Case Study (Okta)

Created by	S.Kaushik
Created time	@January 20, 2026 8:12 PM
Category	Strategy doc
Last edited by	S.Kaushik
Last updated time	@January 22, 2026 9:14 PM

Professional GRC Case Study

By

Kaushik Sathyamurthy

This case study is for educational and portfolio purposes only. All analysis is based on publicly available information and does not reflect Okta's internal systems, confidential information, controls, or risk posture.

This report presents a hypothetical GRC and ISRM assessment of Okta Inc., a global Identity and Access Management (IAM) provider, used as a case study to demonstrate enterprise risk analysis

Table of contents

Section 1: Case Study Scope & Rationale

This assessment examines the technology sector with a focus on the packaged software industry, which underpins secure, efficient, and scalable digital transformation. As organisations increasingly adopt cloud services, hybrid work models, and data-centric operating environments, packaged software provides standardised, deployable solutions that accelerate digital agility, reduce time-to-market, and strengthen cybersecurity posture (UXmatters 2024). Compared to bespoke systems, packaged platforms integrate more effectively with modern IT architectures and regulatory frameworks, making them particularly relevant for enterprise risk management analysis.

Okta Inc. was selected as a representative Identity and Access Management (IAM) provider to model enterprise GRC and ISRM practices within a cloud-native identity platform. IAM services play a critical role in protecting sensitive information by enforcing secure authentication, authorisation, and access controls across distributed environments. The global IAM market is forecast to reach USD 80 billion by 2030, driven by escalating cybersecurity threats and increasing regulatory requirements (MarketsandMarkets 2024).

Okta differentiates itself from competitors such as Ping Identity and ForgeRock through its Zero Trust architecture, passwordless authentication capabilities (FastPass), and AI-driven threat detection. The platform serves over 17,000 customers and has been recognised as a Gartner Magic Quadrant Leader for Access Management for eight consecutive years (Okta 2024).

Okta's strong market position is reflected in FY2024 revenue of USD 2.27 billion and a market capitalisation of approximately USD 12 billion (Investors Business Daily 2024). This position contrasts with a series of publicly reported security incidents in 2022 and 2023, as well as a patent-related legal dispute reported in 2025 (Bloomberg Law 2025; VentureBeat 2025). These events underscore both the organisation's commercial significance and its exposure to security, legal, and third-party risk domains, making Okta a suitable subject for enterprise risk analysis.

Section 2 and 3: Discussion of Information and Sources Accessed:

Source: Enterprise Authentication Architectures: Comparing Kerberos, Active Directory, and Okta for Cloud Data Platforms - Uppaluri

Evidence collected:

The article analyses Okta's integration mechanisms in comparison with legacy systems such as Kerberos and Active Directory. It identifies both strengths and limitations in Okta's API-first architecture and token management approach. This analysis provides insight into Okta's

architectural design choices and the operational complexity of modern identity management ecosystems (Uppaluri 2025).

Bias discussion:

The research is peer reviewed and methodologically sound, but it presents an optimistic perspective due to its reliance on laboratory-based testing. The absence of real-world user behaviour and routine organisational conditions limits the generalisability of the findings.

Further information required:

Additional evidence on session control, authentication flows, and real-world operational use is required to fully assess identity lifecycle management and contextual security controls.

Source: Data Breach Investigations Report – Verizon Business

Evidence Collected: Cross-sector trends in data breaches were observed, with particular attention to the frequent occurrence of identity-based incidents and misconfigurations in cloud environments. These findings provide insight into the external environment in which Okta operates (Verizon 2024).

Bias Discussion: The report exhibits a negative bias, as it relies primarily on voluntary disclosures from North America. Breaches from other regions or those that were not publicly reported are therefore not captured.

Further Information Required: Additional reports covering other regions, such as those published by ACSC and ENISA, should be reviewed to obtain a more comprehensive understanding of global data breach trends.

Source: Magic Quadrant for Access Management – Gartner 2024

Evidence Collected: Okta has been consistently recognized as a market leader by Gartner; however, rising client concerns and dissatisfaction following a series of recent security breaches were also noted. These insights provide an understanding of the competitive landscape and the evolving customer perception of Okta (Guthrie et al. 2024).

Bias Discussion: Gartner's ratings may reflect a positive commercial bias, as they rely on vendor-sponsored analyst input and client surveys, which can favor prominent providers such as Okta. Additional information, including customer attrition data, renewal rates, and independent customer reviews, should be examined to validate Gartner's observations and strengthen understanding of Okta's external perception.

Section 4: Internal and External Context Internal Analysis

Organizational Culture and Objectives: Okta fosters a workplace culture characterized by transparency, integrity, teamwork, and continuous learning, with a strong emphasis on security and customer success. Diversity, equity, and inclusion are prioritized, and hybrid work models are supported to enhance employee well-being and flexibility (Johnson 2019).

Internal Stakeholders and Organizational Management: Okta is overseen by co-founders Todd McKinnon (CEO) and Frederic Kerrest (COO), with strategic governance and oversight provided by the board of directors and executive leadership. Critical functions such as digital identity protection are managed by internal teams, including cybersecurity, engineering, identity and access management platform developers, and governance functions (The Org n.d.).

Okta demonstrates significant capabilities across its people, systems, and financial resources. The company leverages a skilled workforce and annual revenue exceeding $2 billion to support ongoing research and development and product innovation. While repeated layoffs between 2022 and 2024 have raised concerns regarding internal stability and strategic direction, Okta continues to maintain strong technical capabilities, including Zero Trust architecture, global cloud infrastructure, and partnerships with AWS, Microsoft, and Google (Council 2025; Amazon Web Services n.d.; Uppaluri 2025).

