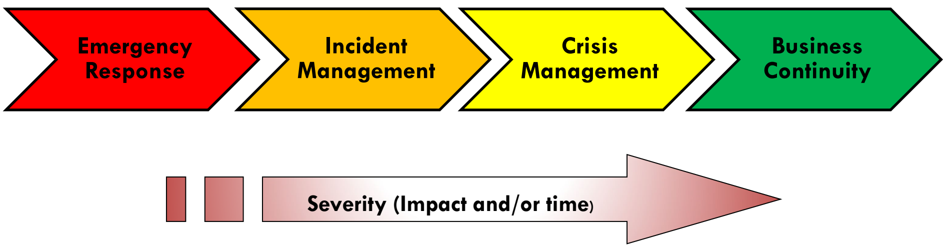
Threat Assessment, Risk Management and Response

What is Business Resilience?



Emergency Response Plan (ERP)	Incident Management Plan (IMP)	Crisis Management Plan (CMP)	Business Continuity Plan (BCP)

Business resilience is the ability an organization has to quickly adapt to disruptions while maintaining continuous business operations and safeguarding people, assets and overall brand equity.

What Is Threat Assessment and Risk Management ?

RISK ANALYSIS
VULNERABILITY
THREAT ASSESSMENT
Residual RISK
THREAT
RISK
Consequences
RISK ASSESSMENT
VULNERABILITY ASSESSMENT
RISK MANAGEMENT

3

Discussion

- What exactly is Threat Assessment and Risk Management
- Identify and evaluate potential Threats and their impacts
- Identify and evaluate Vulnerabilities
- Understanding risk in the context of Risk Management
- Risk Management Methods, Best Practices, Tools and Techniques to assist in development of effective risk management

4

Discussion

What is threat?

THREAT

"**Threat**" is defined as "**the probability/likelihood of an attack or Credible Risk Event against a Target/Asset**".

- ✓ "An **undeclared** intention to take an action resulting in harm, pain or misery
- ✓ A **declared** intention to take an action resulting in harm, pain or misery

THREAT

Threat = Intention + Capability

Threat assessment are not opinions of individuals, they are analytical processes to determine:

- **IF there is threat**
- **WHERE it may come from**
- **HOW it may be perpetrated**

7

Threat in the Context of Security

- Criminal Activity
- Armed Conflict
- Terrorism
- Civil Unrest
- Hazards

8

Criticality/Consequence

Assessment of the nature and scale of the impact of the specific attack; whether minor, significant or substantial, in terms of:

- *loss of life;*
- *injuries;*
- *economic and political;*
- *reputational;*
- *societal*

9

Discussion

What is Vulnerability?

10

Vulnerability?

- Open to attack or damage
- Weakness

<u>In the context of Security</u>

- Characteristics of a target which could be exploited in an attack; or the ease by which the target may be attacked
- Is it physical, administrative, logical, technical?

11

Vulnerability Assessment

- Process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system
- Must consider exposure to threat and measures implemented by the target to protect itself

Threat = Intent + Capability

12

Likelihood or Exposure

- The possibility that a given event will occur in qualitative terms, e.g. High, Medium, Low or Unlikely, Remote, Possible, Probable, Likely. Quantitative equivalent of Likelihood is Probability.

Likelihood = Threat (I+C) x Vulnerability

13

What is risk?

14

Risk

Possibility of an event, either positive or negative, occurring that will have an impact on the achievement of an objectives. Risk is measured in terms of Likelihood/Probability and Consequence/Severity.

15

Security Context of Risk

- Risk is a judgment of the probability of an attack being successfully carried out against a target
- It involves not only threat, but also the ease by which the target may be attacked — the **vulnerability**

Risk = Likelihood X Severity

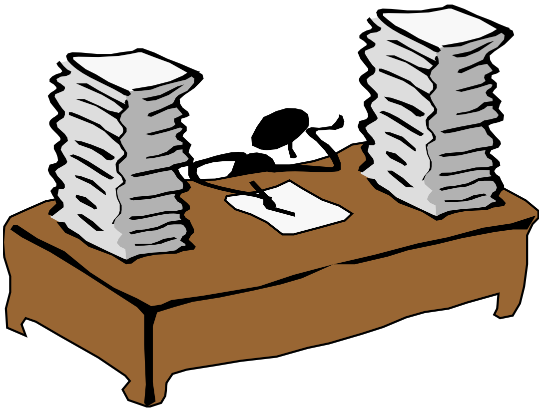
CONVENTIONAL WISDOM

Very little one can do to affect the threat. Therefore, action concentrates on reducing **The Vulnerability**.

