Discovery Phase:
Insider Threat Risk Modeling for BillyBank

BillyBank is a multinational investment bank modeled after JPMorgan Chase. Numbers are made up, but were based off of the bank's real scale, sensitive data, and regulatory obligations.

1/ Organizational Hierarchical Structure

A. C-level Executives (9 people)

Built based on "Executive CSuite Team of JPMorgan Chase [2025]" [1]

Title	Role
Chairman & Chief Executive Officer (CEO)	Leads BillyBank's global strategy, operations, and corporate vision.
Chief Risk Officer (CRO)	Manages enterprise risk, credit, and operational risk frameworks.
Chief Data & Analytics Officer (CDAO)	Oversees firmwide data strategy, analytics platforms, and governance.
Chief Financial Officer (CFO)	Directs financial planning, accounting, and corporate reporting.
Chief Operating Officer (COO)	Oversees firmwide strategy, technology, and global operations.
Chief Information Officer (CIO)	Leads enterprise technology, architecture, and innovation efforts.
Chief Information Security Officer (CISO)	Leads cyber threat defense as well as maintaining the bank's global security posture.
Chief Human Resources Officer (CHRO)	Responsible for talent strategy, employee engagement, compensation and benefits.
General Counsel (GC)	Oversees all legal matters across the firm's global operations.

[1] https://digitaldefynd.com/IQ/meet-the-executive-csuite-team-of-jpmorgan-chase/

B. Organizational Layers

BillyBank uses a hierarchical structure to manage 50,000 staff across different regions globally:

C-Level → Regional Directors → Group Managers → Team Leads → Employees/Contractors

C. Headcount and Average Salaries

Based on "JPMorgan Chase & Co Executive Salaries & other compensation," [2]

Level	Approx Number	Typical Compensation
C-Level Executives	9	$10,000,000
Regional Directors	50	$350,000
Group Managers	300	$200,000
Team Leads	1,143	$150,000
Employees (full-time)	~41,000	$100,000
Contractors / Temporary Staff	~6,000	$80,000

Total Workforce: ~50,000

[2] https://www.salary.com/research/executive-compensation/jpmorgan-chase-and-co-executive-salary

2/ Security and People Expenditure

A. People Expenditure

BillyBank employs ~50,000 people worldwide (44,500 full-time employees, ~6,000 contractors). Compensation benchmarks are drawn from banking pay data like Glassdoor, Salary.com for JPMC.

Level	Count	Avg Compensation (Base + Bonus)	Annual Cost (USD)	Notes
C-Level Executives (CEO, CRO, CDAO, CFO, COO, CIO, CISO, CHRO, GC)	9	$10,000,000	$90,000,000	Typical for global bank execs; CEO pay alone often >$30M
Regional Directors	50	$350,000	$17,500,000	Region-level leadership, heavy compliance exposure
Group Managers	300	$200,000	$60,000,000	Business & tech managers
Team Leads	1,143	$150,000	$171,450,000	Includes senior IT/security leads
Employees (full-time)	~41,000	$100,000	$4,100,000,000	Analysts, associates, ops, engineers
Contractors / Temp Staff	~6,000	$80,000	$480,000,000	Mix of IT support, short-term project staff

Total: ~$4.92B annually

B. Contracts and Costs

Vendor / Contract Type	**Number of Contracts**	**Annual Cost (USD)**	**Purpose**
Cloud Service Providers (AWS, Azure, GCP)	3	$50M total	Multi-region storage, compute, disaster recovery
Security SaaS (DLP, UEBA, PAM, IAM)	5	$12M total	Insider threat detection, monitoring, and privileged access management
Managed Security Services	2	$20M total	24/7 monitoring and incident response
Compliance & Audit Services	4	$5M total	Regulatory audits for SOX, PCI-DSS, GDPR compliance

- Total number of active contracts: 14, totaling ~$87M annually
- Each contract is reviewed annually for scope and cost.
- These contracts form the baseline for current security coverage. Gaps in coverage will be highlighted in our risk modeling and used to justify mitigation strategies.

C. Solutions and Costs

Costs are modeled on industry averages from Gartner security spend benchmarks and vendor pricing.

Solution Type	Example Vendors	Model (Subscription vs. Upfront)	Annual / Upfront Cost (USD)
Cloud Service Providers	AWS, Azure	Usage-based subscription	~$35M annually
Data Loss Prevention (DLP)	Forcepoint	SaaS subscription	$2M annually
Privileged Access Management (PAM)	CyberArk	License + subscription	$2M annually
Firewalls / IDS / IPS	Cisco, Palo Alto	Upfront hardware + annual support	$4M upfront + $1M annual maintenance
Compliance & Audit Services	Deloitte, PwC	Engagement contracts	$4M annually

Total: ~$44M annually (plus $4M upfront hardware)

3. Revenue & Costs

Based on [3] "Financial Highlights," 2023. Available: https://www.jpmorganchase.com/content/dam/jpmc/jpmorgan-chase-and-co/investor-relations/documents/financial-highlights-2023.pdf

