Information Security Strategy

Overview :

Global leader in ride-hailing, food delivery, and mobility services Uber Technologies Inc., maintains a sophisticated information security policy which is reflected deeply within this document. Uber as a cloud-native enterprise operating in over 70 countries, is deeply invested in data analytics; therefore, it has to manage incredibly large data sets that include user geo locations, payment details, driver records, and real-time analytics. With the increasing intricacy of Uber's multifaceted operations, shifting cybersecurity risks, and strict compliance mandates like CCPA and GDPR, Uber faces distinct requirements for a comprehensive safeguard strategy.

This document lays out an effective Uber business strategy by aligning it with security investment to improve sustainable operational resilience, reduce risks, and enhance Uber's security maturity within one to three years. Even though ISO/IEC 27001 will not serve as the primary framework, it is intended to fill in control gaps and fortify key domains which will positioned Uber better strategically defensively. Ultimately, Uber will achieve a balanced progressive security approach that goes hand in hand with proactive compliance, business innovation, mitigation of regulatory scrutiny, and intel-driven compliance policies.

Organizational Context and Assumptions:

With its main office in the US, Uber Technologies Inc. is a global company that offers ride-hailing, freight logistics, Uber Eats food delivery, and autonomous vehicle research services. With its headquarters in San Francisco, Uber operates in over 70 countries and 10,000 cities globally. The company connects more than 130 million monthly active users with over 5 million drivers via its mobile-based platform. Uber's core services are supported by its cloud-native, highly scalable architecture, which makes use of AWS and Google Cloud. Pricing, routing, and fraud prevention all depend on its developments in artificial intelligence and machine learning.

Size, sector, critical assets, regulatory landscape

Uber is an international technology and mobility company with almost 30,000 employees and over 70 countries where its services operate. Its major platforms are Uber-ride-share, Uber Eats-food delivery, Uber Freight-trucking services, and Uber for Business. The highest-valued assets of the company are operational core assets, including pricing and routing algorithms, driver data such as licenses and background checks, and users' personal data, e.g., names, locations, and credit card details. These operational core assets are hosted on the cloud infrastructure and powered by artificial intelligence and machine learning. The systems of Uber are laws and are under regulations since it operates internationally.

This includes GDPR in Europe, CCPA and CPRA in the US, PCI DSS for secure payment processing, and HIPAA for health services. The company also complies with Brazil's LGPD and any labor laws applicable to gig workers in each country. The wide array of diverse legal requirements places security and compliance as an utmost priority for the company.

Stakeholder analysis (board, IT, users, regulators)

The board of directors oversees and applies strategic governance to risk and compliance. Executive management acts operationally for setting priorities in customer trust. Infrastructure and security are aspects under IT and security teams. End users (drivers and riders) expect respective privacy and service continuity. Regulators monitor compliance with the laws-Recruitment, data protection, and transportation. Third-party vendors and associates also have to do with the security ecosystem.

Define the current cybersecurity posture and threat environment

Uber has created its cyber security capabilities, especially since the incidents of a year ago. Also, it is a high-profile digital platform that is often targeted. Dangers include phishing, credentials theft, cloud misconscience, malicious internal formula, unsafe APIs and third-party weaknesses. While Uber has monitoring, encryption and access control, it should continue to improve due to its changing environment.

Identify business drivers (e.g., digital transformation, regulatory pressure)

Prominent commercial drivers include global expansion, digital change initiative such as AI-powered dynamics, increasing demand for user privacy and security and pressure from regulators and stakeholders to improve data regime. The need to prevent reputed damage and ensure compliance in each market is central for Uber's ongoing security investment strategy.

Five Strategic Information Security Goals (1–3 Year Horizon)

Goal1: Strengthen Access and Identity Management (IAM)

Strengthen access and identification management (IAM) Uber's first strategic goal is to reach out to all internal systems and platforms and strengthen identification management. This involves adopting zero trust approach, applying multi-factor authentication (MFA), and to limit user privileges to role-based access control (RBAC). By doing this, Uber can reduce the risk of unauthorized access, especially with compromised credentials or internal formula hazards. This goal is of average through full MFA adoption, centralized access management and reduction in incidents related to access.

Strategic Objective:

Implement a Zero Trust-based identity and access framework to ensure that only authorized users can access critical systems.

Success Indicator: Lowering complete MFA enforcement, centralized access control, and access related events.

Main strategy: Deploy MFA, single sign-on (SSO), RBAC and automated user access reviews.

Kpis: 100% MFA Adoption Violation of <1% per audit 98% provision accuracy

risk mitigation: Credentials reduce the risks of theft, unauthorized access and internal formula.

