CLOUDAVIZE

IT Risk Assessment Checklist

Risk Identification :

- [ ] Are IT assets identified and categorized (hardware, software, data, services)?
- [ ] Are potential threats to IT assets identified (internal, external, natural, human-caused)?
- [ ] Are vulnerabilities in IT systems and processes identified?
- [ ] Are potential impacts of risks on business operations and objectives considered?
- [ ] Are stakeholders involved in the risk identification process?

Risk Analysis :

- [ ] Are identified risks analyzed to determine their likelihood and impact?
- [ ] Are qualitative and/or quantitative risk assessment methods used?
- [ ] Are risk scenarios developed to understand potential consequences?
- [ ] Are existing controls and safeguards considered in risk analysis?

Risk Evaluation :

- [ ] Are risks prioritized based on their severity and business impact?
- [ ] Are risk acceptance criteria defined and communicated?
- [ ] Are risk tolerance levels established for different types of risks?
- [ ] Are risk assessment results documented and reviewed by management?

Risk Treatment/Mitigation :

- [ ] Are risk mitigation strategies developed for prioritized risks (reduce, transfer, accept, avoid)?
- [ ] Are specific controls and actions identified to mitigate risks?
- [ ] Are risk mitigation plans documented and implemented?
- [ ] Are responsibilities assigned for risk mitigation actions?
- [ ] Are costs and benefits of risk mitigation options considered?

Risk Monitoring and Review :

- [ ] Is the IT risk assessment process conducted regularly (at least annually)?
- [ ] Are identified risks and mitigation plans monitored and tracked?
- [ ] Are risk assessments updated to reflect changes in the IT environment and business landscape?
- [ ] Are risk assessment results communicated to relevant stakeholders?
- [ ] Is the effectiveness of risk mitigation controls evaluated?

You can find this checklist at

https://www.cloudavize.com/it-risk-assessment-checklist