UNIVERSITAS MULIA

M. Zulfariansyah, S.Kom., M.TI

Managing Information Security Risk

Session 3

Contents

UNIVERSITAS MULIA

Importance of Risk Management

Manajemen risiko adalah proses yang memungkinkan manajer TI menyeimbangkan biaya operasional dan ekonomi dari tindakan perlindungan dan mencapai keuntungan dalam keberhasilan tujuan dengan melindungi sistem dan data TI yang mendukung misi organisasi mereka.

Proses ini tidak unik untuk lingkungan TI; memang itu meliputi pengambilan keputusan di semua bidang kehidupan kita sehari-hari.

Ambil contoh keamanan rumah, misalnya. Banyak orang memutuskan untuk memasang sistem keamanan rumah dan membayar biaya bulanan ke penyedia layanan agar sistem ini dipantau untuk perlindungan properti mereka yang lebih baik.

UNIVERSITAS MULIA

Integration Of Risk Management Into SDLC

Manajemen risiko yang efektif harus sepenuhnya diintegrasikan ke dalam SDLC. SDLC sistem TI memiliki lima fase:

1. - inisiasi,
2. - pengembangan atau akuisisi,
3. - implementasi,
4. - operasi atau pemeliharaan, dan
5. - penyelesaian

Metodologi manajemen risiko adalah sama dengan fase SDLC dimana penilaian risiko selalu dilakukan meskipun pada tahap yang sedang dikerjaan.

Manajemen risiko adalah proses berulang yang dapat dilakukan selama setiap fase utama SDLC.

UNIVERSITAS MULIA

Table 2-1 Integration of Risk Management into the SDLC

SDLC Phases	Phase Characteristics	Support from Risk Management Activities
Phase 1—Initiation	The need for an IT system is expressed and the purpose and scope of the IT system is documented	• Identified risks are used to support the development of the system requirements, including security requirements, and a security concept of operations (strategy)
Phase 2—Development or Acquisition	The IT system is designed, purchased, programmed, developed, or otherwise constructed	• The risks identified during this phase can be used to support the security analyses of the IT system that may lead to architecture and design trade-offs during system development
Phase 3—Implementation	The system security features should be configured, enabled, tested, and verified	• The risk management process supports the assessment of the system implementation against its requirements and within its modeled operational environment. Decisions regarding risks identified must be made prior to system operation
Phase 4—Operation or Maintenance	The system performs its functions. Typically the system is being modified on an ongoing basis through the addition of hardware and software and by changes to organizational processes, policies, and procedures	• Risk management activities are performed for periodic system reauthorization (or reaccreditation) or whenever major changes are made to an IT system in its operational, production environment (e.g., new system interfaces)
Phase 5—Disposal	This phase may involve the disposition of information, hardware, and software. Activities may include moving, archiving, discarding, or destroying information and sanitizing the hardware and software	• Risk management activities are performed for system components that will be disposed of or replaced to ensure that the hardware and software are properly disposed of, that residual data is appropriately handled, and that system migration is conducted in a secure and systematic manner

UNIVERSITAS MULIA

Key Roles

- **Manajemen senior.** Manajemen senior, di bawah standar kepedulian yang pantas dan tanggung jawab utama untuk pencapaian misi, harus memastikan bahwa sumber daya yang diperlukan diterapkan secara efektif untuk mengembangkan kemampuan yang diperlukan untuk menyelesaikan misi. Mereka juga harus menilai dan memasukkan hasil kegiatan penilaian risiko ke dalam proses pengambilan keputusan. Program manajemen risiko yang efektif yang menilai dan memitigasi risiko misi terkait TI memerlukan dukungan dan keterlibatan manajemen senior.

- **Chief Information Officer (CIO).** CIO bertanggung jawab atas perencanaan, penganggaran, dan kinerja TI agensi termasuk komponen keamanan informasinya. Keputusan yang dibuat dalam bidang-bidang ini harus didasarkan pada program manajemen risiko yang efektif.

- **Pemilik Sistem dan Informasi**. Pemilik sistem dan informasi bertanggung jawab untuk memastikan bahwa terdapat kontrol yang tepat untuk mengatasi integritas, kerahasiaan, dan ketersediaan sistem dan data TI yang mereka miliki. Biasanya pemilik sistem dan informasi bertanggung jawab atas perubahan pada sistem TI mereka. Karenanya, mereka biasanya harus menyetujui dan menandatangani perubahan pada sistem TI mereka (mis., Peningkatan sistem, perubahan besar pada perangkat lunak dan perangkat keras). Pemilik sistem dan informasi karenanya harus memahami peran mereka dalam proses manajemen risiko dan sepenuhnya mendukung proses ini.

