Information Security Management System Proposal for Adobe Inc

Security management in practice Course.

Advisor:

Prof. Le Hai Duong

In specialisation

by

Mr: Le Thanh Phuong Nam

ID (IU): ITITWE19025_ ID (UWE): 23083609

International University - Vietnam National University HCMC

University of the West of England

Pitching Youtube Link: https://youtu.be/1DEsSIUwX6o

December 2024

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1. INTRODUCTION

1.1. Business Overview

Figure 1. Organisation Logo

Adobe Inc. (*Figure 1*) was selected for this Information Security Management System (ISMS) report not only because it is one of the top software US vendors in the creative industries related to graphic design, publishing, and digital marketing.

1.2. Business model

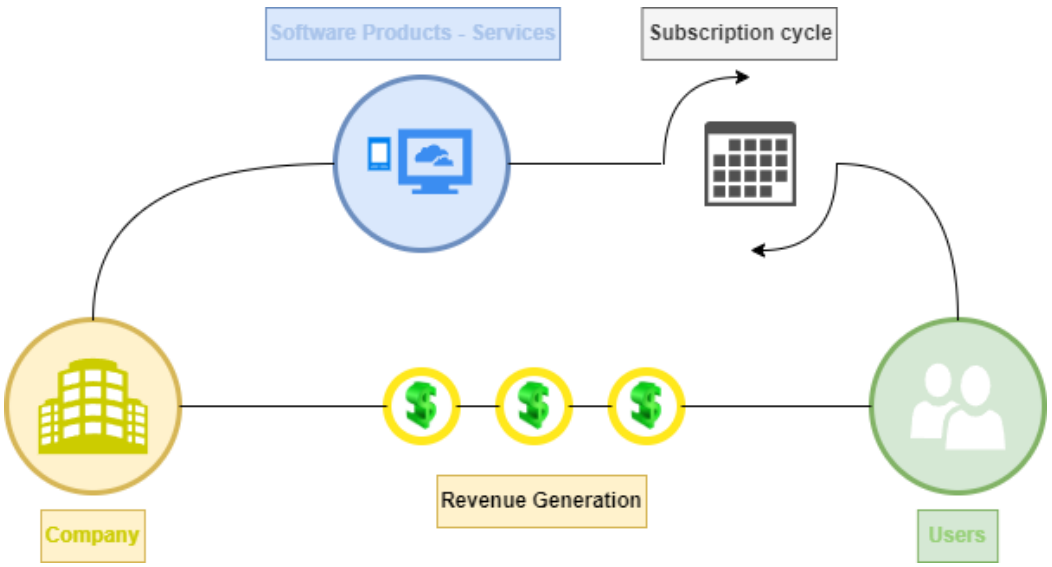

Figure 2. Business Model Diagram

Adobe operates primarily on (*Figure 2*) a SaaS (software as a service) model by installing directly from a web browser, most focusing on subscription-based services from 2013 such as all its Creative Cloud software, which require an annual or monthly payment from the customer to access their services. (Daniel Pereira, 2024)

1.3. Strategic Objectives

- Maintain and grow market leadership in digital marketing and creative software
- Apply machine learning, and AI (artificial intelligence) to improve customer experience.
- Enhance customer belief by ensuring information security.
- Deliver new cloud-based solutions to optimise performance.

2. ORGANISATIONAL CONTEXT

2.1. Internal Organization

According to the recruitment section, Adobe recruits annually thousands of positions divided into different teams or departments to handle specific tasks to serve many facilities in many countries. Employees exchange information through email and meetings.

2.1.1. Hierarchy:

2.1.1.1. Leaders (Adobe Inc., n.d.):

- Chair and Chief Executive Officer: [Shantanu Narayen]
- Chief Marketing Officer and Executive Vice President, Global Marketing: [Lara Balazs]
- Chief Strategy Officer and Executive Vice President, Design & Emerging Products: [Scott Belsky]
- Chief People Officer and Executive Vice President, Employee Experience: [Gloria Chen]
- Chief Financial Officer and Executive Vice President, Finance, Technology Services and Operations [Dan Durn]
- President, Digital Experience Business [David Wadhwani]

2.1.1.2. Teams (Adobe Inc., n.d.):

Depending on the purpose, each large team has managers leading smaller teams, whose task is to compile statistics and report back to leaders.

