Buku Ajar & Modul
Praktikum Perkuliahan

SISTEM INFORMASI

ITATS
INSTITUT TEKNOLOGI ADHI TAMA SURABAYA

MANAJEMEN RISIKO TEKNOLOGI INFORMASI

Buku Ajar & Modul Perkuliahan Teori, Kerangka Kerja ISO 31000:2018, Standar Keamanan ISO/IEC 27005:2018, Analisis Kualitatif/Kuantitatif (ALE), Risk Register, serta Mitigasi BCP/DRP Berbasis Rencana Pembelajaran Semester (RPS)

Adib Pakarbudi, S.Kom., M.Kom.

Edisi Pertama, 2025/2026

PROGRAM STUDI S1 SISTEM INFORMASI
FAKULTAS TEKNIK ELEKTRO DAN TEKNOLOGI INFORMASI
INSTITUT TEKNOLOGI ADHI TAMA SURABAYA

BUKU AJAR & MODUL PERKULIAHAN

MANAJEMEN RISIKO TEKNOLOGI INFORMASI

Buku Ajar & Modul Perkuliahan Teori, Kerangka Kerja ISO 31000:2018, Standar Keamanan ISO/IEC 27005:2018, Analisis Kualitatif/Kuantitatif (ALE), Risk Register, serta Mitigasi BCP/DRP Berbasis Rencana Pembelajaran Semester (RPS)

Manajemen Risiko TI (25136036) - S1 Sistem Informasi ITATS

Dosen Pengembang RPS & Pengampu:

Adib Pakarbudi, S.Kom., M.Kom.

Bobot: 3 SKS (Semester 6 - Teori)
Program Studi S1 Sistem Informasi
Fakultas Teknik Elektro dan Teknologi Informasi
Institut Teknologi Adhi Tama Surabaya (ITATS)
Edisi Pertama, Tahun Akademik 2025/2026

KATA PENGANTAR

Puji dan syukur kami panjatkan ke hadirat Tuhan Yang Maha Esa atas limpahan rahmat dan karunia-Nya sehingga buku ajar dan modul perkuliahan "Manajemen Risiko Teknologi Informasi (Kode MK: 25136036)" ini dapat diselesaikan dengan baik.

Ketergantungan organisasi modern dan dunia enterprise terhadap sistem informasi dan teknologi digital membawa peluang strategis yang luar biasa besar, namun secara bersamaan melahirkan ancaman risiko siber, gangguan operasional, kebocoran data rahasia, serta kegagalan kepatuhan regulasi yang dapat melumpuhkan kelangsungan bisnis. Mata kuliah Manajemen Risiko TI membekali mahasiswa Program Studi S1 Sistem Informasi ITATS dengan pemahaman mendalam tentang tata kelola risiko enterprise, model tata kelola Tiga Lini Pertahanan (Three Lines of Defense), kerangka kerja standar internasional ISO 31000:2018 dan ISO/IEC 27005:2018, metodologi identifikasi aset kritis, analisis risiko kualitatif matriks 5x5 maupun kuantitatif (SLE, ARO, ALE), penyusunan Risk Register profesional, hingga perancangan strategi mitigasi melalui Business Continuity Plan (BCP) dan Disaster Recovery Plan (DRP).

Buku modul perkuliahan ini disusun secara sistematis mengacu pada Rencana Pembelajaran Semester (RPS) resmi Kurikulum 2025 ITATS, mencakup 5 Bahan Kajian Pokok yang dipetakan ke dalam 5 Bab Utama:

1. Konsep Dasar Manajemen Risiko TI, Taksonomi Risiko, & Model Tata Kelola Tiga Lini Pertahanan (Three Lines Model).
2. Kerangka Kerja Standar Manajemen Risiko Global: ISO 31000:2018 & ISO/IEC 27005:2018.
3. Risiko Keamanan Informasi (CIA Triad), Pengendalian Internal, & Penyusunan Risk Register Enterprise.

4. Analisis & Evaluasi Risiko Aset Sistem Informasi: Metode Kualitatif (Matriks 5x5), Semi-Kuantitatif, & Kuantitatif (ALE).
5. Strategi Penanganan Risiko (4T: Treat, Tolerate, Transfer, Terminate) serta Perancangan BCP dan DRP (RTO & RPO).

Buku ini juga memuat panduan lengkap penugasan terstruktur resmi RPS (Kuis Konsep 5%, Resume Jurnal Standar 5%, Resume Video Mitigasi 5%, Perancangan Risk Response 20%, Manajemen Risiko ISO 31000 25%, dan Manajemen Risiko Aset ISO 27005 40% dengan total kumulatif 100%).

Penulis menyampaikan terima kasih yang tulus kepada Ketua Program Studi Sistem Informasi ITATS, pimpinan Fakultas Teknik Elektro dan Teknologi Informasi, serta seluruh sivitas akademika atas dukungan moril dan diskusi. Semoga modul perkuliahan ini menjadi referensi akademik bermutu dalam mencetak Sarjana Sistem Informasi yang berdaya saing tinggi dan berwawasan tata kelola enterprise yang tangguh.

Kritik dan saran konstruktif senantiasa kami nantikan demi penyempurnaan di masa mendatang.

Surabaya, Februari 2025

Dosen Pengampu,

Adib Pakarbudi, S.Kom., M.Kom.

PETUNJUK PENGGUNAAN & PETA KOMPETENSI RPS

Buku modul perkuliahan ini dirancang berbasis Outcome-Based Education (OBE) untuk perkuliahan teori 3 SKS (tanpa praktikum laboratorium) melalui kombinasi metode Pembelajaran Berbasis Masalah (Problem-Based Learning), Telaah Jurnal Ilmiah, Analisis Studi Kasus Insiden TI Enterprise, Simulasi Perhitungan Kerugian Kuantitatif (ALE), dan Penyusunan Portofolio Dokumen Tata Kelola Risiko Terstruktur.

Bagi Dosen Pengampu:

1. Memandu perkuliahan sesuai dengan roadmap 16 Pertemuan pada RPS resmi ITATS.
2. Memfasilitasi diskusi analitis mengenai regulasi perlindungan data, ancaman siber kontemporer, dan audit kepatuhan tata kelola TI.
3. Melakukan evaluasi berkala berbasis rubrik terstandar untuk menilai pemahaman konsep, resume jurnal/video, serta portofolio Risk Register dan rencana mitigasi BCP/DRP mahasiswa.

Bagi Mahasiswa:

1. Pahami Capaian Pembelajaran Lulusan (CPL-9 dan CPL-10) serta Capaian Pembelajaran Mata Kuliah (CPMK-2 dan CPMK-3).

2. Pelajari konsep tata kelola ISO 31000:2018 dan ISO/IEC 27005:2018 di setiap bab perkuliahan.

3. Kerjakan seluruh Lembar Kerja Penugasan Terstruktur (Worksheets) yang merepresentasikan tugas resmi RPS:

- Tugas 1: Kuis Pemahaman Konsep Manajemen Risiko TI & Model Three Lines (Minggu 1-4 | Bobot 5%).

- Tugas 2: Resume Jurnal Ilmiah Standar Manajemen Risiko TI (Minggu 1-4 | Bobot 5%).
- Tugas 3: Resume Video Proses Mitigasi Risiko Aset Informasi (Minggu 1-4 | Bobot 5%).
- Evaluasi Tengah Semester (UTS): Penilaian Konsep ISO 31000 & Identifikasi Aset Kritis (Minggu 8).
- Tugas 4: Perancangan Risk Response Terhadap Hasil Analisis Risiko (Minggu 5-15 | Bobot 20%).
- Tugas 5: Penerapan Kerangka Kerja Manajemen Risiko TI ISO 31000 (Minggu 9-15 | Bobot 25%).
- Tugas 6: Manajemen Risiko Aset Informasi Berbasis ISO/IEC 27005 (Minggu 5-15 | Bobot 40%).
- Evaluasi Akhir Semester (UAS): Uji Portofolio Dokumen Risk Register & Rencana Kontinuitas BCP/DRP (Minggu 16 | Bobot 25%).

Capaian Pembelajaran Lulusan (CPL) & CPMK

Kode	Deskripsi Capaian Pembelajaran (RPS Resmi)
CPL-9	Mampu memahami dan menerapkan kode etik dalam penggunaan informasi maupun data pada perancangan dan implementasi suatu sistem pada organisasi.
CPL-10	Memiliki kemampuan merencanakan, menerapkan, memelihara serta meningkatkan sistem informasi organisasi untuk mencapai tujuan dan sasaran organisasi yang strategis baik jangka pendek maupun jangka panjang.
CPMK-2 (35%)	Mampu menerapkan kode etik dalam penggunaan informasi data pada perancangan, implementasi dan penggunaan suatu sistem.
CPMK-3 (65%)	Mampu memelihara sistem informasi organisasi untuk mencapai tujuan organisasi jangka pendek.

Pemetaan Sub-CPMK & Bobot Penilaian Tugas RPS

Sub-CPMK & Bobot	Kemampuan Akhir Tiap Tahapan Belajar
SubCPMK 1 (Minggu 1-4 | 15%)	Mampu menguraikan konsep dasar manajemen risiko dalam konteks sistem informasi, definisi, jenis risiko, dan Three Lines of Defense [C2, A7, P14].
SubCPMK 2 (Minggu 5-8 | 20%)	Mampu mengevaluasi efektivitas kerangka kerja ISO 31000 (arsitektur & prinsip) dan standar ISO 27005 (konsep & aplikasi) [C2, A10, P14].
SubCPMK 3 (Minggu 9-11 | 20%)	Mampu mengidentifikasi risiko keamanan informasi, pengendalian internal, dan menyusun dokumen Risk Register organisasi [C2, A10, P14].
SubCPMK 4 (Minggu 12-14 | 20%)	Mampu menganalisis risiko terhadap aset sistem informasi menggunakan metode kualitatif matriks 5x5 dan kuantitatif ALE [C3, A10, P14].
SubCPMK 5 (Minggu 15-16 | 25%)	Mampu merancang mitigasi risiko (opsi 4T) dan strategi kontinuitas sistem melalui Business Continuity Plan (BCP) dan Disaster Recovery Plan (DRP) [C4, A10, P14].