The organization's objectives align with its core mission of connecting people securely with the right technology. Strategic initiatives include expanding the customer base, advancing artificial intelligence to improve identity management and threat detection, and securing large enterprise contracts, as evidenced by the growth in high-value accounts (du Preez 2024).

Strategic Initiatives and Risk Mitigation: To support its objectives, Okta has implemented plans and policies aimed at enhancing its identity and access management offerings through AI and automation, as well as strengthening partnerships with cloud providers. The 2024 login bypass vulnerability highlighted security gaps with potential implications for customer trust. In response, QA processes, OAuth governance, and token sanitization were improved, demonstrating resilience and maintaining competitiveness in a market that includes rivals such as OneLogin, which offer simpler or more cost-effective IAM solutions (Lawler 2024).

External Analysis

Business Environment: Okta experienced significant growth in 2024, with revenue increasing 14% to $665 million and earnings rising 52%, surpassing expectations (Investors Business Daily 2024). This performance reflects a robust business model and strong market demand. To sustain momentum, continued scaling of operations and consistent delivery are required to meet growing enterprise identity and access management needs.

Social Environment: Public concern regarding data privacy has intensified, particularly following high-profile breaches. Okta has responded by prioritizing digital identity protection, including the implementation of stricter security protocols after the 2022–2023 breach (Investors Business Daily 2024). While this strengthens reputation and aligns with public expectations, it also increases pressure to maintain incident-free operations.

Regulatory Environment: Compliance with regulatory frameworks such as NIST CSF in the U.S. and the Australian Essential Eight, with emphasis on multi-factor authentication, is mandatory (Cybersecurity Dive 2024a). As regulations evolve, Zero Trust security implementations must remain adaptable across jurisdictions to avoid potential compliance gaps and penalties.

Cultural Environment: Following the 2023 breach, internal initiatives were implemented to strengthen Okta's security culture. Investments in more robust systems and enhanced practices have been made to rebuild customer trust and proactively address potential threats (Cybersecurity Dive 2024b). These efforts indicate a shift from reactive responses toward embedding security as a core organizational value.

Competitive Environment: Okta operates in a competitive landscape alongside major players such as Salesforce and Microsoft. Its focus on integrating identity solutions with emerging technologies, including single sign-on, provides specialised value. However, higher pricing may prompt price-sensitive customers to select competitors offering bundled suites (MarketWatch 2024). Continued differentiation through innovation and service depth remains critical.

Financial Environment: Year-over-year revenue growth of 14% in Q3 2024 underscores Okta's strong financial performance (Investors Business Daily 2024). Despite this, economic downturns may impact IT budgets, particularly in large enterprises. Sustaining financial stability will require demonstrating measurable value and considering pricing adjustments for sensitive markets.

Political Environment: Increased government focus on cybersecurity presents opportunities for Okta, especially in securing public sector contracts (MarketWatch 2024). These opportunities are accompanied by heightened scrutiny and compliance requirements. Effective navigation of the political landscape will depend on maintaining transparency, ensuring compliance, and demonstrating adaptability in contract execution.

SWOT Analysis

Strengths	Weaknesses
Strong revenue growth (14% YoY in Q3 2024), more than what analysts had expected indicates solid business performance and resilience (Investor's Business Daily 2024).	The number of layoffs from 2022 to 2024 has left many companies with a weak infrastructure and no clear strategy, reflecting internal instability (Council 2025).
The market leader in IAM with more than 17,000 clients and consistent Gartner recognition reinforcing brand credibility and trust (Business Wire 2024).	The Security issues like the 2024 login bypass bug can affect customer trust highlight technical vulnerabilities (Lawler 2024).
The latest technologies such as the Zero Trust framework and AI threat detection enhance competitive edge which strengthens its security offerings (du Preez 2024).	Has a more focused product offering than competitors who offer full suite solutions like Microsoft limiting versatility (Software World n.d.).
Strategic partnerships with Microsoft, Google and AWS enhance service integration and market reach (Amazon Web Services n.d.).	Pricing is higher than that of competitors like OneLogin which may hinder market share in price- sensitive segments (Software World n.d.).

Opportunities	Threats
Increasing demand for IAM and cybersecurity solutions globally create scope for innovation (Okta 2025b).	Has strong competitors which include Microsoft, Salesforce and OneLogin leading to pricing and innovation pressure (MarketWatch 2024).
Integration of AI and generative identity security can enhance the identity solutions (du Preez 2024).	Strict data privacy laws (e.g. GDPR, CCPA) increase regulatory pressure and compliance cost (Cybersecurity Dive 2024b).
Market growth and the capture of large enterprise businesses can increase the revenue of Okta, expanding its client base (Ohlen 2024).	Political instability and regulatory risks can be a challenge to growth (MarketWatch 2024).
The public's interest in privacy and identity security increases the need for IAM services making Okta a great contender for its innovative solution (Investors Business Daily 2024).	The company's image and investment attractiveness have been damaged by frequent security incidents, affecting stakeholder confidence (Investors Business Daily 2024).

Section 5: Stakeholder Identification and Analysis

Effective risk management requires the identification and assessment of individuals and entities that influence, or are influenced by, the organization's operations. This analysis examines Okta's internal and external stakeholders, providing a comprehensive view of how each entity impacts not only the risk landscape but also the operational, financial, legal, and reputational dimensions of identity and access management.

