VISION

Third Party Risk

Seran Sathyaseelan
April 10,2024

Table of Contents

1.1
Purpose

The purpose of this Third-Party Risk Report is to systematically identify, assess, and manage potential risks associated with third-party vendors engaged by VISION. Third-party vendors play a crucial role in supporting various aspects of VISION's operations, including technology infrastructure, service delivery, and facility management. However, reliance on external parties also introduces inherent risks, such as data breaches, service disruptions, or non-compliance with security standards.

By establishing a comprehensive Third-Party Risk Register, VISION aims to systematically identify and document potential risks associated with each third-party vendor, considering factors such as likelihood and impact. Through this process, the severity of identified risks is evaluated based on their likelihood and potential impact on VISION's operations, data security, and regulatory compliance. Subsequently, appropriate mitigation strategies are developed and implemented to address identified risks, including contractual agreements, security controls, and oversight measures.

Regular review and update of the Third-Party Risk Register are conducted to reflect changes in the risk landscape and ensure that mitigation measures remain effective over time. By proactively managing third-party risks, VISION aims to enhance the resilience and security of its operations, safeguard sensitive data, and maintain compliance with regulatory requirements.

This report serves as a foundational document for ongoing risk management efforts, providing insights into the potential impact of third-party engagements on VISION's overall risk posture and informing decision-making processes related to vendor selection, oversight, and risk mitigation.

2.1
Scope

The scope of this Third-Party Risk Report encompasses all third-party vendors engaged by VISION across various operational domains, including but not limited to technology infrastructure, software services, managed services, and facility management. VISION recognizes the critical role that third-party vendors play in supporting its operations and acknowledges the associated risks inherent in such engagements.

This report systematically identifies and assesses potential risks associated with third-party vendors, considering factors such as likelihood and impact. The scope includes the evaluation of risks related to data security, service availability, regulatory compliance, and overall business

continuity. Furthermore, the scope extends to the development and implementation of mitigation strategies to address identified risks effectively.

3.1
Executive Summary

The Third-Party Risk Assessment undertaken by VISION has yielded crucial insights into potential vulnerabilities and threats arising from external vendor relationships. Through a comprehensive evaluation process, various risks, including data breaches, service disruptions, and compliance gaps, have been identified, shedding light on the multifaceted nature of risks inherent in third-party engagements. Furthermore, the assessment has highlighted that certain risks possess a moderate to high likelihood of occurrence and could result in significant impacts on VISION's operations, data security, and regulatory compliance if materialized. In response to these findings, VISION emphasizes a shared responsibility model, delineating clear roles and responsibilities for both VISION and its vendors in mitigating risks and upholding security standards. To address identified risks, VISION is implementing robust mitigation strategies, encompassing stringent vendor selection criteria, clear contractual agreements, regular monitoring and oversight, and proactive incident response planning. Moreover, the assessment underscores the importance of continuous improvement in risk management practices, emphasizing the need for ongoing monitoring, review, and adaptation to evolving threats. By leveraging these key findings, VISION aims to strengthen its third-party risk management framework, bolster resilience, and safeguard its operations and data against external threats, thereby ensuring the security and trust of its stakeholders.

4.1
Analysis

The Risk Register for VISION's third-party engagements presents a thorough analysis of potential risks across various vendor categories. At the forefront is the risk associated with VISION's Cloud Service Provider (CSP), which entails the possibility of data breaches or unauthorized access to the company's cloud infrastructure. Rated with a high likelihood of occurrence (7 out of 10) and severe impact (9 out of 10), this risk underscores the critical need for robust security measures and vigilant monitoring. Similarly, the risk posed by Software as a Service (SaaS) applications highlights the potential for service disruptions or data breaches, warranting proactive mitigation strategies to maintain operational continuity. Managed Service Providers (MSPs) also present a moderate risk due to potential gaps in security monitoring or incident response capabilities, necessitating closer oversight and collaboration. Conversely, risks associated with Cleaning and Snack Vendors are rated lower, reflecting a decreased likelihood and impact on asset security. However, risks related to Data Processing and Storage Services are rated high due to the significant consequences of data integrity issues or non-compliance with regulations. The Risk Register underscores the importance of prioritizing

mitigation efforts based on the likelihood and impact of each risk, enabling VISION to strengthen its risk management practices and safeguard its operations and data against external threats.

