



IT Risk Management - Approach Paper

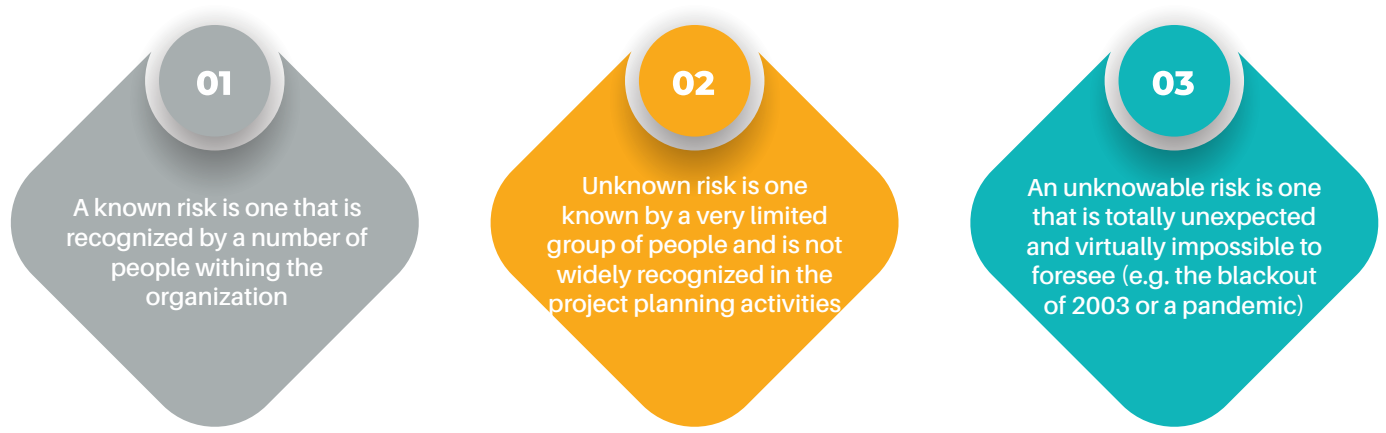
Understanding Risks

Risk is defined as an uncertain event or condition, that if it materializes, has a effect on objectives and strategy of the organization.

Risks are composed of three elements: the risk Event, the Impact and the Probability of the risk event occurring.

A risk can have a positive impact or a negative impact. Many tend to only focus on risks that will have a negative impact. But if there could be any positive impact it could be good to document that also.

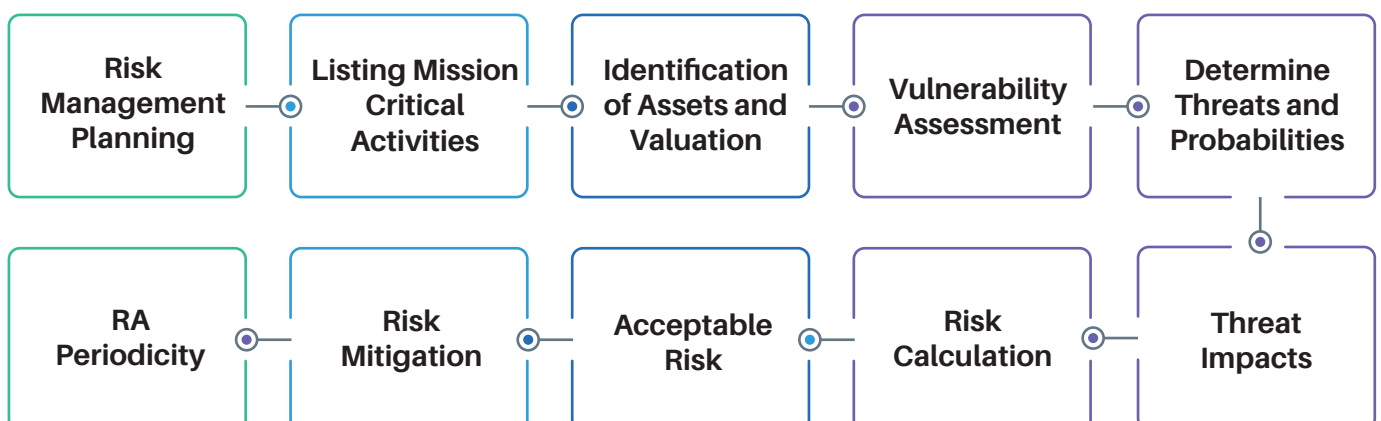
It is often helpful to define 'types' of risks which are known, unknown, and unknowable.



