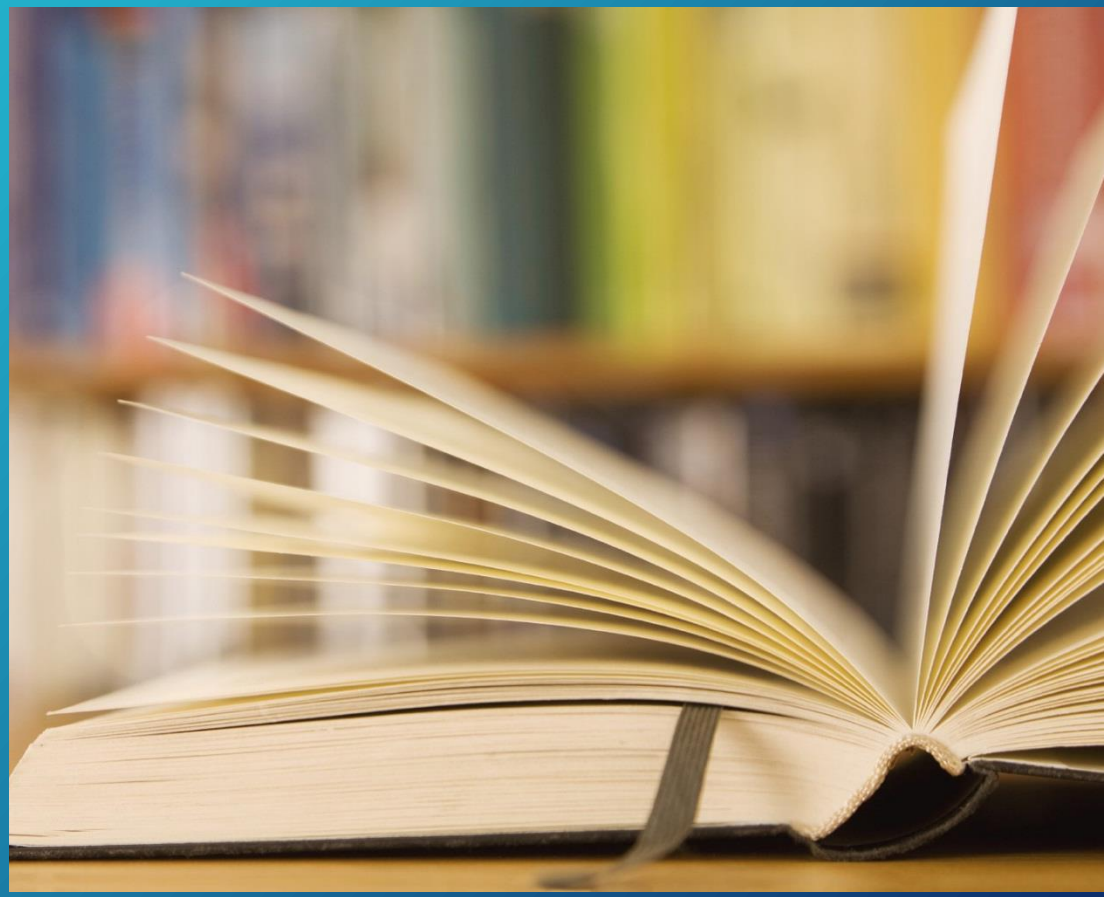
SEKOLAH TINGGI TEKNOLOGI
TERPADU NURUL FIKRI
CHARACTER BUILDING CAMPUS
STT - NF

RISK MANAGEMENT



Keamanan Sistem Informasi – Aditya Putra, ST., MT.

Agenda

RISK

- Definisi
- Risk Level
- Risk Matrix

RISK MANAGEMENT

RESPONSIBILITIES IN RISK MANAGEMENT

RISK MANAGEMENT PHASE

RISK MANAGEMENT FRAMEWORK

- NIST
- COBIT

BEST PRACTICE

RISK - Definisi & Faktor Penyebab Resiko

DEFINISI

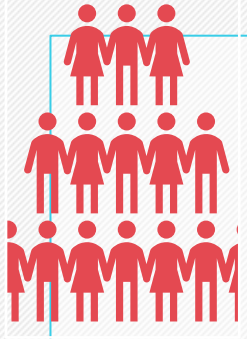
- Risk adalah tingkat ketidakpastian atau potensi kerugian yang dapat timbul dari sebuah kejadian yang merusak pada sistem

FAKTOR PENYEBAB RESIKO

Adanya kelemahan pada sistem (Vulnerability)

Kemungkinan terjadinya sebuah serangan (Threat)

Dampak dari serangan yang berhasil (Impact)