Roadmap Perkuliahan 16 Pertemuan & Korelasi Penugasan RPS

Minggu	Bahan Kajian & Topik Perkuliahan	Bentuk Evaluasi / Tugas
Minggu 1-2	Konsep Dasar Manajemen Risiko TI & Konteks SI/TI (Bahan Kajian 1 / SubCPMK 1)	Kuliah Teori, Diskusi Taksonomi Risiko, Tugas: Kuis Pemahaman (5%)
Minggu 3-4	Tata Kelola Risiko & Model Three Lines of Defense (Bahan Kajian 1 / SubCPMK 1)	Studi Kasus Tata Kelola, Tugas: Resume Jurnal (5%) & Video Mitigasi (5%)
Minggu 5-7	Kerangka Kerja ISO 31000:2018 & ISO/IEC 27005:2018 (Bahan Kajian 2 / SubCPMK 2)	Kuliah & Diskusi Kelompok Penerapan Standar ISO
Minggu 8	Evaluasi Tengah Semester (UTS)	Ujian Portofolio Analisis Standar ISO 31000 & Konteks Organisasi

Minggu	Bahan Kajian & Topik Perkuliahan	Bentuk Evaluasi / Tugas
Minggu 9-11	Risiko Keamanan Informasi & Penyusunan Risk Register (Bahan Kajian 3 / SubCPMK 3)	Telaah Aset Kritis, Threat-Vulnerability Identification, Form Risk Register
Minggu 12-14	Analisis & Evaluasi Risiko: Kualitatif Matriks 5x5 & Kuantitatif ALE (Bahan Kajian 4 / SubCPMK 4)	Simulasi Perhitungan SLE, ARO, ALE, Penentuan Risk Appetite & Heatmap
Minggu 15	Strategi Penanganan Risiko (4T) & Perancangan BCP/DRP (Bahan Kajian 5 / SubCPMK 5)	Penyusunan RTO/RPO, Failover Server, & Prosedur Tanggap Darurat Bencana
Minggu 16	Evaluasi Akhir Semester (UAS)	Presentasi Portofolio Dokumen Manajemen Risiko TI Terpadu (Bobot 25%)

DAFTAR ISI

HALAMAN JUDUL & IDENTITAS MATA KULIAH 1

KATA PENGANTAR DOSEN PENGAMPU 2

PETUNJUK PENGGUNAAN & PETA KOMPETENSI RPS 4

DAFTAR ISI 7

BAB 1: KONSEP DASAR MANAJEMEN RISIKO TI & THREE LINES MODEL 9

1.1 Hakikat Risiko dan Urgensi Manajemen Risiko TI 9

1.2 Taksonomi & Kategori Risiko Teknologi Informasi 10

1.3 Anatomi Risiko: Aset, Ancaman, Kerentanan, & Dampak 11

1.4 Model Tata Kelola Tiga Lini Pertahanan (Three Lines) 12

1.5 Lembar Kerja 1 (Tugas RPS): Analisis Risiko & 3 Lines 13

1.6 Rangkuman & Soal Evaluasi Bab 1 15

BAB 2: KERANGKA KERJA STANDAR: ISO 31000 & ISO/IEC 27005 16

2.1 Arsitektur Manajemen Risiko ISO 31000:2018 16

2.2 Delapan Prinsip Manajemen Risiko ISO 31000:2018 17

2.3 Standar Manajemen Risiko Keamanan ISO/IEC 27005:2018 18

2.4 Alur Siklus Proses Manajemen Risiko ISO/IEC 27005 19

2.5 Lembar Kerja 2 (Tugas RPS & UTS): Penetapan Konteks 21

2.6 Rangkuman & Soal Evaluasi Bab 2 (Evaluasi UTS) 22

BAB 3: RISIKO KEAMANAN INFORMASI & RISK REGISTER 24

3.1 Pilar Keamanan Informasi: CIA Triad & Non-Repudiation 24

3.2 Pengendalian Internal (Internal Controls) Sistem 25

3.3 Metodologi Identifikasi Risiko & Skenario Ancaman 26

3.4 Struktur & Anatomi Risk Register Enterprise 27

3.5 Lembar Kerja 3 (Tugas RPS): Penyusunan Risk Register 29

3.6 Rangkuman & Soal Evaluasi Bab 3 30

BAB 4: ANALISIS & EVALUASI RISIKO: KUALITATIF & KUANTITATIF (ALE) 31

4.1 Tiga Pendekatan Analisis Risiko Sistem Informasi 31

4.2 Analisis Kualitatif & Matriks Risiko 5x5 (Heatmap) 32
4.3 Analisis Kuantitatif Finansial: Formula SLE, ARO, & ALE 33
4.4 Analisis Biaya-Manfaat Kontrol (Cost-Benefit Analysis) 34
4.5 Lembar Kerja 4 (Tugas RPS): Analisis Kuantitatif ALE 35
4.6 Rangkuman & Soal Evaluasi Bab 4 36
BAB 5: STRATEGI PENANGANAN RISIKO (4T), BCP, & DRP 38
5.1 Empat Opsi Strategis Penanganan Risiko (4T Framework) 38
5.2 Perancangan Business Continuity Plan (BCP) 39
5.3 Perancangan Disaster Recovery Plan (DRP): RTO & RPO 40
5.4 Alternatif Lokasi Pemulihan Bencana (DR Site) 41
5.5 Lembar Kerja 5 (Tugas RPS & UAS): Risk Response & DRP 42
5.6 Rangkuman & Soal Evaluasi Bab 5 (Evaluasi Akhir UAS) 43
BAGIAN AKHIR: GLOSARIUM, RUBRIK PENILAIAN, & PUSTAKA RPS 45
Glosarium Istilah Manajemen Risiko TI (A-Z) 45
Rubrik Penilaian & Matriks Korelasi Tugas RPS (Bobot 100%) 48
Daftar Pustaka Utama Sesuai RPS Resmi ITATS 50
Profil Dosen Pengembang RPS & Pengampu 50

BAB 1: KONSEP DASAR MANAJEMEN RISIKO TI & MODEL TIGA LINI PERTAHANAN

Capaian Pembelajaran Bab (Bahan Kajian RPS)

1. Mendefinisikan hakikat risiko, ketidakpastian (uncertainty), dan urgensi tata kelola risiko TI dalam organisasi modern.
2. Mengklasifikasikan taksonomi risiko TI: Risiko Strategis, Operasional, Keamanan Siber, Kepatuhan Regulasi, dan Finansial.
3. Menganalisis hubungan sebab-akibat antar-komponen fundamental risiko: Aset Kritis, Ancaman (Threats), Kerentanan (Vulnerabilities), dan Dampak Bisnis.
4. Menguraikan arsitektur tata kelola Three Lines Model (IIA 2020) yang mencakup Governing Body, Lini 1 (Operasional), Lini 2 (Manajemen Risiko), dan Lini 3 (Audit Internal).
5. Menyelesaikan penugasan terstruktur resmi RPS: Kuis Pemahaman Konsep (5%), Resume Jurnal Ilmiah (5%), dan Resume Video Mitigasi Aset Informasi (5%).

1.1 Hakikat Risiko dan Urgensi Manajemen Risiko TI

Dalam standar internasional ISO 31000:2018, risiko didefinisikan secara presisi sebagai 'efek dari ketidakpastian terhadap pencapaian sasaran organisasi' (effect of uncertainty on objectives). Efek di sini dapat berupa deviasi positif (peluang / upside risk) maupun deviasi negatif (ancaman kerugian / downside risk).

Dalam konteks sistem informasi dan teknologi digital, Risiko TI (IT Risk) adalah potensi terjadinya peristiwa yang berkaitan dengan kegagalan perangkat lunak, infrastruktur jaringan, kesalahan manusia (human error), serangan siber berbahaya, bencana alam, atau ketidakmampuan vendor pihak ketiga yang dapat mengancam integritas, ketersediaan, dan kerahasiaan data serta kelangsungan proses bisnis perusahaan.

Manajemen Risiko TI bukan bertujuan untuk menghilangkan seluruh risiko menjadi nol persen (Zero Risk adalah hal yang mustahil

dan tidak ekonomis), melainkan mengendalikan dan mengarahkan tingkat risiko agar tetap berada dalam batas toleransi yang dapat diterima oleh manajemen puncak (Risk Appetite & Risk Tolerance).

Risk Appetite vs. Risk Tolerance

• Risk Appetite: Jumlah dan jenis risiko yang siap diambil organisasi dalam rangka mengejar tujuan strategisnya (misal: siap menerima risiko downtime aplikasi non-kritis selama 2 jam demi efisiensi biaya infrastruktur).

• Risk Tolerance: Batas deviasi maksimal yang masih dapat ditolerir sebelum tindakan korektif darurat wajib dieksekusi.

1.2 Taksonomi & Kategori Risiko Teknologi Informasi

COBIT 2019 (Domain APO12 - Managed Risk) membagi risiko TI ke dalam 5 domain strategis:

1. Risiko Strategis TI: Ketidakselarasan antara strategi investasi teknologi dengan tujuan bisnis jangka panjang perusahaan.
2. Risiko Operasional TI: Gangguan terhadap jalannya proses bisnis harian akibat kegagalan server, bug aplikasi inti (Core System), atau padamnya pasokan listrik data center.
3. Risiko Keamanan Siber (Cybersecurity Risk): Ancaman serangan peretasan (Ransomware, Phishing, SQL Injection, DDoS) yang membocorkan data pribadi atau merusak basis data.
4. Risiko Kepatuhan & Regulasi (Compliance Risk): Risiko denda hukum dan sanksi pencabutan izin operasional akibat pelanggaran undang-undang perlindungan data pribadi (seperti UU No. 27 Tahun 2022 tentang PDP di Indonesia atau standar PCI-DSS di sektor perbankan).
5. Risiko Finansial TI: Kerugian moneter langsung akibat pembengkakan biaya proyek perangkat lunak atau kerugian finansial akibat terhentinya layanan transaksi digital konsumen.