Identifying the 'unknown' risks is one of the major goals of a risk management process. Documenting the known risks and capturing as many of the unknown risks as possible reduces the number of surprises and provides a methodical approach to address the them.

The Risk Management Process

Skillmine defines the risk management process as the "systematic process of identifying, analysing, and responding to IT risks". The model for the risk management process is shown below.



Risk Management Planning

Risk management planning is the key to establishing a common understanding of :

- The project's key parameters/metrics.
- The sensitivity of those parameters.
- Management's risk tolerance.

In the planning process, the key parameters evaluation criteria needs to be agreed and established to be categorized into various impact areas like

- Business performance,
- Product capability,
- Schedule, etc.
- Once the key parameters are established, the impact of each should be developed. For instance, if a key parameter is weight, then the sensitivity of weight to the product should be established.

Listing Mission Critical Activities

The first step in carrying out a risk assessment is to list out the mission critical activities, on which the organization depends in order to meet the commitments to its customers, employees, shareholders, and other stakeholders.

Identification of Assets and Valuation

The organization may be dealing with various Information Assets. These may include client information, user information, company information and other such information assets. This step will determine those information assets, whose Confidentiality, Integrity and Availability(CIA) must be ensured. In order to prioritize our risk assessment efforts, it is important to determine the value of these assets. The valuation of the assets is done in terms of impact to the organization if there is a loss of CIA of the information. Criticality should be determined based on the following:

1
Assets that can have an impact on personal or assets safety

2
One that has sensitive information which could be at risk

3
One that cannot be allowed to get corrupted or damaged

4
One that cannot be allowed to get interrupted for over an hour and soon

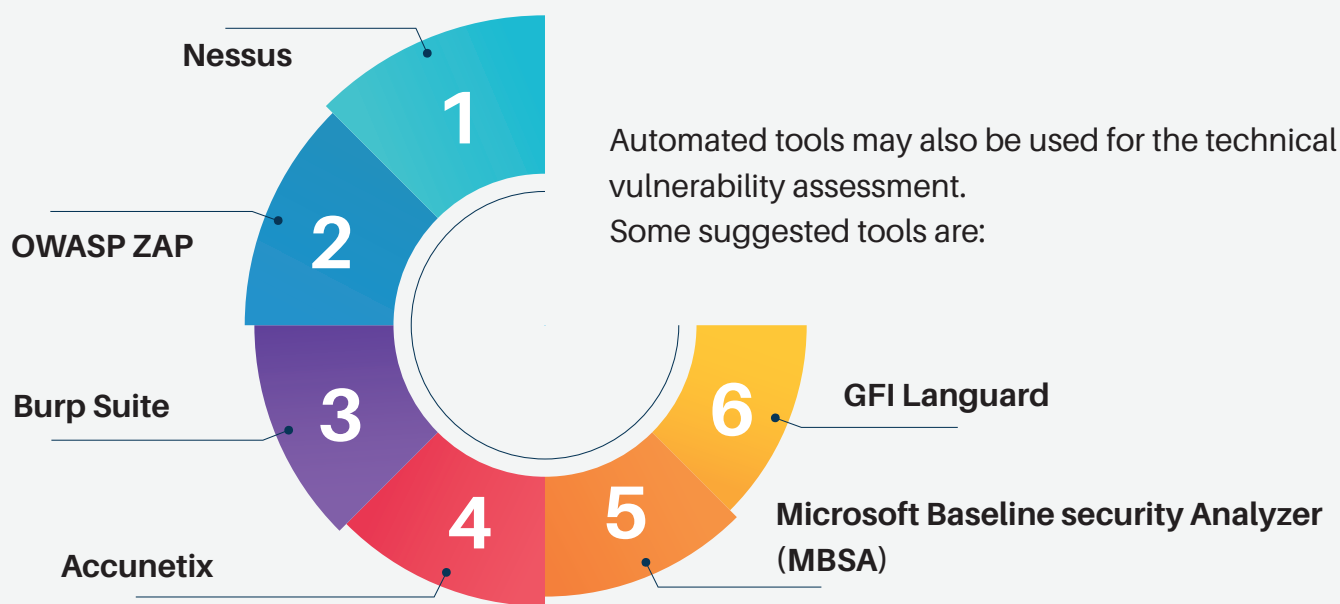
5
Assets that have an extensive impact on compliance with regulations

6
Assets that have significant financial or business importance

Vulnerability Assessment

Vulnerabilities in systems are inherent weaknesses that occur either due to a design flaw or an implementation flaw.