16

Risk Assessment

A series of processes that evaluates the identified threats and vulnerabilities to determine the probability of occurrence and assigns priorities to them



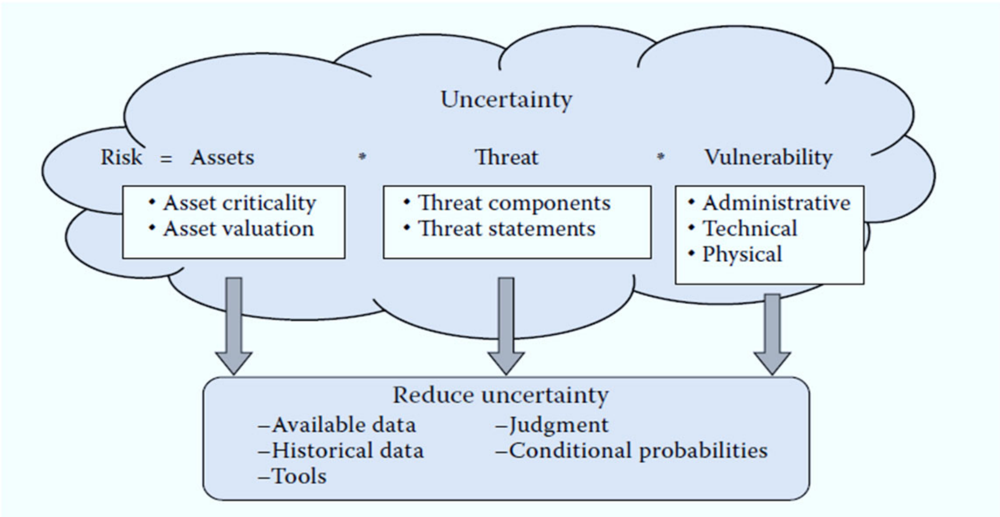
17

The Concept of Risk Management

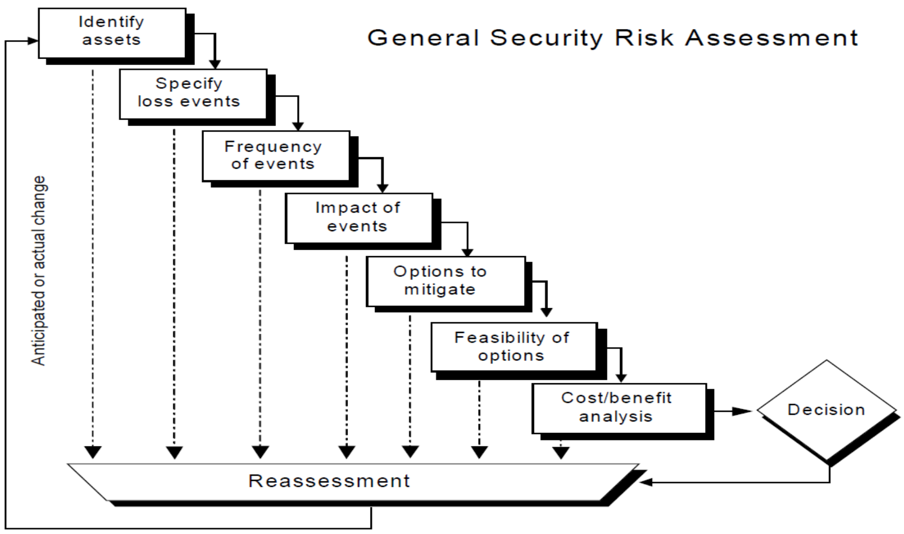
18

Risk Management process

- Systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, monitoring and reviewing risk*
- *ISO 73:2009 “Risk Management – Vocabulary”



SRM Flow Chart

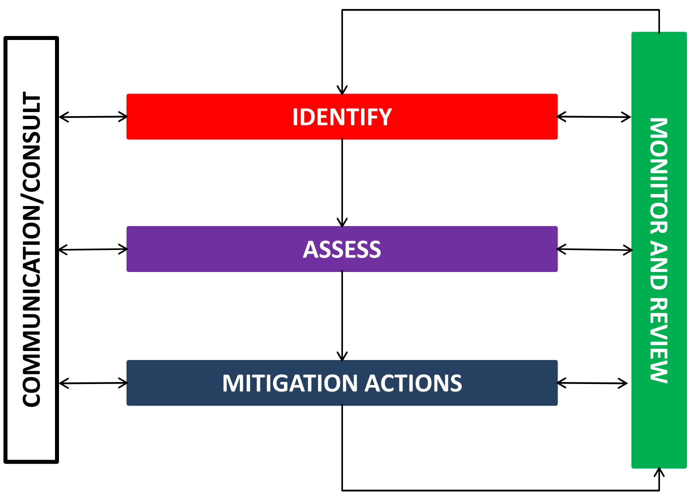


Process Flow Chart. This flow chart graphically represents this process.