1.3 Anatomi Risiko: Aset, Ancaman, Kerentanan, & Dampak

Hubungan sebab-akibat risiko keamanan informasi dirumuskan dalam model:

`Risiko = Ancaman (Threat) x Kerentanan (Vulnerability) x Nilai Aset (Asset Value)`

- Aset (Asset): Segala sesuatu yang memiliki nilai ekonomi bagi organisasi (Basis Data Pelanggan, Source Code Aplikasi, Server Data Center, Reputasi Merek).
- Ancaman (Threat): Potensi kejadian eksternal atau internal yang dapat merugikan aset (Malware, Hacker, Kebakaran Gedung, Karyawan yang Curang).
- Kerentanan (Vulnerability): Celah kelemahan pada sistem atau prosedur yang dapat dieksploitasi oleh ancaman (Port server yang terbuka tanpa autentikasi, Sistem operasi yang belum ditambal/unpatched, Kebijakan kata sandi yang lemah).
- Dampak (Impact): Tingkat kerugian finansial, hukum, dan operasional jika ancaman berhasil mengeksploitasi kerentanan aset tersebut.

Prinsip Celah Keamanan (Vulnerability Window)

Ancaman sebesar apa pun (misal: ribuan peretas siber di internet) TIDAK AKAN menghasilkan insiden risiko selama TIDAK ADA kerentanan (vulnerability) pada aset sistem informasi. Tugas utama analis risiko TI adalah menutup kerentanan sistem melalui kontrol keamanan yang berlapis!

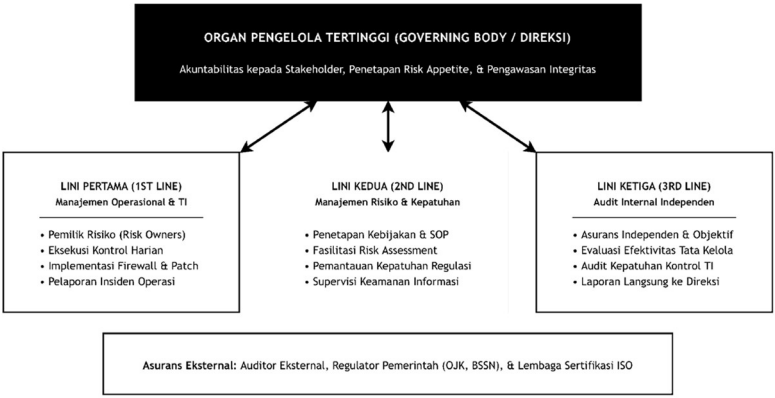
1.4 Model Tata Kelola Tiga Lini Pertahanan (The Three Lines Model)

The Institute of Internal Auditors (IIA, 2020) merumuskan model tata kelola organisasi modern yang memastikan pembagian

peran dan tanggung jawab yang tegas dalam pengelolaan risiko enterprise:

1. Governing Body (Dewan Direksi & Dewan Komisaris): Memegang akuntabilitas tertinggi kepada pemangku kepentingan (Stakeholders), menetapkan kebijakan umum tata kelola, dan menentukan batas selera risiko (Risk Appetite).
2. Lini Pertama (1st Line of Defense - Manajemen Operasional & Unit TI):
    - Bertindak sebagai Pemilik Risiko (Risk Owners).
    - Bertanggung jawab langsung mengidentifikasi, mengelola, dan mengendalikan risiko operasional sehari-hari.
    - Mengimplementasikan kontrol keamanan teknis (Konfigurasi Firewall, Patching, Manajemen Akses Pengguna, Antivirus).
3. Lini Kedua (2nd Line of Defense - Unit Manajemen Risiko & Kepatuhan):
    - Memberikan keahlian metodologis, memfasilitasi kerangka kerja penilaian risiko, dan menetapkan standar SOP keamanan.
    - Memantau pelaksanaan kepatuhan regulasi eksternal secara berkelanjutan.

4. Lini Ketiga (3rd Line of Defense - Unit Audit Internal Independen):
    - Memberikan asurans objektif dan independen kepada Dewan Direksi mengenai efektivitas tata kelola dan kontrol Lini 1 dan Lini 2.
    - Melakukan audit berkala secara menyeluruh tanpa intervensi pihak operasional.



Gambar 1.1: Model Tata Kelola Tiga Lini Pertahanan (The Three Lines Model - IIA 2020)

Aktivitas Pembelajaran & Penugasan Terstruktur: LEMBAR KERJA 1 (TUGAS RPS MINGGU 1-4): Analisis Konsep Risiko & Three Lines of Defense

Kerjakan penugasan terstruktur mandiri/kelompok untuk memenuhi penilaian SubCPMK 1 (Bobot 15%): Kuis Konsep (5%), Resume Jurnal (5%), dan Resume Video Mitigasi Aset Informasi (5%).

Bagian A: Identifikasi Komponen Risiko Kasus Perbankan Digital

Komponen / Parameter Risiko	Deskripsi / Isian Analisis
1. Aset Kritis yang Dianalisis:	Basis Data Rekening Nasabah & Server Core Banking
2. Ancaman Teridentifikasi (Threat):	Serangan Brute Force & Phishing kredensial administrator
3. Kerentanan Sistem (Vulnerability):	Autentikasi belum mewajibkan Multi-Factor Authentication (MFA)
4. Estimasi Dampak Bisnis (Impact):	Pencurian dana nasabah, tuntutan hukum denda UU PDP, kerugian reputasi
5. Rekomendasi Kontrol Pengendalian:	Wajib implementasi FIDO2/MFA & enkripsi data at-rest AES-256

Bagian B: Pemetaan Peran Three Lines of Defense pada Insiden Kebocoran Data

Komponen / Parameter Risiko	Deskripsi / Isian Analisis
Peran Lini 1 (Divisi TI & Database Admin):	Melakukan isolasi server terinfeksi dan patch celah keamanan segera
Peran Lini 2 (Divisi Manajemen Risiko & Legal):	Menghitung tingkat keparahan insiden dan lapor ke regulator BSSN/OJK

Peran Lini 3 (Auditor Internal TI):	Mengaudit forensik kronologi kegagalan kontrol dan lapor ke Direksi
Status Resume Jurnal Ilmiah Standar ISO:	Lengkap terlampir (Menganalisis artikel jurnal akreditasi SINTA/Scopus)
Status Resume Video Mitigasi Aset:	Lengkap terlampir (Merangkum video studi kasus mitigasi ransomware)

Lembar Refleksi & Evaluasi Kasus:

1. Jelaskan mengapa suatu organisasi yang tidak memisahkan peran Lini 1 (Operasional TI) dan Lini 3 (Audit Internal) sangat rentan mengalami kegagalan tata kelola risiko:
2. Bagaimana konsep 'Risk Appetite' memandu perbankan dalam memutuskan apakah suatu fitur transfer instan baru boleh dirilis ke publik?

Rangkuman Eksekutif BAB 1

- Risiko adalah efek dari ketidakpastian terhadap pencapaian sasaran organisasi (ISO 31000:2018).
- Komponen risiko mencakup Aset bernilai, Ancaman eksternal/internal, Kerentanan celah sistem, dan Dampak kerugian bisnis.
- Taksonomi risiko TI terbagi atas risiko Strategis, Operasional, Siber, Kepatuhan Regulasi, dan Finansial.
- • Model Three Lines of Defense membagi tanggung jawab atas: Lini 1 (Pemilik Risiko Operasional), Lini 2 (Pengawas Manajemen Risiko & Kepatuhan), dan Lini 3 (Asurans Audit Internal Independen).

Soal Evaluasi Pemahaman BAB 1

1. Uraikan definisi risiko menurut standar ISO 31000:2018 dan jelaskan mengapa konsep Zero Risk merupakan hal yang tidak realistis bagi sistem informasi enterprise!

2. Jelaskan perbedaan mendasar antara Ancaman (Threat) dan Kerentanan (Vulnerability) disertai contoh kasus nyata pada aplikasi web e-commerce!
3. Uraikan struktur dan peran masing-masing lini dalam The Three Lines Model (IIA 2020) serta jelaskan garis pelaporan independen dari Lini Ketiga ke Dewan Direksi!
4. Bagaimana sebuah organisasi sistem informasi menentukan batas Risk Appetite dan Risk Tolerance dalam mengadopsi teknologi Cloud Computing?

BAB 2: KERANGKA KERJA STANDAR INTERNASIONAL: ISO 31000 & ISO/IEC 27005

Capaian Pembelajaran Bab

1. Menganalisis arsitektur komprehensif ISO 31000:2018 yang menghubungkan Prinsip, Kerangka Kerja (Framework), dan Proses Manajemen Risiko.
2. Menguraikan 8 Prinsip Penciptaan Nilai ISO 31000:2018 sebagai fondasi budaya sadar risiko (Risk-Aware Culture).
3. Menjelaskan siklus kepemimpinan dan komitmen (Leadership & Commitment) dalam mengintegrasikan manajemen risiko ke dalam tata kelola enterprise.
4. Menguasai standar manajemen risiko keamanan informasi ISO/IEC 27005:2018 dan keterkaitannya dengan sistem manajemen keamanan informasi ISO/IEC 27001.
5. Menguraikan tahapan proses ISO/IEC 27005: Penetapan Konteks, Penilaian Risiko (Identifikasi, Analisis, Evaluasi), Penanganan Risiko, dan Penerimaan Residu Risiko.
1. 6. Menyelesaikan evaluasi portofolio Ujian Tengah Semester (UTS) berbasis analisis kerangka kerja standar ISO (Bobot 20% kumulatif).

2.1 Arsitektur Manajemen Risiko ISO 31000:2018

International Organization for Standardization merilis ISO 31000:2018 sebagai panduan umum manajemen risiko terstandarisasi yang berlaku universal untuk semua jenis industri dan sektor organisasi. Arsitektur ISO 31000 dibangun di atas tiga pilar utama yang saling terhubung:

1. Prinsip (Principles): Fondasi filosofis yang menyatakan bahwa tujuan utama manajemen risiko adalah penciptaan dan perlindungan nilai (Value Creation and Protection).

2. Kerangka Kerja (Framework): Struktur organisasi, mandat, kepemimpinan, dan integrasi tata kelola yang menjamin proses manajemen risiko tertanam ke dalam seluruh aktivitas bisnis.
3. Proses (Process): Penerapan sistematis dari kebijakan, prosedur, dan praktik pengelolaan risiko melalui tahapan penilaian, mitigasi, komunikasi, dan pemantauan berkala.