Table 1: Stakeholder ranking

Rank	Stakeholder	Relevance	Risk Involvement	Influence Level	Type
1	Customers (Apple, Open AI, CVS, Scale AI)	The Customers fall in the frontline in case of a system/ network breach and are directly dependent on Okta for IAM services.	Data Breaches or Service failure affect client operations, SLA violations, and reputational trust (Okta Inc.2025).	Very High – revenue and brand risk	E
2	Board of Directors	They set the strategic risk direction and oversee corporate governance.	Sets risk appetite, approves controls, and responds to major incidents (Okta Inc.2025b).	Very High – influences legal, regulatory, and reputational outcomes	I
3	Executive Leadership (CEO, COO)	They set the overall risk tolerance, approve major	Set security priorities, approve critical risk	Very High – decisions impact company	I

		investments and define the corporate strategy.	initiatives, and oversee compliance (Okta Inc.2025b).	direction and reputation	
4	Platform Engineering and IT Operations Teams	They ensure reliable platform performance, secure development and innovation across Okta's platform.	Ensure secure development, platform uptime, roadmap planning and Collaborative compliant service delivery (Todd 2015).	High – product integrity, system reliability, and market competitiveness, breach prevention.	I
5	Legal, Compliance & Risk Oversight Teams	They ensure that all the legal and regulatory compliance are met and advice or mitigating any identified risks.	Manage contracts, track compliance, conduct audits, evaluate internal controls, and provide legal-risk guidance (David 2022).	High – legal protection, regulatory alignment, and continuous risk monitoring	I
6	Third Party (Solution Providers, Suppliers, Technology Partners)	They are responsible for deploying Okta's offerings and maintaining the organisation's vast cloud infrastructure.	Misconfigurations, delays, or failures can affect system availability and cause service outages (data leaks) (Lawler 2024).	High – operational dependency	E
7	Media and Tech Analysts (Wired, Bloomberg, Axios)	They shape external narrative, influencing investor confidence and customer sentiment following public cybersecurity disclosures.	A breach will amplify negative coverage can cause reputational damage and affect market perceptions (Coombs 2015).	High – reputational and response risk	E
8	Investors & Shareholders (Vanguard, BlackRock)	They expect finance growth and demand disclosure of cyber risk.	React to risk disclosures (e.g., breaches, lawsuits) by influencing board governance and share prices (Investor's Business Daily 2025).	High – strategic financial influence	E
9	Cyber Insurance Providers (e.g., AIG, Marsh)	They help pay breach and lawsuit costs. Premiums depend on how strong Okta's security looks.	After a breach they can deny payment, increase costs, or demand stronger controls affecting Okta directly (AIG 2024).	Medium – financial risk planning	E
10	Regulators (FedRAMP, NIST, AICPA , ACSC)	Their certifications open Okta's door to big public- sector and high-security clients. Their rules define Okta's minimum-security line.	A breach can trigger probes, fines, or a stop-work order. Public reports can damage Okta's name even more. (Cybersecurity Dive 2024b; Okta 2025a).	Medium – legal and operational risk	E

E = External Stakeholder, **I** = Internal Stakeholder

Section 6: Risk Management Context

This analysis evaluates key information security risks that could affect Okta's ability to deliver reliable identity and access management services. Focus areas include credential theft, multi-factor authentication fatigue, tool misuse, misconfigurations, and non-compliance with legal obligations such as GDPR and CCPA. The scope has been refined to prioritize risks with the greatest potential impact on business continuity, customer trust, and regulatory compliance. Risks are assessed across people, processes, and technology using a qualitative risk matrix, providing insights to support informed decision-making, minimize operational disruption, and achieve strategic security objectives.

Section 7: Risk Evaluation Criteria

The assessment applies criteria derived from ISO/IEC 27005, adapted to Okta's position as a global identity and access management provider. Historical incidents and threat intelligence were used to evaluate risks in terms of likelihood and business impact, with prioritization conducted through a risk matrix to guide mitigation efforts.

Table 2: Consequence Scale

Level	Consequence	Impact Domains	Justification
1 – Insignificant	No impact on users or operations	Internal only	Phishing attacks or identity and access management misconfigurations could bypass existing safeguards and compromise accounts, despite previous mitigation efforts, such as those following the 2022 Oktapus incident (Rustam 2022).
2 – Minor	Minor inconvenience, no breach	Operational	Internal login systems may experience instability during product feature rollouts, potentially disrupting internal operations even if client-facing services remain unaffected (Chan 2021).
3 – Moderate	Temporary service disruption	Trust, availability, compliance	Service-level agreement violations or platform degradation could occur due to external third-party network failures, resulting in diminished client trust and operational delays for Okta-integrated platforms (Australian Cyber Security Centre 2023).
4 – Major	Operational /Reputational damage	Legal, trust, client services	Vulnerabilities in Okta's support infrastructure may be exploited to access sensitive customer session tokens, as demonstrated by the October 2023 breach affecting BeyondTrust and 1Password (Sergiu 2023).
5 – Catastrophic	System compromise, data breach	Legal, financial, reputation	Compromise of third-party vendors could provide attackers limited access to internal systems, impacting multiple customers, as observed in the January 2022 Sitel breach (David 2022).