Standardized Checklists may be used for the assessment of various critical systems and processes. Refer to the Annexure for the checklist for specific systems.



Determine Threats and its Probabilities, Impacts

Threats are events that will exploit vulnerability to cause a loss of CIA. Threats are usually classified into Natural and Man-made. Some examples of threats to the Organization could be- hackers attacking the Organization, resource crunch that causes part or whole of the server to become non-operational, wrong data input that causes part or whole of the web application to malfunction, etc. There may be controls already in place for such threats. When evaluating the threats and their impact, we will consider the controls that are already in place. For instance, if there are adequate input validation controls, then the impact from wrong data input is highly reduced.

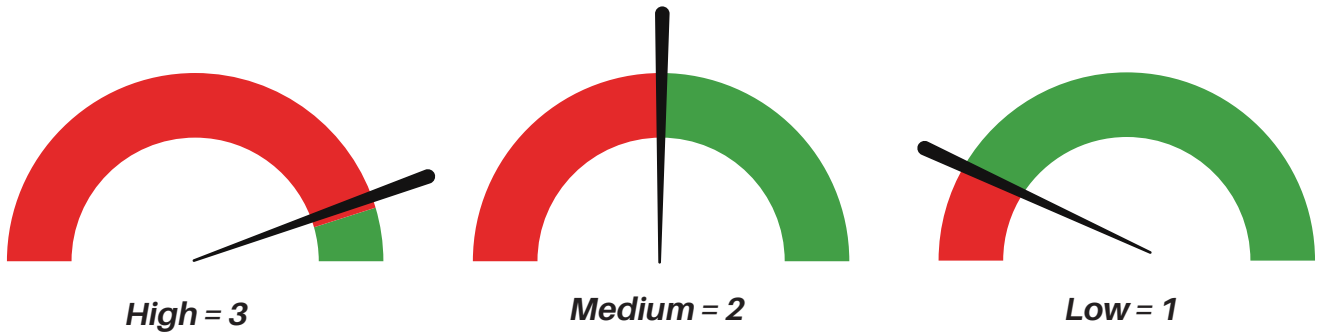
Not all threats are to be considered equal For instance, threats from a cyclone may be ignored, whereas hackers attacking the website are serious threats that may affect the ability of the organization to function, and must be taken into account while assessing the Organizational Security Posture.

The impact of threat is directly related to the value of the asset. It is measured in terms of loss to the organization in case there is a breach of the asset that eventually leads to a loss of Confidentiality, Integrity, Availability, or a combination of these of the information.

Risk Calculation

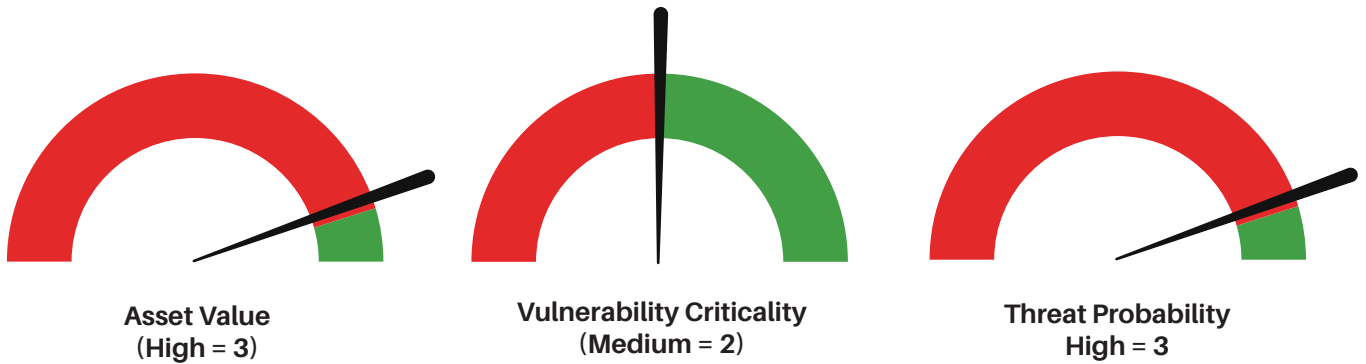
The following formulas may be used for calculating the risk from various threats:

$$\text{Risk} = \text{Asset Value} \times \text{Vulnerability Criticality} \times \text{Threat Probability}$$



Thus, the Risk can be a value between 1 and 27.