2.2 Delapan Prinsip Manajemen Risiko ISO 31000:2018

Agar pengelolaan risiko efektif dan berdaya guna, ISO 31000:2018 menetapkan 8 prinsip pokok:

1. Terintegrasi (Integrated): Manajemen risiko adalah bagian tak terpisahkan dari seluruh aktivitas operasional dan pengambilan keputusan organisasi.
2. Terstruktur dan Komprehensif (Structured and Comprehensive): Memberikan hasil yang konsisten, terukur, dan dapat dibandingkan di seluruh unit kerja.
3. Disesuaikan (Customized): Kerangka kerja dan proses disesuaikan dengan konteks internal, eksternal, dan profil risiko khas organisasi.
4. Inklusif (Inclusive): Melibatkan seluruh pemangku kepentingan (Stakeholders) secara tepat waktu agar perspektif mereka dipertimbangkan.
5. Dinamis (Dynamic): Mampu mengantisipasi, mendeteksi, dan merespons perubahan ancaman lingkungan bisnis baru secara lincah.
6. Informasi Terbaik yang Tersedia (Best Available Information): Berdasarkan data historis yang valid, estimasi ilmiah, dan ekspektasi masa depan.

7. Faktor Manusia dan Budaya (Human and Cultural Factors): Mengakui bahwa perilaku manusia, kapabilitas kognitif, dan budaya organisasi sangat memengaruhi efektivitas kontrol.
8. Perbaikan Berkelanjutan (Continual Improvement): Manajemen risiko terus-menerus disempurnakan melalui proses pembelajaran dan evaluasi berkala.

Prinsip Utama: Value Creation & Protection

Manajemen risiko bukan sekadar beban administratif atau pemenuhan kepatuhan semata (Compliance Tick-Box), melainkan alat strategis untuk melindungi aset yang ada dan membuka peluang bisnis baru secara aman.

2.3 Standar Manajemen Risiko Keamanan Informasi ISO/IEC 27005:2018

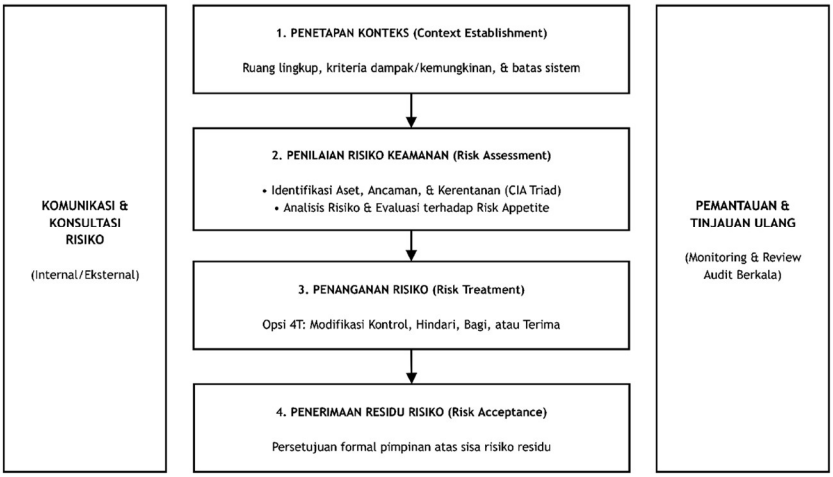
Jika ISO 31000 bersifat umum untuk seluruh risiko enterprise, maka ISO/IEC 27005:2018 dirancang secara khusus untuk memberikan panduan teknis mendalam mengenai manajemen risiko keamanan informasi (Information Security Risk Management / ISRM). Standar ini menjadi panduan pendukung utama bagi implementasi klausul 6.1 (Actions to address risks and opportunities) pada standar ISO/IEC 27001 (Sistem Manajemen Keamanan Informasi / SMKI).

Fokus utama ISO/IEC 27005 adalah melindungi tiga aspek pilar kerahasiaan, keutuhan, dan ketersediaan data (CIA Triad: Confidentiality, Integrity, Availability) terhadap seluruh aset informasi milik organisasi.

2.4 Alur Siklus Proses Manajemen Risiko ISO/IEC 27005

Proses ISO/IEC 27005 terdiri atas serangkaian tahapan iteratif:

1. Penetapan Konteks (Context Establishment): Menentukan ruang lingkup sistem informasi yang dinilai, kriteria evaluasi risiko (skala dampak finansial/hukum dan skala probabilitas), serta struktur tim pengkaji.
2. Penilaian Risiko Keamanan Informasi (Information Security Risk Assessment):
    - Identifikasi Risiko: Mengidentifikasi inventaris aset informasi, ancaman spesifik, kerentanan sistem, dan kontrol eksisting.
    - Analisis Risiko: Menghitung tingkat besaran risiko (kuantitatif / kualitatif).
    - Evaluasi Risiko: Membandingkan tingkat risiko terhitung dengan kriteria selera risiko (Risk Appetite) untuk menentukan prioritas penanganan.
3. Penanganan Risiko (Risk Treatment): Memilih opsi mitigasi keamanan (menerapkan kontrol Annex A ISO 27001, transfer risiko, atau hindari aktivitas berisiko).
4. Penerimaan Risiko Residu (Risk Acceptance): Persetujuan formal dari pimpinan eksekutif terhadap sisa risiko yang masih tertinggal setelah kontrol diterapkan.
5. Komunikasi, Konsultasi, Pemantauan, & Tinjauan Ulang: Memastikan seluruh pihak terinformasi dan melakukan pengujian efektivitas kontrol secara berkala.



Gambar 2.2: Alur Proses Manajemen Risiko Keamanan Informasi ISO/IEC 27005:2018

Studi Komparasi ISO 31000 vs ISO/IEC 27005

• ISO 31000: Bersifat 'High-Level Strategic', memandu tata kelola seluruh risiko bisnis perusahaan (keuangan, hukum, pasar, operasional, TI).

• ISO/IEC 27005: Bersifat 'Domain-Specific Technical', memberikan metodologi langkah demi langkah untuk mengamankan aset informasi, basis data, jaringan, dan kode program dari ancaman siber.

Aktivitas Pembelajaran & Penugasan Terstruktur: LEMBAR KERJA 2 (TUGAS RPS MINGGU 5-8 & EVALUASI UTS): Penetapan Konteks ISO 31000 & 27005

Susun dokumen penetapan konteks manajemen risiko sistem informasi enterprise kelompok Anda berbasis ISO 31000 dan ISO/IEC 27005 sebagai komponen portofolio penilaian Ujian Tengah Semester (UTS - Bobot 20% kumulatif).

Bagian A: Penetapan Ruang Lingkup & Konteks Organisasi (Context Establishment)

Komponen / Parameter Risiko	Deskripsi / Isian Analisis
1. Nama Entitas / Sistem Informasi yang Dinilai:	Sistem Informasi Rekam Medis Elektronik (RME) Rumah Sakit Sehat Sejahtera
2. Regulasi Hukum yang Berlaku (Compliance):	Permenkes No. 24 Tahun 2022 tentang Rekam Medis & UU PDP No. 27 Tahun 2022
3. Pernyataan Selera Risiko (Risk Appetite Direksi):	Toleransi nol (Zero Tolerance) terhadap insiden kebocoran rekam medis pasien
4. Kriteria Skala Dampak Finansial Kritis (Level 5):	Kerugian moneter > Rp 1.000.000.000 atau sanksi penutupan izin rumah sakit
5. Batas Waktu Tinjauan Ulang Risiko (Review Period):	Setiap 6 bulan sekali atau jika terjadi pembaruan arsitektur sistem inti

Bagian B: Evaluasi 8 Prinsip ISO 31000 pada Kebijakan TI

Komponen / Parameter Risiko	**Deskripsi / Isian Analisis**
Penerapan Prinsip 'Integrated':	Prosedur risk assessment wajib dilakukan sebelum rilis software baru

Penerapan Prinsip 'Customized':	Kriteria dampak disesuaikan dengan standar akreditasi rumah sakit
Penerapan Prinsip 'Best Available Info':	Menggunakan log audit SIEM, log firewall, dan data insiden siber BSSN
Penerapan Prinsip 'Human & Cultural':	Mengadakan pelatihan kesadaran keamanan siber (Security Awareness) rutin
Status Kesiapan Berkas Portofolio UTS:	Lengkap terverifikasi untuk evaluasi kelulusan SubCPMK 2

Lembar Refleksi & Evaluasi Kasus:

1. Jelaskan mengapa kepemimpinan dan komitmen (Leadership & Commitment) dari Dewan Direksi menjadi faktor penentu utama keberhasilan penerapan kerangka kerja ISO 31000 dalam sebuah enterprise:

.....

2. Bagaimana keterkaitan antara tahapan Risk Assessment pada ISO/IEC 27005 dengan pemilihan kontrol keamanan pada standar ISO/IEC 27001?

Rangkuman Eksekutif BAB 2

- ISO 31000:2018 menyediakan arsitektur umum tata kelola risiko berbasis 8 Prinsip, Kerangka Kerja Kepemimpinan, dan Siklus Proses.
- Delapan prinsip ISO 31000 menjamin penciptaan dan perlindungan nilai organisasi secara berkelanjutan.
- ISO/IEC 27005:2018 adalah standar khusus untuk manajemen risiko keamanan informasi guna melindungi kerahasiaan, keutuhan, dan ketersediaan data (CIA Triad).
- • Tahapan ISO 27005 mencakup penetapan konteks, penilaian risiko (identifikasi, analisis, evaluasi), penanganan risiko, dan penerimaan risiko residu secara formal.

Soal Evaluasi Pemahaman BAB 2

1. Uraikan 3 pilar arsitektur dalam standar ISO 31000:2018 (Prinsip, Kerangka Kerja, dan Proses) dan jelaskan bagaimana ketiganya saling berinteraksi!
2. Sebutkan dan jelaskan secara ringkas 4 dari 8 Prinsip Manajemen Risiko menurut ISO 31000:2018!
3. Jelaskan hubungan fungsional antara standar ISO/IEC 27001 (Sistem Manajemen Keamanan Informasi) dan standar ISO/IEC 27005 (Manajemen Risiko Keamanan Informasi)!
4. Uraikan tahapan demi tahapan dalam siklus proses manajemen risiko keamanan informasi menurut ISO/IEC 27005:2018!

