Universitas Esa Unggul

Smart, Creative and Entrepreneurial

Analisis Resiko Sistem Informasi

www.esaunggul.ac.id

Risk Analysis Introduction

Pertemuan 1

Dosen Pengampu: Alivia Yulfitri (2017)

Prodi Sistem Informasi - Fakultas Ilmu Komputer

MATERI SEBELUM UTS

1. Introduction
2. Risk Analysis Definition
3. Risk Analysis: Methodology
4. Risk Analysis: Methodology 2
5. Contoh Risk Analysis
6. Studi kasus: Risk Analysis
7. Studi kasus: Framework

Universitas Esa Unggul

MATERI SETELAH UTS

8. Analisis kuantitatif
9. Analisis kualitatif
10. Studi kasus: analisis resiko menggunakan kualitatif
11. Risk Analysis: Deliverables and Work Plan
12. Studi kasus: deliverable risk analysis
13. Risk Analysis: Tools and Usage
14. Evaluasi dan studi kasus

Universitas Esa Unggul

Reference

- *Information Security Risk Analysis*, by Thomas R. Peltier
  - Identifies basic elements of risk analysis and reviews several variants of qualitative approaches
- "Information Security Risk Assessment: Practices of Leading organizations", By GAO
  - http://www.gao.gov/special.pubs/ai99139.pdf
  - Case studies of risk analysis procedures for four companies
- "Risk Management Guide for Information Technology Systems", NIST
  - http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
  - Outlines steps for risk assessment

Overview

- Definition and Purpose Of Risk Analysis
  - Elements of Risk Analysis
  - Quantitative vs Qualitative Analysis
- Quantitative Example
- Qualitative Example

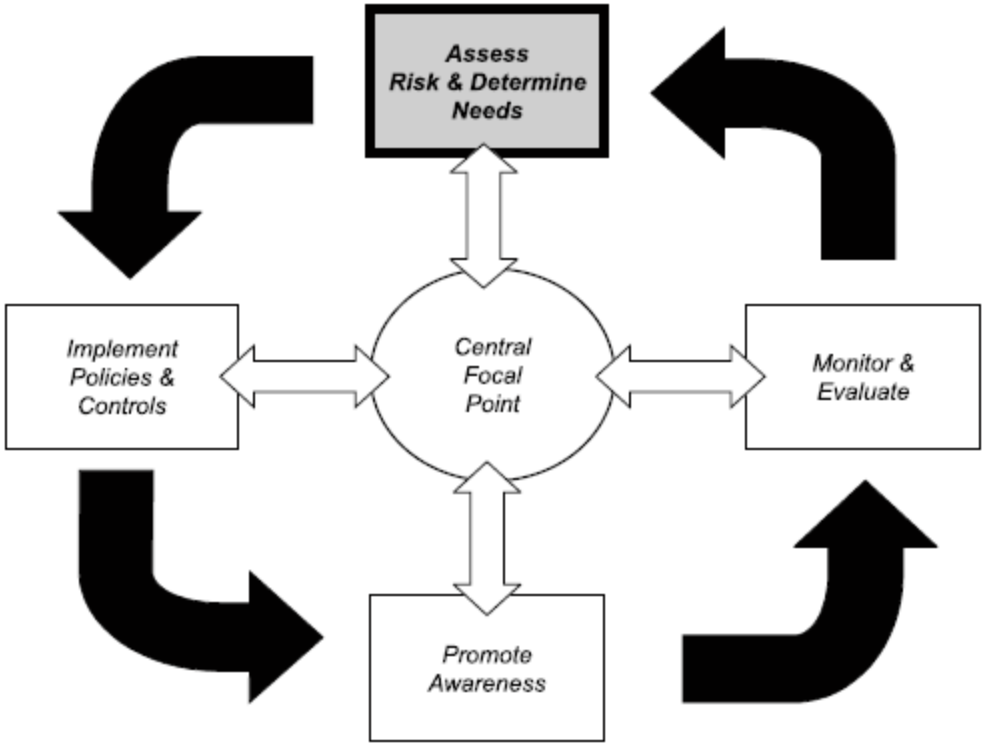
Goal of Risk Analysis

- "If you know the enemy and know yourself, you need not fear the result of a hundred battles."
  - Sun Tzu, Art of War

What is Risk?

- The probability that a particular threat will exploit a particular vulnerability
- Need to systematically understand risks to a system and decide how to control them.

Risk Management Cycle



From GAO/AIMD-99-139

What is Risk Analysis?

- The process of identifying, assessing, and reducing risks to an acceptable level
  - Defines and controls threats and vulnerabilities
  - Implements risk reduction measures
- An analytic discipline with three parts:
  - Risk assessment: determine what the risks are
  - Risk management: evaluating alternatives for mitigating the risk
  - Risk communication: presenting this material in an understandable way to decision makers and/or the public

Benefits of Risk Analysis

- Assurance that greatest risks have been identified and addressed
- Increased understanding of risks
- Mechanism for reaching consensus
- Support for needed controls
- Means for communicating results

Basic Risk Analysis Structure

- Evaluate
  - Value of computing and information assets
  - Vulnerabilities of the system
  - Threats from inside and outside
  - Risk priorities
- Examine
  - Availability of security countermeasures
  - Effectiveness of countermeasures
  - Costs (installation, operation, etc.) of countermeasures
- Implement and Monitor

Who should be Involved?

