Topic 2 Discussion 2

An organization has numerous stakeholders, and the organization may have a different obligation to each stakeholder group. It is essential to recognize organizational internal and external stakeholders and their influence, and, in return, the organization's obligations related to each stakeholder. Discuss different methods such as technical controls and administrative controls that an organization can implement to reduce risk when establishing business relationships with external organizations.

Hello Class,

When establishing business relationships with external organizations, it is crucial for an organization to recognize its internal and external stakeholders, as well as the varying obligations it has towards each group. Internal stakeholders, such as employees and management, have a direct influence on the organization's operations and culture, while external stakeholders, including customers, suppliers, and regulatory bodies, can impact the organization's reputation and compliance status(Sukianto, 2025). To mitigate risks associated with these relationships, organizations can implement a combination of technical controls and administrative controls.

Technical controls involve the use of technology to protect sensitive information and ensure secure interactions with external parties(Swanagan, 2023). For instance, organizations can employ encryption to safeguard data transmitted between themselves and external partners, ensuring that confidential information remains protected from unauthorized access. Additionally, implementing firewalls and intrusion detection systems can help monitor and control incoming and outgoing network traffic, thereby reducing the risk of cyber threats. Regular security assessments and vulnerability scans can also identify potential weaknesses in the organization's systems, allowing for timely remediation(Bevin, 2022).

On the other hand, administrative controls focus on the policies, procedures, and practices that govern how an organization operates. Establishing clear guidelines for vendor management is essential; this includes conducting thorough due diligence on potential partners to assess their security practices and compliance with relevant regulations. Organizations should also implement training programs for employees to raise awareness about security risks associated with external relationships and the importance of adhering to established protocols(Chatterton, 2024). Furthermore, creating a robust incident response plan ensures that the organization is prepared to address any security breaches or compliance issues that may arise from external partnerships.

References:

Bevin, L. (2022, June 23). *Top 5 Best Internal Controls for Cyber Risk Mitigation*. ZenGRC. https://www.zengrc.com/blog/top-best-internal-controls-for-cyber-risk-mitigation/

Chatterton, C. (2024, June 18). *Risk Management Techniques: Understanding Different Approaches and How to Apply Them*. Hyperproof. https://hyperproof.io/resource/risk-management-techniques/

Sukianto, A. (2025, January 2). *10 Ways to Reduce Cybersecurity Risk for Your Organization*. Upguard. https://www.upguard.com/blog/reduce-cybersecurity-risk

Swanagan, M. (2023, December 7). *The 3 types of security controls (expert explains)*. PurpleSec; PurpleSec. https://purplesec.us/learn/security-controls/