JP Morgan Chase IT Audit Review: Ensuring Security and Compliance in Digital Operations

Team 8 Industry - Financial Services

Prajakta Bhavsar
Komal Lohar
Jimmy Cheng
Lohya Sujith Valiveti
Akash Muddana

Company overview

- **Company:** JPMorgan Chase & Co.
- **Headquarters**: Based in New York, United States of America
- **Global Operations:** Operates worldwide
- **Assets (as of Dec 31, 2023):** $3.9 trillion
- **Stockholders' Equity (as of Dec 31, 2023):** $327.9 billion
- **Core Sectors:** Investment banking, consumer and small business financial services, commercial banking, financial transaction processing, asset management
- **Customer Base:** Millions of customers, primarily in the U.S.
- **Clientele:** Serves prominent corporate, institutional, and government clients globally

- Risk Assessment with Analysis

Risk	Risk Description	Process	Business Objectives	Control Objectives	Control Description	Control Type	Control Frequency	Control Method
Fraudulent Activities	Unauthorized access, manipulation of financial data	Customer Account Management	Secure Customer Assets	Ensure robust authentication mechanisms	Implementation of multi-factor authentication for customer login	Preventative	Continuous	Automated
Non-Compliance	Failure to comply with regulatory requirements	Compliance Monitoring	Regulatory Compliance	Establish a compliance monitoring program	Conduct periodic compliance audits to assess adherence to regulations	Detective	Periodic	Manual
Data Breaches and Cybersecurity Incidents	Unauthorized access to sensitive information	Cybersecurity Management	Protect Customer Data	Implement multi-layered security controls	Regularly update security patches and conduct penetration testing to identify vulnerabilities	Preventative, Detective	Continuous, Periodic	Automated, Mixed

Management Overview

Operations:

-Diverse operations spanning investment banking, consumer and small business financial services, commercial banking, financial transaction processing, and asset management
-Global presence with operations extending worldwide

Objectives:

-Drive growth and profitability
-Enhance customer experience and satisfaction
-Manage risk effectively
-Create shareholder value

Strategies:

-Expand market share through innovation and customer-centric products/services
-Optimize operational efficiency and cost management
-Invest in technology and digital transformation initiatives
-Strengthen risk management practices and regulatory compliance

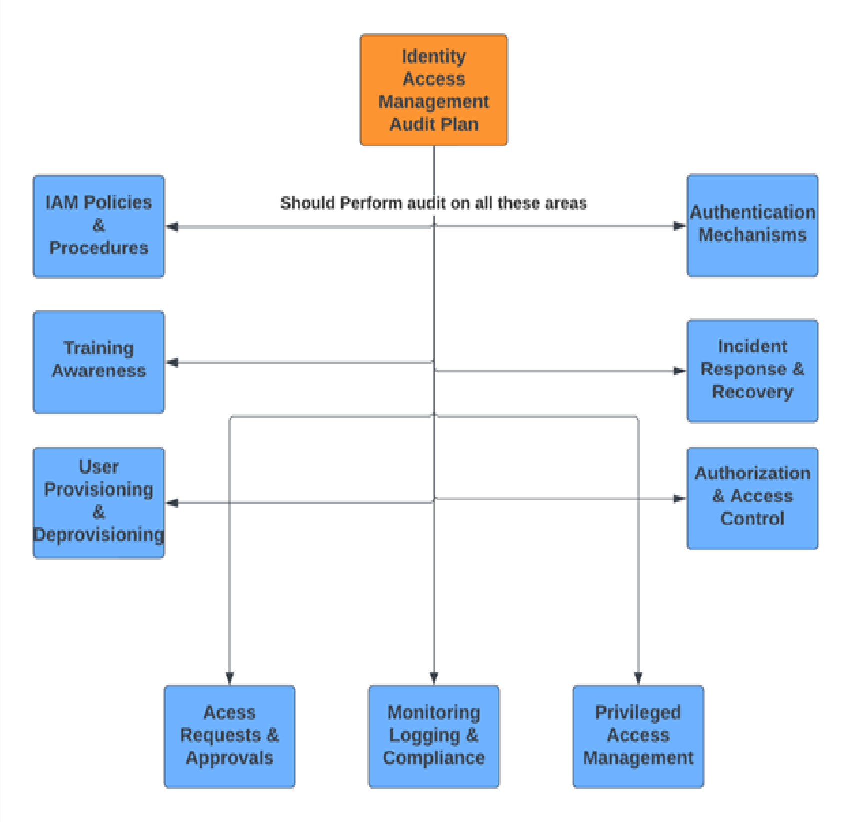
Significant Risks:

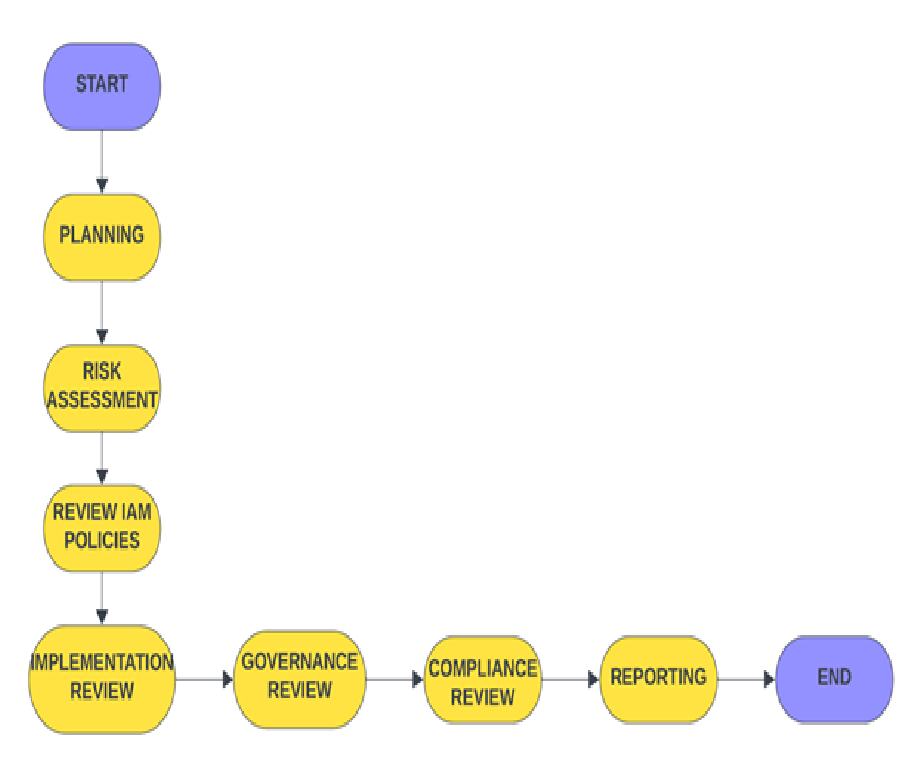
-Regulatory compliance and legal risks
-Credit risk associated with lending activities
-Market risk from fluctuations in interest rates, exchange rates, and asset prices
-Operational risk including cybersecurity threats, system failures, and human error
-Reputational risk stemming from adverse publicity or customer dissatisfaction