Key Roles

- **Manajer Bisnis dan Fungsional.** Manajer yang bertanggung jawab untuk operasi bisnis dan proses pengadaan TI harus mengambil peran aktif dalam proses manajemen risiko. Para manajer ini adalah individu dengan wewenang dan tanggung jawab untuk membuat keputusan trade-off yang penting untuk pencapaian misi. Keterlibatan mereka dalam proses manajemen risiko memungkinkan pencapaian keamanan yang tepat untuk sistem TI, yang, jika dikelola dengan benar, akan memberikan efektivitas misi dengan pengeluaran sumber daya yang minimal.

- **ISSO.** Manajer program keamanan TI dan petugas keamanan komputer bertanggung jawab atas program keamanan organisasi mereka, termasuk manajemen risiko. Oleh karena itu, mereka memainkan peran utama dalam memperkenalkan metodologi yang tepat dan terstruktur untuk membantu mengidentifikasi, mengevaluasi, dan meminimalkan risiko pada sistem TI yang mendukung misi organisasi mereka. ISSO juga bertindak sebagai konsultan utama dalam mendukung manajemen senior untuk memastikan bahwa kegiatan ini berlangsung secara berkelanjutan.

- **Praktisi Keamanan TI.** Praktisi keamanan TI (mis. Administrator jaringan, sistem, aplikasi, dan basis data; spesialis komputer; analis keamanan; konsultan keamanan) bertanggung jawab atas penerapan persyaratan keamanan yang tepat dalam sistem TI mereka. Ketika perubahan terjadi di lingkungan sistem TI yang ada (misalnya, perluasan konektivitas jaringan, perubahan infrastruktur dan kebijakan organisasi yang ada, pengenalan teknologi baru), praktisi keamanan TI harus mendukung atau menggunakan proses manajemen risiko untuk mengidentifikasi dan menilai potensi baru risiko dan menerapkan kontrol keamanan baru yang diperlukan untuk melindungi sistem TI mereka.

Risk Assessment

Risiko adalah fungsi dari kemungkinan sumber-ancaman tertentu menjalankan potensi kerentanan tertentu, dan dampak yang dihasilkan dari peristiwa buruk itu pada organisasi.

- *Langkah 1 Karakterisasi Sistem (Bagian 3.1)*
- *Langkah 2 Identifikasi Ancaman (Bagian 3.2)*
- *Langkah 3 Identifikasi Kerentanan (Bagian 3.3)*
- *Langkah 4 Analisis Kontrol (Bagian 3.4)*
- *Langkah 5 Penentuan Kemungkinan (Bagian 3.5)*
- *Langkah 6 Analisis Dampak (Bagian 3.6)*
- *Langkah 7 Penentuan Risiko (Bagian 3.7)*
- *Langkah 8 Rekomendasi Kontrol (Bagian 3.8)*
- *Langkah 9 Dokumentasi Hasil (Bagian 3.9).*

