Universitas Esa Unggul

Smart, Creative and Entrepreneurial

www.esaunggul.ac.id

Best Practise Manajemen Risiko TI
(IT Risk Management)

Oleh : Yulhendri

Sistem Informasi - Fakultas Ilmu Komputer

Definition

Risk is the effect of uncertainty on objectives, whether positive or negative

Risk Management: Identification, assessment, and prioritization of risks

Involves coordination and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events or to maximize the realization of opportunities

Sources

Uncertainty in financial markets

Project failures (at any phase in design, development, production, or sustainment life-cycles)

Legal liabilities

Credit risk

Accidents

Natural causes and disasters Deliberate
attack from an adversary Uncertain or
unpredictable root-cause

Others ...

Ideal Risk Management

Prioritizing risks with the greatest loss (or impact) and the greatest probability of occurrence

Risks with lower probability of occurrence and lower loss are handled in descending order

In practice the process of assessing overall risk can be difficult

Balancing resources used to mitigate between risks with high probability of occurrence but lower loss versus a risk with high loss but lower probability of occurrence can often be mishandled

Intangible Risk Management

Identifying a new type of a risk with 100% probability of occurring but is ignored by organization due to lack of identification ability

For example, when deficient knowledge is applied to a situation, a knowledge risk materializes

Relationship risk appears when ineffective collaboration occurs

Directly reduce productivity of knowledge workers, decrease cost effectiveness, profitability, service, quality, d reputation, bran value, and earnings quality

Allows risk management to create immediate value from risk identification and reduction that reduce productivity

Risk Management Methodology

Identify and characterize threats

Assess vulnerability of critical assets to specific threats

Determine likelihood and impact of the risks

Identify ways to reduce those risks

Prioritize risk reduction measures based on a strategy

Risk Management Principles

Create value

Resources expended to mitigate risk should be less than the consequence of inaction (the gain should exceed the pain)

be an integral part of organizational processes

be part of decision making process

explicitly address uncertainty and assumptions

be systematic and structured

Risk Management Principles (cont'd)

- be based on the best available information
- be tailorable
- take human factors into account
- be transparent and inclusive
- be dynamic, iterative and responsive to change
- be capable of continual improvement and enhancement
- be continually or periodically re-assessed

Risk Management Process

- ISO 31000
  1. Establishing the context
     - identification of risk in a selected domain of interest
     - planning the remainder of the process
     - mapping out
       - the social scope of risk management
       - the identity and objectives of stakeholders
       - the basis upon which risks will be evaluated, constraints.
     - defining a framework for the activity and an agenda for identification
     - developing an analysis of risks involved in the process
     - mitigation or solution of risks using available technological, human and organizational resources.
  2. Identification: source and problem analysis
  3. Assessment

Risk Options

- Design a new business process with adequate built-in risk control and containment measures from the start
- Periodically re-assess risks accepted in ongoing processes as a normal feature of business operations and modify mitigation measures
- Transfer risks to an external agency (insurance company, etc)
- Avoid risks altogether (i.e. closing down a particular high-risk business unit/department)

Risk Response

- Avoidance

  Eliminate, withdraw from or not become involved

- Reduction

  Optimize, Mitigate

- Sharing

  Transfer, outsource or insure

- Retention

  Accept and budget

Risk Management Plan

- Select appropriate controls or countermeasures to measure each risk
- Propose applicable and effective security controls for managing the risks
- Contain a schedule for control implementation and responsible persons for those actions
- Approval from the appropriate level of management for risk mitigation

Risk Management Plan (cont'd)

- According to ISO/IEC 27001, after risk assessment prepare a Risk Treatment Plan (document the decisions about how each of the identified risks shou ld be handled)
- Mitigation of risks often means selection of security controls; it should be documented in a Statement of Applicability, which identifies which particular control objectives and controls from the standard have been selected, and why
- Implementation follows all of the planned methods for mitigating the effect of the risks

Risk Management Plan (cont'd)

- Initial risk management plans will never be perfect
- Practice, experience, and actual loss results will necessitate changes in the plan and contribute information to allow possible different decisions to be made in dealing with the risks being faced
- Risk analysis results and management plans should be updated periodically. There are two primary reasons for this:
  - To evaluate whether the previously selected security controls are still applicable and effective
  - To evaluate the possible risk level changes in the business environment