Table 3: Likelihood Scale

Level	Likelihood	Justification
1 – Rare	Theoretically possible	A full system compromise remains a theoretical possibility, as demonstrated by incidents such as the 2020 SolarWinds breach, but no such compromise has been observed at Okta.
2 – Unlikely	Uncommon, needs specific conditions	Minor operational disruptions may result from third-party errors, exemplified by the March 2022 Sitel-related breach (David 2022).
3 – Possible	Occasionally seen in the industry	Token misuse and integration misconfigurations have caused moderate service impacts at Okta and comparable identity and access management providers.
4 – Likely	Frequent attempts, moderate success	Credential phishing and credential stuffing attacks have frequently targeted Okta users, with moderate success rates (Salman 2024).
5 – Almost Certain	Ongoing or highly expected	Multi-factor authentication fatigue is an emerging threat, highlighted by the 2022 Uber breach, which exploited weaknesses in Okta-based authentication (Salman 2024).

These levels are informed by threat patterns in IAM systems and past breaches involving Okta and similar providers.

Risk Matrix

Figure 1. Risk matrix

Section 8: Asset Identification

Key assets within Okta Inc.'s identity and access management platform are identified and assessed. Valuation considers traditional security principles including confidentiality, integrity, and availability, alongside extended considerations such as accountability, authenticity, and reliability. Each asset is evaluated in terms of interdependencies, potential business impact, regulatory significance, and influence on stakeholder trust.

Table 4: Asset Identification

Asset Type	Asset	Value & Interdependencies	Security Primitives Affected	Source / Justification
Information	Session tokens & authentication logs	Secure system control depends on these. If breached, attackers can impersonate users, disrupt operations, and violate customer	Confidentiality, Integrity, Authenticity	VentureBeat (2025)

		SLAs, damaging business trust.		
Information	Customer identity store (PII, SSO profiles)	Core to identity verification and regulatory compliance. Breach risks include legal fines, lawsuits, loss of clients, and damage to brand reputation.	Confidentiality, Integrity, Reliability	Authomize (2023)
Software	Admin Console (IAM control plane)	Governs access rights and provisioning. A compromise here exposes full system control, causes governance issues, and risks audit failure.	Confidentiality, Availability, Accountability	Bloomberg Law (2025)
Infrastructure	API Gateway & Load Balancers	Vital to real-time traffic handling. Outages disrupt authentication flow, delay services, breach SLAs, and frustrate customers.	Availability, Reliability	ThousandEyes (2022)
Infrastructure	Office spaces, workstations, servers, VPNs	Essential for daily operations and compliance reporting. Damage or theft affects continuity, delays decision-making, and reduces availability of secure access.	Availability, Integrity	Cybersecurity Dive (2024a)
Process	Incident response & breach notification SOPs	Enables timely legal compliance and audit readiness. Weak SOPs increase incident damage and regulatory penalties.	Accountability, Availability	Lily (2023)
Data Repositories	Audit logs & access records	Required for audit trails and post-breach reviews. Missing logs obstruct investigations, affect legal reporting, and reduce transparency.	Integrity, Accountability, Non-repudiation	Cybersecurity Dive (2024a)
Human Assets	IAM engineers and support staff	Integral to secure configuration and response. Human error or phishing leads to leaks, misconfigurations, and insider attacks.	Integrity, Authenticity, Reliability	Cybersecurity Dive (2024a)
Third-Party Access	External engineer credentials, integrations	High-privilege third-party access via Auth0 and similar platforms are frequent attack vectors; poor control can expose internal systems.	Confidentiality, Integrity, Reliability	Lawler (2024)
Intangibles	Customer trust & brand equity	Public confidence drives revenue. Repeated incidents reduce brand value, customer retention, and investor interest—affecting long-term viability.	All (C, I, A, Accountability, Authenticity)	Investor's Business Daily (2024)

These assets form the foundation of Okta's IAM operations and are prioritised in risk evaluation due to their regulatory importance, operational criticality, and influence on stakeholder trust.

Section 9: Essential Elements

Table 5: Essential Elements

Basis for Selecting Data (Category)	Essential Element (Purpose / Objective / Relevant Issue)
Mission and Vision Alignment	Okta's mission is to provide secure access across all digital environments, while its vision emphasizes enabling full identity control. The organization's ongoing commitment to large-scale user security management supports both market expansion and its innovation cycle (Okta 2025b; Nasdaq 2025).
Customer Trust and Brand Image	Sustaining strong customer trust is critical for business growth. Transparent breach responses, combined with enhanced user protection strategies, reinforce Okta's market position and uphold its reputation (Cybersecurity Dive 2024b; VentureBeat 2025).
Financial Performance and Operational Resilience	Revenue growth relies on securing large enterprise contracts and maintaining operational continuity through effective breach management (Investors Business Daily 2025; Ohlen 2024).
Regulatory Compliance	Okta maintains compliance with regulations such as GDPR, CCPA, and HIPAA, supported by robust governance structures that reduce legal risk and facilitate entry into sensitive industries (Cybersecurity Dive 2024a; Okta 2025a).
Physical Infrastructure (Authentication Servers, Data Centres)	Its physical infrastructure demonstrates high availability, redundancy, and cyber protection, ensuring service commitments are upheld and large-scale outages are prevented (Okta 2025a; Lawler 2024).
Technology Stack (API Gateway, MFA Systems)	To defend against phishing, credential theft, and emerging cloud threats, secure APIs and multi-factor authentication systems are employed to safeguard identity workflows at every stage (VentureBeat 2025; Lawler 2024).
Human Resources (IAM Operations Team)	A highly trained and security-conscious IAM team underpins operational stability by mitigating insider threats and ensuring trustworthy authentication processes (Council 2025; Okta 2025a).