Frekuensi terjadinya serangan (Likelihood)

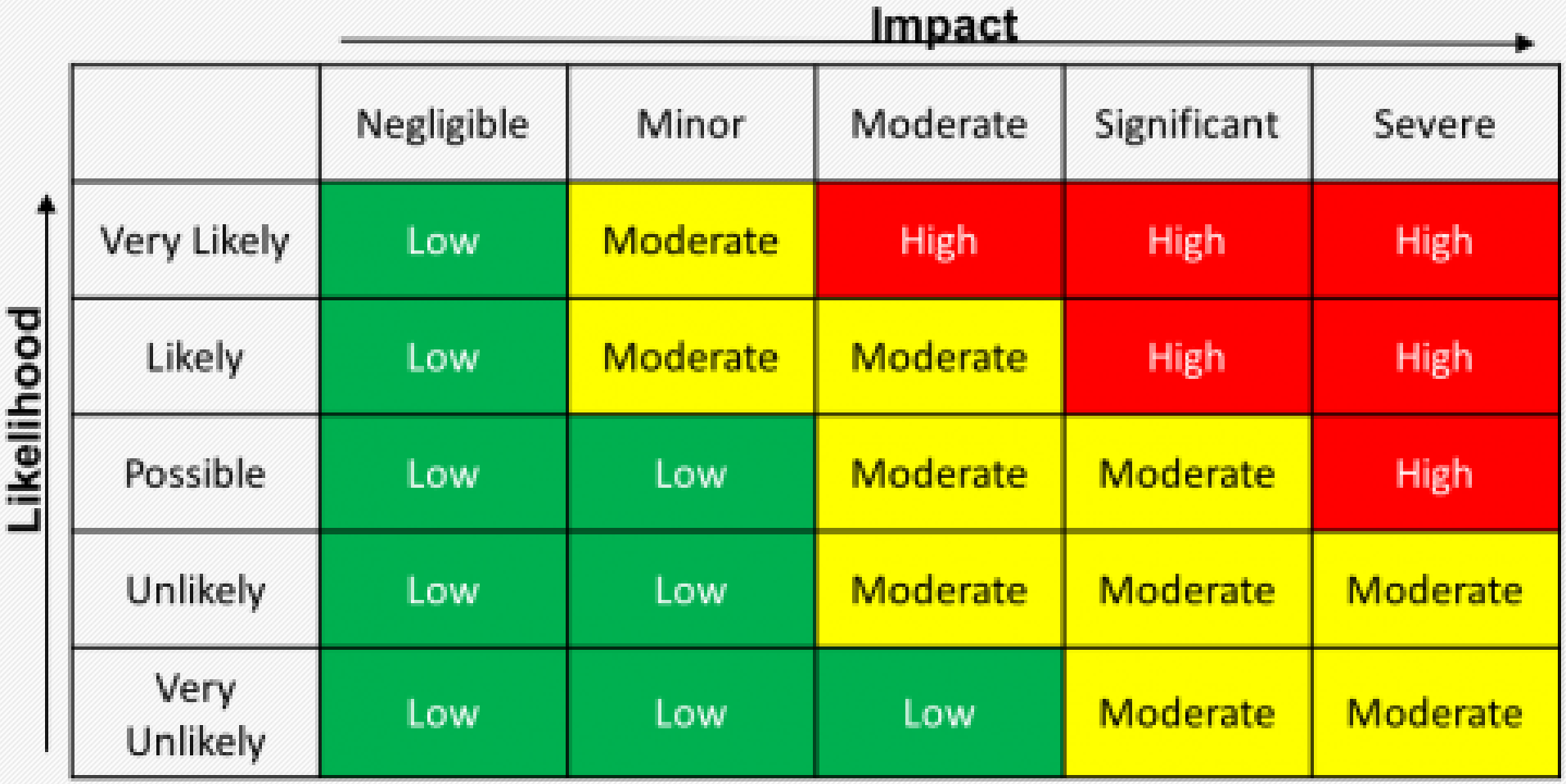
RISK - Risk Level

- Risk dikategorikan ke dalam beberapa tingkat tergantung perhitungan potensi dampaknya terhadap system
- Level Dampak dari sebuah resiko tergantung dari nilai asset dan resource yang terpengaruh dan seberapa parah kerusakan yang diakibatkan

LOW	MEDIUM	HIGH
• Sistem memproses/menyimpan data public • Sistem dapat dengan mudah direcover dan dibangun ulang • Layanan yang tersedia bersifat informasional	• Sistem memproses/menyimpan data non-public/internal organisasi • Sistem memiliki mekanisme internally trusted pada jaringan • Layanan yang tersedia bersifat normal atau layanan penting	• Sistem memproses/menyimpan data rahasia/sangat terbatas • Sistem memiliki mekanisme highly trusted pada jaringan • Layanan yang tersedia bersifat critical dan luas

