# Manajemen Resiko Teknologi Informasi dan Sistem Informasi

LPMP KALIMANTAN SELATAN

kubuntu

# Daftar Isi

- Latar belakang
- Tujuan dan Kegunaan
- Metodologi Risk Management
- Summary

# Pendahuluan

- Setiap Organisasi memiliki tujuan, dalam era digital ini otomasi sistem informasi dan teknologi informasi digunakan sebagai dukungan untuk mencapai tujuan tersebut.
- Manajemen resiko memegang peranan penting sebagai tindakan perlindungan bagi aset informasi dan seluruh hal yang berkaitan dengan Teknologi informasi

# Tujuan dan Kegunaan

- Resiko Merupakan Dampak negatif yang diakibatkan oleh kelemahan (vulnerability).
- Manajemen resiko merupakan proses identifikasi resiko, mengkaji resiko, dan membuat tindakan untuk mengurangi resiko pada batasan yang dapat diterima.

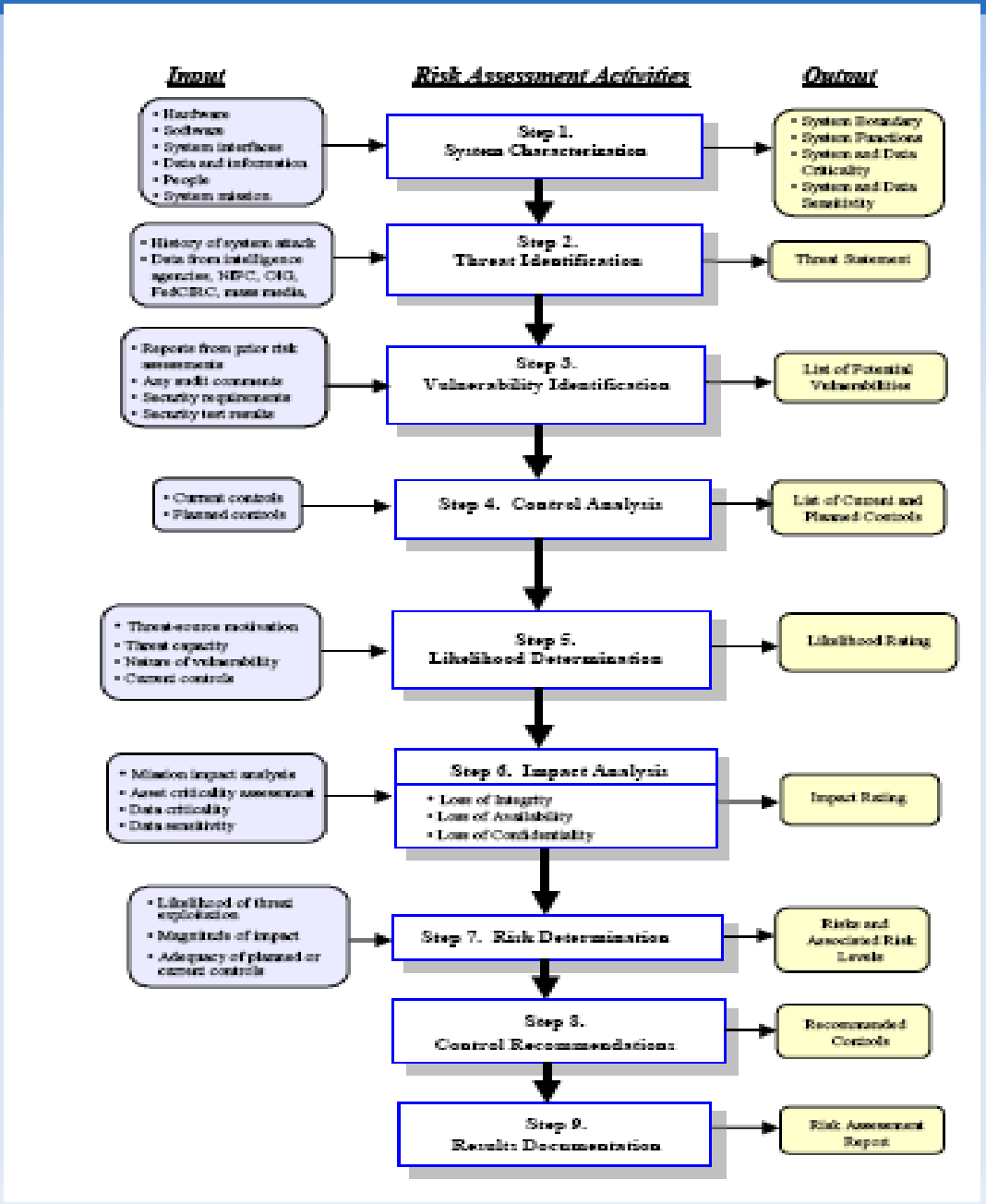
# Tujuan dan Kegunaan

- Kegunaan yang diharapkan adalah :
  - Pengamanan yang baik bagi IT/IS yang berfungsi sebagai penyiman, pengolah, dan penyebar informasi bagi organisasi.
  -

# Risk Asessment

- Risk Asessment merupakan tahapan pertama pada metodologi manajemen resiko.
- Beberapa tahapan penting dalam Risk Asessment :
  - System Characterization
  - Threat Identification
  - Vulnerability Identification
  - Control Analysis
  - Likelihood determination
  - Impact Analysis.
  - Risk Determination
  - Control recommendations
  - Result Documentation.

# Risk Assessment



# Risk Asessment

- System Characterization
  - Melakukan identifikasi batasan sistem yang ada, sehingga dapat dengan jelas melihat batasan fungsionalitas.
- Batasan tersebut didapatkan dengan cara :
  - Mengumpulkan informasi mengenai sistem yang berkaitan seperti
    - Hardware
    - Software
    - System interface ( internal and external connectivity)

# Risk Assesment

- Data and Information
- Person who support and use the IT system.
- System mission
- System and data critically.
- System and data sensitivity.

# Risk Asessment

- Functional Requirements Of IT systems
- Users Of The system
- System security policies governing the IT system.