Third-Party Vendors and Supply Chain	Proactive oversight of third-party vendors mitigates risks to integrated data environments, preventing vulnerabilities in external partners from affecting internal systems (VentureBeat 2025; Cybersecurity Dive 2024a).
Research and Innovation (AI-driven Identity Security)	Okta leverages AI and machine learning to anticipate identity-based threats, enabling personalized authentication experiences and adaptive security solutions that scale with user demand (du Preez 2024; Okta 2025b).

Section 10: Approaches to Risk Identification

Okta's primary risks were identified through a structured three-step process.

1. An open brainstorming session was conducted to capture potential threats, ranging from leaked session tokens to supplier failures. This exercise produced a comprehensive list of possible risks.
2. Identified risks were mapped to Okta's critical business elements, including trust, regulatory compliance, and service continuity, by evaluating which risks could compromise these areas. This approach ensured the analysis was directly aligned with business objectives, customer expectations, and legal obligations.
3. Historical incidents, such as the 2022 vendor breach, were reviewed, and scenario analyses were performed to assess potential impacts on uptime and reputation. Combining creative ideation with structured evaluation resulted in a risk register aligned with Okta's strategic priorities.

Section 11: Risk Identification

Table 6: Risk Identification

Class	**Risk statement**	**Source of risk**	**Threat event / Incident**	**Impact / Consequence**	**Vulnerability** ***info-sec only***	**Timing & Location**	**Capability** ***(D)***	**Possible / Existing controls**
InfoSec (D)	If a phishing attack compromises user accounts, there is a risk of unauthorised access, which could affect customer trust and Okta's objectives (Mirkasymov & Martinez 2022).	External phishers	Spoofed Okta login mail / SMS	C-High, I-Med, Rep-High	Phishable MFA; low user awareness	Ongoing – remote, global	High	FIDO2 MFA, user training, mail filters
InfoSec (D)	If users are confused by repeated MFA prompts, they may fall for scams, which can cause reputational and security damage (Salman 2024).	Crimeware groups	Push- bomb social	I-High, Rep-High, Legal	Unlimited push; UX fatigue	Off- hours logins, cloud	Med	Rate limit push, adaptive MFA
InfoSec (A)	If ransomware attacks occur, it may lock down critical services and break contracts with commercial partners, causing serious conflict with the company's goals (Sergiu 2023).	Admin error	Wrong policy on sync server	I-High, A-Med, Cost	Manual provisioning; no lint	Mid- 2023, customer data centre	—	Change management, config audit
InfoSec (A)	If access controls are weak, users with excessive privileges can expose sensitive data, leading to non-compliance, which is the opposite of the company's compliance goal (Bloomberg Law 2025).	IAM engineers	Priv- escalation via bad role	C-High, I- High, GDPR fine	Incomplete access review	Sprints, cloud console	—	SOPs, peer review, templates
InfoSec (D)	If a super-admin is tricked	Nation- state APT	Spear- phish / 0-day	Catastrophic tenant loss	Break glass without FIDO2	Crisis periods, global	High	HW tokens, session

	by a hacker, a major data breach can occur, putting the platform and stakeholder trust at risk and threatening the platform's integrity (Bloomberg Law 2025).							monitor, network seg
Business	If the system is subjected to too much traffic, it can cause major disruptions of service with non-compliance to service agreements, which devalues the company's goals (Thousand Eyes 2022).	Infra capacity	High- traffic outage	Fin- High, Trust- High	Scale tests lacking	Q-end spikes, US-E	—	LB, HA design, synthetic tests
Business	If new privacy laws add complexity to auditing, it can lead to delays that affect compliance, revenue goals, and management's direction on regulatory compliance (Cybersecurity Dive 2024a).	Regulatory change	Audit failure / notice	Fin- High, Sales impact	Small compliance team	Annual audits, EU/US	—	ISO 27001, gap scans, legal watch
Business	If security incidents generate bad press, investors may be deterred, lowering the company’s value and undermining the objective of maintaining investor confidence (MarketWatch 2024).	Shareholders	Post- breach sell-off	Cap- Loss, Government pressure	Weak comms	Post-incident,NASDAQ	—	IR comms plan, transparency
Environmental	If a geopolitical conflict or pandemic forces border closures, shutting key datacentres and suppliers, the resulting identity-service delays cut revenue and damage Okta’s brand image (Okta 2025a).	Geopolitics, pandemics	Border shut, DC offline, staff sick	A -Catastrophic Fin – High	Single region, supplier gaps	Global, ongoing	—	Multi region DR, zero trust remote, supplier mix
InfoSec (D)	If a vendor’s device is compromised, session data may be leaked, exposing	Third party vendor	Sitel- style session theft	C-High, I- High, Cost	Over privy vendor access	Vendor RDP window s	Med	JIT access, session record, vendor audit

	customers and damaging third-party trust, which threatens the objective of protecting customer data (Bradbury 2022).							

Legend: C = Confidentiality, I = Integrity, A = Availability, H = High, M = Medium, Rep = Reputation, Fin= Financial, Rev = Revenue, Cap = Capital, D =Deliberate, A = Accidental, InfoSec = Information Security

Section 12: Business Risk

Risk Identification: Infrastructure Strain, Compliance Gaps & Economic Volatility

Risk Statement:

If Okta is unable to scale infrastructure during peak demand, maintain alignment with evolving compliance requirements, or respond effectively to market and tariff changes, service disruptions, certification delays, and diminished stakeholder confidence may occur. These challenges could ultimately result in client loss and negatively impact long-term strategic objectives (Okta 2025a; Cybersecurity Dive 2024a).