Threat & Risk Management

21

Risk Management process



Threat & Risk Management

22

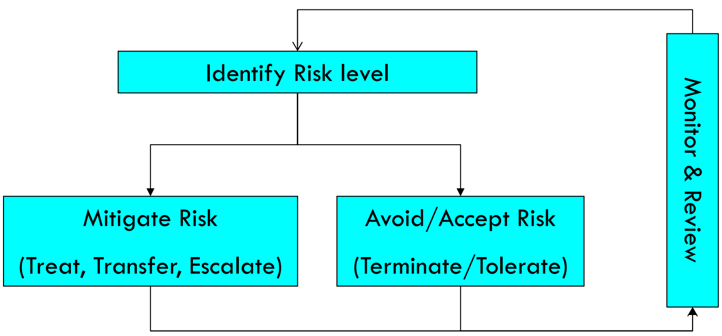
Risk Response Options

The 4TEs of risk response options;

- Tolerate
- Terminate
- Transfer
- Treat

Focus is on lowering Risk to As Low As Reasonably Practicable (ALARP). The security posture is commensurate with the prevailing risk profile.

Responses to Risk



RISK ASSESSMENT

- Assess residual risks

Residual risk

Acceptable level
Pass until next review

Unacceptable level
Further mitigation actions required

Critical Success Factor

COMMUNICATION!

Keys to Effective Communication

- Credibility
- Confidentiality
- Mutual respect
- Commitment
- Expertise (including good quality information)
- Empathy
- Recognition that individual decisions may be based more on values than on evidence

27

Communication Aims

- Achieve a common understanding of risks
- Develop credible procedures
- Improves understanding of what needs to be done
- Build trust and encourages shared decision making
- Reduces misperceptions and misunderstandings
- Strengthen working relationship among participants

28

Communication Process

- Consistent
- Open
- Transparent
- Documented
- All-hands in

Threat & Risk Management

29

- Loss of credibility
- Costly debate and conflict
- Diversion of attention and resources
- Lack of support

Threat & Risk Management

30

Key Success Factor

PREPAREDNESS!

Characteristics of Unpreparedness

- Surprise
- Insufficient information when you need it most
- Rapid escalation of events
- Events outpace decision making
- Events outpace response capability
- Confusion
- Communication problems
- Failure of routine structures

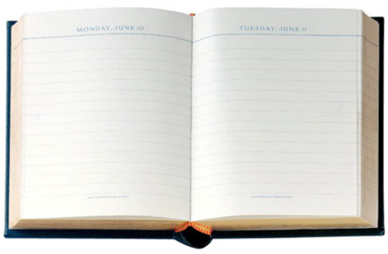
Characteristics of Unpreparedness

- Resources isolated or inaccessible
- Routine decision-making fractured
- Media attention focused
- Demand for information normally exceeding its availability
- Loss of control
- Important interests at stake

33

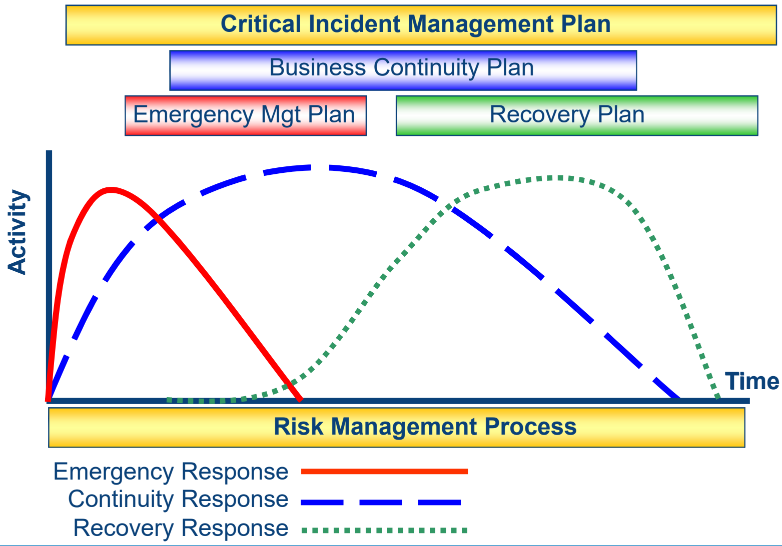
Key Success Factor

DOCUMENTATION!



34

Integration



35