Thus, for example, If the values for Asset, Vulnerability Criticality, and Threat Probability are as follows:



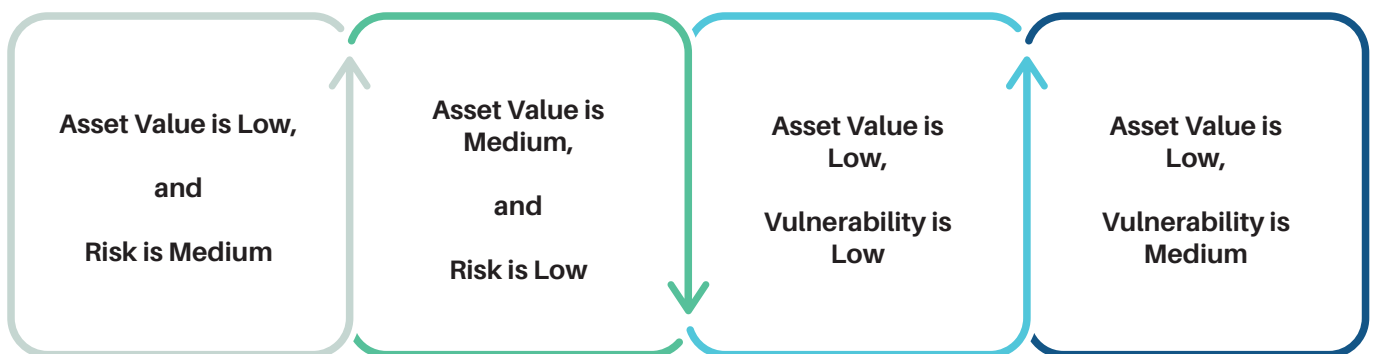
The Risk value will be $(3 \times 2 \times 3)$ (High) = 18

The final risk is categorized as detailed in the Risk Assessment Sheet.

Acceptable Risk

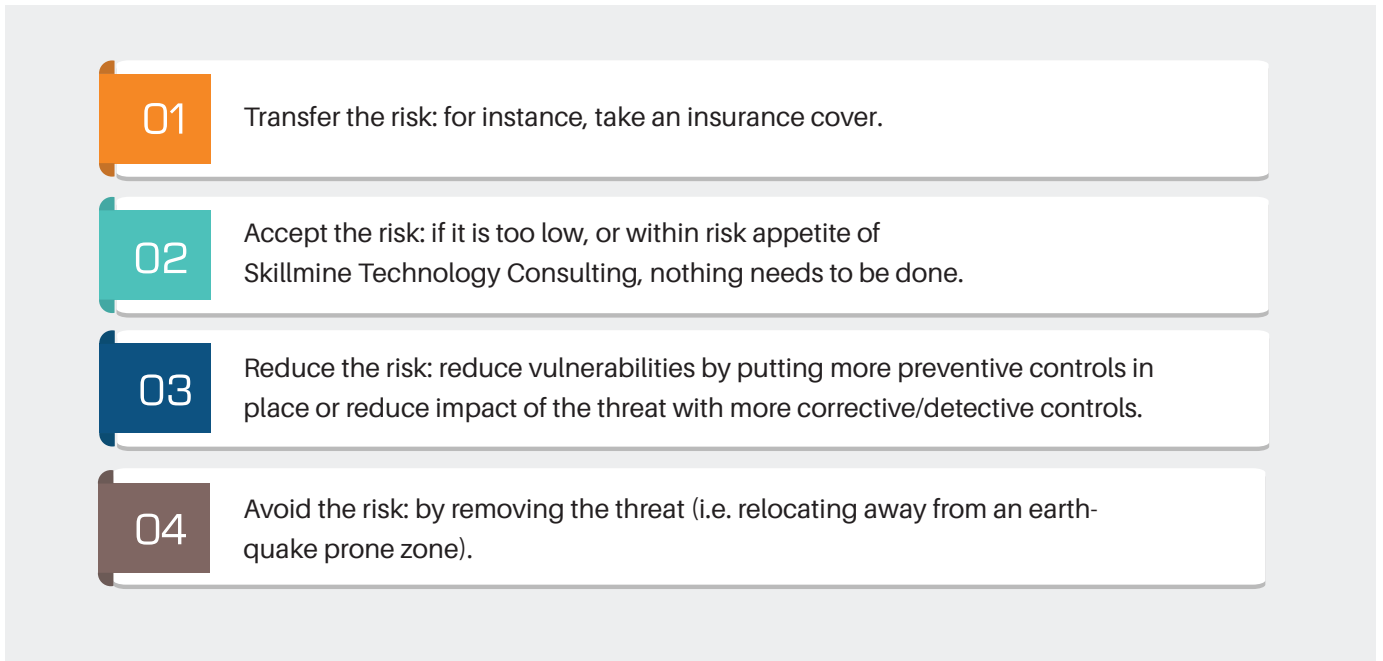
Based on the above values, and the formulas described above, a particular value will be the final risk for each asset.

