**NIST 800-39 defines 3 tiers of risk management (National institute of standards &technology) Organizational tier** – Concerned with the risk to the business as a whole **Business process tier** – Deals with a major function within the organization **Information Systems tier** – Addresses risk from an information system perspective

* **NIST 800-30** focused on computer systems and IT security issues. Establishes a 6 step Risk Management framework for **Federal Systems**

Categorize the information system, Select the security controls, implement security controls, assess security controls, Authorize the information system, Monitor the security controls

**FRAP - Facilitated Risk Analysis Process -**Focuses only on systems **that really need assessing, to reduce cost and time obligations**. Stresses pre-screening activities so that **RA steps are carried only on items that need it most Used to analyze one system, application or business process at a time** **It does not support the idea of calculating exploitation probability or ALE. Goal is ensuring efficiency and cost effectiveness by keeping the assessment scope simple and small**

**OCTAVE -** **Intended to be used in situations where people manage and direct the risk evaluation within their organization. Relies on idea that people working in the organization are best positioned to understand Risk and what is needed to address them. The scope of the Assessment is very wide than FRAP. The individuals perform assessment via facilitated workshops**

* **AS/NZ 4360 -** **Takes a broader approach to Risk management.** This risk methodology is more **focussed on the health of the company from a business point of view than security. It can be used to understand the company financial, capital, human, and business decision risks**

**Failure Mode and Effects Analysis -**This is commonly used **in product development and operational environments.** Goal is to **identify failure points and either fix or reduce the impact of the failure. It is used in Assurance Risk Management because of the level of detail, variables and complexity. This is not useful to detect complex failure modes involving multiple systems**

**Fault Tree Analysis- Most useful approach to identify failures in more complex environments and** systems. An un-desired effect is taken as the root and events that can contribute to this effect are added as a tree. Some common software failures that can be explored .False alarms, Insufficient error handling, Sequencing or order, Incorrect timing outputs, Valid but not expected outputs.

**CRAMM -**CCTA Risk Analysis and Management Method. **Created by UK and its automated tools are sold by Siemens. Works in three distinct stages. Define objectives, Assess risks, Identify countermeasures. It is a completely automated way of Risk Assessment…**