UNIVERSITAS MULIA

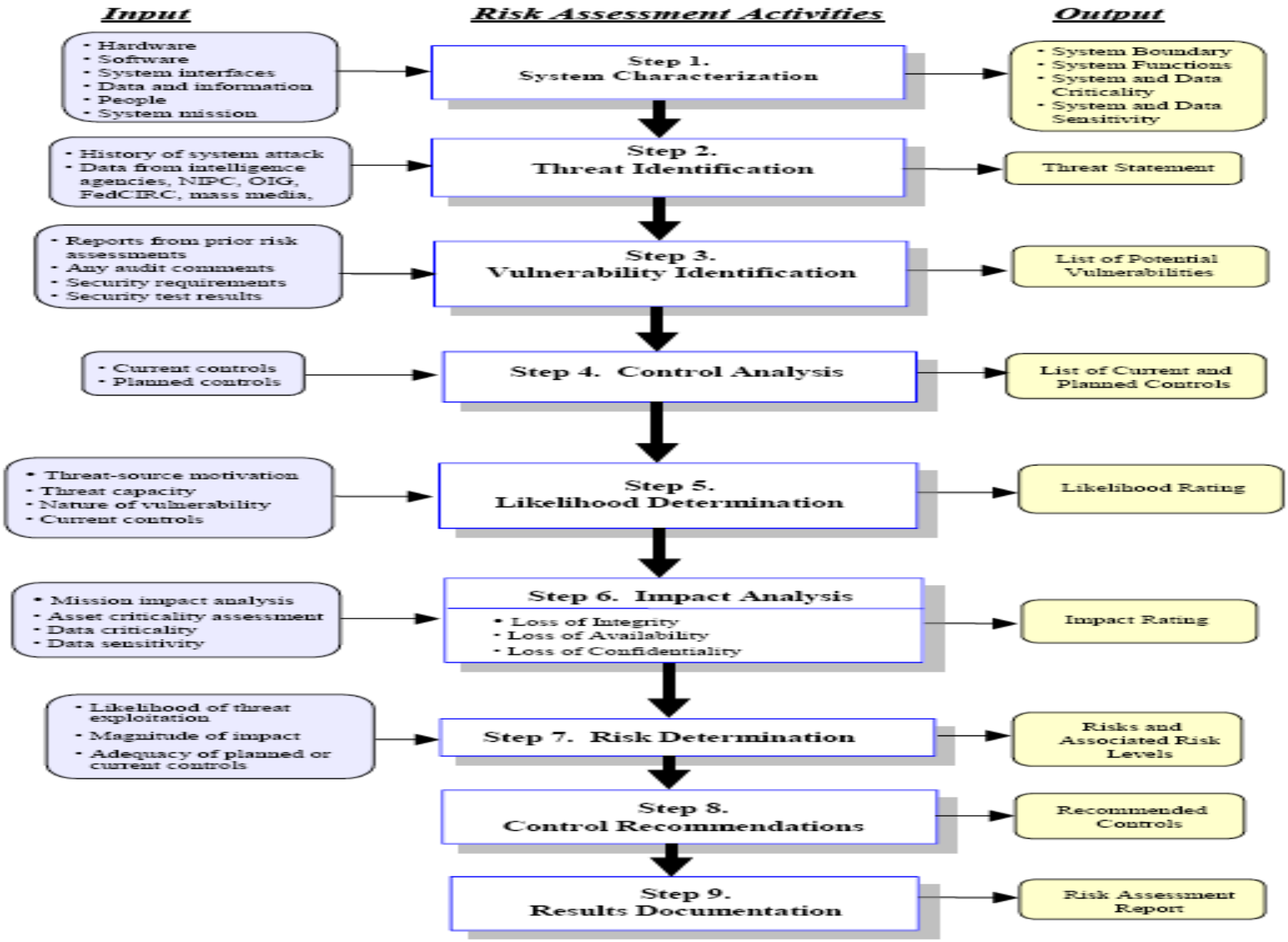

Figure 3-1. Risk Assessment Methodology Flowchart

System Characterization

System-Related Information

- Hardware
- Software
- System interfaces (e.g., internal and external connectivity)
- Data and information
- Persons who support and use the IT system
- 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

UNIVERSITAS MULIA

Information-Gathering Techniques

Questionnaire

On-site Interviews.

Document Review.

Use of Automated Scanning Tool.

Output from Step 1 Characterization of the IT system assessed, is a good picture of the IT system environment, and delineation of system boundary

UNIVERSITAS MULIA

Threat Identification

Identifikasi Sumber Ancaman:

Tujuan langkah ini adalah untuk mengidentifikasi sumber ancaman potensial dan menyusun pernyataan ancaman yang berisi daftar sumber ancaman potensial yang berlaku untuk sistem TI yang sedang dievaluasi.

Motivasi dan sumber daya untuk melakukan serangan membuat manusia berpotensi menjadi sumber ancaman yang berbahaya.

Informasi ini akan berguna bagi organisasi yang mempelajari lingkungan ancaman manusia mereka dan menyesuaikan pernyataan ancaman manusia mereka.