- Security Experts
- Internal domain experts
  - Knows best how things really work
- Managers responsible for implementing controls

Identify Assets

- Asset – Anything of value
- Physical Assets
  - Buildings, computers
- Logical Assets
  - Intellectual property, reputation

Example Critical Assets

- People and skills
- Goodwill
- Hardware/Software
- Data
- Documentation
- Supplies
- Physical plant
- Money

Threats

- An expression of intention to inflict evil injury or damage
- Attacks against key security services
  - Confidentiality, integrity, availability

Example Threat List

- T01 Access (Unauthorized to System - logical)
- T02 Access (Unauthorized to Area - physical)
- T03 Airborne Particles (Dust)
- T04 Air Conditioning Failure
- T05 Application Program Change (Unauthorized)
- T06 Bomb Threat
- T07 Chemical Spill
- T08 Civil Disturbance
- T09 Communications Failure
- T10 Data Alteration (Error)
- T11 Data Alteration (Deliberate)
- T12 Data Destruction (Error)
- T13 Data Destruction (Deliberate)
- T14 Data Disclosure (Unauthorized)
- T15 Disgruntled Employee
- T16 Earthquakes
- T17 Errors (All Types)
- T18 Electro-Magnetic Interference
- T19 Emanations Detection
- T20 Explosion (Internal)
- T21 Fire, Catastrophic
- T22 Fire, Major
- T23 Fire, Minor
- T24 Floods/Water Damage
- T25 Fraud/Embezzlement
- T26 Hardware Failure/Malfunction
- T27 Hurricanes
- T28 Injury/Illness (Personal)
- T29 Lightning Storm
- T30 Liquid Leaking (Any)
- T31 Loss of Data/Software
- T32 Marking of Data/Media Improperly
- T33 Misuse of Computer/Resource
- T34 Nuclear Mishap
- T35 Operating System Penetration/Alteration
- T36 Operator Error
- T37 Power Fluctuation (Brown/Transients)
- T38 Power Loss
- T39 Programming Error/Bug
- T40 Sabotage
- T41 Static Electricity
- T42 Storms (Snow/Ice/Wind)
- T43 System Software Alteration
- T44 Terrorist Actions
- T45 Theft (Data/Hardware/Software)
- T46 Tornado
- T47 Tsunami (Pacific area only)
- T48 Vandalism
- T49 Virus/Worm (Computer)
- T50 Volcanic Eruption

Vulnerabilities

- Flaw or weakness in system that can be exploited to violate system integrity.
  - Security Procedures
  - Design
  - Implementation
- Threats trigger vulnerabilities
  - Accidental
  - Malicious

Example Vulnerabilities

- *Physical*
- *V01 Susceptible to unauthorized building access*
- *V02 Computer Room susceptible to unauthorized access*
- *V03 Media Library susceptible to unauthorized access*
- *V04 Inadequate visitor control procedures*
- *(and 36 more)*
- *Administrative*
- *V41 Lack of management support for security*
- *V42 No separation of duties policy*
- *V43 Inadequate/no computer security plan policy*
- *V47 Inadequate/no emergency action plan*
- *(and 7 more)*
- *Personnel*
- *V56 Inadequate personnel screening*
- *V57 Personnel not adequately trained in job*
- *…*
- *Software*
- *V62 Inadequate/missing audit trail capability*
- *V63 Audit trail log not reviewed weekly*
- *V64 Inadequate control over application/program changes*
- *Communications*
- *V87 Inadequate communications system*
- *V88 Lack of encryption*
- *V89 Potential for disruptions*
- *…*
- *Hardware*
- *V92 Lack of hardware inventory*
- *V93 Inadequate monitoring of maintenance personnel*
- *V94 No preventive maintenance program*
- *…*
- *V100 Susceptible to electronic emanations*

Controls/Countermeasures

- Mechanisms or procedures for mitigating vulnerabilities
  - Prevent
  - Detect
  - Recover
- Understand cost and coverage of control
- Controls follow vulnerability and threat analysis

Example Controls

- C01 Access control devices - physical
- C02 Access control lists - physical
- C03 Access control - software
- C04 Assign ADP security and assistant in writing
- C05 Install-/review audit trails
- C06 Conduct risk analysis
- C07Develop backup plan
- C08 Develop emergency action plan
- C09 Develop disaster recovery plan
- ...
- C21 Install walls from true floor to true ceiling
- C22 Develop visitor sip-in/escort procedures
- C23 Investigate backgrounds of new employees
- C24 Restrict numbers of privileged users
- C25 Develop separation of duties policy
- C26 Require use of unique passwords for logon
- C27 Make password changes mandatory
- C28 Encrypt password file
- C29 Encrypt data/files
- C30 Hardware/software training for personnel
- C31Prohibit outside software on system
- ...
- C47 Develop software life cycle development program
- C48 Conduct hardware/software inventory
- C49 Designate critical programs/files
- C50 Lock PCs/terminals to desks
- C51 Update communications system/hardware
- C52 Monitor maintenance personnel
- C53 Shield equipment from electromagnetic interference/emanations
- C54Identify terminals

Risk/Control Trade Offs

- Only Safe Asset is a Dead Asset
  - Asset that is completely locked away is safe, but useless
  - Trade-off between safety and availablity
- Do not waste effort on efforts with low loss value
  - Don’t spend resources to protect garbage
- Control only has to be good enough, not absolute
  - Make it tough enough to discourage enemy

DISKUSI

- Common Questions
  - What are the assets?
  - What are the vulnerabilities?
  - What are the threat-sources?
  - What are possible controls?