3.2.1 Cybersecurity Risk Treatment & Monitoring

Contents

Version	Adjustment Date	Approved By	Approval Date
2.0	4/7/2024	Saud Alsulami	7/7/2024

1. Risk Treatment

Selection of Risk Treatment Options: Based on the risk assessment outcomes, choose appropriate risk treatment options for each identified risk. These options include risk avoidance, reduction, sharing (transfer), and acceptance.

2. Risk Reduction

- Implementation of Controls: Deploy necessary security controls to mitigate identified risks. This includes technical controls (like firewalls and encryption), administrative controls (such as policies and training), and physical controls (like access control systems).
- Control Effectiveness: Regularly evaluate the effectiveness of these controls in reducing risks to an acceptable level.

3. Risk Avoidance

- Decision-Making: Decide to avoid certain risks by not engaging in activities that introduce these risks or by changing aspects of the organization's operations.
- Documentation and Justification: Document the rationale behind each risk avoidance decision.

4. Risk Sharing (Transfer)

- Risk Transfer Mechanisms: For risks that can be transferred, explore options like cybersecurity insurance or outsourcing certain functions to third parties with specialized security expertise.
- Contractual Agreements: Ensure that all risk transfer mechanisms are backed by appropriate legal agreements, clearly stating the responsibilities of all parties involved.

5. Risk Acceptance

- Formal Acceptance: Accept risks that are deemed as low impact or those for which treatment is not feasible due to cost or other constraints.
- Documenting Acceptance: Document the decision-making process, including the rationale for accepting each risk.

6. Risk Monitoring and Review

- Continuous Monitoring: Establish procedures for the ongoing monitoring of each risk and the effectiveness of its treatment.
- Regular Reviews: Conduct regular reviews of the risk landscape, treatment plans, and monitoring processes to ensure they remain relevant and effective in light of any changes in the organization's environment or operations.

7. Reporting and Communication

- Regular Reporting: Prepare and submit regular risk assessments on the status of risk treatment and monitoring activities.
- Stakeholder Communication: Ensure that relevant stakeholders are kept informed about risks and their treatment. This includes executive management, department heads, and, where applicable, external parties such as regulators or partners.

8. Updating Risk Treatment and Monitoring Processes

- Process Improvement: Continuously improve the risk treatment and monitoring processes based on feedback, audit findings, and changes in the external and internal environment.
- Policy Alignment: Regularly update the Cybersecurity Risk Treatment and Monitoring processes to align with the overall Cybersecurity Risk Assessment Policy and the organization's strategic objectives.