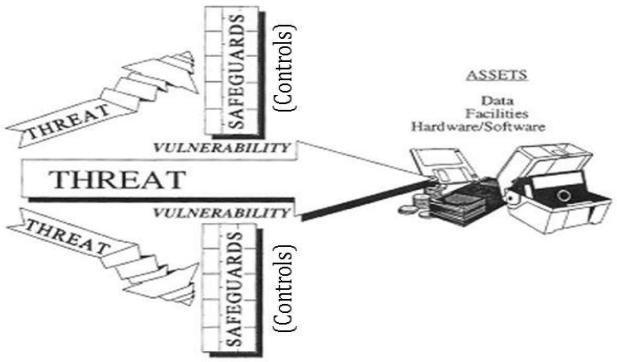
ISMS Excerpts – Risk Management Procedure

RISK MANAGEMENT

RISK

Risk is the possibility that a **threat** exploits a **vulnerability** in an information asset, leading to an adverse **impact** on the organization

- **Threat**: Something that might cause harm
- **Vulnerability:** A weakness that might be exploited
- **Impact:** Financial damage *etc*



Risk Management

- The process of understanding and responding to factors that may lead to a failure in the confidentiality, integrity or availability of an information or information system.

"Information Security is Everyone's Responsibility"

THREAT AND VULNERABILITY - EXAMPLES

THREAT		VULNERABILITY
Fire		Absence of Emergency Evacuation Plan
Earth quakes		No preparation against environmental Threats
Failure of a/c or water supply, telecom services, transport services		Absence of recording & monitoring of Temperature & RH in DC, Hub/UPS rooms
Breach of confidentiality, Theft of media or documents or information, Tampering with S/W and H/W		Weak controls on using IM systems
Equipment failure/malfunctioning		Inefficiency in operation and maintenance of supporting utilities
Unauthorized use/Misuse use of equipments and facilities, Use of counterfeit or copied software, Illegal processing of data		Lack of adequate process for handling project movements
Error in use, Misuse of rights		Absence of regular review of User's access rights and privileges

"Information Security is Everyone's Responsibility"

RISK ANALYSIS

- Risk Identification
  - List the information security needs and expectations of interested parties and identify the risks involved in meeting these needs and expectations.
  - Interested parties are persons or organizations that can influence an organization's information security / business continuity, or persons or organizations that can be affected by an organization's information security or business continuity activities.

- Risk Assessment
  - Analyze the risks for probability and impact
  - Arrive at Risk Rating
  - Decide on Risk response based on Rating

"Information Security is Everyone's Responsibility"

RISK RESPONSE

- Risk Response Development
  - Mitigating Risk
    - Reducing the likelihood an adverse event will occur
    - Reducing impact of adverse event
    - Risk Treatment Plan has to be created for risk mitigation
  - Avoiding Risk
    - Changing the project plan to eliminate the risk or condition
  - Transferring Risk
    - Paying a premium to pass the risk to another party
    - Requiring Build-Own-Operate-Transfer (BOOT) provisions
  - Accept Risk
    - Making a conscious decision to accept the risk
    - Risk Assessment has to be created for Risk Acceptance

"Information Security is Everyone's Responsibility"

aspire SYSTEMS
attention. always.