Managing a parent company as an outsourcing provider, challenges and solutions.

Five Pillars to reduce risks on Outsourcing

Pr. Nsiangani, Expert Information Security & Cyber Defense

Introduction

As a financial institution, Company XYZ is responsible for safeguarding sensitive customer information and maintaining compliance with various regulatory requirements. This can be a challenging task, especially when it comes to managing the information security and compliance of Company B, a material outsourcing provider to Company XYZ. In this white paper, we will explore the challenges that Company XYZ faces in managing the information security and compliance of Company B, and we will provide five pillars for success in overcoming these challenges.

One of these pillars is regular reporting in the form of operational KPIs, supported by various reports on vulnerabilities management, threats hunting, SIEM, patching, hardening reviews, and malware. These KPIs must be aligned with Company XYZ's security strategy, objectives, and risk appetite, and they must demonstrate

ownership of the information security risks and a proactive approach to risk management. By regularly tracking and reporting on these metrics, Company XYZ can ensure that it is effectively managing the information security risks associated with its relationship with Company B.

However, achieving this level of visibility and control can be difficult, especially when dealing with a complex and dynamic outsourcing relationship, such as B is in effect also a parent company to XYZ.

In this white paper, we will delve into the specific challenges that Company XYZ faces in managing the information security and compliance of Company B, and we will provide actionable recommendations for overcoming these challenges. By following these recommendations, Company XYZ can build a robust and effective information security program that supports its business objectives and helps to protect the sensitive customer information that it is entrusted with.

However, achieving this level of visibility and control can be difficult, especially when dealing with a complex and dynamic outsourcing relationship. In this white paper, we will delve into the specific challenges that Company XYZ faces in managing the information security and compliance of Company B, and we will provide actionable

recommendations for overcoming these challenges. By following these recommendations, Company XYZ can build a robust and effective information security program that supports its business objectives and helps to protect the sensitive customer information that it is entrusted with.

The Problem and Risks:

As a company that has a parent company that also provides material outsourcing services, XYZ faces a number of risks and challenges when it comes to managing compliance and information security. One of the main risks is the potential for non-compliance with relevant regulations and industry standards. This could occur if B fails to implement appropriate policies and procedures, or if XYZ does not adequately monitor and enforce compliance with these policies and procedures. This could result in significant fines and other penalties for XYZ, as well as damage to its reputation and credibility with regulatory authorities and stakeholders.

Another risk for XYZ is the potential for unauthorized access to or misuse of sensitive information. As a parent company, B may have access to a wide range of sensitive information about XYZ, including financial data, intellectual property, and customer information. If this information is not adequately protected, or if it is used for inappropriate purposes, it could lead to significant financial and reputational damage for XYZ. This risk is further compounded by the increasing prevalence of cyber threats and other information security risks, which can be difficult to detect and mitigate.

In addition to these risks, XYZ may also face challenges in managing the relationship with B in a way that promotes compliance and information security. For example, there may be conflicts of interest that arise between the two companies, which could make it difficult to ensure that B is acting in the best interests of XYZ. Similarly, there may be tensions around the sharing of sensitive information, as XYZ may need to balance the need for transparency and accountability with the need for confidentiality and security.

Another potential problem for XYZ is demonstrating compliance to external stakeholders, such as regulatory authorities and customers. In this context, it will be important for XYZ to have robust documentation and record-keeping systems in place, as well as processes for reporting and disclosing any compliance issues or concerns. However, if these systems are inadequate or if XYZ fails to effectively communicate with external stakeholders, it may be difficult for the company to demonstrate that it is meeting all relevant compliance requirements.

Finally, XYZ will need to be prepared to respond to any compliance issues that may arise, whether they are related to B or to the company itself. This will involve having a clear plan in place for addressing and resolving any issues that are identified, as well as communicating with regulatory authorities and other stakeholders to ensure that they are aware of the steps that XYZ is taking to address the issue. However, if XYZ is not adequately prepared to respond to compliance issues, it may struggle to effectively address and resolve these issues in a timely and effective manner.

Overall, managing compliance and information security in the context of a parent company like B presents a number of risks and challenges for XYZ. These risks and challenges include the potential for non-compliance with relevant regulations and standards, the risk of unauthorized access to or misuse of sensitive information, difficulties in managing the relationship with B in a way that promotes compliance and security, challenges in demonstrating compliance to external stakeholders, and the need to be prepared to respond to compliance issues. By addressing these risks and challenges effectively, XYZ can minimize the potential impacts on the company and demonstrate its commitment to compliance and security to stakeholders.

.