- Team lists:
    - Engineering And Product
    - Design
    - Research
    - Sales and Customer Experience
    - Marketing and Stragegy
    - Finance and Operations
    - Legal and Government Relations
    - Employee Experience

2.1.2. Security Handling:

In my understanding, Adobe assigns the Engineering And Product team the responsibility of maintaining security, compliance, and discipline around their systems and products from smaller teams working in Security-related teams (Adobe Inc., n.d.) According to ISO 27001, Adobe uses processes, and proactive monitoring to address vulnerabilities and ensure data is secure and available. (ISO/IEC 27001:2022, 2022) Various data sources were used and analyzed by the Security Operations Center ("SOC") within Adobe Security Coordination Center ("SCC"). (Adobe Inc., 2020) They have established a system to ensure security awareness for all

employees.(Fielding, 2021) Additionally, they have replaced the software security awareness team for employees through The Adobe Software Security Engineering Team (ASSET) certification.(Kebbel-Wyen, 2012)

2.2. External Interactions

- Customers: Interact with Adobe through websites, emails, social media channels, events, and especially cloud-based platforms, such as Adobe Creative Cloud.
- Third Parties: Vendors, cloud service providers, and software integration partners in providing services through contracts. (ENISA, n.d.)
- Regulators: Compliance with the General Data Protection Regulation (GDPR), California Consumer Privacy Rights (CCPA), and international privacy laws ensures secure customer interactions (Data Protection and Compliance, n.d.)

2.3. Differences Between Internal and External Interactions:

Aspect	Internal Interactions	External Interactions
Control	Hierarchical oversight, strict access control	Regulated via contracts
Security Policies	Compliance (ISO 27001)	Legal and regulatory obligations
Data Exchange	Within internal systems: email, meeting	Encrypted communication via APIs, VPN

Table 1.*Internal and External Interactions Comparison*

According to the table (Table 1), External interactions can pose more risks because of the lack of complete control over the parties involved.

2.4. Assumptions

1. **Resources**: Adobe has sufficient financial and human resources to implement ISMS controls.
2. **Organizational structure**: Departments work together to ensure information security.
3. **Responsibility**: Each employee is responsible for complying with security policies.
4. **Hierarchy**: A well-defined reporting structure with leadership buy-in for ISMS policies.

5. **Processes**: Existing basic incident response, risk assessment, and supplier management processes that are ISO 27001 compliant, but need to be improved. (ISO/IEC 27001:2022, 2022)
6. **Technology**: Adobe has modern cloud-based platforms and tools for ISMS integration.

3. RISK ASSESSMENT: Risk Identification

3.1. Threat Analysis:

According to Adobe's approaches to current threats, identifying threats could exploit vulnerabilities and compromise Adobe's information security systems (Adobe Inc., 2020) as below:

3.1.1. External Threats

- Cyberattacks: Adobe remains a target for cybercriminals, as demonstrated by the 2013 breach where attackers accessed tens of millions of user accounts primarily through phishing, ransomware, and distributed denial of service (DDoS) attacks. (Ishita, 2023)
- Supply Chain Attacks: Because Adobe has partners, third parties, and services vendors can inadvertently expose themselves to a mass attack as the network that links data between them can be compromised by one party's negligence.

3.1.2. Internal Threats

- **Employee Negligence**: The primary threat often stems from human error due to training errors that can lead to personal data or financial information leakage. (ISO/IEC 27005, n.d.)
- **Insider Threats**: Malicious elements from within the company may, due to dissatisfaction with treatment policies compromise systems, steal private information to give outsiders, and competitors, unauthorized access to copies of documents, software, designs, and business plans.