BAB 3: RISIKO KEAMANAN INFORMASI & PENYUSUNAN RISK REGISTER

Capaian Pembelajaran Bab (Bahan Kajian RPS)

1. Menganalisis pilar keamanan informasi CIA Triad (Confidentiality, Integrity, Availability) dan konsep Non-Repudiation dalam konteks ancaman digital.
2. Mengklasifikasikan jenis-jenis pengendalian internal (Internal Controls): Administratif, Teknis, dan Fisik, serta fungsi Preventif, Detektif, dan Korektif.
3. Menguasai metodologi identifikasi risiko: inventarisasi aset primer/pendukung, katalog ancaman (Threat Catalog), dan pemetaan kerentanan sistem.
4. Menyusun dokumen Risk Register standar enterprise sebagai instrumen pelacakan risiko dinamis (Living Document).
5. Menyelesaikan penugasan terstruktur resmi RPS: Penerapan Kerangka Kerja Manajemen Risiko Aset Informasi Berbasis ISO/IEC 27005 (Bobot 20% terpadu).

3.1 Pilar Keamanan Informasi: CIA Triad & Non-Repudiation

Keamanan informasi bertujuan melindungi aset data dari segala bentuk ancaman yang dapat merusak kelangsungan bisnis. Tiga pilar fundamental keamanan informasi (CIA Triad):

1. Kerahasiaan (Confidentiality): Menjamin bahwa informasi hanya dapat diakses oleh pihak, entitas, atau proses yang memiliki hak otorisasi resmi (misal: enkripsi basis data rekam medis, pembatasan hak akses berbasis peran / RBAC).
2. Keutuhan (Integrity): Menjamin akurasi, kelengkapan, dan keaslian data dari perubahan yang tidak sah atau manipulasi yang disengaja (misal: penggunaan cryptographic hash SHA-256, digital signature, dan kontrol validasi input).
3. Ketersediaan (Availability): Menjamin bahwa sistem informasi, server, dan data dapat diakses oleh pengguna yang berhak tepat

saat dibutuhkan (misal: redundansi server berkonfigurasi High Availability, proteksi anti-DDoS, dan pasokan cadangan UPS).

Aspek pendukung tambahan mencakup Non-Repudiation (Penyangkalan Tidak Sah), di mana pelaku transaksi digital tidak dapat menyangkal tindakan yang telah dilakukannya berkat adanya jejak audit forensik dan sertifikat digital.

3.2 Pengendalian Internal (Internal Controls) Sistem Informasi

Pengendalian internal adalah kebijakan, prosedur, dan mekanisme teknis yang dirancang untuk memberikan keyakinan memadai bahwa risiko dapat dicegah atau ditangani. Klasifikasi pengendalian internal:

A. Berdasarkan Karakteristik Implementasi:
   - Kontrol Administratif / Manajerial: Kebijakan tertulis, SOP operasi, pakta integritas karyawan, dan pelatihan Security Awareness rutin.
   - Kontrol Teknis / Logis: Konfigurasi Firewall, Intrusion Detection System (IDS), Enkripsi TLS 1.3, Multi-Factor Authentication (MFA), dan Sistem Manajemen Hak Akses (IAM).
   - Kontrol Fisik: Kartu akses pintu RFID ke ruang server, kamera CCTV 24/7, sensor pemadam api gas FM-200, dan pengunci rak server.
   - Berdasarkan Fungsi Waktu Aksi:
   - Kontrol Preventif (Mencegah): Memblokir terjadinya insiden sebelum terjadi (misal: Firewall memblokir port mencurigakan).
   - Kontrol Detektif (Mendeteksi): Mengidentifikasi dan membunyikan alarm saat insiden sedang terjadi (misal:

Sistem SIEM mendeteksi percobaan login gagal 100 kali berturut-turut).

- Kontrol Korektif (Memperbaiki): Memulihkan sistem ke kondisi normal setelah insiden terjadi (misal: Restore data dari backup cloud).

Konsep Defense-in-Depth (Pertahanan Berlapis)

Jangan pernah mengandalkan satu jenis kontrol saja! Kombinasikan kontrol administratif (kebijakan password), kontrol fisik (pintu server terkunci), dan kontrol teknis (enkripsi data) secara simultan untuk menciptakan lapisan perlindungan yang kokoh.

3.3 Metodologi Identifikasi Risiko & Skenario Ancaman

Proses identifikasi risiko sistem informasi mengikuti tahapan terstruktur ISO/IEC 27005:

1. Inventarisasi Aset Informasi: Membedakan antara Aset Primer (Data Bisnis, Proses Bisnis Kunci) dan Aset Pendukung (Hardware Server, Software OS/Aplikasi, Jaringan, Fasilitas Gedung, dan Personel SDM).
2. Identifikasi Ancaman (Threat Identification): Menggunakan basis data ancaman global (seperti MITRE ATT&CK atau katalog ENISA) untuk memetakan ancaman yang relevan (misal: Malware Ransomware, Ransom-DDoS, Orang Dalam / Insider Threat, Bencana Banjir).
3. Penilaian Kerentanan (Vulnerability Assessment): Mengidentifikasi celah kelemahan teknis menggunakan basis data CVE (Common Vulnerabilities and Exposures) dan pemindaian alat keamanan (seperti Nessus / OpenVAS).

3.4 Struktur & Anatomi Risk Register Enterprise

Risk Register adalah dokumen induk (Living Document) yang mencatat seluruh profil risiko organisasi secara transparan dan terukur. Struktur kolom standar Risk Register profesional mencakup:

1. ID Risiko (Unique Risk Identifier, misal: `RSK-IT-001`).
2. Deskripsi Skenario Risiko (Kondisi Sebab -> Peristiwa -> Dampak).
3. Aset Kritis & Pemilik Risiko (Asset Owner / Risk Owner).
4. Tingkat Risiko Inheren (Inherent Risk: Tingkat Kemungkinan dan Dampak SEBELUM kontrol diterapkan).
5. Pengendalian Eksisting (Existing Controls) & Evaluasi Efektivitasnya.
6. Tingkat Risiko Residu (Residual Risk: Tingkat Kemungkinan dan Dampak SETELAH kontrol diterapkan).
7. Rencana Tindakan Mitigasi (Risk Treatment Plan) & Target Waktu Penyelesaian (Target Deadline).

Risiko Inheren vs. Risiko Residu

• Risiko Inheren (Inherent Risk): Besaran risiko alamiah yang ada sebelum organisasi menerapkan kontrol keamanan apa pun.

• Risiko Residu (Residual Risk): Sisa risiko yang tetap ada setelah seluruh kontrol dan prosedur mitigasi diimplementasikan secara optimal.

Aktivitas Pembelajaran & Penugasan Terstruktur: LEMBAR KERJA 3 (TUGAS RPS MINGGU 9-11): Penyusunan Risk Register Enterprise

Kerjakan penugasan terstruktur kelompok untuk menyusun dokumen Risk Register aset teknologi informasi enterprise sesuai standar ISO/IEC 27005 (SubCPMK 3 | Bobot 20% terpadu).

Bagian A: Matriks Identifikasi Risiko & CIA Triad (Contoh Skenario)

Komponen / Parameter Risiko	Deskripsi / Isian Analisis
1. Risk ID & Nama Skenario:	RSK-SEC-01: Serangan Ransomware mengenkripsi Server Basis Data Transaksi
2. Aset Kritis Terdampak:	Server Database PostgreSQL (Aset Pendukung) & Data Saldo Nasabah (Aset Primer)
3. Dimensi CIA yang Terancam:	Ketersediaan (Availability) lumpuh & Keutuhan (Integrity) terancam enkripsi jahat
4. Ancaman & Kerentanan Utama:	Ancaman: Sindikat Phishing LockBit | Kerentanan: Port RDP 3389 terbuka ke internet
5. Risk Owner yang Bertanggung Jawab:	Kepala Divisi Infrastruktur & Keamanan TI (CISO / IT Security Lead)

Bagian B: Penetapan Skor Inheren, Kontrol Eksisting, & Residu

Komponen / Parameter Risiko	Deskripsi / Isian Analisis
Skor Risiko Inheren (Tanpa Kontrol):	Kemungkinan: 4 (Sering) x Dampak: 5 (Kritis) = Skor 20 (Risiko Sangat Tinggi - Merah)

Kontrol Eksisting Saat Ini:	Antivirus bawaan OS di server & backup manual mingguan ke harddisk eksternal
Efektivitas Kontrol Eksisting:	Kurang Memadai (Backup mingguan berisiko kehilangan data transaksi 7 hari)
Rencana Kontrol Tambahan (Treatment):	Tutup port RDP, pasang EDR (Endpoint Detection & Response), backup otomatis immutable 3-2-1
Target Skor Risiko Residu Pasca Mitigasi:	Kemungkinan: 2 (Jarang) x Dampak: 3 (Sedang) = Skor 6 (Risiko Rendah - Hijau)

Lembar Refleksi & Evaluasi Kasus:

1. Jelaskan mengapa suatu dokumen Risk Register tidak boleh bersifat statis (hanya dibuat saat audit) melainkan wajib diperbarui secara berkala sebagai dokumen hidup (Living Document):
2. Bagaimana strategi Anda dalam memastikan bahwa setiap butir risiko dalam Risk Register memiliki penanggung jawab yang jelas (Risk Owner)?

Rangkuman Eksekutif BAB 3

- Keamanan informasi berpusat pada perlindungan CIA Triad (Confidentiality, Integrity, Availability) dan Non-Repudiation.
- Pengendalian internal diklasifikasikan ke dalam Administratif, Teknis, dan Fisik, serta fungsi Preventif, Detektif, dan Korektif.
- Identifikasi risiko memetakan interaksi antara Aset bernilai, Ancaman eksternal/internal, dan Celah kerentanan sistem.
- • Risk Register adalah instrumen standar enterprise yang mendokumentasikan skenario risiko, risiko inheren, kontrol, risiko residu, dan penanggung jawab aksi.