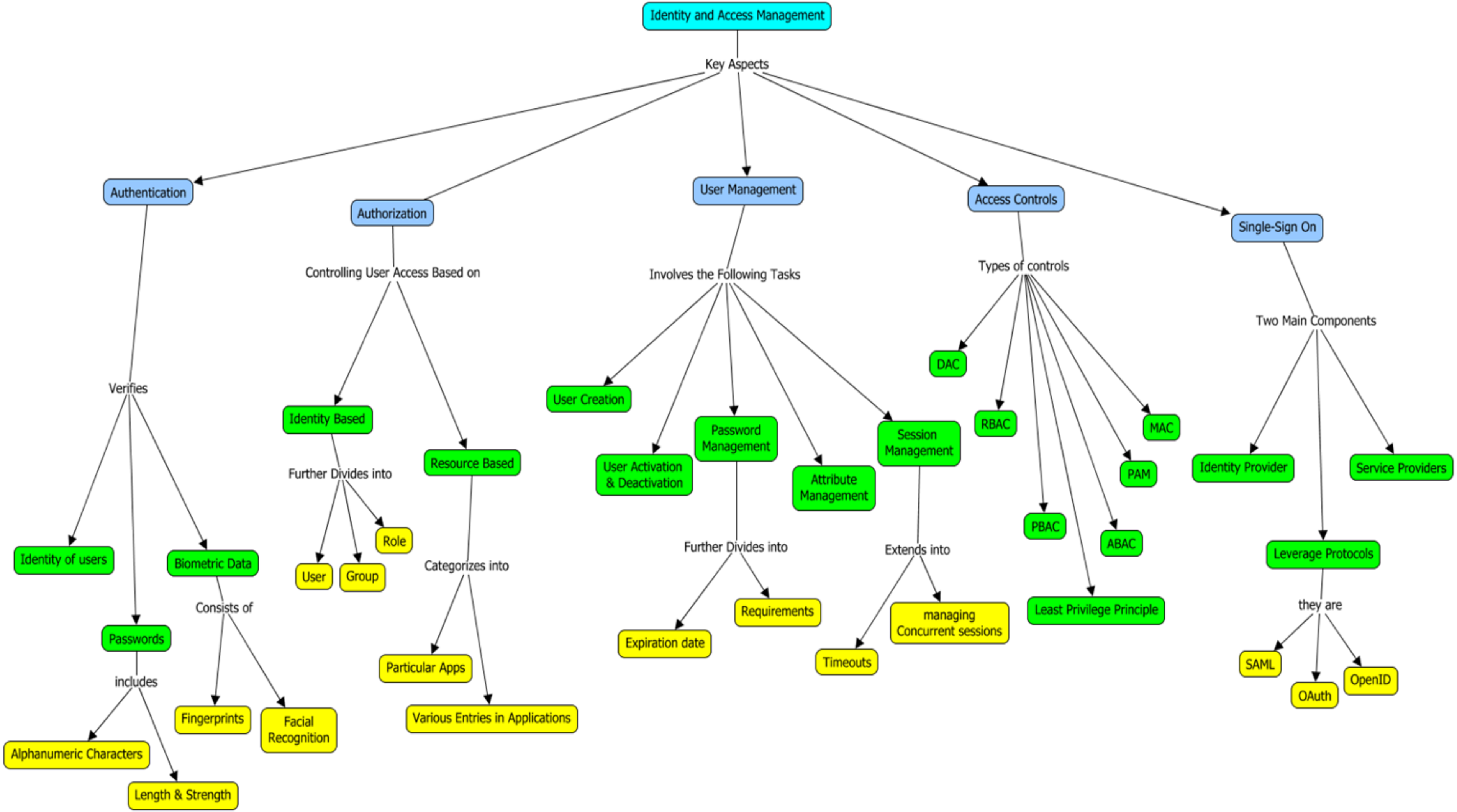
Management Control Assessment

- **Governance Structure:**
  -Clear roles and responsibilities for board, management, and committees.
  -Effective oversight and accountability mechanisms.
  -Alignment with regulatory requirements and industry best practices.
  -Commitment to integrity, ethics, and transparency.
- **Internal Control Environment:**
  -Strong tone emphasizing controls, risk management, and compliance.
  -Robust control activities across credit, market, operational, and regulatory risks.
  -Consistent policies and procedures for efficient operations.
  -Continuous monitoring and evaluation of controls.
- **Risk Management Processes:**
  -Comprehensive framework for risk identification, assessment, and mitigation.
  -Rigorous methodologies for prioritizing key risks.
  -Transparent risk appetite guiding decision-making.
  -Regular review and adaptation to changing conditions.
- **Compliance Programs:**
  -Robust programs ensuring adherence to laws and regulations.
  -Effective training on responsibilities and obligations.
  -Proactive monitoring to prevent compliance violations.
  -Strong culture of compliance and accountability.