Risk Management Challenges

- Prioritizing risk management processes too highly could keep an organization from ever completing a project or even getting started
- Do differentiate between risk and uncertainty -- Risk can be measured by impacts x probability
- If risks are improperly assessed and prioritized, time can be wasted in dealing with risk of losses that are not likely to occur
- Spending too much time assessing and managing unlikely risks can divert resources that could be used more profitably
- Unlikely events do occur but if risk is unlikely enough to occur it may be better to simply retain risk and deal with the result if loss does occur
- Qualitative risk assessment is subjective and lacks consistency
- Primary justification for a formal risk assessment process is legal and bureaucratic

Enterprise Risk Management Definition

Methods and processes used by organizations to manage risks and seize opportunities related to the achievement of their objectives

Its framework involves

- Identifying particular events or circumstances relevant to the organization's objectives (risks and opportunities)
- Assessing them in terms of likelihood and magnitude of impact
- Determining a response strategy
- Monitoring progress and assurance

Definition (cont'd)

In short, ERM is also a risk-based approach to managing an company, corporation, enterprise's integrating concepts of internal control, Sarbanes-Oxley Act for U.S corps and Strategic Planning

Benefits

- Identifying and addressing risk and opportunities proactively
- Company or business will protect and create value for their stakeholders such as owners, employees, customers, regulators, and society in general

ERM Framework

- Known as Risk Response Strategy:
  - Avoidance: exiting the activities giving rise to risk
  - Reduction: taking action to reduce the or likelihood impact related to the risk
  - Alternative Actions: deciding and considering other feasible steps to minimize risks
  - Share or Insure: transferring or sharing a portion of the risk, to fi na nee it
  - Accept: no action is taken, due to a cost or benefit decision

Risk Types and Examples

- Hazard risk

  Liability torts, Property damage, Natural catastrophe
- Financial risk

  Pricing risk, Asset risk, Currency risk, Liquidity risk
- Operational risk

  Customer satisfaction, Product failure, Integrity, Reputational risk
- Strategic risks

  Competition, Social trend, Capital availability

ERM Processes

- **Establishing Context**

  Understanding current conditions the organization operates on an internal, external and risk management context

  Identifying Risks

- Documenting material threats to organization's achievement of its objectives and representation of areas the organization may exploit for competitive advantage

  Analyzing/Quantifying Risks

- Creating probability distributions of outcomes for each materia l risk

ERM Processes (cont'd)

- **Integrating Risks**

  Aggregating all risk distributions, reflecting correlations and portfolio effects, formulating results of impact on company key performance metrics

- **Assessing or Prioritizing Risks**

  Determining contribution of each risk to aggregate risk profile, and doing prioritization

- **Treating or Exploiting Risks**

  Crafting strategies for controlling and exploiting various risks

- **Monitoring and Reviewing**

  Measuring and monitoring risk environment and performance of risk management strategies

ERM Objectives

- Companies manage risks and have various departments or functions ("risk functions") that identify and manage particular risks
- Each risk function varies in capability and how it coordinates with other risk functions Main goal
- and challenge is improving this capability, coordination, integration of output to provide a unified picture of risk for stakeholders and improving organization's ability to manage enterprise risks effectively

ERM Challenges

- Identifying executive sponsors
- Establishing a common risk language or glossary
- Describing the enterprise's risk appetite (take or not)
- Identifying and describing risks in risk inventory
- Implementing risk-ranking methodology to prioritize risks within and across functions
- Setting up Risk Committee and or Chief Risk Officer to coordinate certain activities of entire risk functions

ERM Challenges (cont'd)

- Establishing ownership for particular risks and responses
- Calculating Cost-Benefit Analysis of risk management effort.
- Developing action plans to ensure risks are appropriately managed
- Developing consolidated reporting for various stakeholders
- Monitoring results of actions taken in mitigating risk
- Ensuring efficient risk coverage by internal auditors, consulting teams, and other evaluating entities
- Developing technical ERM framework that enables secure participation by third parties and remote employees