Soal Evaluasi Pemahaman BAB 3

1. Uraikan ketiga dimensi dalam CIA Triad (Confidentiality, Integrity, Availability) beserta contoh serangan nyata yang mengancam masing-masing dimensi tersebut!
2. Jelaskan klasifikasi pengendalian internal sistem informasi berdasarkan fungsi waktu aksinya (Kontrol Preventif, Detektif, dan Korektif) disertai contoh implementasinya!
3. Apa yang dimaksud dengan konsep Defense-in-Depth dalam arsitektur keamanan informasi dan mengapa konsep ini sangat dianjurkan oleh standar ISO/IEC 27005?
4. Uraikan komponen-komponen kritis yang wajib ada di dalam sebuah tabel Risk Register enterprise dan jelaskan perbedaan mendasar antara Risiko Inheren dan Risiko Residu!

BAB 4: ANALISIS & EVALUASI RISIKO: KUALITATIF, SEMI-KUANTITATIF, & KUANTITATIF (ALE)

Capaian Pembelajaran Bab

1. Membedakan karakteristik, kelebihan, dan kelemahan metode analisis risiko Kualitatif, Semi-Kuantitatif, dan Kuantitatif penuh.
2. Merancang dan menerapkan Matriks Penilaian Risiko 5x5 (Heatmap Likelihood vs. Impact) untuk mengelompokkan tingkat keparahan risiko.
3. Menghitung metrik kerugian finansial kuantitatif secara presisi: Single Loss Expectancy (SLE), Annual Rate of Occurrence (ARO), dan Annualized Loss Expectancy (ALE).
4. Mengevaluasi kelayakan investasi keamanan TI menggunakan metode Analisis Biaya-Manfaat Kontrol (Cost-Benefit Analysis / Return on Security Investment - ROSI).
5. Menyelesaikan penugasan terstruktur resmi RPS: Analisis & Evaluasi Risiko Aset Sistem Informasi Organisasi (Bobot 20% terpadu).

4.1 Tiga Pendekatan Analisis Risiko Sistem Informasi

Setelah ancaman dan kerentanan aset diidentifikasi, tahap selanjutnya adalah mengukur besaran risiko melalui analisis risiko (Risk Analysis). Standar ISO/IEC 27005 membagi pendekatan analisis ke dalam 3 paradigma:

1. Analisis Kualitatif (Qualitative Risk Analysis): Menggunakan skala deskriptif kata-kata (Sangat Rendah, Rendah, Sedang, Tinggi, Ekstrem) berdasarkan pertimbangan para ahli (Expert Judgment). Sangat cepat, hemat biaya, dan ideal untuk risiko reputasi atau risiko kepatuhan hukum yang sulit dinilai dengan uang.
2. Analisis Semi-Kuantitatif (Semi-Quantitative Analysis): Memberikan skor numerik (misal: skala 1 sampai 5) pada variabel

probabilitas dan dampak untuk menghitung indeks skor gabungan tanpa mengonversinya menjadi nilai rupiah murni.

3. Analisis Kuantitatif Penuh (Quantitative Risk Analysis): Menggunakan data statistik frekuensi dan nilai moneter riil (Rupiah / Dollar) untuk menghitung potensi kerugian finansial tahunan secara eksak.

4.2 Analisis Kualitatif & Matriks Risiko 5x5 (Risk Heatmap)

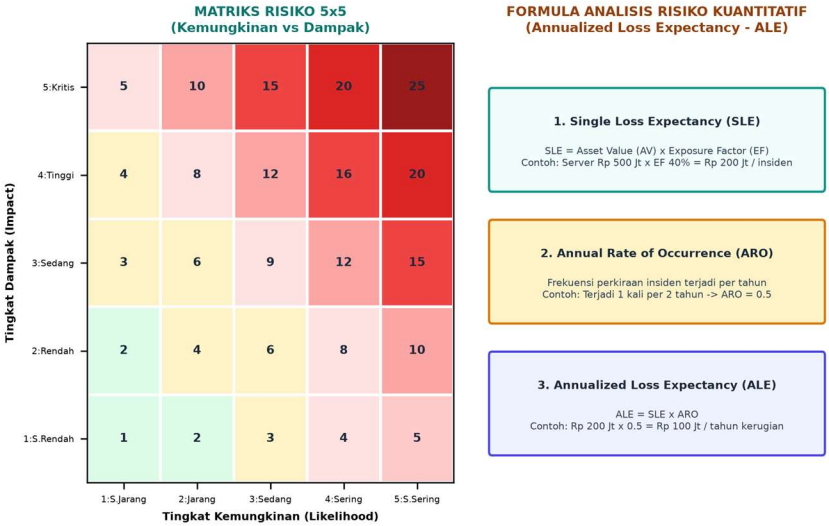
Matriks Risiko 5x5 menggabungkan dua sumbu pengukuran:

- Sumbu Horizontal - Tingkat Kemungkinan (Likelihood - L):
  1 = Sangat Jarang (< 1 kali per 5 tahun), 2 = Jarang (1 kali per 2-5 tahun), 3 = Sedang (1 kali per tahun), 4 = Sering (1 kali per bulan), 5 = Sangat Sering (Hampir setiap hari).
- Sumbu Vertikal - Tingkat Dampak Bisnis (Impact - I):
  1 = Sangat Rendah (< Rp 10 Jt), 2 = Rendah (Rp 10 - 50 Jt), 3 = Sedang (Rp 50 - 200 Jt), 4 = Tinggi (Rp 200 Jt - 1 Miliar), 5 = Kritis / Katastropik (> Rp 1 Miliar / Pidana Hukum).
- Indeks Tingkat Risiko dihitung dengan perkalian: `Skor Risiko = Likelihood x Impact` (Rentang nilai 1 hingga 25).
- Kategori Zona Keparahan:
- Zona Hijau (Skor 1 - 4): Risiko Rendah (Low) - Cukup dimonitor dalam operasional harian.
- Zona Kuning (Skor 5 - 9): Risiko Sedang (Medium) - Diperlukan tindakan perbaikan terjadwal.
- Zona Oranye/Merah Muda (Skor 10 - 14): Risiko Tinggi (High) - Membutuhkan rencana penanganan manajemen senior.
- Zona Merah Tua (Skor 15 - 25): Risiko Kritis (Critical / Extreme) - Membutuhkan tindakan mitigasi darurat segera sebelum sistem dihentikan sementara.

4.3 Analisis Kuantitatif Finansial: Formula SLE, ARO, & ALE

Analisis kuantitatif menjadi bahasa yang paling dipahami oleh jajaran Direksi Keuangan (CFO) karena menyajikan proyeksi kerugian dalam satuan mata uang (NIST SP 800-30):

1. Single Loss Expectancy (SLE): Total estimasi kerugian finansial yang timbul dari satu kali kejadian insiden tunggal:
   `SLE = Asset Value (AV) x Exposure Factor (EF)`
   - Asset Value (AV): Nilai penggantian aset atau nilai ekonomi aset bagi perusahaan.
   - Exposure Factor (EF): Persentase perkiraan kerusakan aset saat insiden terjadi (rentang 0% hingga 100%).
2. Annual Rate of Occurrence (ARO): Estimasi jumlah frekuensi keterjadian insiden yang sama dalam kurun waktu satu tahun (misal: terjadi 2 kali setahun -> `ARO = 2.0`; terjadi sekali setiap 4 tahun -> `ARO = 0.25`).
3. Annualized Loss Expectancy (ALE): Total kerugian finansial tahunan yang diproyeksikan dari skenario risiko tersebut:
   `ALE = SLE x ARO`



Gambar 4.1: Matriks Analisis Risiko 5x5 & Formula Kuantitatif ALE (SLE x ARO)

[STUDI KASUS & SIMULASI RISIKO] Contoh Perhitungan ALE Kasus Serangan Siber pada Server E-Commerce

- Nilai Aset Server & Basis Data (AV) = Rp 800.000.000
- Exposure Factor Serangan Ransomware (EF) = 50% (Kerugian data & downtime)
- SLE = Rp 800.000.000 x 50% = Rp 400.000.000 per insiden
- Frekuensi Perkiraan Terjadi (ARO) = 0.5 (Satu kali insiden per 2 tahun)
- Proyeksi Kerugian Tahunan (ALE) = Rp 400.000.000 x 0.5 = Rp 200.000.000 / Tahun!

4.4 Analisis Biaya-Manfaat Kontrol (Cost-Benefit Analysis / CBA)

Manajemen tidak boleh membeli sistem keamanan yang biayanya lebih mahal daripada potensi kerugian yang dicegahnya. Kelayakan investasi kontrol keamanan dihitung dengan formula Cost-Benefit Analysis (CBA):

`Nilai Manfaat Bersih (CBA) = (ALE Awal - ALE Pasca Kontrol) - Biaya Tahunan Kontrol (ACS)`

- Jika nilai `CBA > 0`, maka investasi kontrol keamanan dinilai SANGAT LAYAK (Memberikan penghematan bersih).
- Jika nilai `CBA < 0`, maka kontrol dinilai terlalu mahal (Over-Engineered) dan harus dicari alternatif kontrol yang lebih efisien.

Aktivitas Pembelajaran & Penugasan Terstruktur: LEMBAR KERJA 4 (TUGAS RPS MINGGU 12-14): Analisis Risiko Kuantitatif ALE & Matriks 5x5

Lakukan simulasi analisis risiko kuantitatif (SLE, ARO, ALE) dan hitung Cost-Benefit Analysis (CBA) kontrol keamanan pada skenario sistem enterprise kelompok Anda (SubCPMK 4 | Bobot 20% terpadu).