Goal 2: Improve third-party risk management

The second goal is to improve third-party risk management. As Uber depends on many vendors and external services, he should assess and monitor these relationships more effectively. This includes making a full vendor inventory, reviewing safety before onboarding, and frequent tracking vendors access and activity. Strengthening the region reduces the risk of data violations caused by unsafe third-party systems.

Strategic objective: Control the risks related to the seller through structured onboarding, access range and continuous monitoring.

Success Indicator: The seller inventory was completed, all high -risk vendors evaluated, and immediately addressed the risks.

Main strategy: Pre-pronounced security review, API access control, seller classification and periodic audit.

Kpis: 90% vendors evaluated before onboarding <30 days to solve the seller risks 100% audit coverage for important vendors

risk mitigation: Unprotected third-party prevents data leaks or violations arising from integration.

Goal 3: Increase data protection and encryption

The third goal focuses on increasing data security and encryption. Uber must ensure that all individual and sensitive data - such as rider information, driver profiles and trip history - have been safely encrypted in both transit and comfort. In addition, data loss prevention (DLP) tools should be applied to detect and prevent unauthorized data transfer. This will help Uber to comply with data safety laws and reduce the possibility of data exposure.

Strategic objective: Control the risks related to the seller through structured onboarding, access range and continuous monitoring.

Success Indicator: The seller inventory was completed, all high -risk vendors evaluated, and immediately addressed the risks.

Main strategy: Pre-pronounced security review, API access control, seller classification and periodic audit.

Strategic objective: Secure sensitive data through complete encryption, classification and DLP policies.

Success Indicator: No uninterrupted data exposure; Complete compliance of data protection laws. Main strategy: Apply encryption in comfort and transit, deploy DLP tool, and apply data retention regulations.

Kpis: 100% encryption coverage for important data 95% decrease in DLP Alert 90%+ audit compliance score.

Risk mitigation: Prevents data violations, fines and reputed damage under GDPR/CCPA.

Goal 4: Strengthen Incident Response and Detection

The fourth goal is to build a sharp and clever event reaction and detection system. Uber needs to shorten the time it takes to find out, respond and recover from safety events. It can be obtained by using automatic monitoring devices, improvement in the system that detects the system and running regular security drills. With rapid detection and well -prepared teams, Uber can limit the effects of any cyber attack.

Strategic objective: Detect the dangers and expedite the response through automation and preparations.

Success Indicator: Effective handling of rapid response time and events.

Main strategy: Increase Siem/SOAR, Run Red/Blue Team Drill, maintain the event playbook.

Kpis: MTTD <10 minutes MTTR <2 hours 100% playbook coverage.

Risk mitigation: The breech limits the effect and ensures regulatory compliance through timely response.

Goal 5: Mitigate Insider Threats

The fifth goal is to reduce the risk of internal formula hazards by strong control, continuous monitoring and establishing employee awareness programs. The dangers of the insider can unknowingly generate mistakes by partners with malicious tasks and access to employees, contractors, or Uber's system. To address this, Uber must implement behavioral analytics tools to detect abnormal activity, review regular access and apply the principle of at least privilege in all departments. Equally important security is to promote the culture of awareness. All employees should receive targeted training on identifying suspicious behavior, handling sensitive data responsibly and reporting potential safety concerns. By combining technical controls with frequent education, Uber can reduce the risks related to internal formula and improve the initial identity and reaction.

Strategic objective: Reduce internal risks through behavior monitoring, strict access control and staff awareness.

Success Indicator: Less insider events and strong security behavior in teams.

Main strategy: Use behavioral analytics, conduct access reviews, and provide insider threat training.

Kpis: 40% decrease in internal events 100% training complete Monthly review of privileged accounts.

Risk mitigation: Increasing confidence and compliance, both deliberately and accidental insider addresses risks.

Action Plan:

The table below maps one key initiative to each strategic goal, providing a clear breakdown of each initiative's description, timeline, stakeholders, dependencies, and resource needs.

Goal	Initiative	Description & Purpose	Timeline	Owners / Stakeholders	Dependencies	Budget / Resources
Goal 1: Strengthen IAM	Enterprise IAM Rollout	Deploy centralized identity management (SSO + MFA) across Uber's internal systems to reduce access-related risks.	Month 1–3	IT Security Team, HR, App Owners	System integration readiness, user directory updates	Software licenses, internal training sessions
Goal 2: Improve Third-Party Risk Management	Vendor Risk Program Launch	Build a vendor risk framework including pre-contract evaluation, risk tiers, and periodic audits.	Month 2–5	Vendor Management, Legal, Security	Contract access, vendor cooperation	Compliance tools, audit staff hours
Goal 3: Enhance Data Protection	Encryption & DLP Upgrade	Encrypt sensitive data at rest/in transit and apply DLP across data flows to prevent unauthorized leaks.	Month 3–6	Data Engineering, IT Ops, Compliance	Data classification, system audit logs	DLP licensing, storage encryption tools