Risk Functions

- Strategic planning

  Identifying external threats and competitive opportunities, along with strategic initiatives to address them
- Marketing

  Understanding target customer to ensure product or service alignment with its requirements
- Compliance & Ethics

  Monitoring compliance with code of conduct and directing fraud investigations
- Accounting / Financial compliance

  Complying with Sarbanes-Oxley which identifies financial reporting risks

Risk Functions (cont'd)

- Law Department

  Managing litigation and analyzing emerging legal trends that impact the organization

- Insurance

  Ensuring proper insurance coverage for the organization

- Treasury

  Ensuring cash is sufficient to meet business needs, while managing risk related to commodity pricing or foreign exchange

- Operational Quality Assurance

  Verifying operational output is tolerable

Risk Functions(cont'd)

Operations management

Ensuring business runs day-to-day and related barriers are surfaced for resolution

Credit

Ensuring any credit provided to customers is appropriate their ability to pay

Customer service

Ensuring customer complaints are handled promptly and root causes are reported to operations for resolution

Internal audit

Evaluating effectiveness of entire risk functions and recommending improvements

Internal Audit Role

- Beside IT Audit, they play an important role in evaluating organization risk management processes and advocating continued improvement
- Should not take any direct responsibility for making risk management decisions for the enterprise or managing risk management function
- Perform an annual risk assessment of the enterprise
- Develop audit engagements plan
- Involves review of various risk assessments performed by enterprise: strategic plans, competitive benchmarking, and SOX top-down risk assessment

IT Risk Management

IT Risk Concept

- Part of business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise
- Consists of IT-related events that could potentially impact the business
- Occur both uncertain frequency and magnitude
- It creates challenges in meeting strategic goals and objectives
- Due to IT's importance to the overall business, IT risk should be treated like other key business risks.

Risk IT Framework

Framework

- Integrate the management of IT risk with the overall ERM
- Compare assessed IT risk with risk appetite and risk tolerance of the organization
- Understand how to manage the risk