3.1.3. Physical Threats

- Physical security risks are often losses from equipment theft or damage during the company's storage process causing technical problems. In addition, unexpected disasters from the environment such as floods causing loss of property should also be noticed.

3.1.4. Compliance and Legal Risks

- Adobe must comply with strict regulations (GDPR, CCPA) and non-compliance with them can result in legal penalties for the organization, which can lead to loss of belief from customers and partners. (week 4 Legislation, n.d.)

3.2. Vulnerability Assessment:

Adobe has a policy of proactively monitoring production environments to identify and address vulnerabilities that could compromise data security as they can be easily exploited by the threats mentioned above (Adobe Inc.,

2020). Additionally, security reports have highlighted key vulnerabilities including: (UpGuard, 2024)

3.2.1. Technical Vulnerabilities

- Outdated or Unpatched Systems: Existing systems running outdated encryption (TLS 1.2) may expose Adobe to data breaches.
- Unmaintained Web Assets: Sites marked as "unmaintained" increase the attack surface and reach for cybercriminals.
- Weak DNS Configurations: Lack of DNSSEC and CAA records leaves Adobe vulnerable to DNS spoofing and certificate misuse.
- HSTS and HTTPS Gaps: HTTP Strict Transport Security (HSTS) is not fully enforced on subdomains, which can enable Man-in-the-Middle (MITM) attacks.

3.2.2. Human Vulnerabilities

- Lack of Security Awareness: Employees are vulnerable to being tricked into revealing credentials and social engineering attacks.
- Misconfiguration of Cloud Services: Cloud Service Misconfiguration: Errors in cloud setup can lead to data being exposed to the public, similar to previous incidents of other cloud service providers (Information Risk Management, 2023)

3.2.3. Process Weaknesses

- Ineffective Incident Management: Incident monitoring and response protocols delay mitigation and increase the threat.
- Weak Access Controls: Over-privileged accounts without proper Role-Based Access Control (RBAC) increase internal threats.

3.3. Risk Sources:

Understanding where risks stem from the key is to establishing effective risk treatment plans for Adobe organisation including:

3.3.1. Technological Risk Sources

- **Web Applications**: Web Applications: Adobe's SaaS products such as Creative Cloud and Document Cloud are significant targets for cyberattacks.
- **Infrastructure Vulnerabilities**: Infrastructure Vulnerabilities: Adobe's reliance on cloud, server, and IoT platforms increases its exposure to risks such as DDoS and unauthorized access from unwanted parties.

3.3.2. Human Risk Sources

- **Internal Users**: Employees, developers, and vendors may inadvertently or intentionally expose sensitive data.

- **Third-Party Vendors**: Affiliated vendors that do not have security controls as stringent as Adobe's current systems can introduce vulnerabilities into the supply chain. (06_Policy Tutorial, n.d.)

3.3.3. Compliance and Governance

- **GDPR Non-Compliance**: GDPR Non-Compliance: Adobe processes customer data globally, making it subject to GDPR and CCPA. Therefore, violations risk legal liability that can affect money and reputation. (05_legislation, n.d.)
- **Data Protection**: Customer Personally Identifiable Information (PII) and intellectual property, also known as copyright, are high-profile targets. (Data Protection and Compliance, n.d.)

3.3.4. Environmental and Physical Sources

- **Natural Disasters**: Natural Disasters: Damage to a data centre can disrupt system operations through environmental threats such as earthquakes or floods.
- **Device Theft**: Loss of a laptop or mobile device containing sensitive data poses a risk of data breach and leakage.

4. RISK ASSESSMENT: Risk Analysis

4.1. Define Likelihood and Impact Levels:

There are two parameters used to assess each type of risk:

4.1.1. Likelihood (L):

1. **Rare (1):** Highly unlikely to happen.
2. **Unlikely (2):** Occurs occasionally but infrequently.
3. **Possible (3):** Moderate likelihood of occurrence.
4. **Likely (4):** High chance of occurring regularly.
5. **Almost Certain (5):** Risk is expected to occur frequently.