The criteria for acceptable risk are:



Risk Mitigation

Based on Skillmine Technology Consulting's risk appetite, the following approaches may be taken for dealing with the risk:



- 01** Transfer the risk: for instance, take an insurance cover.
- 02** Accept the risk: if it is too low, or within risk appetite of Skillmine Technology Consulting, nothing needs to be done.
- 03** Reduce the risk: reduce vulnerabilities by putting more preventive controls in place or reduce impact of the threat with more corrective/detective controls.
- 04** Avoid the risk: by removing the threat (i.e. relocating away from an earthquake prone zone).

RA Periodicity

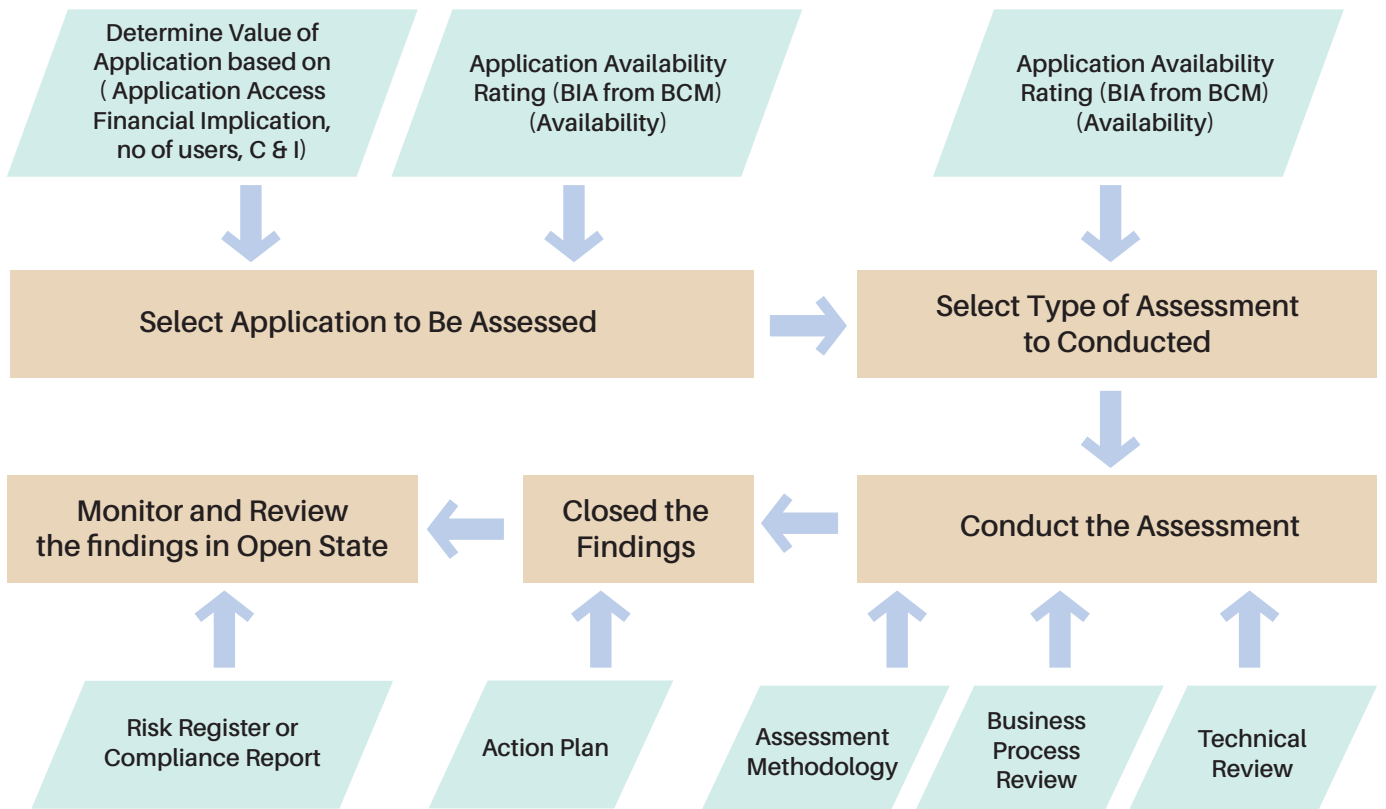
The risk assessment will be carried out at least once every year or as and when new systems or applications or significant network modifications are made. Adequate precautions must be taken to ensure that the Risk Assessment exercise is conducted in a way to minimize the risk of disruptions to business processes.