Risk IT Categories

- IT Benefit/Value enabler

  Missed opportunity to increase business value by enabled or improved processes

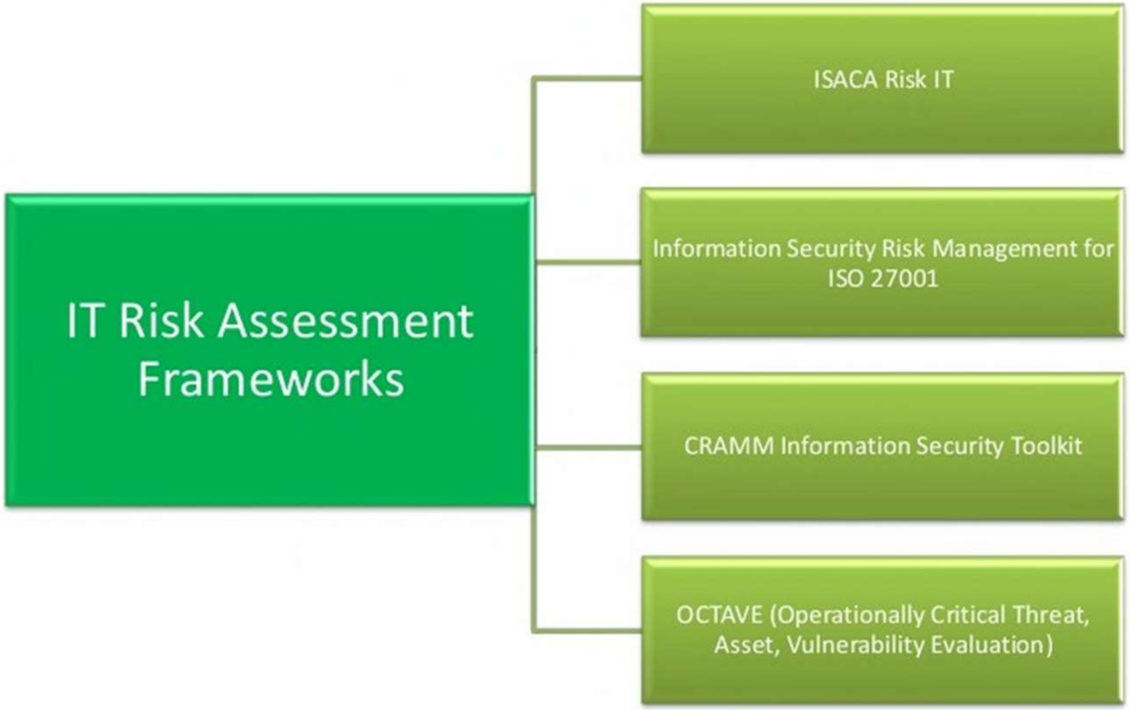
- IT Program/Project delivery

  Related to the management of IT related projects intended to enable or improve business

- IT Operation and Service Delivery

  Day by day IT operations and service delivery that can bring issues, inefficiency to the business operations of an organization

Risk Assessment



IT Risk Assessment Frameworks

- ISACA Risk IT
- Information Security Risk Management for ISO 27001
- CRAMM Information Security Toolkit
- OCTAVE (Operationally Critical Threat, Asset, Vulnerability Evaluation)

IT Risk ASSESSMENT

- Definition of risk assessment

The potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the assets. The impact or relative severity of the risk is proportional to the business value of the loss/damage and to the estimated frequency of the threat.

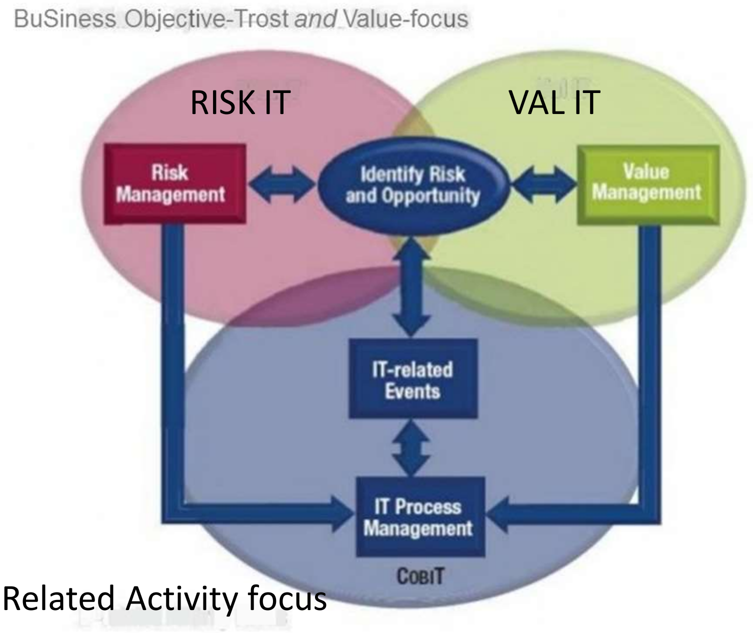
IT Risk ASSESSMENT

Components of risk assessment

- Threats to, and vulnerabilities of, processes and/or assets (including both physical and information assets)
- Impact on assets based on threats and vulnerabilities
- Probabilities of threats (combination of the likelihood and frequency of occurrence)

Risk IT Extends Val IT and COBIT

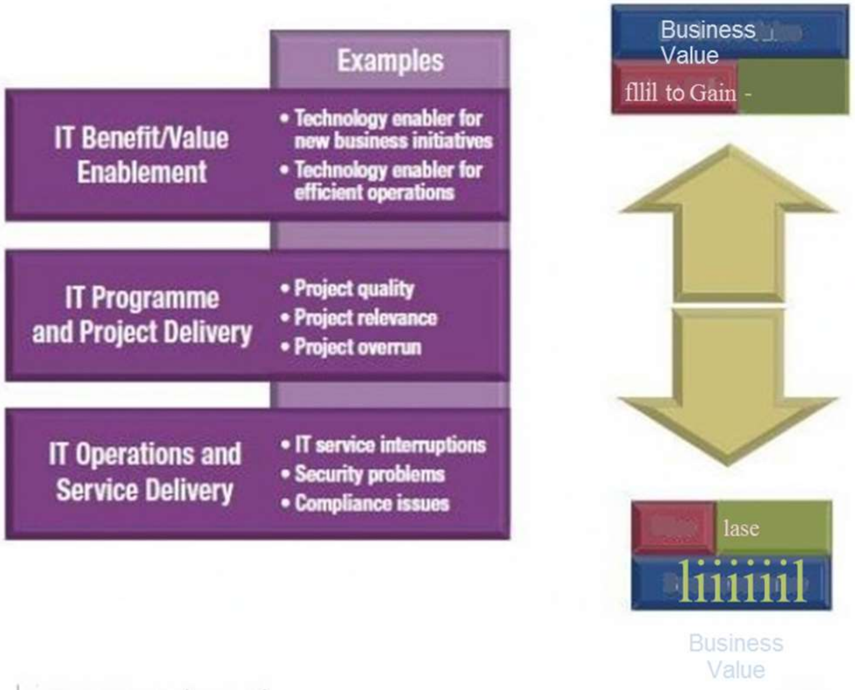
Risk IT complements and extends COBIT and Val IT to make a more *complete* IT governance resource.