- System security Architecture
- Current Network Topology
- Information Storage Protection that safeguards system and data availability, integrity, confidentiality.
- Flow of Information
- Technical Control used for the IT system.
- Management Control used for the IT system

# Risk Asessment

- Operational control used for the IT system
- Physical security environment of the IT system
- Environmental security implemented for the IT system processing environment (e.g.,controls for humidity, water, power, pollution, temperature, and chemicals).

# Risk Asessment

- Threat Identification
  - Threat merupakan potensi yang ditimbulkan akibat adanya kelemahan (vulnerability)
  - Vulnerability merupakan kerawanan/kelemahan yang dapat di eksploitasi sehingga menjadi threat.
- Threat Source identification:
  - Natural Threats.
  - Human Threats
  - Evironmental Threats

# Risk Asessment

- Human threats,motivation and action

| Threat-Source | Motivation | Threat Actions |
|---|---|---|
| Hacker, cracker | Challenge<br>Ego<br>Rebellion | • Hacking<br>• Social engineering<br>• System intrusion, break-ins<br>• Unauthorized system access |
| Computer criminal | Destruction of information<br>Illegal information disclosure<br>Monetary gain<br>Unauthorized data alteration | • Computer crime (e.g., cyber stalking)<br>• Fraudulent act (e.g., replay, impersonation, interception)<br>• Information bribery<br>• Spoofing<br>• System intrusion |

# Risk Asessments

| | | |
|---|---|---|
| Terrorist | Blackmail<br>Destruction<br>Exploitation<br>Revenge | • Bomb/Terrorism<br>• Information warfare<br>• System attack (e.g., distributed denial of service)<br>• System penetration<br>• System tampering |
| Industrial espionage (companies, foreign governments, other government interests) | Competitive advantage<br>Economic espionage | • Economic exploitation<br>• Information theft<br>• Intrusion on personal privacy<br>• Social engineering<br>• System penetration<br>• Unauthorized system access (access to classified, proprietary, and/or technology-related information) |