UNIVERSITAS MULIA

Table 3-1. Human Threats: Threat-Source, Motivation, and Threat Actions

Threat-Source	Motivation	Threat Actions
Hacker, cracker	Challenge Ego Rebellion	• Hacking • Social engineering • System intrusion, break-ins • Unauthorized system access
Computer criminal	Destruction of information Illegal information disclosure Monetary gain Unauthorized data alteration	• Computer crime (e.g., cyber stalking) • Fraudulent act (e.g., replay, impersonation, interception) • Information bribery • Spoofing • System intrusion
Terrorist	Blackmail Destruction Exploitation Revenge	• Bomb/Terrorism • Information warfare • System attack (e.g., distributed denial of service) • System penetration • System tampering
Industrial espionage (companies, foreign governments, other government interests)	Competitive advantage Economic espionage	• Economic exploitation • Information theft • Intrusion on personal privacy • Social engineering • System penetration • Unauthorized system access (access to classified, proprietary, and/or technology-related information)
Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees)	Curiosity Ego Intelligence Monetary gain Revenge Unintentional errors and omissions (e.g., data entry error, programming error)	• Assault on an employee • Blackmail • Browsing of proprietary information • Computer abuse • Fraud and theft • Information bribery • Input of falsified, corrupted data • Interception • Malicious code (e.g., virus, logic bomb, Trojan horse) • Sale of personal information • System bugs • System intrusion • System sabotage • Unauthorized system access

Vulnerability Identification

Kerentanan:

Kelemahan atau kelemahan dalam prosedur, desain, implementasi, atau kontrol internal sistem keamanan yang dapat dilakukan (secara tidak sengaja dipicu atau dieksploitasi secara sengaja) dan mengakibatkan pelanggaran keamanan atau pelanggaran kebijakan keamanan sistem.

Output dari Langkah 3 :

Daftar kerentanan sistem (pengamatan) yang dapat dilakukan oleh sumber ancaman potensial

UNIVERSITAS MULIA

Control Analysis

Tujuan dari langkah ini adalah untuk menganalisis kontrol yang telah dilaksanakan, atau yang direncanakan untuk implementasi, oleh organisasi untuk meminimalkan atau menghilangkan kemungkinan (atau kemungkinan) ancaman yang menggunakan kerentanan sistem.

Keluaran dari Langkah 4: Daftar kontrol saat ini atau yang direncanakan digunakan untuk sistem TI untuk mengurangi kemungkinan kerentanan sedang dilakukan dan mengurangi dampak dari peristiwa yang merugikan tersebut.

UNIVERSITAS MULIA

Likelihood Determination

Table 3-4. Likelihood Definitions

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.

Output from Step 5 Likelihood rating (High, Medium, Low)

UNIVERSITAS MULIA

Impact Analysis

Tujuan dari langkah ini adalah untuk menganalisis kontrol yang telah dilaksanakan, atau yang direncanakan untuk implementasi, oleh organisasi untuk meminimalkan atau menghilangkan kemungkinan (atau kemungkinan) ancaman yang menggunakan kerentanan sistem.

Keluaran dari Langkah 4: Daftar kontrol saat ini atau yang direncanakan digunakan untuk sistem TI untuk mengurangi kemungkinan kerentanan sedang dilakukan dan mengurangi dampak dari peristiwa yang merugikan tersebut....

UNIVERSITAS MULIA

Impact Analysis

- **Kehilangan Integritas**. Integritas sistem dan data mengacu pada persyaratan bahwa informasi harus dilindungi dari modifikasi yang tidak tepat. Integritas hilang jika perubahan tidak sah dilakukan pada data atau sistem TI baik dengan tindakan disengaja atau tidak disengaja. Jika hilangnya integritas sistem atau data tidak diperbaiki, penggunaan berkelanjutan dari sistem yang terkontaminasi atau data yang rusak dapat mengakibatkan ketidakakuratan, penipuan, atau keputusan yang salah. Juga, pelanggaran integritas mungkin merupakan langkah pertama dalam serangan yang berhasil terhadap ketersediaan atau kerahasiaan sistem. Untuk semua alasan ini, kehilangan integritas mengurangi jaminan sistem TI.

- **Kehilangan Ketersediaan.** Jika sistem TI yang kritis-misi tidak tersedia bagi pengguna akhir, misi organisasi mungkin terpengaruh. Hilangnya fungsi sistem dan efektivitas operasional, misalnya, dapat mengakibatkan hilangnya waktu produktif, sehingga menghambat kinerja pengguna akhir dari fungsi mereka dalam mendukung misi organisasi.