BuSiness Objective-Trost *and* Value-focus
RISK IT
VAL IT
Risk Management
Identify Risk and Opportunity
Value Management
IT-related Events
IT Process Management
CobiT
IT Related Activity focus

IT-related Risk Management

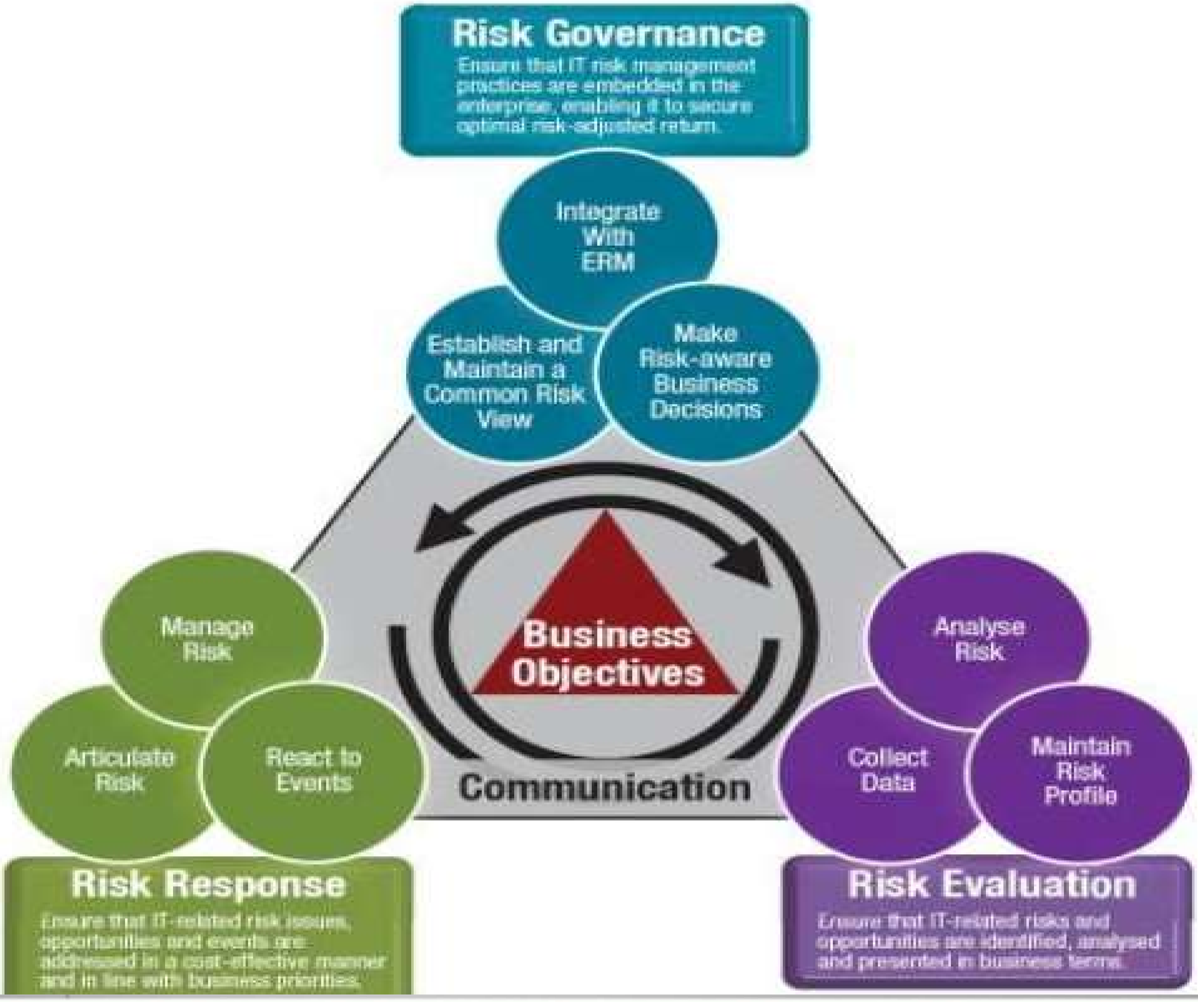
Risk IT is not limited to information security. covers *a//* IT•related risks, including:

- Late project delivery
- Not achieving enough value from IT
- Compliance
- Misalignment
- Obsolete or inflexible IT architecture
- IT service problems



	Examples
IT Benefit/Value Enablement	• Technology enabler for new business initiatives • Technology enabler for efficient operations
IT Programme and Project Delivery	• Project quality • Project relevance • Project overrun
IT Operations and Service Delivery	• IT service interruptions • Security problems • Compliance issues

Risk IT Three Domains



Risk Governance: Ensure that IT risk management practices are embedded in the enterprise, enabling it to secure optimal risk-adjusted return.

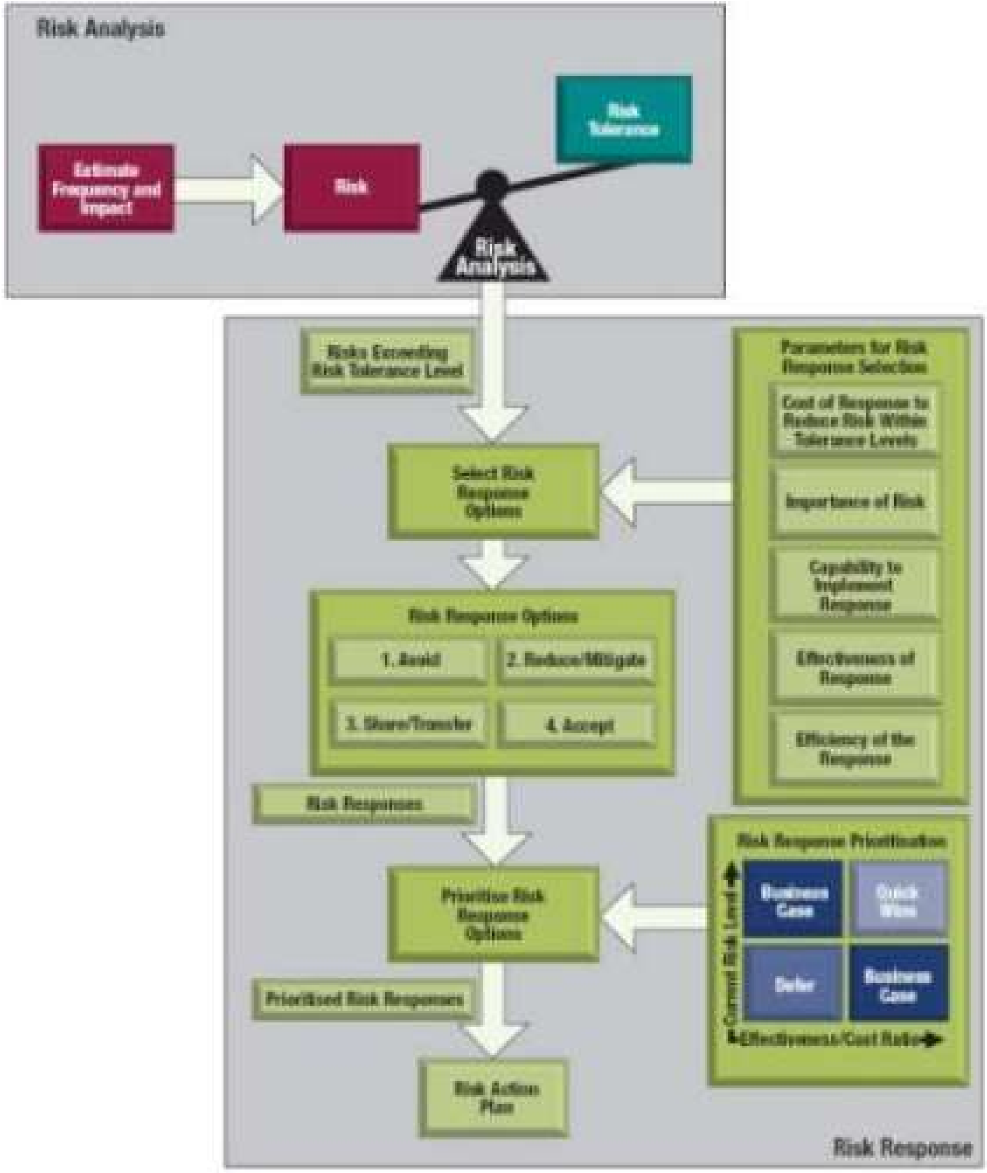
Risk Response: Ensure that IT-related risk issues, opportunities and events are addressed in a cost-effective manner and in line with business priorities.