- Annual Revenue: ~$130B
- Net Income (Profit): ~$40B annually
- Operating Expenses: ~$90B annually
- People + Security Costs (~$5.0B) = ~5% of total operating expenses

4. Security Systems

A. Current Security Systems

Area	Systems in Place	Purpose
Network Security	Firewalls, IDS/IPS, VPNs	Protect internal networks and prevent unauthorized access
Endpoint Security	Antivirus, MDM, disk encryption	Secure laptops, desktops, and mobile devices
Identity & Access Management (IAM)	Multi-factor authentication (MFA), RBAC, PAM	Control and monitor privileged access
Data Security	DLP tools, encrypted storage, secure cloud solutions	Prevent exfiltration of sensitive data
Monitoring & Analytics	UEBA, SOC 24/7 monitoring, SIEM	Detect anomalous user behavior, insider threats, and policy violations
Compliance Controls	SOX, PCI-DSS, GDPR audits	Maintain regulatory compliance across regions

B. Security Gaps / Areas for Improvement

Gap	Risk Impact	Relevance to Consulting Deliverables
Predictive Insider Threat Detection	Current monitoring is largely reactive	Enables risk modeling and heatmap simulation
Geo-Redundant Storage	Some critical trading or PII systems rely on single-region storage	Feeds into EAL calculations for operational disruption
Vendor Security Audits	Manual audits limit coverage	Supports recommendations for risk reduction in third-party access
Emerging Threat Awareness	AI-deepfake attacks, Q-day risk not modeled	Can be incorporated into gamified training and scenario simulations
Security Awareness Programs	Training is periodic, not interactive	Directly informs gamified, scenario-based training prototype

5. Project Benefits / Deliverables

A. Tangible Outcomes & Methodology Mapping

Deliverable 1: Risk Model & Heatmap

- Tangible Outcome:
    - Quantifies insider threat likelihood and potential impact on confidentiality, integrity, and compliance. Visualizes high-risk regions and roles

- Methodology / Framework Used:
    - SEI CERT Insider Datasets[3] [4] for real behavioral scenarios
    - Linear Regression to identify predictors of malicious/negligent insider behavior
    - Monte Carlo Simulation to calculate Expected Annual Loss (EAL) by employee type, contractor status, and region

- Notes:
    - The SEI CERT dataset contains synthetically generated logs from actual insider events. Using this dataset will help us
        a) model user behaviours across different roles
        b) identify key predictors like unusual login times, file exfiltrations, email filtering
        c) simulate risk exposure for BillyBank's hierarchical structure.
    - Produces heatmap for leadership decision-making that is not just theoretical but based on real life insider threat indicators, potentially feeds into dashboard and training scenarios

Deliverable 2: Gamified Training Prototype

- Tangible Outcome: Leadership experiences insider threat events interactively, sees real-time outcomes of detection, response, and preventive controls

- Methodology / Framework Used:
    - Scenario-based simulation using SEI dataset logs and BillyBank hierarchical/access structure
    - Game mechanics for engagement (points, progress, branching outcomes)

- Notes:
    - Integration of emerging threats (AI/deepfake, Q-day risk)
    - ~3–5 min demo in presentation; can be scaled to full employee training program for broader awareness

[3] https://www.kaggle.com/datasets/nitishabharathi/cert-insider-threat

[4] https://www.sei.cmu.edu/library/insider-threat-test-dataset/

Deliverable 3: Executive Dashboard Prototype

- Tangible Outcome: Interactive visualization of insider risk exposure; allows leadership to simulate mitigation strategies and see ROI/EAL reduction in real time
- Methodology / Framework Used
    - Data visualization tools (e.g., Tableau, PowerBI)
    - Heatmap integration with Monte Carlo outputs
    - Scenario sliders for mitigation actions (PAM coverage, training, UEBA thresholds)
- Notes
    - Demonstrates impact of investments on risk reduction, directly linking to business outcomes
    - More likely to be a strategy recommendation rather than implementation

B. Intangible Outcomes

- Increased awareness of insider risk patterns, especially cross-border and contractor exposure.
- Experience of impact of AI/deepfake and emerging technology risks in a safe, interactive environment.
- Demonstrates the value of data-driven decision-making for security investment (ROI visible through dashboard and heatmap).

C. Approach to Realize Outcomes

1. Risk Modeling → Heatmap

- Use SEI CERT dataset to simulate insider behaviors relevant to BillyBank roles.
- Apply regression to determine predictive features (e.g., unusual access times, file downloads, deviations from normal workflow).
- Monte Carlo simulations to compute EAL for each department/region/role combination.

2. Gamified Training Prototype

- Build scenarios that mirror SEI dataset insider events.
- Include branching outcomes based on participant actions (detect, escalate, ignore).
- Integrate emerging risks (deepfake phishing, Q-day) for realism.
- Use feedback loops: show how timely detection mitigates financial and compliance impact.

3. Dashboard

- Connect Monte Carlo & regression outputs to an interactive visualization.
- Allow leadership to adjust mitigation parameters (training coverage, PAM access, UEBA sensitivity) and see EAL changes instantly.