- **Kehilangan Kerahasiaan.** Kerahasiaan sistem dan data mengacu pada perlindungan informasi dari pengungkapan yang tidak sah. Dampak dari pengungkapan informasi rahasia yang tidak sah dapat berkisar dari membahayakan keamanan nasional hingga pengungkapan data Undang-Undang Privasi. Pengungkapan yang tidak sah, tidak terduga, atau tidak disengaja dapat mengakibatkan hilangnya kepercayaan publik, rasa malu, atau tindakan hukum terhadap organisasi.

UNIVERSITAS MULIA

Quantitative versus Qualitative Assessment

Keuntungan utama dari analisis dampak kualitatif adalah bahwa ia memprioritaskan risiko dan mengidentifikasi bidang-bidang untuk perbaikan segera dalam mengatasi kerentanan.

Kelemahan dari analisis kualitatif adalah bahwa ia tidak memberikan pengukuran spesifik yang dapat dikuantifikasi mengenai besarnya dampak, oleh karena itu membuat analisis biaya-manfaat dari setiap kontrol yang direkomendasikan menjadi sulit.

Keuntungan utama dari analisis dampak kuantitatif adalah bahwa ia memberikan pengukuran besaran dampak, yang dapat digunakan dalam analisis biaya-manfaat dari kontrol yang direkomendasikan.

Kerugiannya adalah bahwa, tergantung pada rentang numerik yang digunakan untuk menyatakan pengukuran, makna analisis dampak kuantitatif mungkin tidak jelas, yang mengharuskan hasil ditafsirkan secara kualitatif. Faktor tambahan sering harus dipertimbangkan untuk menentukan besarnya dampak.

UNIVERSITAS MULIA

Matrix & Description of Risk Level

Table 3-6. Risk-Level Matrix

Threat Likelihood	Impact		
	Low (10)	*Medium* (50)	*High* (100)
High (1.0)	Low 10 X 1.0 = 10	Medium 50 X 1.0 = 50	High 100 X 1.0 = 100
Medium (0.5)	Low 10 X 0.5 = 5	Medium 50 X 0.5 = 25	Medium 100 X 0.5 = 50
Low (0.1)	Low 10 X 0.1 = 1	Low 50 X 0.1 = 5	Low 100 X 0.1 = 10

Risk Scale: High (>50 to 100); Medium (>10 to 50); Low (1 to 10)[8]

Table 3-7. Risk Scale and Necessary Actions

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.

Control Recommendations

Selama langkah proses ini, kontrol yang dapat memitigasi atau menghilangkan risiko yang diidentifikasi, yang sesuai dengan operasi organisasi, disediakan. Tujuan dari kontrol yang direkomendasikan adalah untuk mengurangi tingkat risiko pada sistem TI dan datanya ke tingkat yang dapat diterima.

Faktor-faktor berikut harus dipertimbangkan dalam merekomendasikan kontrol dan solusi alternatif untuk meminimalkan atau menghilangkan risiko yang teridentifikasi:

- Efektivitas opsi yang disarankan (mis., Kompatibilitas sistem)
- Legislasi dan regulasi
- Kebijakan organisasi
- Dampak operasional
- Keamanan dan keandalan.

UNIVERSITAS MULIA

Risk Mitigation

Mitigasi risiko, proses kedua manajemen risiko, melibatkan memprioritaskan, mengevaluasi, dan menerapkan kontrol pengurangan risiko yang tepat yang direkomendasikan dari proses penilaian risiko.

Karena penghapusan semua risiko biasanya tidak praktis atau hampir tidak mungkin, itu adalah tanggung jawab manajemen senior dan manajer bisnis dan fungsional untuk menggunakan pendekatan biaya terendah dan menerapkan kontrol yang paling tepat untuk mengurangi risiko misi ke tingkat yang dapat diterima, dengan minimal dampak buruk pada sumber daya dan misi organisasi.

