Risk Assessment Template

Risk Assessment Template is structured document that used to identify and manage the risk associate within an organization’s assets, processes and systems. This is a vital tool for assessing potential threats, vulnerabilities and the impact to the organization.

In the context of ISO 27001, the Risk Assessment Template serves as foundation for the identifying risks to the information security and determining that the most appropriate controls to mitigate them. The template helps organizations document and also track the entire risk assessment process in a consistent and organized manner.

There are some key components of this template such as,

* Risk ID : unique identifier number for each risk
* Asset ID: unique identifier number for the asset
* Risk Description :A detailed description of the risk
* Rating: The probability of the risk occurring
* Impact Rating: The potential damage or consequences if the risk occurs.
* Risk Level: Level of the risk (risk that cause high impact are usually the top priority)
* Control Measures: The specific security controls or measures that are currently in place to mitigate the risk.
* Mitigation Plan: Actions or strategies that need to be implemented to reduce or eliminate the risk.
* Risk Owner: The individual or department responsible for managing and mitigating the risk.
* Target Completion Date: The deadline by which the risk mitigation actions should be completed.
* Status :The current progress of the risk management process

1. Risk Identification templated

A Risk Assessment Template is useful in a systematic manner, within an organization to describe possible risks and threats concerning all the information resources. This way, the contingent cannot be limited to the so-called ‘top risks,’ which can be fixed by creating an exhaustive list of ideas of what can go wrong. For instance, a company can post risks such as data loss, unauthorized or malicious internal users access and Malware and viruses for each asset or system.

2. Consistent Evaluation of Risk

The template allows the organization to assess the likelihood of occurrence and the severity of each risk following and objective procedure so that it can compare various risks using similar metrics. This ensures that risks are evaluated without compromise and with reasonable standard acknowledged.

For example:

* Rating: What is the likelihood of this risk (Low, Medium or High)?
* Impact Rating: If it occurs what is the consequence or severity low, medium or high?
* It enables you to know which risks are most acute and require your intervention.

3. Risk Prioritization

Both likelihood and impact can be used to formulate a risk level (for example, Low, Medium or High). This assist organizations to manage risks well especially so as to ensure that those that have maximum impact of the business are handled as a priority. For example, control activities at high risk level indicate that there should be heightened risk management efforts to put in place controls while low risk items may not Call for immediate action.

4. Informed Decision-Making

After the risks have been assessed, the template guides one in decision making as to how best to deal with the risks that are involved. It helps senior management to have information on which to base right decisions on, the controls to implement, resources to apply and timelines for risk management.

5. Record of Other Control Measures

A Risk Assessment Template is a useful tool for documenting existing controls; it also identifies places that need additional controls. Perhaps that is why this kind of documentation is critical for adherence to ISO 27001 since it proves that the organization addresses risks.

For example, risks like unauthorized access to sensitive systems might require controls such as:

* Multi-factor authentication
* Encryption
* Regular monitoring and audits

6. Compliance with ISO 27001

ISMS according to ISO 27001 stipulates that organizations should conduct risks assessments in an organization. By the use of the Risk Assessment Template the organization is about to meet some of the compliance requirement and policy standards since the documentation provides a structure of identifying, assessing and managing risks.

As the part of implementing risk assessment process, templates used during the audit also become the evidence to prove that the organisation has implemented systematic approach towards managing information security risks.

7. Accountability and Ownership

A Risk Assessment Template puts someone in charge of each of the risks that have been identified which means that someone is charge of managing them. Such accountability means risk cannot be hidden and are well managed since they are being checked.

For example, an individual who has been instituted as the IT Security Officer would be responsible for managing risks face concerning the organization’s financial database as the risk owner while the HR Manager shall manage risks that relate to employee records.

8. Proactive Risk Mitigation

The template contains the subheadings of mitigation plans and control measures to show how each risk will be managed. It is a measure that eliminates the possibility of such events happening and assessing the risks in advance of the actual occurrence a security threat or a business interruption.

9. Continuous Monitoring and Improvement

Risk assessment is not an activity that goes round once, it is an iterative process and should be reviewed from time to time. The template also assists in monitoring status of each risk so that organization can come back and make change depending on structure processes or assets. This leads to an ongoing improvement of the ISMS.