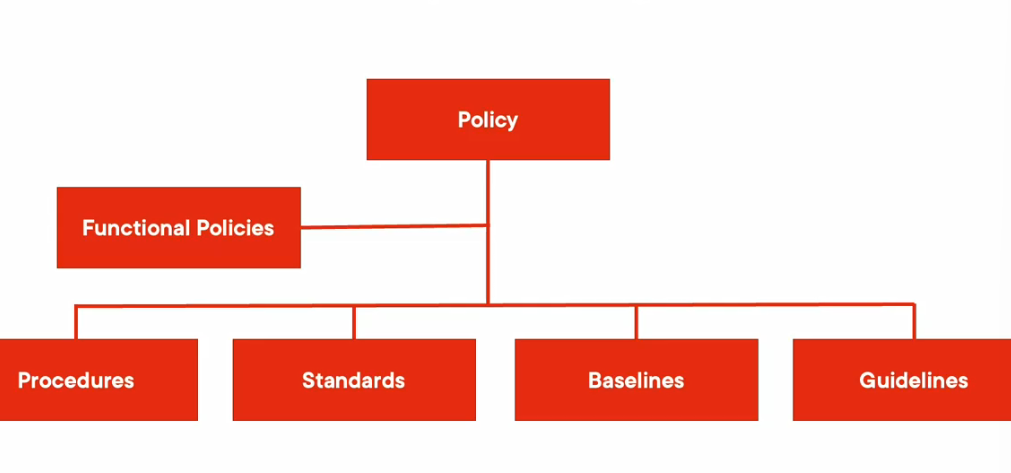
**Security Principles for CCSM**

Purpose of Information Assurance/Security-

1. Comply with Laws and Reg

Elements of Security- People, Tech, Physical/env- The right people doing the right things in a right way.

Policy, Procedures, Standards and Guidelines-



Policies-

1. Provide direction
2. Signed by mgmt.

Procedures-

1. Mandates how stg has to be done. We should have a clear procedure/step-by-action to provision stg
2. Be the support for the policy intent. Procedures help interpret what policy intent is.

Standards-

1. Mandate required quipments,software,solns
2. Compliance with good practices(ISO 27001)

Baselines-

1. It says that there are mandate min acceptable levels of action
2. Ex- basic equipment config, patches, network config, pwd length.

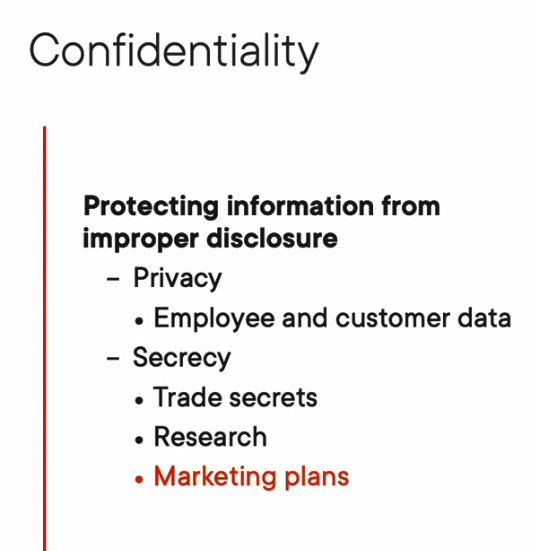
Guidelines-

1. There are the recommendations/suggestions, which are mandatory like above.

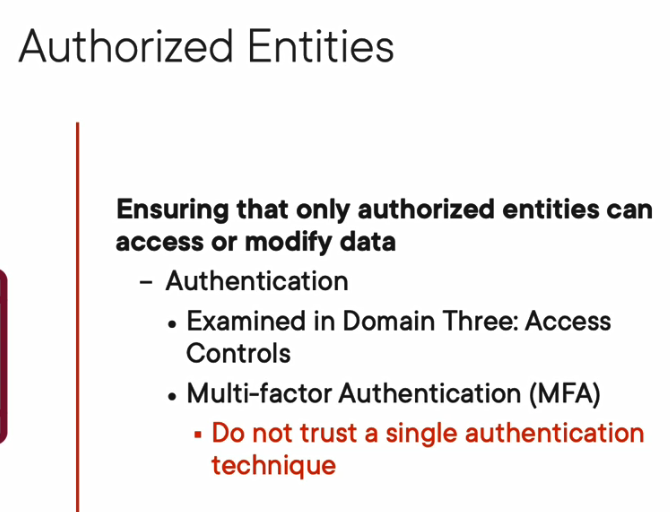
**Information security Traid- CIS traid**