# Risk Asessments

| | | |
|---|---|---|
| Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees) | Curiosity<br>Ego<br>Intelligence<br>Monetary gain<br>Revenge<br>Unintentional errors and omissions (e.g., data entry error, programming error) | • Assault on an employee<br>• Blackmail<br>• Browsing of proprietary information<br>• Computer abuse<br>• Fraud and theft<br>• Information bribery<br>• Input of falsified, corrupted data<br>• Interception<br>• Malicious code (e.g., virus, logic bomb, Trojan horse)<br>• Sale of personal information<br>• System bugs<br>• System intrusion<br>• System sabotage<br>• Unauthorized system access |

# Risk Asessments

- Vulnerability identification
  - Vulnerability merupakan kelemahan sistem yang mengakibatkan terjadinya pelanggaran keamanan.

| Vulnerability | Threat-Source | Threat Action |
|---|---|---|
| Terminated employees' system identifiers (ID) are not removed from the system | Terminated employees | Dialing into the company's network and accessing company proprietary data |
| Company firewall allows inbound telnet, and *guest* ID is enabled on XYZ server | Unauthorized users (e.g., hackers, terminated employees, computer criminals, terrorists) | Using telnet to XYZ server and browsing system files with the *guest* ID |

# Risk Asessments

- Vulnerability identification

| | | |
|---|---|---|
| The vendor has identified flaws in the security design of the system; however, new patches have not been applied to the system | Unauthorized users (e.g., hackers, disgruntled employees, computer criminals, terrorists) | Obtaining unauthorized access to sensitive system files based on known system vulnerabilities |

# Risk Asessments

- Vulnerability identification

| Vulnerability | Threat-Source | Threat Action |
|---|---|---|
| Data center uses water sprinklers to suppress fire; tarpaulins to protect hardware and equipment from water damage are not in place | Fire, negligent persons | Water sprinklers being turned on in the data center |

# Risk Asessments

- Vulnerability resource
  - Dokumen risk asessment yang pernah ada.
  - Vulnerability list
  - Temuan kelemahan keamanan sistem pada dokumen audit.
  - Vendor advisories

# Risk Asessments

- Development of security requirements checklist.
  - Management
  - Operational
  - Technical

- Security Criteria

| Security Area | Security Criteria |
|---|---|
| **Management Security** | • Assignment of responsibilities<br>• Continuity of support<br>• Incident response capability<br>• Periodic review of security controls<br>• Personnel clearance and background investigations<br>• Risk assessment<br>• Security and technical training<br>• Separation of duties<br>• System authorization and reauthorization<br>• System or application security plan |

- Security Criteria

| | |
|---|---|
| **Operational Security** | • Control of air-borne contaminants (smoke, dust, chemicals)<br>• Controls to ensure the quality of the electrical power supply<br>• Data media access and disposal<br>• External data distribution and labeling<br>• Facility protection (e.g., computer room, data center, office)<br>• Humidity control<br>• Temperature control<br>• Workstations, laptops, and stand-alone personal computers |

- Security Criteria

| | |
|---|---|
| **Technical Security** | • Communications (e.g., dial-in, system interconnection, routers)<br>• Cryptography<br>• Discretionary access control<br>• Identification and authentication<br>• Intrusion detection<br>• Object reuse<br>• System audit |

# Risk Asessment

- Control Analysis : merupakan proses analisa dengan melihat control apa saja yang sudah ada, untuk meminimalisir kelemahan yang ada.
- Control Analysis Technique : dengan melihat kebutuhan sistem secara menyeluruh (management, operational and technical security)

# Risk Asessments

- Likelihood determination

| Likelihood Level | Likelihood Definition |
|---|---|
| High | The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective. |
| Medium | The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability. |
| Low | The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised. |

# Risk Asessments

- Impact Analysis : merupakan tahapan penetuan prioritas dari dampak kelemahan pada sistem berdasarkan pada sensitifitas dan kritikalitas sistem.
  - System mission (e.g., the processes performed by the IT system)
  - System and data criticality (e.g., the system's value or importance to an organization)
  - System and data sensitivity.