Cyber Security Risk Assessment Process Areas

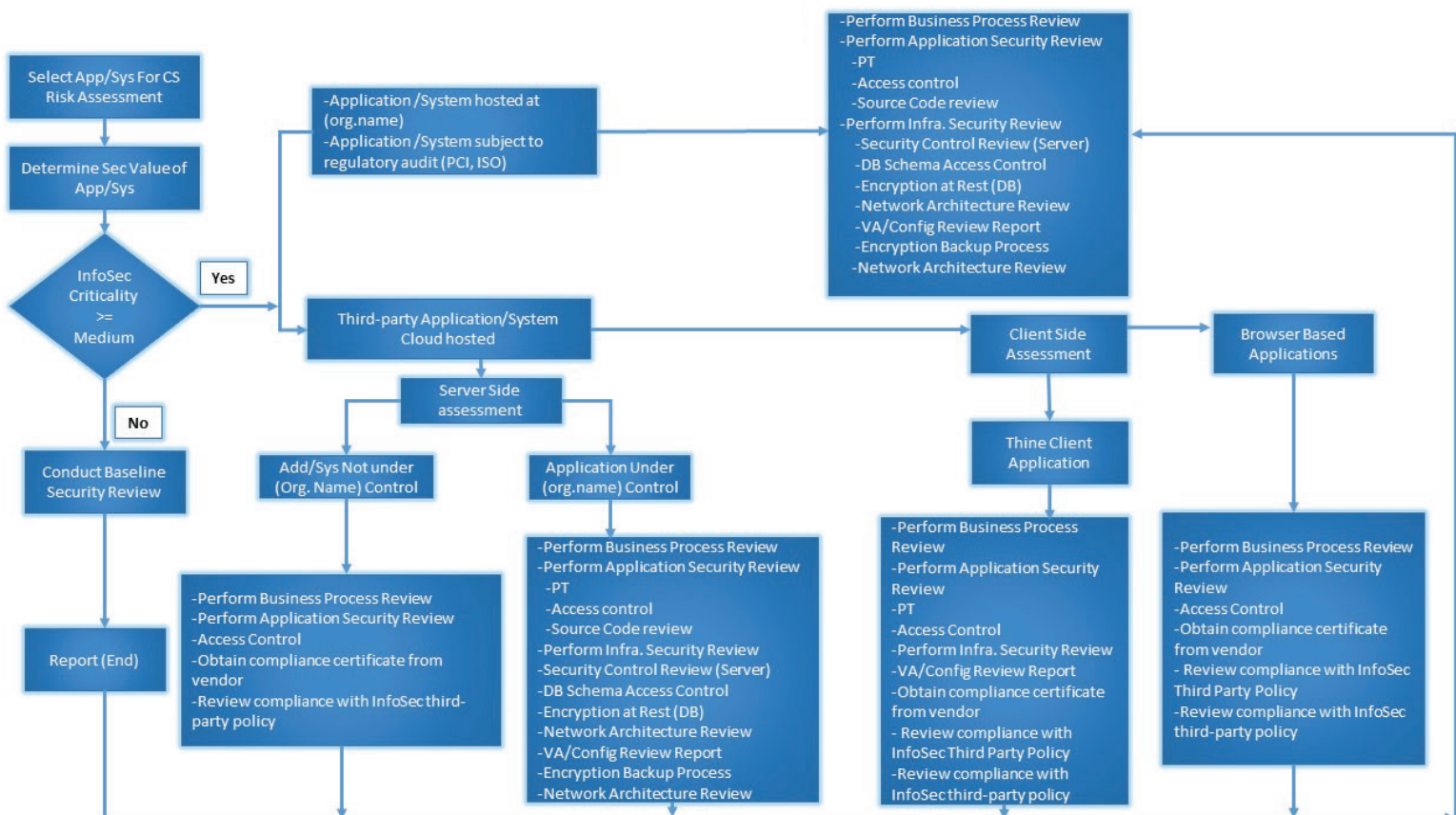


- 01** Application Security Assessment
- 02** Infra. Security Assessment
- 03** Security Process Review
- 04** N/W System Architecture Review
- 05** Source Code Review
- 06** Baseline Security Review