Risk Evaluation: Ensure that IT-related risks and opportunities are identified, analysed and presented in business terms.

Risk Respons

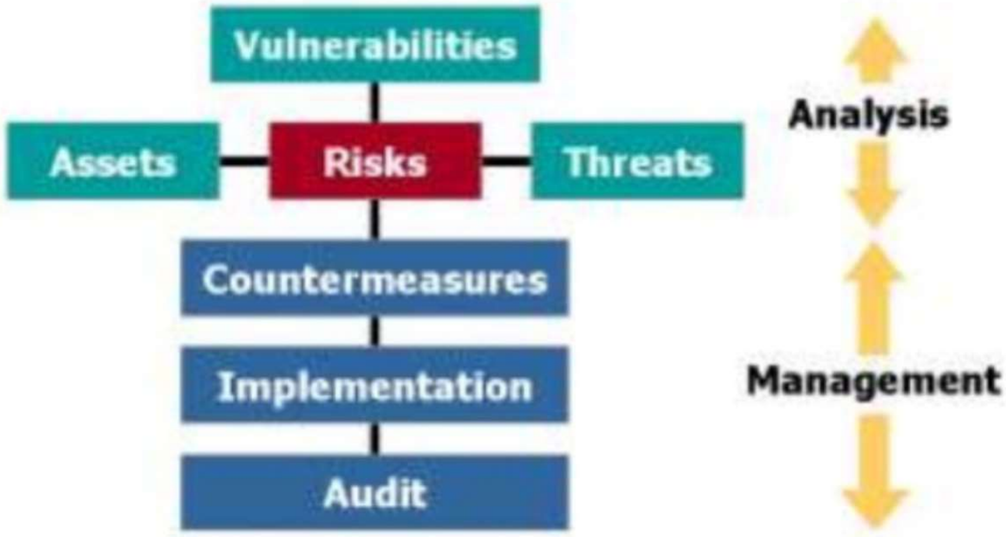
The purpose of defining a risk response is to bring risk in line with the defined risk tolerance for the enterprise after due risk analysis.

In other words, a response needs to be defined such that future residual risk (=current risk with the risk response defined and implemented) is as much as possible (usually depending on budgets available) within risk tolerance limits.