# Risk Asessments

- Tiga Sasaran Keamanan :
  - Loss of Integrity, *improper modification*
  - Loss of Availability, *If a mission-critical IT system is unavailable to its end users, the organization's mission may be affected*
  - Loss of Confidentiality, *System and data confidentiality refers to the protection of information from unauthorized disclosure.*

# Risk Asessments

- Risk Level

| Risk Level | Risk Description and Necessary Actions |
|---|---|
| **High** | If an observation or finding is evaluated as a high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible. |
| **Medium** | If an observation is rated as medium risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time. |
| **Low** | If an observation is described as low risk, the system's DAA must determine whether corrective actions are still required or decide to accept the risk. |

# Risk Asessments

- Control recommendation
  - Effectiveness of recommended options (e.g., system compatibility)
  - Legislation and regulation
  - Organizational policy
  - Operational impact
  - Safety and reliability.

# Risk Asessment

- Risk Mitigation : *prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment Process.*
  - **Risk Assumption.** *To accept the potential risk and continue operating the IT system or to implement controls to lower the risk to an acceptable level*
  - ***Risk Avoidance.*** *To avoid the risk by eliminating the risk cause and/or consequence (e.g., forgo certain functions of the system or shut down the system when risks are identified)*
  - ***Risk Limitation.*** *To limit the risk by implementing controls that minimize the adverse impact of a threat's exercising a vulnerability (e.g., use of supporting, preventive, detective controls)*
  - ***Risk Planning.*** *To manage risk by developing a risk mitigation plan that prioritizes, implements, and maintains controls*

# Risk Asessments

- **Research and Acknowledgment.** *To lower the risk of loss by acknowledging the vulnerability or flaw and researching controls to correct the vulnerability*
- **Risk Transference.** *To transfer the risk by using other options to compensate for the loss, such as purchasing insurance.*

# Risk Asessments

- Technical Security Control
  - **Support**
  - **Prevent**
  - **Detect and Recover**

# Risk Asessments

- ***Supporting Technical Controls***
  - ***Identification.***
  - ***Cryptographic Key Management.***
  - ***Security Administration.***
  - ***System Protections.***
- ***Preventive Technical Controls***
  - ***Authentication***
  - ***Authorization.***
  - ***Access Control Enforcement.***
  - ***Nonrepudiation.***

# Risk Asessments

- **Protected Communications**
- **Transaction Privacy**

- **Detection and recovery**
  - **Audit.**
  - **Intrusion Detection and Containment**
  - **Proof of Wholeness.**
  - **Restore Secure State.**
  - **Virus Detection and Eradication**

# Risk Asessments

- **Management Security Controls**
  - **Preventive Management Security Controls**
    - **Assign security responsibility to ensure that adequate security is provided for the mission-critical IT systems**
    - **Develop and maintain system security plans to document current controls and address planned controls for IT systems in support of the organization's mission**
    - **Implement personnel security controls, including separation of duties, least privilege, and user computer access registration and termination**
    - **Conduct security awareness and technical training to ensure that end users and system users are aware of the rules of behavior and their responsibilities in protecting the organization's mission.**

# Risk Asessments

- ***Detection Management Security Controls***
  - ***Implement personnel security controls, including personnel clearance, background investigations, rotation of duties***
  - ***Conduct periodic review of security controls to ensure that the controls are effective***
  - ***Perform periodic system audits***
  - ***Conduct ongoing risk management to assess and mitigate risk***
  - ***Authorize IT systems to address and accept residual risk.***

# Risk Asessments

- Operational Security Control
  - ***Preventive Operational Controls***
    - ***Control data media access and disposal (e.g., physical access control, degaussing method)***
    - ***Control software viruses***
    - ***Safeguard computing facility (e.g., security guards, site procedures for visitors, electronic badge system, biometrics access control, management and distribution of locks and keys, barriers and fences)***
    - ***Secure wiring closets that house hubs and cables***
    - ***Provide backup capability (e.g., procedures for regular data and system backups, archive logs that save all database changes to be used in various recovery scenarios)***

# Risk Asessments

- Protect laptops, personal computers (PC), workstations
- Protect IT assets from fire damage (e.g., requirements and procedures for the use of fire extinguishers, tarpaulins, dry sprinkler systems, halon fire suppression system)
- Provide emergency power source (e.g., requirements for uninterruptible power supplies, on-site power generators)
- Control the humidity and temperature of the computing facility (e.g., operation of air conditioners, heat dispersal).

# Summary

- Please Suumarize your ideas.
- Feels free to contact me at yudho_s@yahoo.com