for sophisticated attacks. Criminal groups use LLMs to write polymorphic malware (evading signature-based detection), generate highly personalized spear-phishing emails at scale, and produce voice deepfakes impersonating JPMC executives. Adversarial AI also threatens JPMC's own AI systems: attackers may inject poisoned data into JPMC's fraud detection models, causing systematic misfires, or manipulate AI-driven credit scoring systems through adversarial inputs. Jamie Dimon explicitly warned in April 2026 that while AI will eventually help defense, it is "first making [companies] more vulnerable", and JPMC is testing Anthropic's Mythos model as part of its AI security program.

Business Impact: Dramatically increased success rate of phishing, BEC, and social engineering attacks; potential subversion of AI-driven fraud detection systems; erosion of trust in AI-generated outputs across trading and risk management functions.

Primary Controls:

- AI Threat Modeling Co-Pilot (AITMC): JPMC's GenAI tool that identifies nine more threats on average than human analysts and improves threat modeling efficiency by 20%
- Adversarial robustness testing of all production AI/ML models (red-teaming AI systems)
- Human-in-the-loop oversight for high-stakes AI outputs (fraud alerts, credit decisions)
- AI model governance framework with audit trails, version control, and drift detection

- AI-powered deepfake detection integrated into email security and telephony systems

Interacting Risk Note: JPMC's AI investments are a dual-use sword: the same models that improve fraud detection (a control) also introduce new vulnerabilities if the models themselves are compromised (a risk). This creates a positive feedback loop requiring AI security to be treated as a first-class risk category in its own right.

Risk ET-02: Quantum Computing Threat to Cryptographic Infrastructure ("Harvest Now, Decrypt Later")

Field	Detail
Risk ID	ET-02
Crown Jewel Targeted	All encrypted data (customer PII, trading communications, interbank messages, authentication systems)
Threat Actor	Nation-state actors (China, Russia) with quantum computing programs
CIA Impact	Confidentiality (retroactive decryption); Integrity (forging digital signatures)
Likelihood	Low (within 5 years); Medium (within 10 years)

Impact	High
Risk Priority	**Medium** (future-oriented)

Scenario: Nation-state adversaries are currently executing "harvest now, decrypt later" strategies — collecting encrypted JPMC communications and financial data today, with the intent of decrypting them once sufficiently powerful quantum computers become available. JPMC CEO Jamie Dimon named "harvest now, decrypt later" as a key strategic risk in 2026. A cryptographically relevant quantum computer would render RSA and ECC encryption — the backbone of JPMC's TLS connections, SWIFT messaging, and digital signatures — entirely vulnerable. JPMC is investing in quantum computing research and quantum-resistant encryption.[3

Business Impact: Retroactive disclosure of years of encrypted client communications, M&A deal data, trading strategies, and authentication credentials. The collapse of the public-key infrastructure underpinning all digital banking operations. Existential threat to JPMC's data confidentiality posture.

Primary Controls:

- NIST Post-Quantum Cryptography (PQC) standards implementation roadmap — JPMC has a quantum computing team dedicated to identifying real-world applications and quantum-safe migration
- Crypto-agility architecture enabling rapid algorithm migration as PQC standards finalize

- Quantum Key Distribution (QKD) research investments through JPMC's $1.5T Security and Resiliency Initiative
- Inventory of high-value long-lived encrypted data requiring priority re-encryption

Risk Response: Mitigation (proactive PQC migration); Avoidance (minimize long-term sensitive data retention); Acceptance of residual risk during transition period

Risk ET-03: Digital Asset and Blockchain Infrastructure Compromise

Field	Detail
Risk ID	ET-03
Crown Jewel Targeted	Kinexys Digital Assets platform; JPM Coin on public blockchain; $1B+ daily blockchain transaction volume
Threat Actor	Criminal organizations; nation-state actors; protocol-level hackers
CIA Impact	Integrity (smart contract manipulation); Availability (blockchain network disruption); Confidentiality (private key theft)
Likelihood	Medium

Impact	High
Risk Priority	**High**

Scenario: As JPMC expands its Kinexys blockchain payments platform and deploys JPM Coin on public blockchain networks, it inherits unique risks absent from traditional banking: smart contract vulnerabilities enabling unauthorized fund releases, cross-chain[22] bridge exploits (the Kelp DAO breach in 2026 demonstrated how such attacks can erase $20B in value within days), 51% attacks on networks JPMC relies upon, and private key management failures that would cause irretrievable asset loss. Unlike traditional banking reversals, blockchain transactions are immutable.

Business Impact: Irreversible financial losses if private keys are compromised; reputational damage undermining institutional client trust in JPMC's digital asset capabilities; regulatory scrutiny from OCC, SEC, and NYDFS regarding digital asset custody practices.