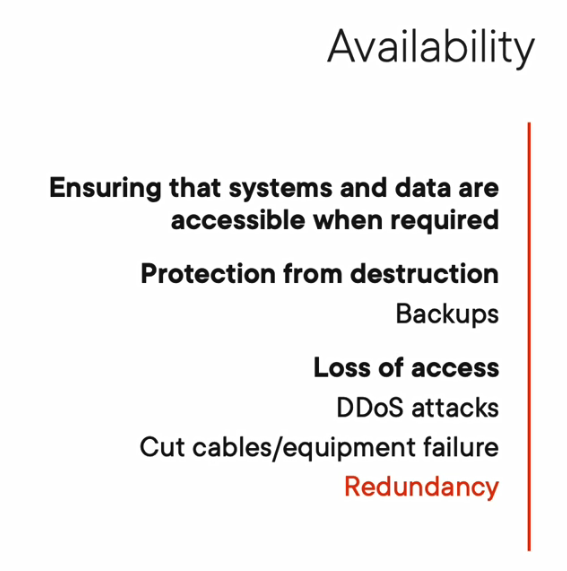
CIA- Confidentiality,Integrity,Availability

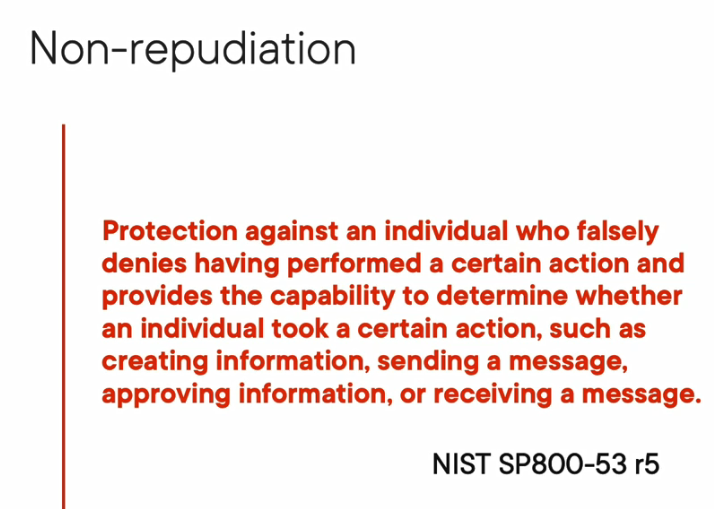






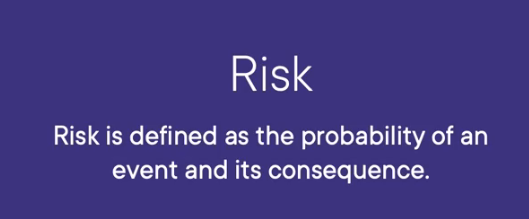


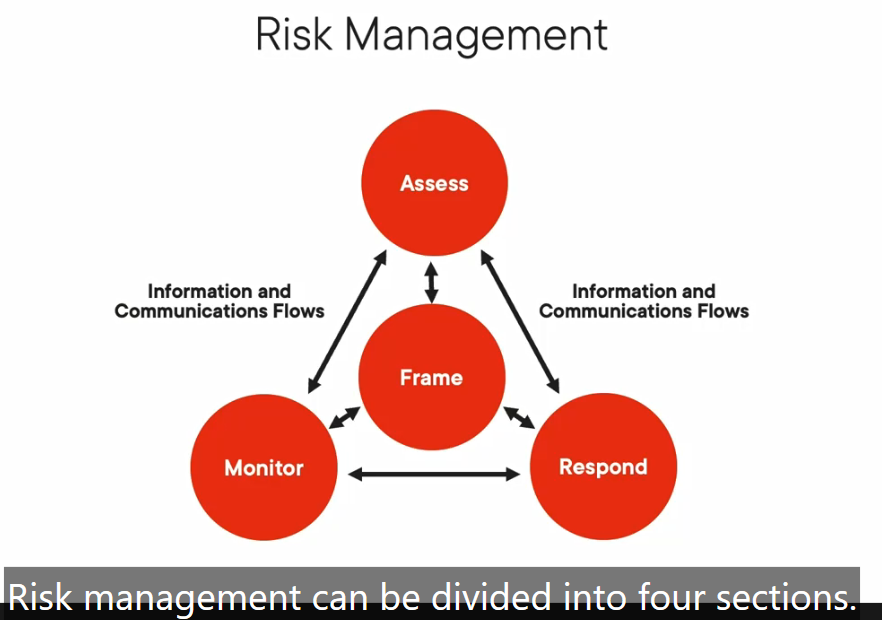




SECURITY PRINCIPLES FOR CCSM-

1. Info Sec concepts and Governance
2. Risk mgmt.
3. Security controls
4. (ISC)2 Code of Ethics





Frame- to understand the business, competition,laws,culture, what kind of business