Risk Analysis
Estimate Frequency and Impact
Risk
Risk Tolerance
Risk Analysis
Risks Exceeding Risk Tolerance Level
Select Risk Response Options
Parameters for Risk Response Selection
Cost of Response to Reduce Risk Within Tolerance Levels
Importance of Risk
Capability to Implement Response
Effectiveness of Response
Efficiency of the Response
Risk Response Options
1. Avoid
2. Reduce/Mitigate
3. Share/Transfer
4. Accept
Risk Responses
Prioritise Risk Response Options
Risk Response Prioritisation
Current Risk Level
Business Case
Quick Wins
Defer
Business Case
Effectiveness/Cost Ratio
Prioritised Risk Responses
Risk Action Plan
Risk Response

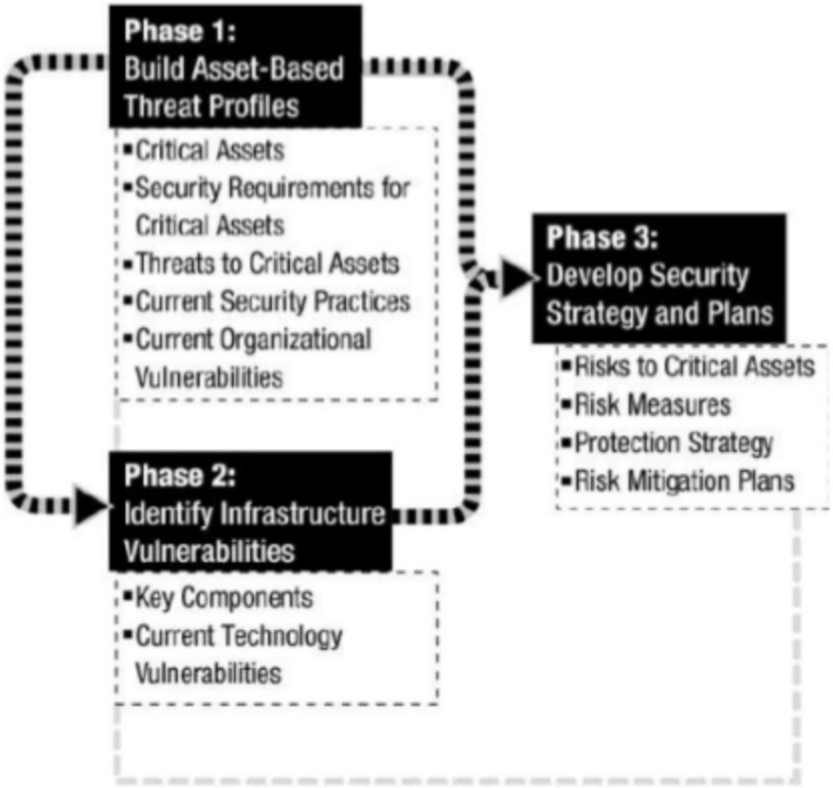
toolkit

- Provides staged and disciplined approach towards IT risk assessment



Source: http://www.cramm.com/overview/howitworks.htm

CERT OCTAVE



Phase 1:
Build Asset-Based Threat Profiles

- Critical Assets
- Security Requirements for Critical Assets
- Threats to Critical Assets
- Current Security Practices
- Current Organizational Vulnerabilities

Phase 2:
Identify Infrastructure Vulnerabilities

- Key Components
- Current Technology Vulnerabilities

Phase 3:
Develop Security Strategy and Plans

- Risks to Critical Assets
- Risk Measures
- Protection Strategy
- Risk Mitigation Plans

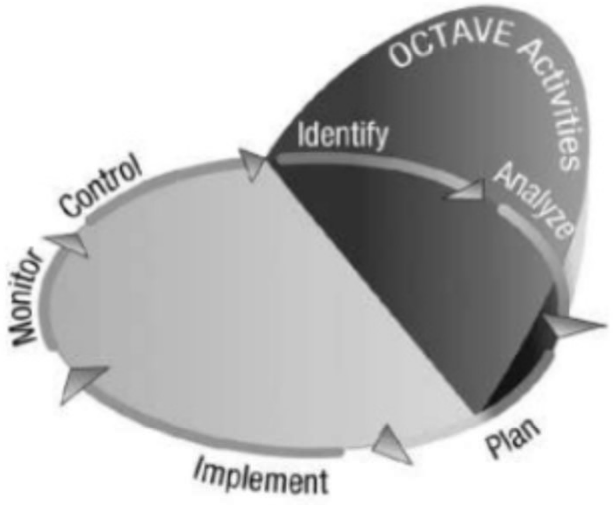


Figure 3: OCTAVE and Risk Management Activities

Thank You