**Application Risk Assessment**

A risk is nothing but intersection of assets, threats and vulnerability. 

A+T+V = R

NIST SP 800-30 Risk Management Guide for Information Technology Practitioners defines risk as a function of the likelihood of a given threat-source exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization.

So the main components of Risk Assessment are:

* **Threats**
* **Vulnerability**
* **Impact (i.e. potential loss)**
* **Likelihood of occurrence (i.e. the probability that an event – threat successful exploit of a vulnerability – will occur)**

**Threats** is anything that can exploit a vulnerability accidentally or intentionally and destroy or damage an **asset**. Asset can be anything people, property or information. Asset is what we are trying to protect and a threat is what we are trying to protect against.

**Vulnerability** means gap or weakness in our protection efforts.

**Threat Source** is a method to exploit a vulnerability or a situation either intentionally or unintentionally. For example a Malicious Software to which a virus or worm attaches to spread itself in the system and to others computer via email containing either virus as a attachment or as a link. If this email is shared by sender without knowing the malicious purpose of attachment or link then, this will be unintentional threat source otherwise it will be an intentional threat source.

The complete process of handling Risk can be divided into following stages:

1. Context Establishment
2. Risk Assessment
   * Risk Identification
   * Risk Estimation
   * Risk Evaluation
3. Risk Management/ Mitigation
   * Risk Assumption
   * Risk Avoidance
   * Risk Limitation
   * Risk Planning
   * Research and Acknowledgement
   * Risk Transference
4. Risk Communication
5. Risk Monitoring and Review
6. IT Evaluation and Assessment

**1. Context Establishment**

In this step information about the organization and basic criteria, purpose, scope and boundaries of risk management activities are obtained. In addition to this data, it is important to gather details about the organization in charge of risk management activities.

Organization’s mission, values, structure, strategy, locations and cultural environment are studied to have a deep understanding of it’s scope and boundaries.   
The constraints (budgetary, cultural, political, technical) of the organization are to be collected and documented as guide for next steps.

The main role inside organization in charge of risk management activities can be seen as:

1. Senior Management
2. Chief information officer (CIO)
3. System and Information owners
4. the business and functional managers
5. the Information System Security Officer (ISSO) or Chief information security officer (CISO)
6. IT Security Practitioners
7. Security Awareness Trainers

Risk Management is a recurrent activity, on the other hand Risk assessment is executed at discrete points and until the performance of the next assessment. Risk Assessment is the process of evaluating known and postulated threats and vulnerabilities to determine expected loss. It also includes establishing the degree of acceptability to system operations. Risk Assessment receives input and output from Context establishment phase and output is the list of assessed risk risks, where risks are given priorities as per risk evaluation criteria.

1. **Risk Identification –** In this step we identify the following:
   * assets
   * threats
   * existing and planned security measures
   * vulnerabilities
   * consequence
   * related business processes
   * list of asset and related business processes with associated list of threats, existing and planned security measures
   * list of vulnerabilities unrelated to any identified threats
   * list of incident scenarios with their consequences
2. **Risk Estimation –** There are 2 methods for Risk Assessment:

**1. Quantitative Risk Assessment –** This methodology is not mostly used by the organizations except for the financial institutions and insurance companies. Quantitative risk is mathematically expressed as Annualised Loss Expectancy (ALE). ALE is the expected monetary loss that can be expected for an asset due to a risk being realised over a one-year period.

ALE= SLE \* ARO

1. Single Loss Expectancy (SLE) is the value of a single loss of the asset. This may or may not be the entire asset. This is the impact of the loss. Annualised Rate of Occurrence (ARO) is how often the loss occurs. This is the likelihood. Theoretically Quantitative risk assessment seems straightforward but there are issues in assigning values to parameters. While the cost of system is easy to define but indirect costs such as value of information, lost production activity and cost to recover are difficult to define accurately. The other element likelihood is not accurately known. Therefore, there is a large margin of error in Quantitative Risk Assessment. Due to unavailability of accurate and complete information it is not cost effective to perform a quantitative risk assessment for a IT System.

**2. Qualitative Risk Assessment –** Qualitative Risk Assessment defines likelihood, impact values and risk in subjective terms, keeping in mind that likelihood and impact values are highly uncertain. Qualitative risk assessments typically give risk results of “High”, “Moderate” and “Low”. Following are the steps in Qualitative Risk Assessment:

**Identifying Threats:** Threats and Threat-Sources must be identified. Threats should include threat-source to ensure accurate estimation. It is important to compile a list of all possible threats that are present across the organization and use this list as the basis for all risk management activities. Some of the examples of threat and threat-source are:

* 1. Natural Threats- floods, earthquakes etc.
  2. Human Threats- virus, worms etc.
  3. Environmental Threats- power failure, pollution etc.

**Identifying Vulnerabilities:**Vulnerabilities are identified by numerous means. Some of the tools are:

Vulnerability Scanners – This is the software the compare the operating system or code for flaws against the database of flaw signatures.