Bagian A: Perhitungan Kuantitatif ALE Skenario Kebocoran Data (Sebelum Kontrol)

Komponen / Parameter Risiko	Deskripsi / Isian Analisis
1. Nilai Aset Total (Asset Value - AV):	Rp 1.200.000.000 (Sistem Transaksi Gateway Pembayaran)
2. Faktor Paparan Kerusakan (Exposure Factor - EF):	60% (Kerusakan operasional, denda regulasi, & kompensasi pelanggan)
3. Single Loss Expectancy (SLE = AV x EF):	Rp 1.200.000.000 x 60% = Rp 720.000.000 per insiden
4. Perkiraan Frekuensi Tahunan (ARO):	0.5 (Perkiraan terjadi 1 kali dalam 2 tahun)
5. Proyeksi Kerugian Tahunan Awal (ALE Awal):	ALE Awal = Rp 720.000.000 x 0.5 = Rp 360.000.000 per tahun

Bagian B: Analisis Biaya-Manfaat Kontrol Keamanan (Setelah Kontrol)

Komponen / Parameter Risiko	Deskripsi / Isian Analisis
Penerapan Kontrol Keamanan Baru:	Langganan Web Application Firewall (WAF) Cloud & Layanan SOC 24/7

Komponen / Parameter Risiko	Deskripsi / Isian Analisis
Biaya Tahunan Kontrol (Annual Cost of Safeguard - ACS):	Rp 60.000.000 per tahun
Proyeksi ALE Pasca Kontrol (ALE Baru):	Rp 36.000.000 per tahun (Tingkat keterjadian dan dampak ditekan 90%)
Penghematan Kerugian Kotor (ALE Awal - ALE Baru):	Rp 360.000.000 - Rp 36.000.000 = Rp 324.000.000 per tahun
Nilai Manfaat Bersih Investasi (CBA):	CBA = Rp 324.000.000 - Rp 60.000.000 = + Rp 264.000.000 (SANGAT LAYAK)

Lembar Refleksi & Evaluasi Kasus:

1. Jelaskan bagaimana analis risiko TI meyakinkan jajaran Dewan Direksi (C-Level) mengenai urgensi penganggaran kontrol keamanan menggunakan bahasa finansial ALE dan CBA:
2. Mengapa analisis risiko kualitatif matriks 5x5 tetap sangat dibutuhkan meskipun suatu organisasi sudah mampu melakukan perhitungan kuantitatif ALE?

Rangkuman Eksekutif BAB 4

Analisis risiko terdiri atas metode Kualitatif deskriptif, Semi-Kuantitatif skor, dan Kuantitatif finansial penuh.

- Matriks 5x5 memetakan Likelihood vs Impact untuk membagi risiko ke dalam zona Hijau, Kuning, Oranye, dan Merah Kritis.
- Formula kuantitatif: SLE = AV x EF; ALE = SLE x ARO mengukur potensi kerugian moneter tahunan dalam satuan rupiah.
- • Cost-Benefit Analysis (CBA) memastikan bahwa biaya investasi kontrol keamanan tidak melebihi nilai kerugian yang dicegahnya.

Soal Evaluasi Pemahaman BAB 4

1. Bandingkan kelebihan dan kelemahan antara metode analisis risiko kualitatif (Matriks 5x5) dan metode analisis risiko kuantitatif (ALE)!
2. Sebuah perusahaan e-commerce memiliki aset server senilai Rp 1.500.000.000. Jika terjadi kegagalan sistem akibat lonjakan traffic, exposure factor diperkirakan sebesar 40% dan insiden tersebut diproyeksikan terjadi 2 kali dalam setahun. Hitunglah nilai SLE dan ALE-nya!
3. Berdasarkan soal nomor 2 di atas, perusahaan berencana menyewa server cadangan autoscaling seharga Rp 120.000.000 per tahun yang mampu mereduksi nilai ALE menjadi Rp 50.000.000. Hitunglah nilai Cost-Benefit Analysis (CBA) investasi tersebut dan simpulkan kelayakannya!
4. Bagaimana analis risiko menentukan batas toleransi zona merah pada Matriks Risiko 5x5 berdasarkan Risk Appetite organisasi?

BAB 5: STRATEGI PENANGANAN RISIKO (4T), BCP, & DISASTER RECOVERY PLAN (DRP)

Capaian Pembelajaran Bab (Bahan Kajian RPS)

1. Menguasai 4 opsi strategis penanganan risiko (The 4T Framework): Treat (Mitigasi), Tolerate (Terima), Transfer (Bagi), dan Terminate (Hindari).
2. Menyusun Rencana Perlakuan Risiko (Risk Treatment Plan) yang memuat kontrol keamanan prioritas, alokasi anggaran, dan penanggung jawab.
3. Merancang dokumen Business Continuity Plan (BCP) berbasis Business Impact Analysis (BIA) untuk menjamin kelangsungan operasional bisnis saat krisis.
4. Menetapkan metrik pemulihan infrastruktur TI pada Disaster Recovery Plan (DRP): Recovery Time Objective (RTO) dan Recovery Point Objective (RPO).
5. Membandingkan opsi Disaster Recovery Site (Hot Site, Warm Site, Cold Site, dan Cloud DR) berdasarkan efisiensi biaya dan kecepatan pemulihan.
6. Menyelesaikan penugasan terstruktur resmi RPS: Perancangan Risk Response Terhadap Hasil Analisis Risiko (Bobot 20%) dan Portofolio Ujian Akhir Semester (UAS - Bobot 25% kumulatif).

5.1 Empat Opsi Strategis Penanganan Risiko (The 4T Framework)

Setelah seluruh risiko dievaluasi pada matriks tingkat keparahan, organisasi wajib menetapkan opsi perlakuan risiko (Risk Treatment). Standar ISO 31000 dan kerangka kerja tata kelola global merangkum opsi penanganan risiko ke dalam Kerangka Kerja 4T:

1. Treat / Mitigate (Modifikasi Risiko): Menerapkan kontrol keamanan tambahan untuk mereduksi tingkat probabilitas keterjadian atau memperkecil dampak kerugian (misal: memasang firewall generasi baru, enkripsi database, dan pelatihan phishing karyawan).
2. Tolerate / Accept (Menerima Risiko): Membiarkan risiko tetap ada tanpa kontrol tambahan karena biaya mitigasi lebih mahal

daripada potensi kerugian atau karena tingkat risiko residu sudah berada di bawah batas Risk Appetite organisasi (harus disetujui secara tertulis oleh Direksi).

3. Transfer / Share (Mengalihkan Risiko): Membagi konsekuensi kerugian finansial kepada pihak ketiga (misal: membeli Polis Asuransi Siber / Cyber Insurance atau mengalihkan pengelolaan server ke penyedia cloud dengan perjanjian Service Level Agreement - SLA 99.99%).
4. Terminate / Avoid (Menghindari Risiko): Menghentikan aktivitas, proyek, atau proses bisnis yang memicu risiko tersebut karena tingkat risikonya terlalu berbahaya dan tidak dapat dimitigasi secara ekonomis (misal: membatalkan peluncuran fitur pembayaran kripto karena ketidakpastian regulasi dan tingginya ancaman fraud).

5.2 Perancangan Business Continuity Plan (BCP)

Business Continuity Plan (BCP) adalah rencana strategis menyeluruh yang mendokumentasikan prosedur kontinjensi agar fungsi-fungsi bisnis esensial organisasi dapat terus beroperasi selama dan setelah terjadinya bencana besar (seperti gempa bumi, kebakaran gedung, atau serangan siber masif).

Langkah Kunci Penyusunan BCP:

1. Business Impact Analysis (BIA): Mengidentifikasi fungsi bisnis kritis perusahaan, mengevaluasi dampak finansial/operasional akibat terhentinya proses bisnis, serta menentukan urutan prioritas pemulihan (Recovery Priority).
2. Prosedur Kontinjensi Operasional: Menyiapkan alur kerja manual darurat jika seluruh sistem komputer mengalami padam total

(misal: pencatatan transaksi manual berbasis kertas saat sistem perbankan offline).

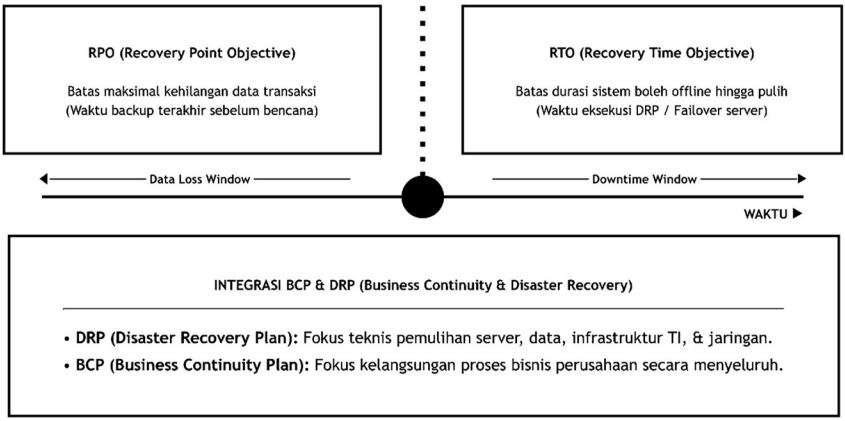
3. Struktur Tim Manajemen Krisis: Menetapkan komando kepemimpinan, protokol evakuasi, dan saluran komunikasi resmi kepada media dan publik.

5.3 Perancangan Disaster Recovery Plan (DRP): RTO & RPO

Jika BCP berfokus pada kelangsungan bisnis secara luas, maka Disaster Recovery Plan (DRP) berfokus secara teknis pada pemulihan infrastruktur teknologi informasi, pusat data (Data Center), server, basis data, dan jaringan komunikasi pasca-bencana.

Dua Parameter Kritis DRP:

1. Recovery Point Objective (RPO): Batas toleransi maksimal kehilangan data transaksi yang dapat diterima oleh organisasi, diukur dalam satuan waktu ke belakang dari saat bencana terjadi. RPO menentukan seberapa sering backup data harus dilakukan (misal: RPO = 1 Jam berarti backup harus dieksekusi setiap jam; kehilangan data transaksi > 1 jam tidak dapat ditolerir).
2. Recovery Time Objective (RTO): Batas toleransi durasi waktu maksimal di mana sistem komputer diperbolehkan offline sebelum layanan berhasil dipulihkan sepenuhnya ke kondisi normal (misal: RTO = 4 Jam berarti server cadangan harus sudah aktif dan melayani pengguna dalam waktu kurang dari 4 jam pasca-insiden).



Gambar 5.1: Arsitektur BCP, DRP, Timeline Pemulihan Bencana, RTO, dan RPO

Trade-Off RTO/RPO vs. Biaya Infrastruktur

Semakin mendekati nol target RTO dan RPO (Zero Data Loss & Instant Recovery), semakin mahal biaya investasi teknologi yang dibutuhkan (memerlukan replikasi sinkron real-time dan redundant data center aktif-aktif)!