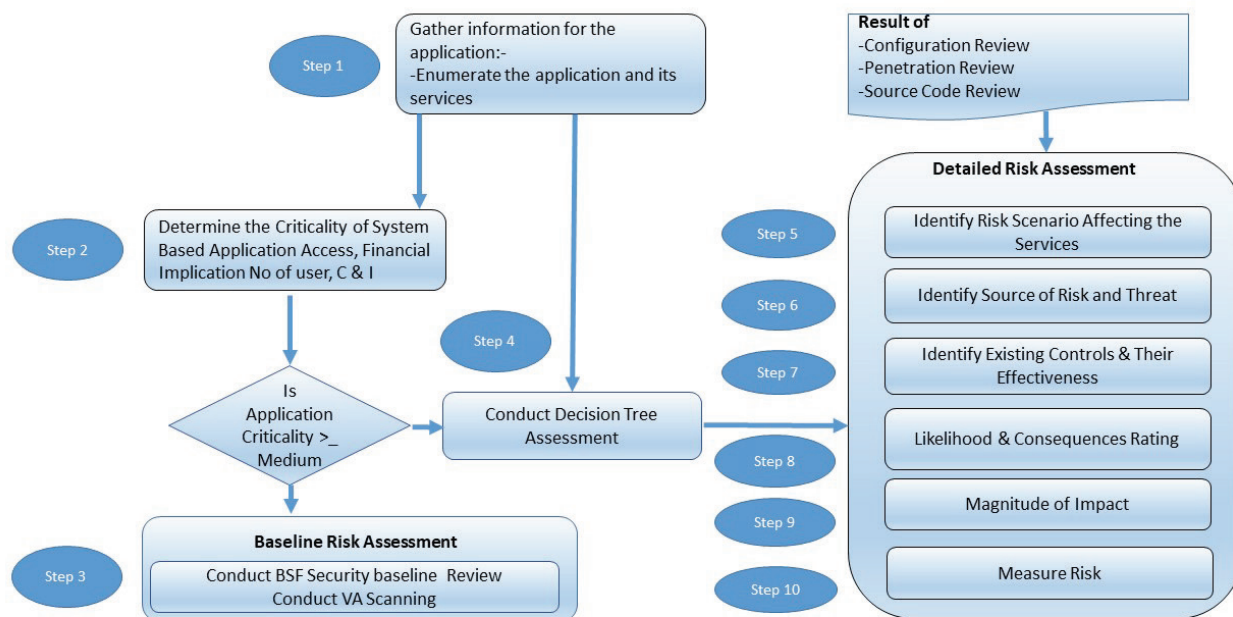
Cyber Security Risk Management Framework



Cyber Security Decision Tree Structure



Cyber Security Risk Assessment Process Flow



Proposed Team Structure Roles and responsibilities

The table below provides a high-level summary of the roles and responsibilities for our team as well as our client's roles and responsibilities.

Proposed team Role	Key Responsibility
Client Stake Holder	Serves as the project sponsor and highest point of escalation for strategic and tactical direction of the project.
Skillmine Advisor	Provides quality assurance oversight and risk management. Acts as a conduit to Skillmine leadership, as necessary.
Skillmine Project Manager	Monitors and provides feedback regarding project direction, project management effectiveness and project status. Makes strategic-level decisions and resolves issues in a timely manner. Provides quality assurance oversight and assists in risk management. Manages Technical resources and provides local on-site testing.
Client Project Manager	Responsible for working with the Skillmine Project Manager to confirm that people and resources are available for the project team to conduct the work. Attends all status meetings and help in issue resolution.
Skillmine Remote Consultants	Responsible for working with the Skillmine Project Manager to confirm that people and resources are available for the project team to conduct the work. Provides advanced technical testing capability for all security Assessments.