Penetration Testing – Human Security analyst will exercise threats against the system including operational vulnerabilities like Social Engineering.

Audit of Operational and Management Controls – Operational and management controls are reviewed by comparing the current documentation to best practices for example ISO 17799 and by comparing actual practices against current documented processes.

1. **Relating Threats to Vulnerabilities:** This is the most difficult and mandatory activity in Risk Assessment. T-V pair list is established by reviewing the vulnerability list and pairing a vulnerability with every threat that applies, then by reviewing the threat list and ensuring that all the vulnerabilities that threat-action/threat can act against have been identified.
2. **Defining Likelihood:** Likelihood is the probability that a threat caused by a threat-source will occur against a vulnerability. Sample Likelihood definitions can be like: Low -0-30% chance of successful exercise of Threat during a one year period Moderate – 31-70% chance of successful exercise of Threat during a one year period High – 71-100% chance of successful exercise of Threat during a one year period This is just a sample definitions. Organization can use their own definition like Very Low, Low, Moderate, High, Very High.
3. **Defining Impact:** Impact is best defined in terms of impact upon confidentiality, integrity and availability. Sample definitions for impact are as follows:

|  | Confidentiality | Integrity | Availability |
| --- | --- | --- | --- |
| Low | Loss of Confidentiality leads to Limited effect on organization | Loss of Integrity leads to Limited effect on organization | Loss of Availability leads to Limited effect on organization |
| Medium | Loss of Confidentiality leads to Serious effect on organization | Loss of Integrity leads to Serious effect on organization | Loss of Availability leads to Serious effect on organization |
| High | Loss of Confidentiality leads to Severe effect on organization | Loss of Integrity leads to Severe effect on organization | Loss of Availability leads to Severe effect on organization |

Examples of Organizational Effect is as follows:

| Effect Type | Effect on Mission Capability | Financial Loss | Effect on Human Life |
| --- | --- | --- | --- |
| Limited Effect | Temporary loss of one or more minor mission capabilities | Under Rs 50, 000 | Minor Harm |
| Serious Effect | Long term loss of one or more minor capabilities or Temporary loss of one or more primary mission capabilities. | Rs 50, 000- Rs 1, 00, 000 | Significant Harm |
| Severe Effect | Long term loss of one or more primary mission capabilities | over  Rs 1, 00, 000 | Loss of life |

**Assessing Risk:** Assessing risk is the process to determine the likelihood of the threat being exercised against the vulnerability and the resulting impact from a successful compromise. Sample Risk Determination Matrix is as follows:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | Impact | | |
| High | Moderate | Low |
| Likelihood | High | High | High | Moderate |
| Moderate | High | Moderate | Low |
| Low | Moderate | Low | Low |

**2. Risk Evaluation –** The risk evaluation process receives as input the output of risk analysis process. It first compares each risk level against the risk acceptance criteria and then prioritise the risk list with risk treatment indications.

**3. Risk Mitigation/ Management –** Risk Mitigation involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment process. Since eliminating all risk in an organization is close to impossible thus, it is the responsibility of senior management and functional and business managers to use the least-cost approach and implement the most appropriate controls to decrease risk to an acceptable level. As per NIST SP 800 30 framework there are 6 steps in Risk Mitigation.

1. **Risk Assumption:** This means to accept the risk and continue operating the system but at the same time try to implement the controls to
2. **Risk Avoidance:** This means to eliminate the risk cause or consequence in order to avoid the risk for example shutdown the system if the risk is identified.
3. **Risk Limitation:** To limit the risk by implementing controls that minimize the adverse impact of a threat’s exercising a vulnerability (e.g., use of supporting, preventive, detective controls)
4. **Risk Planning:** To manage risk by developing a risk mitigation plan that prioritizes, implements, and maintains controls
5. **Research and Acknowledgement:** In this step involves acknowledging the vulnerability or flaw and researching controls to correct the vulnerability.
6. **Risk Transference:** This means to transfer the risk to compensate for the loss for example purchasing insurance guarantees not 100% in all cases but atleast some recovery from the loss.

**4. Risk Communication –** The main purpose of this step is to communicate, give an understanding of all aspects of risk to all the stakeholder’s of an organization. Establishing a common understanding is important, since it influences decisions to be taken.

**5. Risk Monitoring and Review –** Security Measures are regularly reviewed to ensure they work as planned and changes in the environment don’t make them ineffective. With major changes in the work environment security measures should also be updated.Business requirements, vulnerabilities and threats can change over the time. Regular audits should be scheduled and should be conducted by an independent party.

**6. IT Evaluation and Assessment –** Security controls should be validated. Technical controls are systems that need to tested and verified. Vulnerability assessment and Penetration test are used for verifying status of security controls. Monitoring system events according to a security monitoring strategy, an incident response plan and security validation and metrics are fundamental activities to assure that an optimal level of security is obtained. It is important to keep a check on new vulnerabilities and apply procedural and technical controls for example regularly update software.