Risk Management

IT risk refers to the likelihood of an unforeseen and unfavourable business outcome resulting from the exploitation of vulnerabilities within an information system by a specific threat or malicious actor. This risk spectrum encompasses scenarios such as human error, equipment malfunction, cyberattacks, and natural disasters.

The practice of IT risk management entails applying established risk management methodologies to address IT threats effectively. This process encompasses the use of procedures, policies, and tools to systematically identify and assess potential threats and vulnerabilities within the IT infrastructure.

For more details, users can refer to the IT Risk Management Guidelines that are published by RISA.

Below are some best practices in terms of IT Risk Management. There are some steps to deploy to perform good risk management.

Step 1: Formulate a robust risk management Strategy:

The initiation of effective risk management involves the identification and assessment of potential vulnerabilities within an IT environment. Examples of these vulnerabilities include weak system passwords, unpatched systems, and downloads of malicious software. However, the manual process of identification and assessment can be both costly and resource-intensive. To streamline this process, organisations are encouraged to utilise automated tools, such as help desk or service desk software, which come equipped with risk management capabilities. These tools automatically detect and assess risks, promptly alerting security teams to potential issues.

Step 2: Conduct ICT asset management:

To mitigate technology risks effectively, maintain a continuous vigil over IT assets, including routers and servers. Employ reliable asset life cycle management software for automated, centralised network inventory, offering comprehensive insights into asset performance, security, and licensing concerns. Utilise this software to continuously monitor software licence expiration dates and receive automated alerts.

Step 3: Enhance cybersecurity:

Establishing and sustaining a secure IT infrastructure is pivotal in preventing cybersecurity risks. Employ appropriate security tools, policies, and procedures to thwart various threats. In addition to traditional measures like firewalls and antivirus software, integrate advanced security tools such as security information and event management (SIEM) software to bolster security controls. SIEM software, being automated, maintains a detailed log of security events, correlating data for swift threat identification. It facilitates automated responses to security incidents, such as blocking IP addresses linked to unauthorized activities. Leverage built-in templates for generating security and compliance reports.

Step 4: Ensure transparent communication:

Develop robust internal and external communication strategies to convey risk details to relevant parties. Clear communication expedites a coordinated response against evident threats in the IT environment, aiding faster risk mitigation, assessment, and monitoring. When devising your risk communication and management Strategy, seek input from all key stakeholders to comprehend various aspects of a given risk, including affected parties, significant challenges, and potential recovery costs.

Step 5: Implement access control:

Mitigate data security risks by instituting stringent authentication and authorization procedures within your organisation. Modern access management software assists in ensuring that only authorised users access sensitive parts of the network, thereby minimising the risk of insider threats. These tools continuously monitor file system changes to detect unauthorised alterations and generate compliance reports detailing user permissions and activities. Utilise such tools to proactively track privileged users' accounts for unusual activities, enhancing preparedness against advanced threats.

By implementing a comprehensive risk management approach, sectors can better protect their ICT assets and systems from potential threats and vulnerabilities. Regular reviews and updates to the risk management plan ensure that it remains effective in addressing emerging risks.

Revision #1
Created 9 July 2025 21:47:28 by RISA
Updated 9 July 2025 21:47:46 by RISA