The risk is heightened during periods of rapid customer onboarding, changing regulations, or global service rollouts. Past challenges in managing heavy system loads and navigating regional compliance illustrate the importance of building flexible infrastructure and maintaining legal agility (Bloomberg Law 2025; ThousandEyes 2022). Economic uncertainty and rising tariffs further increase operational complexity (MarketWatch 2025).

Risk Analysis:

- **Likelihood:** High – Driven by constant changes in user demand, regulations, and market conditions
- **Consequence:** Very High – Could harm service reliability, financial performance, and stakeholder trust
- **Risk Level:** Extreme (High × Very High)

Treatment Plan:

- **To Reduce Likelihood:**

Multi-region auto-scaling and proactive load testing are employed to manage demand spikes (ThousandEyes 2022). Legal teams monitor regulatory updates and adapt services for specific regions as required (Bloomberg Law 2025).

- **To Reduce Consequence:**

Dynamic failover systems, automated audit logging, and inclusion of service-level agreement credits are implemented to reassure customers (Okta 2025b). Clear and consistent communication with clients and investors is maintained to uphold trust during disruptions (MarketWatch 2024).

- **Risk Sharing**

Vendor responsibilities are explicitly defined in contracts, and cyber insurance is maintained to mitigate potential financial losses (Okta 2025b).

- **Residual Risk:**

Despite controls, sudden regulatory changes or unexpected traffic surges may still occur. These are addressed through regular audits and crisis response drills (Cybersecurity Dive 2024b).

- **Monitoring:**

High-traffic scenarios are simulated regularly, compliance is reviewed monthly, and financial and operational resilience is tracked quarterly to ensure preparedness and responsiveness (Okta 2025a; VentureBeat 2025).

Section 13. Information Security Risk (Deliberate)

Risk Identified: Unauthorised access to admin systems through stolen credentials and misconfigurations.

Risk Statement:

If attackers gain access through stolen login credentials, weak vendor controls, or misconfigured user settings, they may compromise Okta's administrative systems and customer accounts. Potential consequences include leakage of sensitive data, service outages, legal exposure, and reputational damage (Bradbury 2022; VentureBeat 2025).

Risk Analysis (ISTRA Method)

The risk analysis was performed using the ISTRA methodology, a structured approach developed by Dr. Sue Dudley. This method evaluates the intent, capability, and resources of potential adversaries to assess the likelihood and potential impact of deliberate threats.

Table 7. ISTRA metrics

ISTRA Factor	Rating	Reasoning
Intent	High	Financially and politically driven attackers target IAM platforms (Rustam & Martinez 2022).
Capability	High	Skilled actors exploit known weaknesses using advanced tools (VentureBeat 2025).
Likelihood	Very Likely	These attacks are common in the industry (Salman 2024).
Adversary Type	High	Includes organised crime groups and state-linked actors (Council 2025).

Consequence: Catastrophic – High financial losses, regulatory fines, customer churn, and severe reputational damage due to multi-tenant impact and trust erosion. (Council 2025).

Risk Level: Extreme

Risk Treatment

To Reduce Likelihood:

- Phishing-resistant multi-factor authentication is enforced for administrative users, accompanied by regular training on evolving phishing techniques.
- Automated tools are deployed to review access settings and detect misconfigurations proactively (Cybersecurity Dive 2024a).
- Administrative access is limited in duration, with just-in-time approvals and role-based access controls implemented.

To Reduce Consequences:

- Administrative environments are isolated from live systems, with privileged users made aware of their responsibilities.
- Access is restricted strictly to necessary tasks, with all changes logged and responsible parties notified.
- Real-time alerts on suspicious actions are configured to enable rapid response by security teams.

Risk Sharing:

- Security obligations are incorporated into vendor contracts.
- Cyber insurance is maintained to mitigate potential financial and legal impacts (AIG 2024).

Residual Risk:

Risks associated with vendor misuse or token exposure remain. These are mitigated through ongoing user awareness programs, third-party assessments, and enforcement of responsibility across all human touchpoints (Cybersecurity Dive 2024a; Council 2025).

Monitoring and Review:

- Administrative activity is monitored in real time to detect anomalies early.
- Automated checks are performed for changes to access and permissions.
- Quarterly reviews with leadership re-evaluate threat levels.
- Full audits are conducted every six months to test MFA, admin controls, and breach response readiness.

Targeting administrative access represents a critical threat to Okta's operations and reputation. Effective mitigation requires strong controls, responsible vendor management, and continuous monitoring to sustain trust and ensure regulatory compliance.

Section 14: Information Security Risk (Accidental)

Risk Identified: Access misconfiguration due to human error.

Risk Statement:

Misconfigurations in identity and access settings due to human error may allow unauthorized users to access internal or customer systems. Potential consequences include data breaches, regulatory non-compliance, and reputational damage, all of which can undermine stakeholder trust (Okta 2025a; Salman 2024).

This risk is particularly prevalent during policy updates or vendor integrations, where errors in role-based access control, overlooked privilege escalations, or absence of review controls are commonly observed. Historical incidents, including the 2022 issue with Okta's support partner and the 2023 session token leak, demonstrate the tangible impact of such misconfigurations (Bradbury 2022; Gatlan 2023). The risk is further exacerbated by system complexity and the lack of comprehensive post-deployment checks (Cybersecurity Dive 2024a).

Risk Analysis:

A qualitative approach is suitable as it accounts for the unpredictability of human error and its context- dependent impact (Lawler 2024).

- **Likelihood: High –** Frequent due to ongoing configuration changes (Rustam & Martinez 2022).
- **Consequence: Very High –** Can result in exposure of customer data and likely to cause high financial loss, operational downtime, high legal/compliance risk, and high impact on customer trust. (Wired 2023; Gatlan 2023).