RISK – Risk Matrix

- Risk Matrix digunakan untuk mengukur skala resiko yang dipengaruhi oleh likelihood dan impact



	Negligible	Minor	Moderate	Significant	Severe
Very Likely	Low	Moderate	High	High	High
Likely	Low	Moderate	Moderate	High	High
Possible	Low	Low	Moderate	Moderate	High
Unlikely	Low	Low	Moderate	Moderate	Moderate
Very Unlikely	Low	Low	Low	Moderate	Moderate

RISK MANAGEMENT

Risk Management adalah proses untuk mengurangi dan menjaga resiko pada level wajar dengan cara implementasi program keamanan yang terukur

Keuntungan Risk Management:

- Meningkatkan proses penanganan resiko
- Memungkinkan petugas keamanan untuk merespon situasi genting secara efektif
- Meminimalisir dampak resiko finansial organisasi
- Pendefinisian yang jelas tentang security control yang sesuai

RISK RESPONSIBILITIES

- Siapa saja penanggung jawab dalam Manajemen Resiko?

Senior Management	• Support dalam penentuan kebijakan makro keamanan informasi organisasi
Chief Information Officer	• Berperan dalam Perencanaan, Penganggaran, dan Performa IT berdasarkan program Risk Management
IT Security Program Manager and Comp Sec Officer	• Bertanggung jawab dalam program keamanan informasi organisasi • Berperan dalam mengimplementasikan security control
Security Awareness Trainers	• Berperan dalam mengembangkan dan menyediakan pelatihan proses Risk Management

RISK MANAGEMENT PHASE

1. RISK IDENTIFICATION

Mengidentifikasi sumber/penyebab serta dampak dari resiko internal dan eksternal yang dapat mengganggu keamana organisasi

- Pahami mekanisme kerja operasional IT organsasi
- Pahami lingkungan internal dan eskternal organasasi
- Temukan dan perkirakan dampak dari resiko

2. RISK ASSESSMENT

- Tahap ini menguji resiko organisasi dan menyediakan perkiraan **likelihood** dan **impact** dari resiko
- Risk Assessment adalah proses iterative berupa penentuan prioritasi dalam rangka mitigasi resiko
- Tahap ini akan menghasilkan nilai kuatitatif dan kualitatif resiko
- 2 hal yang dilakukan dalam tahap ini adalah **RISK ANALYSIS** dan **RISK PRIORITIZATION**

RISK MANAGEMENT PHASE

3. RISK TREATMENT

- Risk Treatment adalah proses menentukan dan mengimplementasikan Tindakan yang sesuai pada resiko
- Resiko diperlakukan sesuai dengan severity level-nya
- Keputusan atau Langkah yang diambil pada fase ini didasarkan pada hasil Risk Assessment

Risk Treatment Steps

ELIMINATE
- Implementasikan pengendalian resiko untuk mengurangi ancaman vulnerability-nya

TRANSFER
- Delegasikan tanggung jawab resiko sesuai bidangnya

MITIGATE
- Kurangi resiko dengan mengimplementasikan control yang sesuai dengan threat/vulnerabilitynya

ACCEPT
- Resiko menjadi wajar jika impact-nya sudah tak seberapa

AVOID
- Hilangkan penyebab dan dampak resiko

PLANNING
- Kelola resiko dengan perencanaan mitigasi dengan memprioritaskan, mengimplementasikan, dan menjaga control resiko

RESEARCH AND ACKNOWLEDGEMENT
- Lakukan Riset untuk mengendalikan resiko seefektif mungkin

RISK MANAGEMENT PHASE

4. RISK TRACKING ANG REVIEW

RISK TRACKING

- Fase ini bertujuan untuk menemukan adanya resiko baru yang bisa terjadi
- Fase Tracking menjamin control yang sesuai dalam menangani resiko
- Fase ini mencakup monitoring peluang, dampak, status, dan munculnya resiko

RISK REVIEW

- Fase Review mengevaluasi performa dari strategi Risk Management yang diimplementasikan
- Tahap ini mencakup Reporting yang menjamin management menyadari dan mengetahui resiko paling utama sehingga mereka bisa membuat perencanaan untuk mengurasi resiko dengan baik

RISK MANAGEMENT FRAMEWORK - NIST

- Framework Risk Management NIST adalah proses yang terstruktur dan kontinyu yang mengintegrasikan keamana informasi ke dalam SDLC