Assess- After understanding the business, we can assess the risk, results of the assessments are fed back to mgmt in Frame area.

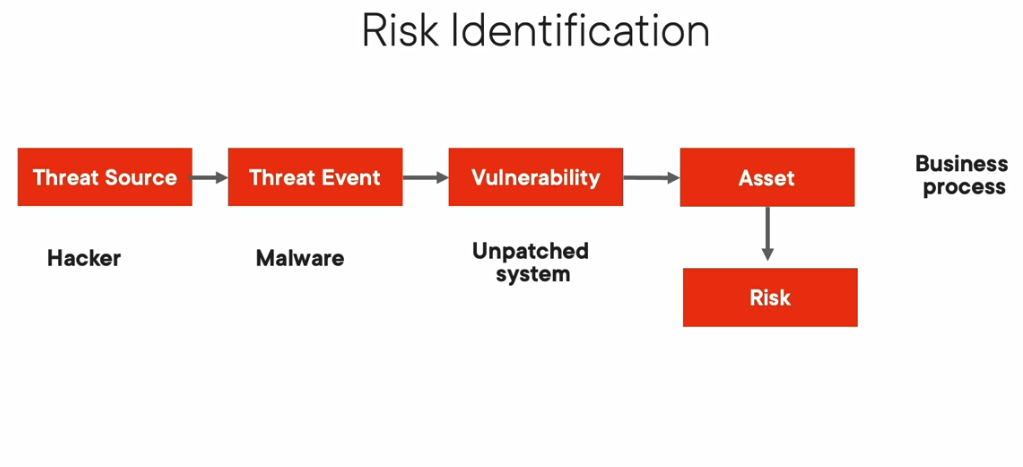
Risk treatment- Should we accept, cease the activity, try to reduce the risk. These are some options for risk response and risk treatment.

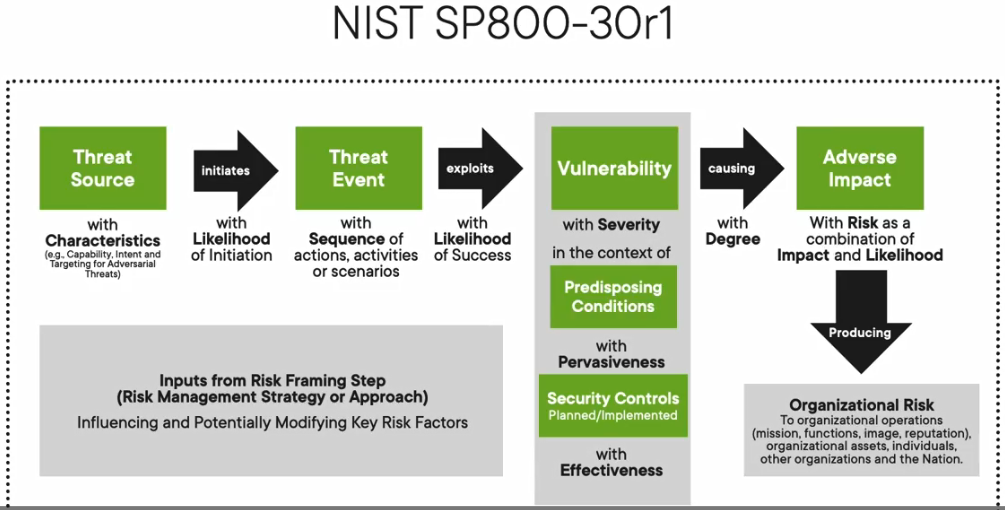
Since, risk is always changing, we should always monitor and respond and send it mgmt. and assess.

Risk Mgmt-

1. Risk Identification







1. Risk Identification/Assessment Requirements-