Goal 4: Strengthen Incident Response	IR Playbooks & Drill Program	Develop incident playbooks for common scenarios and conduct Red/Blue team simulations.	Month 4–7	SOC Team, IT, Security Awareness Team	Finalized risk scenarios, SOC availability	IR automation tools, training hours
Goal 5: Mitigate Insider Threats	Insider Threat Awareness Campaign	Launch behavior monitoring tools and deliver specialized insider risk training to all staff.	Month 5–8	HR, Security, Department Managers	Policy updates, training platform	Awareness materials, UEBA software license

Strategic Roadmap:

To effectively implement Uber's information safety strategy, a phased roadmap is proposed in the horizon three times: short-term (0–3 months), mid-term (4–8 months), and long-term (9–12+ months). Each phase is given priority based on the readiness of the risk, business effects, cost-effectiveness and the readiness of Uber to deploy the necessary controls.

Short-term (0-3 months)

Focus: High risk decrease, rapid victory, fundamental control.

Initiative: Post multi-factor authentication (MFA) in all internal systems Launch Enterprise-Wide Single Sign-On (SSO) solution Sellers start inventory and classification Conduct Insider Threat Awareness Training.

Justification: These initiatives provide immediate risk reduction (eg, unauthorized access and preventing account acquisition) with relatively low cost and high organizational readiness. They also do ground tasks for subsequent efforts.

Mid-term (4-8 months)

Focus: detection, visibility and advanced protection .

Initiative: Apply behavioral-based user surveillance (UEBA) Data Loss Prevention (DLP) deploy equipment Operate the red/blue team and follow the general event scenarios Start an encryption rollout in important systems .

Justification: These efforts meet medium-to-high risk decrease and are modestly complicated to deploy. Professional value is important, especially in the event reaction readiness and improving data regime.

Long term (9–12+ month)

Focus: maturity, adaptation and automation.

Initiative: Access a complete access review and policy enforcement Conduct the third-party audit and formalize the seller scoring system Integrate devsecops in development life cycle Extend global compliance monitoring with alerting.

Justification: These efforts require larger resource commitments and cultural or process changes, but offer long-term efficiency, resilience, and regulatory assurance. They are best implemented once foundational layers are stabilized.

Prioritization Logic Summary

The table below summarizes the prioritization logic used to phase each initiative based on risk reduction potential, business value, cost-benefit, and organizational readiness.

Criteria	Short-Term	Mid-Term	Long-Term
Risk Reduction	Immediate (access risks)	Medium (insider/data)	High (long-term resilience)
Business Value	High	High	High
Cost-Benefit Ratio	High (low cost, big win)	Medium	Medium to Low
Readiness	High	Medium	Requires prior progress

Gap Assessment:

ISO/IEC 27001 shows strong alignment in major areas, including comparison of Uber's current security practices with access control, encryption and reaction to the event. Uber SSO uses MFA and data encryption extensively. However, ISO alignment can be formally strengthened by automatic and major management processes. In the third-party risk management, Uber conducts proper hard work, but a standardized seller will benefit from the risk cycle, including periodic reviews and contract-based security segment. Additionally, while the event response abilities exist, ISO suggests expansion with regular simulation and department-level playbook to improve preparations. These adjustments are not indicators of non-transportation, but there are opportunities to increase stability and maturity without the need for full ISO certification.

Executive Summary and Recommendations

This information safety strategy outlines a concentrated plan to further strengthen Uber's cyber security maturity by aligning the ISO/IEC 27001 with the best practices. While Uber already maintains strong control in areas such as access management, data encryption and event reaction, this strategy identifies opportunities to increase continuity, efficiency and visibility in its global operation.

The proposed targets include accessing and reinforcing identity control, third-party risk governance, expanding data security measures, pursuing event reaction processes and internal formulas explore the danger and strengthening training. These initiatives are designed to manufacture on existing systems, which ensure continuous improvement in the response to developing dangers and regulatory expectations.

The strategy crosses these enhancement of short, middle and long -term deadlines, which prefer a high risk decrease and commercial value initiative with minimal operating disintegration.

Benefits include better flexibility against cyber attacks, compliance with rules such as GDPR and CCPA and more and more trusts from customers and partners. To be successful, the strategy requires executive-level support to align business units, support training and policy enforcement and approve necessary resource allocation.

By refining his already strong security currency, Uber can remain a global leader in dynamics, protecting data and trust at the core of his services.