UNIVERSITAS MULIA

Risk mitigation

1. • Asumsi Risiko. Untuk menerima risiko potensial dan terus mengoperasikan sistem TI atau menerapkan kontrol untuk menurunkan risiko ke tingkat yang dapat diterima
2. • Penghindaran Risiko. Untuk menghindari risiko dengan menghilangkan penyebab dan / atau konsekuensi risiko (mis., Lupakan fungsi tertentu dari sistem atau mematikan sistem saat risiko diidentifikasi)
3. • Batasan Risiko. Untuk membatasi risiko dengan menerapkan kontrol yang meminimalkan dampak buruk dari ancaman yang melakukan kerentanan (mis., Penggunaan kontrol pendukung, pencegahan, dan detektif)
4. • Perencanaan Risiko. Untuk mengelola risiko dengan mengembangkan rencana mitigasi risiko yang memprioritaskan, mengimplementasikan, dan memelihara kontrol
5. • Penelitian dan Pengakuan. Untuk menurunkan risiko kerugian dengan mengakui kerentanan atau cacat dan meneliti kontrol untuk memperbaiki kerentanan
6. • Pemindahan Risiko. Untuk mentransfer risiko dengan menggunakan opsi lain untuk mengkompensasi kerugian, seperti membeli asuransi.

UNIVERSITAS MULIA

Risk Mitigation Strategy

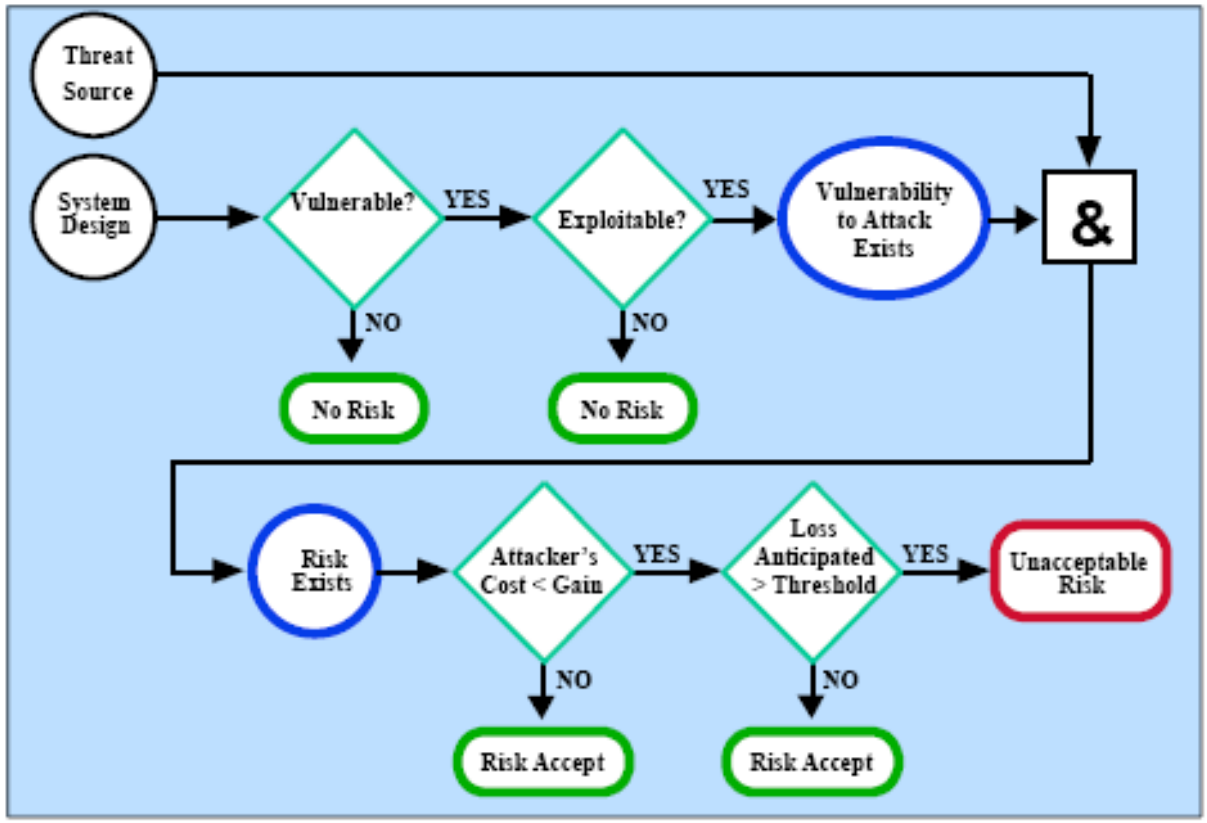

Figure 4-1. Risk Mitigation Action Points

UNIVERSITAS MULIA

Take it easy, No Homework This Week

Thank you

UNIVERSITAS MULIA