Primary Controls:

- Formal smart contract audits by independent security firms before deployment
- Hardware Security Modules (HSMs) for private key storage and signing operations
- Multi-signature authorization requirements for large blockchain transactions
- Blockchain analytics tools monitor transaction patterns for anomalous behavior

[22] TheStreet. (2026, April). JPMorgan issues blunt warning as investors move to safety. https://www.thestreet.com/crypto/markets/jp-morgan-issues-blunt-warning-as-investors-rush-to-safety

- Clear delineation between hot wallet (operational) and cold storage (offline) custody, following industry best practices
- Incident response playbooks specific to blockchain environments (distinct from traditional IT IR)

Risk Response: Mitigation (primary); Avoidance (limiting exposure to most volatile protocols); Transfer (digital asset custody insurance)

Risk ET-04: SaaS Integration Exposure and API Security Failures

Field	Detail
Risk ID	ET-04
Crown Jewel Targeted	Internal data systems exposed through SaaS integrations; customer data processed by cloud-native tools
Threat Actor	Criminal organizations; nation-state actors exploiting the SaaS supply chain
CIA Impact	Confidentiality; Integrity
Likelihood	High
Impact	Medium

Risk Priority	**High**

Scenario: JPMC CISO Patrick Opet publicly warned in 2025 that "the widespread adoption of SaaS solutions has led to the erosion of traditional security boundaries, such as those between APIs and backend systems," and that attackers now have "unprecedented access to sensitive data" through compromised integrations. OAuth tokens and API keys used to connect SaaS tools to JPMC's internal systems become high-value targets: compromising a single widely-used SaaS provider (as in the 2023 Snowflake compromise affecting dozens of financial firms) grants direct access to JPMC's backend data without triggering traditional network-level controls.

Business Impact: Customer data exfiltration without triggering traditional network-level alarms; financial data manipulation through compromised API integrations; supply chain compromise cascading to JPMC's clients.

Primary Controls:

- Sophisticated authorization methods (beyond OAuth) for SaaS-to-internal-system integrations, per Opet's recommendations
- API security gateway with rate limiting, anomaly detection, and token rotation
- Third-party SaaS security assessments integrated into procurement workflow
- Zero Trust principles applied to all API communications (no implicit trust based on network position)
- SaaS usage inventory (Shadow IT discovery) to prevent unauthorized integrations

IX. Interacting Risks

Understanding how JPMC's cyber risks interact, compound, or mitigate each other is as analytically important as analyzing each risk in isolation.

The Resilience-Insider Threat Paradox

JPMC's operational resilience strategy requires broad access — many people with access to critical systems ensure continuity if any single person or team becomes unavailable (BD-01, BD-03). This same breadth of access, however, expands the potential insider threat surface (FT-03). Controls that mitigate this tension include UEBA (detecting anomalous access within the broad user base), mandatory separation of duties, and regular access recertification. The paradox cannot be fully resolved — it must be managed within an explicit risk appetite statement.

AI as Both Risk Amplifier and Defense Multiplier

Generative AI simultaneously increases the attack surface (ET-01: AI-augmented attacks[23]) and provides JPMC's most powerful new defensive capability (the AITMC threat modeling tool, AI fraud detection, behavioral analytics). An attacker who succeeds in poisoning JPMC's AI training data (an adversarial AI attack) could subvert JPMC's primary defensive systems — effectively turning the defense into an attack vector. This creates a compounding risk: ET-01 interacts with every other risk category, both amplifying likelihood and potentially degrading controls.

---

[23] JPMorgan Chase & Co. (2026, April). Fortifying the enterprise: 10 actions for AI-ready cyber resilience. https://www.jpmorganchase.com/about/technology/blog/fortifying-the-enterprise-10-actions-to-take-now-for-ai-ready-cyber-resilien

IP Theft as Reconnaissance for Infrastructure Attacks

As seen in the Coinbase taxonomy model, theft of intellectual property — including JPMC's trading system architecture documents (CD-01) — can serve as reconnaissance for subsequent infrastructure attacks (BD-01, BD-04). Knowing the detailed internal architecture of JPMC's payment systems makes it dramatically easier to craft targeted exploits. Mitigating CD-01 (IP theft) therefore directly reduces the likelihood of successful BD-01 (ransomware) and BD-04 (SWIFT attacks).

Third-Party Concentration and Cascading Failures

BD-03 (cloud provider failure) and ET-04 (SaaS compromise) share a common root cause: excessive dependence on a small number of technology vendors. A single compromise of JPMC's cloud infrastructure by a nation-state actor (ET-01 + BD-03) could simultaneously trigger FT-01 (customer PII breach), BD-01 (ransomware deployment), and RL-01 (NYDFS reporting obligation), creating a multi-category simultaneous incident that overwhelms response capacity. JPMC's multi-cloud architecture directly mitigates this interaction — but the SaaS integration layer (ET-04) reintroduces concentration risk in a less visible form.

Quantum Computing and Encryption — A Slow-Moving but Total Risk

ET-02 (quantum threat) interacts with every confidentiality risk in the taxonomy. When cryptography fails, every data asset loses its confidentiality protection simultaneously. Unlike

operational risks that affect individual systems, quantum decryption would retroactively expose all historical encrypted data — including past M&A communications (CD-02), SWIFT messages (BD-04), and customer PII (FT-01) — in a single catastrophic event. This makes ET-02 the one risk requiring immediate mitigation investment, even at a very low near-term likelihood, because the consequences of delayed action are irreversible.