The Solution:

To effectively manage compliance and information security in the context of a parent company like B, XYZ will need to adopt a comprehensive and proactive approach that addresses all relevant risks and challenges. One way to structure this approach is to focus on five key pillars: policy and procedure development, information security measures, relationship management, compliance demonstration, and incident response.

The first pillar, policy and procedure development, involves developing and implementing policies and procedures that meet all relevant regulations and industry standards. This may involve coordinating with B to ensure that the policies and procedures developed by both companies are consistent and complementary, and regularly reviewing and updating these policies and procedures to ensure that they are still effective and relevant.

The second pillar, information security measures, involves implementing robust technical controls to protect against cyber threats and other information security risks. This may include measures such as data encryption, access controls, and incident response plans. It is also important for XYZ to implement monitoring systems to track key operational KPIs for information security controls such as vulnerability management, SIEM, malware, hardening, and patch management. These monitoring systems should be presented in clear dashboards that are aligned with XYZ's strategy, security objectives, and risk appetite.

The third pillar, relationship management, involves establishing clear lines of communication and roles and responsibilities between XYZ and B, as well as addressing any conflicts of interest that may arise. This may involve developing policies and procedures to ensure that both companies are acting in the best interests of the other, and establishing protocols for the sharing of sensitive information.

The fourth pillar, compliance demonstration, involves developing a comprehensive compliance program that covers all relevant regulations and standards, and regularly reviewing and updating this program to ensure that it remains effective and relevant. It also involves implementing robust documentation and record-keeping systems, as well as processes for reporting and disclosing any compliance issues or concerns to regulatory authorities and other stakeholders.

The final pillar, incident response, involves having a clear plan in place for addressing and resolving any compliance issues that may arise, as well as communicating with regulatory authorities and other stakeholders to ensure that they are aware of the steps that XYZ is taking to address the issue. This may involve conducting investigations, implementing corrective actions, and implementing preventative measures to reduce the risk of future incidents.

Implementing this approach and focusing on these five pillars will help XYZ effectively manage compliance and information security in the context of a parent company like B, and minimize the potential risks and challenges that the company faces. By adopting this approach, XYZ will be able to demonstrate its commitment to compliance and security to regulatory authorities and stakeholders, and protect itself against financial and reputational damage.

Additionally, implementing this approach can also bring benefits to both XYZ and B. By ensuring compliance with all relevant regulations and standards, XYZ can improve its reputation and credibility with regulatory authorities and stakeholders, which may in turn lead to increased business opportunities and customer trust. Similarly, by adopting robust information security measures, XYZ can protect itself against cyber threats and other information security risks, which can help to reduce the potential for financial and reputational damage. For B, implementing these measures can help to ensure that the company is acting in a responsible and compliant manner, which can also improve its reputation and credibility with regulatory authorities and stakeholders.

Overall, adopting a comprehensive and proactive approach that focuses on policy and procedure development, information security measures, relationship management, compliance demonstration, and incident response can help XYZ effectively manage compliance and information security in the context of a parent company like B, and bring benefits to both XYZ and B. By addressing these challenges and adopting best practices, XYZ can minimize the risks and challenges it faces, and demonstrate its commitment to compliance and security to regulatory authorities and stakeholders

Conclusion:

In conclusion, managing compliance and information security in the context of a parent company like B presents a number of challenges and risks for XYZ. To effectively address these challenges and risks, XYZ will need to adopt a comprehensive and proactive approach that focuses on policy and procedure development, information security

measures, relationship management, compliance demonstration, and incident response. By focusing on these five pillars, XYZ can effectively manage B's compliance and information security, and demonstrate its commitment to compliance and security to regulatory authorities and stakeholders.

One key aspect of this approach is the importance of demonstrating ownership of the risks and driving the information security activities. This may involve establishing a clear security strategy and protection needs, and aligning these with a standard such as NIST, ISO 27001, or COBIT. It may also involve establishing key performance indicators (KPIs) to track the effectiveness of the information security measures that are in place. By taking these steps, XYZ can ensure that it is in control of the risks and is proactively managing the information security activities within the company.

It is also important for XYZ to be transparent and accountable in its efforts to manage compliance and information security. This may involve regularly reporting on the company's compliance and security efforts to

regulatory authorities and other stakeholders, and being open and responsive to any issues or concerns that are raised. By being transparent and accountable, XYZ can build trust and credibility with stakeholders, which can help to strengthen the company's reputation and business prospects.

In summary, managing compliance and information security in the context of a parent company like B requires a proactive and comprehensive approach. By focusing on policy and procedure development, information security measures, relationship management, compliance demonstration, and incident response, and by demonstrating ownership of the risks and driving the information security activities, XYZ can effectively manage B's compliance and information security and demonstrate its commitment to compliance and security to regulatory authorities and stakeholders