Table 1.1 - Risk Register for third party risks

Vendor Name	Risk Description	Likelihood (out of 10)	Impact (out of 10)	Overall Risk Rating
Cloud Service Provider (CSP)	Potential data breaches or unauthorized access to VISION's cloud infrastructure	7	9	High
Software as a Service (SaaS)	Risk of service disruptions or data breaches within SaaS applications	5	8	Medium
Managed Service Provider (MSP)	Potential gaps in MSP's security monitoring or incident response capabilities	7	7	Medium
Cleaning and Snack Vendors	Risk of unauthorized access or theft of physical assets or sensitive information	4	5	Low
Data Processing and Storage Services	Risk of data integrity issues or non-compliance with data protection regulations	6	9	High

Other Contractors or Service Providers	Risk of security incidents or breaches related to various contracted services	4	6	Low

4.2
Mitigation

Cloud Service Provider (CSP)

- Multi-Factor Authentication (MFA): Implementing MFA adds an extra layer of security by requiring users to provide multiple forms of verification before accessing cloud services. This helps prevent unauthorized access, even if login credentials are compromised.
- Encryption of Sensitive Data: Encrypting data both in transit and at rest ensures that even if data is intercepted or accessed without authorization, it remains unreadable and unusable to unauthorized parties.
- Regular Access Control Audits: Conducting regular audits of access controls and permissions helps identify any unauthorized access or unusual activity, allowing for prompt remediation to prevent potential breaches.
- Establishment of Incident Response Protocols: Developing clear incident response protocols ensures that in the event of a security breach or incident, the organization can quickly detect, assess, and respond to mitigate the impact and prevent further damage.

Software as a Service (SaaS)

- Service Level Agreements (SLAs): Including SLAs with uptime guarantees and penalties for service disruptions incentivizes SaaS providers to maintain high levels of availability and performance, minimizing the risk of service disruptions that could impact VISION's operations.
- Regular Monitoring and Security Assessments: Continuously monitoring SaaS applications for unusual activity and conducting regular security assessments and audits helps identify and address potential vulnerabilities or security weaknesses before they can be exploited by malicious actors.
- User Access Controls and Strong Authentication Mechanisms: Implementing robust user access controls and authentication mechanisms ensures that only authorized users can access SaaS applications, reducing the risk of unauthorized access and data breaches.

Managed Service Provider (MSP)

- Clear Security Requirements in Contracts: Establishing clear security requirements in contractual agreements ensures that MSPs understand and comply with VISION's security standards and expectations, reducing the risk of security gaps or vulnerabilities.
- Regular Security Assessments and Third-Party Audits: Conducting regular security assessments of MSPs and engaging in third-party audits helps verify the effectiveness of their security controls and identify any areas for improvement or remediation.
- Open Communication Channels: Maintaining open communication channels with MSPs enables VISION to promptly address any security concerns or issues that may arise, fostering collaboration and ensuring that security incidents are addressed in a timely manner.

Cleaning and Snack Vendors

- Limiting Access and Implementing Physical Security Measures: Restricting access to sensitive areas and assets, such as server rooms or storage facilities, and implementing physical security measures such as surveillance cameras and access controls, helps prevent unauthorized access or theft of physical assets or sensitive information.
- Background Checks on Vendor Personnel: Conducting thorough background checks on vendor personnel who have access to VISION's facilities or data helps ensure that only trustworthy individuals are granted access, reducing the risk of insider threats or unauthorized access.

Data Processing and Storage Services

- Encryption of Sensitive Data: Encrypting sensitive data before transmission and storage ensures that even if data is intercepted or accessed without authorization, it remains protected and unreadable to unauthorized parties.
- Access Controls and Authentication Mechanisms: Implementing access controls and authentication mechanisms ensures that only authorized personnel can access sensitive data, reducing the risk of unauthorized access or data breaches.
- Compliance with Data Protection Regulations: Ensuring compliance with data protection regulations through contractual agreements and periodic assessments helps mitigate the risk of data integrity issues or non-compliance penalties.