1. **CATEGORIZE**

   Kelompokkan tingkat criticality sistem informasi berdasarkan dampak jika ada insiden

2. **SELECT**

   Tentukan security control, dan kebijakan berdasarkan risk assessment

3. **IMPLEMENT**

   Implementasikan security control dalam jaringan organisasi

4. **ASSESS**

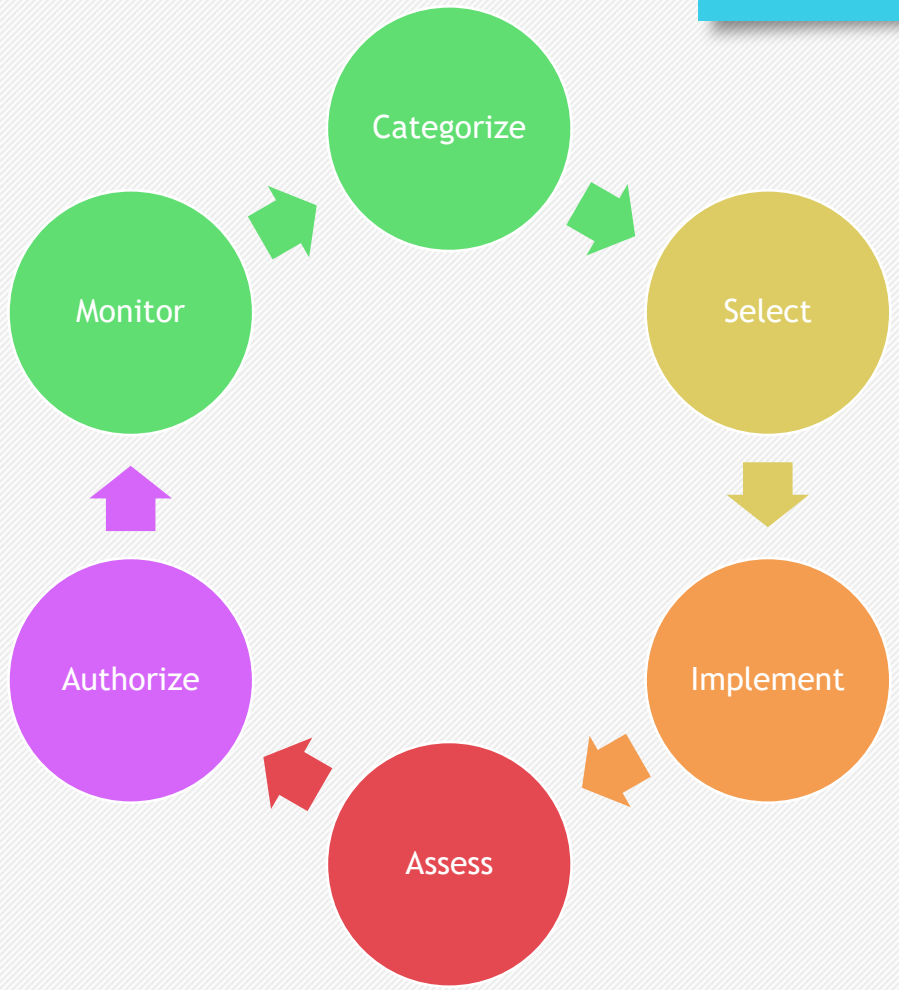
   Uji efektivitas security control

5. **AUTHORIZE**

   Tentukan resiko untuk tiap operasional dan asset organisasi, jika resikonya rendah/wajar, izinkan operasi tersebut berjalan

6. **MONITOR**

   Monitor perubahan yang mungkin terjadi pada sistem informasi yang dapat mempengaruhi security control dan efektivitasnya



RISK MANAGEMENT FRAMEWORK - COBIT

- COBIT adalah framewoek dan toolset pendukung yang memungkinkan manager untuk mengurangi keterbatasan antara kebutuhan control, isu teknis, dan resiko bisnis
- COBIT menekankan pada kesesuaian/compliance terhadap regulasi, membantu organisasi untuk meningkatkan nilai yang dicapai dari IT serta menyederhanakan implementasi tata Kelola IT dan control framework

RISK MANAGEMENT BEST PRACTICE

- Monitor resiko internal dan eksternal organisasi secara periodik
- Buat kebijakan risk management organisasi yang baik
- Implementasikan framework Risk Assessment
- Identifikasi resiko-resiko yang potensial dalam jaringan
- Prioritaskan resiko berbasikan dampak
- Tentukan responsibilities untuk tiap Risk Manager
- Review dan update kebijakan Risk Management yang sudah dibuat