Flow Diagrams


Identity Access Management Audit Plan
Should Perform audit on all these areas
IAM Policies & Procedures
Authentication Mechanisms
Training Awareness
Incident Response & Recovery
User Provisioning & Deprovisioning
Authorization & Access Control
Acess Requests & Approvals
Monitoring Logging & Compliance
Privileged Access Management





Identity and Access Management

Key Aspects

Authentication

Verifies

Identity of users

Passwords

includes

Alphanumeric Characters

Length & Strength

Biometric Data

Consists of

Fingerprints

Facial Recognition

Authorization

Controlling User Access Based on

Identity Based

Further Divides into

User

Group

Role

Resource Based

Categorizes into

Particular Apps

Various Entries in Applications

User Management

Involves the Following Tasks

User Creation

User Activation & Deactivation

Password Management

Further Divides into

Expiration date

Requirements

Attribute Management

Session Management

Extends into

Timeouts

managing Concurrent sessions

Access Controls

Types of controls

DAC

RBAC

PBAC

Least Privilege Principle

ABAC

PAM

MAC

Single-Sign On

Two Main Components

Identity Provider

Leverage Protocols

they are

SAML

OAuth

OpenID

Service Providers

Risk Control Matrix (RCM)

Overall, the RCM process at JPMorgan Chase provides a structured approach to identifying, assessing, and managing risks across the organization, contributing to sound risk management practices and the achievement of business objectives.

* **Risk Identification:** Identify potential risks across operational, financial, regulatory, and strategic aspects using assessments, incident reports, compliance reviews, and audits.
* **Risk Assessment:** Evaluate the significance of identified risks based on their potential impact and likelihood, prioritizing them according to their importance to organizational objectives and risk appetite.
* **Control Definition:** Develop specific controls, such as policies, procedures, automated systems, and monitoring mechanisms, to effectively mitigate identified risks.
* **Risk-Control Mapping:** Associate each identified risk with corresponding controls to ensure alignment and effectiveness without redundancy.
* **Testing and Validation:** Test control effectiveness through assessments, audits, and independent testing to verify they operate as intended and manage associated risks effectively.
* **Monitoring and Reporting:** Continuously monitor risks and controls, reporting status to stakeholders and addressing deficiencies or gaps through remediation efforts.
* **Continuous Improvement:** Adapt the Risk-Control Mapping (RCM) framework to changing landscapes and capture feedback to enhance effectiveness over time.

Audit program with audit steps & Audit fieldwork

Customer Account Management

Control - Authentication
Test Procedure - Penetration testing of system authentication methods
***** Each of the 100 passwords generated from the password generator was used to test security for one particular customer account.
* Informed consent was obtained from all parties involved, including the customer who is the owner of the account, prior to testing.

Compliance Monitoring

Control - Compliance Monitoring (on employees only)
Test Procedure - Organizational compliance assessment
* Selected 2 members of executive management, the data owner, and 5 members from the IT department to conduct a series of interviews.

Cybersecurity Management

Control - Regular security patch updates and penetration testing
Test Procedure - Assessment of organizational security patch development and penetration testing procedure
* Procedure took 2 working days. Day 1 consisted of interviews with the CIO and 5 members responsible for cybersecurity patch development covering areas such as patch strategy, roles and responsibilities, compliance, and monitoring.
* Day 2 consisted on penetration testing using 100 different sets of generated passwords and 10 different sets of biometrics. Report summaries of both activities were then generated.

Our recommendations

- Implement a continuous improvement framework for compliance monitoring and assessment processes, including regular reviews and updates to policies and procedures
- Implement multi-factor authentication (MFA) using a combination of biometrics and passwords. Regularly review and update authentication methods to align with best practices.
- Patch management protocols should be reviewed and updated to reflect industry best practices and guarantee that they keep up with changing security threats. When it is feasible, automate patch deployment to improve productivity and shorten reaction times.