Other Contractors or Service Providers

- Clear Security Requirements and Expectations: Clearly defining security requirements and expectations in contractual agreements ensures that contractors and service providers understand and comply with VISION's security standards, reducing the risk of security incidents or breaches.
- Regular Vendor Risk Assessments: Conducting regular vendor risk assessments helps identify and address any security risks or vulnerabilities associated with third-party contractors or service providers, enabling proactive risk management and mitigation.
- Establishment of Monitoring and Oversight Protocols: Implementing protocols for monitoring and oversight of third-party contractors or service providers helps ensure

ongoing compliance with security requirements and prompt detection and response to any security incidents or breaches.

5.1
Shared Responsibility model

Vision

At VISION, we understand that maintaining the security and integrity of our operations is not solely our responsibility but also a collaborative effort with our third-party vendors. Our commitment to security begins with a rigorous vendor selection process, where we meticulously evaluate potential partners based on their security standards, compliance track record, and overall reliability. Once vendors are onboarded, we establish clear contractual agreements that delineate our security expectations, including data protection measures, incident response protocols, and compliance requirements.

In addition to setting expectations, we take an active role in overseeing and monitoring vendor activities. We conduct regular security assessments to ensure that vendors adhere to our security standards and mitigate potential risks effectively. Furthermore, we provide ongoing training and support to vendors, equipping them with the knowledge and resources they need to uphold our security standards and respond effectively to security incidents. Our goal is to foster a culture of security awareness and accountability throughout our vendor ecosystem.

In the unfortunate event of a security incident, we believe in collaborative problem-solving. We work closely with our vendors to investigate the root cause of the incident, mitigate its impact, and implement corrective measures to prevent similar incidents in the future. By maintaining open lines of communication and transparent collaboration, we ensure that security incidents are addressed promptly and effectively, minimizing disruption to our operations and safeguarding our data and assets.

Vendors

On the vendors' side, we expect nothing less than a commitment to excellence in security practices. Vendors are responsible for implementing and maintaining robust security controls to protect VISION's data and assets. This includes ensuring compliance with relevant security standards and regulations, promptly reporting security incidents, and continuously improving their security posture to adapt to evolving threats. We encourage a proactive approach to security, where vendors actively identify and address potential vulnerabilities before they can be exploited.

Ultimately, our shared responsibility model embodies our commitment to maintaining a secure environment for our operations and data. By working hand in hand with our vendors, we can

effectively mitigate risks, address security challenges, and uphold the highest standards of security and integrity across our organization. Together, we strengthen our collective resilience against security threats and demonstrate our unwavering dedication to protecting the trust and confidence of our stakeholders.

Closing remarks

In conclusion, the comprehensive analysis of VISION's third-party risks underscores the critical importance of managing these risks effectively to safeguard the organization's operations, data security, and regulatory compliance. The identified risks, ranging from potential data breaches and service disruptions to unauthorized access and compliance issues, highlight the diverse and complex challenges posed by third-party relationships. However, by implementing tailored mitigation strategies such as multi-factor authentication, encryption, regular monitoring, and clear contractual agreements, VISION can proactively address these risks and strengthen its overall risk management framework.

Managing third-party risks is paramount in today's interconnected business landscape, where organizations rely on a myriad of external vendors, service providers, and contractors to support their operations. Failure to adequately manage these risks can lead to significant financial losses, reputational damage, regulatory penalties, and even legal liabilities. Moreover, in industries such as healthcare, where sensitive patient data is involved, the stakes are even higher, and the potential impact of third-party breaches or incidents can be devastating.

Therefore, it is imperative for VISION to prioritize the implementation of robust risk management practices and establish a culture of security throughout its third-party relationships. This includes conducting thorough due diligence when selecting and onboarding third-party vendors, establishing clear security requirements and expectations in contractual agreements, and regularly assessing and monitoring third-party performance and compliance.

Appendix

Appendix A - levels to number comparison

Likelihood Scale (1-10)	Impact Scale (1-10)
1-2 - Very Low	1-2 - Very Low
3-4 - Low	3-4 - Low
5-7 - Medium	5-7 - Medium
8-10 - High	8-10 - High