4.1.2. Impact (I):

1. **Insignificant (1):** Negligible or no impact.
2. **Minor (2):** Small impact with limited disruption.
3. **Moderate (3):** Noticeable disruption with operational delays.
4. **Major (4):** Significant damage to business operations and reputation.
5. **Severe (5):** Catastrophic impact; business continuity threatened.

4.2. Calculate Risk Rating (RR):

The Risk Rating (RR) formula:

$$RR=Likelihood(L)\times Impact(I)$$

4.3. Categorize Risks:

Based on the risk ratings, risks are categorized into three main levels:

1. **Low (1–6)** - Manageable Risks
2. **Medium (7–14)** - Require Attention
3. **High (15–25)** - Critical, Immediate Action Needed

4.4. Calculated Risks:

Based on the Likelihood (L) and Impact (I) ratings for each risk based on Adobe's operational context, past incidents, and industry standards such as ISO 27005. (ISO/IEC 27005, n.d.)

Risk	Likelihood (L)	Impact (I)	Risk Rating (RR)	Category
Phishing Attacks	4 (Likely)	5 (Severe)	20	High
Insider Threats	3 (Possible)	4 (Major)	12	Medium
DNS Spoofing	2 (Unlikely)	4 (Major)	8	Medium
Unpatched Systems	3 (Possible)	4 (Major)	12	Medium
Weak Access Controls	5 (Almost Certain)	5 (Severe)	25	High
Device Theft	3 (Possible)	3 (Moderate)	9	Medium
Physical Data Center Risk	1 (Rare)	5 (Severe)	5	Low

Table 2. *Risk Analysis Calculation*

5. RISK ASSESSMENT: Risk Evaluation

5.1. Compare calculated risks against risk acceptance criteria:

Adobe's risks are assessed and calculated (Table 2) above using the risk acceptance criteria defined in ISO 27005 and following best practices for risk classification and prioritization to ensure appropriate treatment or monitoring. (ISO/IEC 27005, n.d.)

Risk	Risk Rating (RR)	Risk Level	Action
Phishing Attacks	20	High	Immediate mitigation.
Weak Access Controls	25	High	Immediate mitigation.
Unpatched Systems	12	Medium	Immediate mitigation.
Insider Threats	12	Medium	Address with controls.
DNS Spoofing	8	Medium	Address with controls.
Device Theft	9	Medium	Address with controls.
Physical Data Center Risk	5	Low	Monitor and review regularly.

Table 3. *Risk Action*

- Acceptance of Low-Risk Scenarios

Risks Rating under 7 (*Physical Data Center Risk* – Table 3) are considered acceptable because they rarely occur but should be monitored and reviewed periodically to ensure they do not lead to serious consequences.

5.2. Prioritize based on business impact:

Adobe's critical systems and processes are prioritized for immediate action (Table 3) due to the potential financial and reputational damage. (Data Protection and Compliance, n.d.)

5.2.1. High-Priority Risks

1. **Weak Access Controls (RR = 25)**
    - **Impact**: Compromised user accounts, unauthorized access to sensitive systems, and potential data breaches.
    - **Reason**: Access control breaches could cause significant damage to Adobe's reputation and expose sensitive customer data.
2. **Phishing Attacks (RR = 20)**

- **Impact**: Loss of credentials leads to unauthorized access, ransomware attacks, and financial fraud.
- **Reason**: This is a common method of exploiting human vulnerabilities and causing significant disruption.

3. **Unpatched Systems (RR = 12)**
    - **Impact**: Exploitation of software vulnerabilities, malware injection, and downtime.
    - **Reason**: Delayed, intermittent software response times provide opportunities for hackers to attack Adobe's infrastructure.