Risk Evaluation:

Using a likelihood vs impact matrix:

Risk Level: Extreme (High × Very High), Supported by evidence from previous Okta breaches and high stakeholder sensitivity (Okta 2025a; Nasdaq 2025).

Treatment Plan:

- **Reduce Likelihood:**

Access changes are peer-reviewed and enforced through structured approvals, supported by staff training on configuration scanning tools to validate changes prior to deployment (Council 2025).

- **Reduce Consequence:**

Time limits are imposed for administrative actions, real-time monitoring by support teams is implemented, and staff are equipped with and follow the breach Incident Response Plan and Business Continuity Plan (Lawler 2024).

- **Risk Sharing:**

Vendor contracts include clauses enforcing human accountability for breach handling and promoting a shared security culture (AIG 2024).

- **Residual Risk:**

Despite existing controls, human error and unforeseen integration issues may persist. These are mitigated through ongoing training, audit logs, and reinforced accountability (VentureBeat 2025; Council 2025).

Monitoring and Review

- Real-time alerting on access policy changes (Okta 2025b)
- Monthly IAM audit reviews (Salman 2024)
- Quarterly governance risk review (Nasdaq 2025)
- Biannual scenario testing of misconfiguration response (Cybersecurity Dive 2024a)

Misconfigurations in access settings represent one of the most common and potentially damaging operational risks. All aspects of identity and reputation must be protected through strict governance, automated safeguards, and continuous review and updates.

Section 15: Environmental Risk – Geopolitical Conflict & Pandemic Resurgence

Risk Statement:

Geopolitical instability or renewed pandemic threats may disrupt Okta's infrastructure or workforce, creating the potential for compromised service delivery and regulatory compliance. Such disruptions could result in stakeholder dissatisfaction, contract losses, and reputational damage (Okta 2025b; Cybersecurity Dive 2024b).

This risk is particularly relevant in regions experiencing conflict, health crises, or pressures related to digital sovereignty. As a global operator, Okta is exposed to regional shutdowns, travel restrictions, and workforce interruptions (Okta Inc. 2025). Additionally, instability may trigger data localisation requirements or new disclosure obligations, complicating compliance efforts and delaying cross-border operations (Okta Inc. 2025).

Risk Analysis:

A qualitative approach is used to assess the evolving and external nature of this risk.

- **Likelihood:** Very High – Escalating geopolitical instability and biosecurity alerts heighten exposure (Okta Inc. 2025)
- **Consequence:** Severe – Impacts include operational downtime, compliance violations, and loss of customer trust (Cybersecurity Dive 2024b)
- **Risk Level:** Extreme (Very High × Severe)

Treatment Plan:

- **To Reduce Likelihood:**

Critical infrastructure is distributed across politically stable regions, and global developments are actively monitored using threat intelligence platforms. A remote-first operational model is maintained to reduce dependence on physical offices (Okta Inc. 2025).

- **To Reduce Consequence:**

Simplified fallback service-level agreements are prepared, crisis response plans are implemented, and legal mechanisms are established in unaffected jurisdictions. Transparent communication with clients and investors is maintained during periods of disruption.

- **Risk Sharing:**

Vendors are engaged under contracts that include geopolitical risk clauses, and business interruption and cyber insurance policies are maintained to mitigate financial impacts from force majeure events (Okta Inc. 2025).

- **Residual Risk**:

Despite these controls, sudden lockdowns, sanctions, or regional disruptions may still occur. These risks are mitigated through regular crisis simulations, redundant staff coverage, and strengthened regional resilience efforts (Okta Inc. 2025).

Monitoring and Review:

- Weekly global threat intelligence briefings
- Monthly regional continuity reviews
- Quarterly assessments of vendor and insurance resilience

Biannual crisis response drills to test real-world preparedness.

References

Amazon Web Services (n.d.), *Okta grows AWS collaboration, drives business growth and revenue through APN Customer Engagements (ACE)*, Amazon Web Services, viewed 5 March 2025. [Online: https://aws.amazon.com/partners/success/Okta/]

AIG 2024, *CyberEdge® cyber insurance policy*, American International Group, New York.

Australian Cyber Security Centre (ACSC) 2023, *Serious vulnerabilities in Atlassian products including Confluence, Jira and Bitbucket*, Cyber.gov.au, viewed 12 April 2025. [Online: https://www.cyber.gov.au/about- us/view-all-content/alerts-and-advisories/serious-vulnerabilities-in-atlassian-products-including-confluence- jira-and-bitbucket]

Bradbury, D 2022, *Okta concludes its investigation into the January 2022 compromise*, Okta, viewed 18 April 2025. [Online:https://www.Okta.com/au/blog/2022/04/Okta-concludes-its-investigation-into-the-january-2022- compromise/]

Business Wire 2024, *Okta named a leader in 2024 Gartner Magic Quadrant for Access Management for eighth consecutive year*, Business Wire, viewed 18 March 2025. [Online: https://www.businesswire.com/news/home/20241205333106/en]

Chan, V 2021, *Op-ed: UniMelb urged to optimise student experience of using Okta Verify*, University of Melbourne Student Union, viewed 18 April 2025 [Online: https://umsu.unimelb.edu.au/news/article/7797/Op-ed- UniMelb-urged-to-optimise-student-experience-of-using-Okta-Verify/]

Council, J 2025, 'Strengthening insider threat programs in identity security', *Journal of Cybersecurity Practices*, vol. 10, no. 2, pp. 56–68.