Blockchain Integrity and Reputational Feedback Loops

ET-03 (digital asset compromise) interacts strongly with reputational risk. A successful attack on JPM Coin — causing irreversible loss of client funds on a public blockchain — would fundamentally undermine JPMC's credibility in the institutional digital asset market, precisely when JPMC is competing for the $13 trillion tokenized asset market. Unlike traditional fraud (where JPMC can compensate clients and restore confidence), blockchain losses are immutable and therefore maximally reputation-damaging. This asymmetry makes ET-03 disproportionately impactful relative to its quantitative loss value.

X. Risk Governance — Lines of Defense

JPMC's cyber risk governance follows an adapted version of the Three Lines[24] of Defense model, extended to five lines of accountability as recommended for financial institutions by ISACA and BIS:

Line	Role	JPMC Function
1st Line	Business owners implementing controls	LOB technology teams, trading desk technologists, and CCB digital banking engineering
2nd Line	Risk management and compliance oversight	Chief Risk Officer (Ashley Bacon); CISO (Patrick Opet); Compliance and Legal
3rd Line	Independent audit and assurance	Internal Audit; external auditors (PwC)
4th Line	Executive management accountability	Operating Committee; CEO Jamie Dimon

[24] ISACA. (2024). The three lines model in cybersecurity governance and risk management. https://www.isaca.org/resources/isaca-journal/issues/2024/volume-1/the-three-lines-model-in-cybersecurity-governance-and-risk-ma

5th Line	Board-level oversight and risk appetite endorsement	Board of Directors; Audit Committee; Risk Committee

The Board endorses JPMC's risk appetite — the firm's explicit statement that while cybersecurity risk cannot be reduced to zero, it must be maintained within bounds that do not threaten client trust, financial stability, or regulatory standing. Jamie Dimon's naming of cyber as the "highest risk" the bank faces reflects the 5th Line's active engagement with this taxonomy's findings.

XI. Risk Appetite Statement

JPMorgan Chase accepts that, as the world's largest bank and a critical node in the global financial system, cyber risk is an inherent and permanent feature of its operating environment — not a problem to be solved, but a risk to be actively managed within defined tolerances.

JPMC's cyber risk appetite is defined as follows:

- **Zero tolerance** for events that threaten systemic financial stability, cause irreversible loss of client assets on blockchain infrastructure, or result in nation-state-level exfiltration of trading algorithms or institutional deal intelligence.
- **Low tolerance** for large-scale customer PII breaches, major payment system disruptions, or regulatory violations carrying material financial penalties or license risk.
- **Medium tolerance** for limited-scope incidents — individual account compromises, short-duration DDoS events, low-scale BEC fraud — that are operationally manageable and can be remediated without systemic impact.
- **Acceptance** that zero-day exploits, AI-augmented attacks, and novel blockchain vulnerabilities may succeed despite best controls; incident response and resilience capabilities are therefore as important as prevention.

The $15B annual technology investment and the $1.5T Security and Resiliency Initiative reflect JPMC's organizational commitment to pushing residual risk toward the lowest achievable level across all categories.

XII. Residual Risk and Compensating Controls

Even after applying the full suite of controls described above, residual cyber risk at JPMC is material and unavoidable. Cyber risk can never be reduced to zero. Key residual risk areas include:

1. **Zero-day exploits:** Vulnerabilities unknown to JPMC and to the security community cannot be patched in advance. JPMC's primary compensating control is rapid detection and containment capability (mean-time-to-detect [MTTD] and mean-time-to-respond [MTTR] metrics), alongside the CISA Known Exploited Vulnerabilities list for prioritizing patch cadence.

2. **Insider threats from sufficiently motivated actors:** No access control system prevents a sufficiently determined insider with legitimate privileges from causing harm over a long timeframe. Compensating controls include behavioral monitoring (UEBA), rotating access reviews, and the insider threat program.

3. **AI system subversion:** As JPMC's defenses become increasingly AI-dependent, adversarial AI attacks targeting JPMC's models constitute a residual risk without settled mitigations. Compensating controls include human oversight of AI outputs, red-teaming of AI systems, and model governance frameworks.

4. **Quantum cryptography transition:** The gap period between today and full PQC migration represents a window of vulnerability for "harvest now, decrypt later" attacks. Compensating

control: minimizing retention of highly sensitive long-lived data and prioritizing PQC migration for the highest-sensitivity communications first.

5. **Blockchain irreversibility:** For ET-03 risks, no compensating control can reverse a completed blockchain transaction. The primary residual risk management approach is insurance, legal preparation, and pre-incident client communication protocols.

Residual risks must be reviewed at least quarterly by the Board Risk Committee and reported annually in JPMC's NYDFS certification and SEC cybersecurity disclosures. Changes in the threat landscape — particularly the maturation of adversarial AI and quantum computing — may elevate residual risks that today's controls no longer adequately address, requiring continuous reassessment.