5.2.2. Medium-Priority Risks

1. **Insider Threats (RR = 12)**
    - **Impact**: Privilege misuse or data leakage from employee systems.
    - **Reason**: Insider threats are less likely but can cause significant damage when they occur.
2. **DNS Spoofing (RR = 8)**
    - **Impact**: Domain hijacking leads to phishing or impersonation sites.
    - **Reason**: While unlikely, DNS spoofing can seriously damage brand integrity.
3. **Device Theft (RR = 9)**
    - **Impact**: Loss of data and credentials if physical devices such as laptops are stolen.
    - **Reason**: A manageable risk mitigated through encryption and physical security principles.

6. RISK TREATMENT

6.1. Treatment Options:

For each risk identified above, treatment options will be selected based on the organization's risk level:

1. **Avoid**: Stop activities that cause the risk, eliminating exposure.
2. **Mitigate**: Implement controls to reduce the risk's likelihood, impact, or both.
3. **Transfer**: Shift the risk with external interactions.
4. **Accept**: Accept residual risks that are manageable.

6.2. Action Plan:

Risk	Treatment Option	Action Plan
Weak Access Controls	Mitigate	- Implement Multi-Factor Authentication (MFA). - Enforce Role-Based Access Control (RBAC) for least-privileged access. - Perform regular audits. (UpGuard, 2024)
Phishing Attacks	Mitigate/Transfer	- Implement regular phishing awareness training for employees. - Deploy advanced email filtering tools. - Acquire cyber insurance coverage. (ISO/IEC 27002:2022, 2022)
Unpatched Systems	Mitigate	- Automate patch management processes. - Perform regular vulnerability scans. - Prioritize patches for critical systems. (ISO/IEC 27005, n.d.)

Insider Threats	Mitigate	- Deploy user activity monitoring tools. - Restrict access to sensitive data through encryption. - Implement employee screening procedures. (Data Protection and Compliance, n.d.)
DNS Spoofing	Mitigate	- Deploy DNSSEC for domain integrity. - Enable Certification Authority Authorization (CAA) records to prevent unauthorized certificate issuance. (UpGuard, 2024)
Device Theft	Mitigate/Accept	- Implement full-disk encryption for devices. - Enable remote wipe capabilities. - Enforce physical security policies. (ENISA, n.d.)

Table 4. *Action Plan*

The Table above (Table 4) lists the actions that should be taken based on the references I have collected.

7. MONITORING AND COMMUNICATION

7.1. Schedule regular reviews:

Adobe needs to schedule regular reviews to manage risks with controls and plan responses to ensure the ISMS effective with evolving business and compliance requirements like ISO 27001 and GDPR. (ISO/IEC 27001:2022, 2022)

- Review Schedule:
  - Monthly Reviews: Perform operational audits of high-risk areas, such as access controls to mitigate fraud.
  - Quarterly Reviews: Vulnerability scans for unpatched systems and risk updates for new tools or changes.
  - Annual Reviews: Management-led review that analyzes incidents, identifies risk trends, and controls performance. Includes penetration testing to validate compliance. (UpGuard, 2024)

Regular reports should be shared with key stakeholders, CFO and Executive Vice President, Finance, Technology Services and Operations; Engineering and Product team to ensure transparency and accountability. (Bartock et al., 2016)

7.2. Monitor changes:

Adobe requires regular monitoring to identify changes in risk and support proactive mitigation as below:

1. **Threat Intelligence:** Use SIEM tools and external feeds to detect threats in real-time. (ISO/IEC 27002:2022, 2022)
2. **System Monitoring:** Automated vulnerability scanning and review of DNS configuration, encryption, and SSL/TLS compliance. (UpGuard, 2024)
3. **Behavioral Monitoring:** Monitor user activity within the allowed scope to detect insider threats or unauthorized activity.
4. **Incident Alerts:** Configure automated alerts to respond immediately to critical violations.

7.3. Update framework:

The ISMS framework will evolve through continuous learning from incidents and reviews, as highlighted by ISO 27001 on key improvements (ISO/IEC 27001:2022, 2022):

1. **Incident Analysis:** Investigate incidents to identify root causes and refine controls.
2. **Control Optimization:** Audit and enhance controls, such as MFA or automated patching, to address vulnerabilities. (UpGuard, 2024)
3. **Framework Revision:** Update policies and procedures to address risks from cloud migration or third-party dependencies.