Council, S 2025, *Okta, SF tech company worth $16 billion, lays off staff after turning first profits*, SFGate, viewed 25 March 2025.[Online: https://www.sfgate.com/tech/article/Okta-layoffs-after-first-profits-20147418.php]

Coombs, WT 2015, *Ongoing crisis communication: planning, managing, and responding*, 4th edn, Sage, Thousand Oaks, CA.

Cybersecurity Dive 2024a, *Okta, with a bruised reputation, rethinks security from the top down*, Cybersecurity Dive, viewed 16 April 2025. [Online: https://www.cybersecuritydive.com/news/Okta-security- revival/708636/]

Cybersecurity Dive 2024b, *Okta overhauls security priorities after past breaches*, Cybersecurity Dive, viewed 21 March 2025[Online: https://www.cybersecuritydive.com/news/Okta-overhaul-priorities-culture- security/709050/]

du Preez, J 2024, 'Artificial intelligence in identity and access management: emerging trends', *Journal of Information Security Research*, vol. 14, no. 1, pp. 30–42.

Gatlan, S 2023, *Okta breach: 134 customers exposed in October support system hack*, Bleeping Computer, viewed 12 April 2025. [Online: https://www.bleepingcomputer.com/news/security/Okta-breach-134-customers- exposed-in-october-support-system-hack/]

Gillan, SL & Starks, LT 2000, 'Corporate governance proposals and shareholder activism', *Journal of Financial Economics*, vol. 57, no. 2, pp. 275–305.

Guthrie, B, Data, A, Harris, N & Murphy, J 2024, *Gartner® Magic Quadrant™ for Access Management*, Gartner, viewed 24 May 2025. [Online: https://www.Okta.com/au/resources/gartner-magic-quadrant-access- management/]

Investor's Business Daily 2025, *Cybersecurity firm Okta posts Q3 earnings, revenue beat; shares jump*, Investor's Business Daily, viewed 19 March 2025. [Online: https://www.investors.com/news/technology/Okta-stock- Okta-earnings-news-q32024/]

Lawler, R 2024, *An Okta login bug bypassed checking passwords on some long usernames*, The Verge, viewed 22 March 2025. [Online: https://www.theverge.com/2024/11/1/24285874/Okta-52-character-login-password- authentication-bypass/]

Lily Hay Newman 2023, *The worst hacks of 2023*, Wired, viewed 22 April 2025. [Online: http://wired.com/story/worst-hacks-2023/]

MarketsandMarkets 2024, *Identity and access management (IAM) market – global forecast to2030*, MarketsandMarkets, viewed 20 March 2025. [Online: https://www.marketsandmarkets.com/Market-Reports/identity- access-management-iam-market-1168.html]

MarketWatch 2024, *As Okta's stock soars on earnings, this stat shows its strategy is paying off*, MarketWatch, viewed 20 March 2025. [Online: https://www.marketwatch.com/story/as-Oktas-stock-soars-on- earnings-this-stat-shows-its-strategy-is-paying-off-6758c0a4]

Mirkasymov, R & Martinez, R 2022, *Roasting 0ktapus: The phishing campaign going after Okta identity credentials*, Group-IB, viewed 20 April 2025. [Online: https://www.group-ib.com/blog/0ktapus/]

Nasdaq 2025, *Okta (Okta) Q4 2025 earnings call transcript*, Nasdaq, viewed 26 April 2025. [Online: https://www.nasdaq.com/articles/Okta-Okta-q4-2025-earnings-call-transcript/]

Okta 2025a, *Annual report 2024*, Okta Investor Relations, viewed 15 March 2025. [Online: https://investor.Okta.com/financials/annual-reports/default.aspx]

Okta 2025b, *Identity and access management vision*, Okta, viewed 12 April 2025. [Online: https://www.Okta.com/company/vision/]

Okta Inc. 2025, *Form 10-K annual report for the fiscal year ended January 31, 2025*, Okta Investor Relations, viewed 25 May 2025. [Online: https://investor.Okta.com/financials/annual-reports/default.aspx]

Okta Inc. 2025b, *Our leadership*, Okta, viewed 12 April 2025. [Online: https://www.Okta.com/company/leadership/]

Okta Inc. 2025c, *Customers*, Okta, viewed 28 April 2025. [Online: https://www.Okta.com/customers/]

Salman, S 2024, *Key findings from our 2023 State of Secure Identity Report*, Okta, viewed 18 April 2025. [Online: https://www.Okta.com/newsroom/articles/key-findings-from-our-2023-state-of-secure-identity-report/]

Software World (n.d.), *Top Okta alternatives & competitors*, SoftwareWorld, viewed 20 March 2025. [Online: https://www.softwareworld.co/competitors/Okta-alternatives/]

ThousandEyes 2022, *The Top Outages of 2022: Analysis and Takeaways* (webinar), ThousandEyes, viewed 26 May 2025. [Online: https://www.thousandeyes.com/resources/emea-top-outages-2022-webinar]

Todd, J 2015, *Software engineering design principles*, Okta Developer Blog, viewed 28 April 2025. [Online: https://developer.Okta.com/blog/2015/05/08/software-engineering-design-principles/]

Uppaluri, VR 2025, 'Enterprise authentication architectures: comparing Kerberos, Active Directory, and Okta for cloud data platforms', *International Journal of Computer Engineering and Technology (IJCET)*, vol. 16, no. 1, pp. 210–219, viewed 24 May 2025. [Online: https://ijcetjournal.org/archive/vol16-issue1- 2025/uppaluri-authentication-architectures.pdf]