4. **Feedback Loops:** Collect insights from stakeholders for continuous improvement. (ISO/IEC 27001:2022, 2022)

8. CONCLUSION

The report presented for the ISO 27001 compliant Information Security Management System (ISMS) for the Adobe organization examines the risks the organization faces in terms of threats to Adobe's operations and assets and recommends plans to mitigate the identified risks. Then, risk assessment vulnerability to fraud needs to be addressed immediately to reduce the risk of data breaches and business disruption. Subsequently, it is followed by the evaluation of risk treatment options to address the risks that had been identified to fulfil Adobe's risk profile and business strategy. Therefore, ongoing cheque-ups, and the revision of incident-based frameworks can effectively respond to new threats, keep Adobe's customers 'confidence and enhance the company's cybersecurity.

9. REFERENCES

05_legislation, n.d. *Legislation,* s.l.: Provided by instructor.

06_Policy Tutorial, n.d. *Access Control Policy,* s.l.: Provided by instructor.

Adobe Inc., 2020. *Adobe's Approach to Managing Data Security Risk.* [Online]
Available at: https://www.adobe.com/corporate-responsibility/data-security-risk.html
[Accessed 12 2024].

Adobe Inc., n.d. *Adobe Executive Profiles.* [Online]
Available at: https://www.adobe.com/about-adobe/leaders.html
[Accessed 12 2024].

Adobe Inc., n.d. *Explore careers in Engineering and Product teams | Adobe careers.* [Online]
Available at: https://www.adobe.com/careers/teams/engineering-and-product.html
[Accessed 12 2024].

Adobe Inc., n.d. *Explore teams in Adobe | Adobe Careers.* [Online]
Available at: https://www.adobe.com/careers/teams.html
[Accessed 12 2024].

Daniel Pereira, 2024. *Adobe Business Model - How Adobe Makes Money?.* [Online]
Available at: https://businessmodelanalyst.com/adobe-business-model/
[Accessed 12 2024].

Data Protection and Compliance, n.d. *Guidance on managing cybersecurity risks for small and medium enterprises,* s.l.: Provided by instructor.

ENISA, n.d. *Cybersecurity Guide for SMEs,* s.l.: Provided by instructor.

Information Risk Management, 2023. *Information Risk Management: Risk Treatment and Controls,* s.l.: Provided by instructor.

ISO/IEC 27001:2022, 2022. *Information Security Management Systems,* s.l.: Provided by instructor.

ISO/IEC 27002:2022, 2022. *Information Security Controls,* s.l.: Provided by instructor.

ISO/IEC 27005, n.d. *Information Security Risk Management,* s.l.: Provided by instructor.

UpGuard, 2024. *Adobe Security Rating, Vendor Risk Report, and Data Breaches.* [Online]
Available at: https://www.upguard.com/security-report/adobe
[Accessed 12 2024].

week 4 Legislation, P. a. G., n.d. *Legislation, Policies, and Governance,* s.l.: Provided by instructor.

Bartock, M., Cichonski, J., Souppaya, M., Smith, M., Witte, G., & Scarfone, K. (2016). *Guide for cybersecurity event recovery*. https://doi.org/10.6028/NIST.SP.800-184

Fielding, J. (2021). Building a culture of security. *Computer Fraud & Security*, *2021*(2), 20–20. https://doi.org/10.1016/S1361-3723(21)00021-X

Ishita, N. S. D. S. D. P. (2023). Adobe Cyber Attack: Vulnerabilities, Impacts and Lessons Learned. *Tuijin Jishu/Journal of Propulsion Technology*, *44*(1), 137–139. https://doi.org/10.52783/tjjpt.v44.i1.2224

Kebbel-Wyen, J. (2012). Training an Army of Security Ninjas. *IEEE Security & Privacy*, *10*(6), 91–93. https://doi.org/10.1109/MSP.2012.159