5.4 Alternatif Lokasi Pemulihan Bencana (Disaster Recovery Site)

Untuk mengantisipasi kehancuran fisik data center utama, organisasi menyiapkan lokasi pemulihan cadangan (Disaster Recovery Center / DRC):

1. Hot Site: Fasilitas DRC yang memiliki perangkat keras identik, jaringan aktif, dan replikasi data transaksi secara real-time. Waktu pemulihan instan (RTO hitungan menit/detik), namun biaya operasional sangat mahal.
2. Warm Site: Fasilitas DRC yang sudah dilengkapi server dan jaringan, namun data terbaru harus direstore terlebih dahulu dari

backup terakhir. Waktu pemulihan hitungan beberapa jam (RTO 4 - 24 Jam), dengan biaya menengah.

3. Cold Site: Fasilitas gedung kosong yang hanya menyediakan ruang, listrik, dan pendingin tanpa perangkat keras komputer. Waktu pemulihan lama (RTO hitungan hari/minggu), namun biaya sangat murah.
4. Cloud Disaster Recovery (Cloud DR / DRaaS): Memanfaatkan infrastruktur cloud publik (AWS/Azure/GCP) untuk replikasi data dinamis dengan model biaya berbasis pemakaian (Pay-as-you-go), menawarkan kombinasi RTO rendah dan efisiensi biaya yang optimal bagi enterprise modern.

Aktivitas Pembelajaran & Penugasan Terstruktur: LEMBAR KERJA 5 (TUGAS RPS MINGGU 15-16 & EVALUASI UAS): Perancangan Risk Response & BCP/DRP

Susun matriks strategi penanganan risiko (4T) dan rancang arsitektur BCP/DRP lengkap dengan target RTO dan RPO untuk sistem informasi enterprise kelompok Anda sebagai syarat kelulusan Ujian Akhir Semester (UAS - Bobot 25% kumulatif).

Bagian A: Matriks Rencana Perlakuan Risiko (Risk Treatment Plan)

Komponen / Parameter Risiko	Deskripsi / Isian Analisis
1. Skenario Risiko yang Ditangani:	RSK-01: Kegagalan Total Data Center Utama akibat Banjir Bandang
2. Opsi Strategi Penanganan (4T):	Kombinasi TREAT (Mitigasi Teknis) dan TRANSFER (Asuransi Operasional)
3. Kontrol Mitigasi yang Diterapkan:	Membangun Cloud DR Site di wilayah geografis berbeda (Surabaya - Jakarta)
4. Penanggung Jawab Eksekusi (Risk Owner):	Kepala Unit Pusat Data & Disaster Recovery Officer
5. Anggaran Investasi & Target Waktu:	Rp 150.000.000 / tahun | Implementasi selesai dalam 3 bulan

Bagian B: Spesifikasi Parameter BCP & Disaster Recovery Plan (DRP)

Komponen / Parameter Risiko	**Deskripsi / Isian Analisis**
Target Recovery Point Objective (RPO):	RPO = 15 Menit (Replikasi data asinkron antar-region setiap 15 menit)
Target Recovery Time Objective (RTO):	RTO = 2 Jam (Failover otomatis DNS dan pengaktifan cluster server di DRC)

Komponen / Parameter Risiko	Deskripsi / Isian Analisis
Tipe Lokasi Cadangan (DR Site):	Cloud Hybrid Hot/Warm Site (Multi-Region Cloud Infrastructure)
Jadwal Pengujian Simulasi Bencana (DR Drill):	Dilakukan simulasi pengalihan sistem (Drill Test) setiap 6 bulan sekali
Status Kesiapan Portofolio Akhir UAS:	Dokumen Manajemen Risiko TI Komprehensif 100% Siap Dipresentasikan

Lembar Refleksi & Evaluasi Kasus:

1. Jelaskan bagaimana keterkaitan yang harmonis antara Business Continuity Plan (BCP) dan Disaster Recovery Plan (DRP) mampu menyelamatkan reputasi dan kelangsungan hidup sebuah bank saat terjadi insiden padam listrik massal (Blackout):

.....

2. Susun dokumen portofolio komprehensif penanganan risiko TI kelompok Anda sebagai pemenuhan tugas akhir evaluasi kelulusan UAS!

Rangkuman Eksekutif BAB 5

- Kerangka 4T membagi opsi penanganan risiko menjadi: Treat (Mitigasi Kontrol), Tolerate (Terima Residu), Transfer (Alihkan Asuransi/SLA), dan Terminate (Hentikan Aktivitas).
- Business Continuity Plan (BCP) menjamin kelangsungan operasional bisnis esensial berbasis analisis dampak bisnis (BIA).
- Disaster Recovery Plan (DRP) memulihkan infrastruktur TI teknis dengan parameter kunci RTO (Batas Waktu Downtime) dan RPO (Batas Kehilangan Data).
- Pilihan DR Site mencakup Hot Site, Warm Site, Cold Site, dan Cloud DR yang disesuaikan dengan kebutuhan RTO/RPO dan anggaran organisasi.

Soal Evaluasi Pemahaman BAB 5

1. Uraikan 4 opsi strategi penanganan risiko dalam The 4T Framework (Treat, Tolerate, Transfer, Terminate) beserta masing-masing 1 contoh penerapannya dalam tata kelola TI enterprise!
2. Jelaskan perbedaan mendasar antara Business Continuity Plan (BCP) dan Disaster Recovery Plan (DRP) serta bagaimana keduanya saling melengkapi saat terjadi krisis!
3. Apa yang dimaksud dengan Recovery Time Objective (RTO) dan Recovery Point Objective (RPO)? Gambarkan hubungan keduanya dalam grafik timeline kejadian bencana!
4. Bandingkan karakteristik fasilitas Hot Site, Warm Site, dan Cloud Disaster Recovery (DRaaS) dalam aspek kecepatan pemulihan dan efisiensi biaya investasi!

GLOSARIUM ISTILAH MANAJEMEN RISIKO TEKNOLOGI INFORMASI (A - Z)

Annual Rate of Occurrence (ARO)	Estimasi frekuensi keterjadian suatu peristiwa risiko tertentu dalam kurun waktu satu tahun kalender.
Annualized Loss Expectancy (ALE)	Proyeksi total kerugian finansial tahunan yang diharapkan dari suatu skenario risiko tertentu, dihitung dengan rumus: ALE = SLE x ARO.
Asset Value (AV)	Total nilai ekonomi moneter dari suatu aset sistem informasi, mencakup biaya pengadaan, nilai data, dan biaya kerugian reputasi jika aset tersebut rusak.
Business Continuity Plan (BCP)	Rencana strategis komprehensif yang mendokumentasikan prosedur darurat agar operasional bisnis esensial organisasi dapat terus berjalan saat terjadi bencana.
Business Impact Analysis (BIA)	Proses sistematis untuk mengidentifikasi fungsi bisnis kritis dan mengevaluasi dampak operasional maupun finansial jika terjadi gangguan pada fungsi tersebut.
CIA Triad	Tiga pilar fundamental keamanan informasi yang mencakup Kerahasiaan (Confidentiality), Keutuhan (Integrity), dan Ketersediaan (Availability).
Cold Site	Fasilitas pemulihan bencana fisik yang menyediakan gedung, daya listrik, dan pendingin tanpa perangkat keras komputer atau data cadangan siap pakai.
Compliance Risk	Risiko terjadinya sanksi hukum, denda finansial, atau pencabutan izin usaha akibat kegagalan organisasi mematuhi undang-undang dan regulasi yang berlaku.
Cost-Benefit Analysis (CBA)	Evaluasi kelayakan finansial dari suatu kontrol keamanan untuk memastikan bahwa biaya tahunan kontrol lebih kecil daripada penghematan kerugian yang dihasilkannya.
Disaster Recovery Plan (DRP)	Rencana teknis terperinci untuk memulihkan infrastruktur teknologi informasi, pusat data (data center), server, dan jaringan setelah terjadinya bencana.

Exposure Factor (EF)	Persentase besarnya kerugian atau kerusakan pada nilai aset yang diakibatkan oleh satu kali insiden ancaman tertentu (rentang 0% s.d. 100%).
Hot Site	Fasilitas pusat data cadangan yang memiliki perangkat keras identik dan replikasi data real-time, siap mengambil alih operasional secara instan pasca-bencana.
Inherent Risk (Risiko Inheren)	Tingkat besaran risiko alamiah yang ada pada suatu sistem sebelum organisasi menerapkan kontrol atau tindakan mitigasi apa pun.
ISO 31000:2018	Standar internasional yang menyediakan prinsip, kerangka kerja, dan proses panduan umum manajemen risiko enterprise secara terintegrasi.
ISO/IEC 27005:2018	Standar internasional khusus yang menyediakan panduan terstruktur mengenai proses manajemen risiko keamanan informasi (Information Security Risk Management).
Likelihood (Kemungkinan)	Peluang atau probabilitas terjadinya suatu peristiwa ancaman siber atau kegagalan sistem dalam kurun waktu tertentu.
Non-Repudiation	Jaminan bahwa pelaku suatu tindakan atau transaksi digital tidak dapat menyangkal keaslian dan keterlibatannya berkat adanya jejak audit forensik.
Recovery Point Objective (RPO)	Batas maksimal kehilangan data transaksi yang masih dapat ditoleransi organisasi pasca-insiden (menentukan frekuensi backup data).
Recovery Time Objective (RTO)	Batas waktu durasi maksimal sistem informasi diperbolehkan offline sebelum layanan berhasil dipulihkan ke kondisi operasional normal.
Residual Risk (Risiko Residu)	Sisa tingkat risiko yang tetap tertinggal setelah seluruh kontrol keamanan dan tindakan mitigasi diimplementasikan secara optimal.
Risk Appetite	Tingkat dan jenis risiko yang siap diambil atau diterima oleh manajemen puncak organisasi dalam rangka mencapai tujuan strategisnya.

Risk Assessment	Keseluruhan proses terstruktur yang mencakup identifikasi risiko, analisis risiko, dan evaluasi risiko terhadap kriteria selera risiko organisasi.
Risk Owner (Pemilik Risiko)	Individu atau unit kerja manajerial yang memiliki wewenang dan akuntabilitas untuk mengelola dan memantau risiko tertentu.
Risk Register	Dokumen induk resmi organisasi yang mencatat seluruh profil risiko teridentifikasi, skor keparahan, kontrol eksisting, dan rencana perlakuan mitigasi.
Risk Tolerance	Batas variasi deviasi maksimal dari pencapaian sasaran yang masih dapat diterima oleh organisasi sebelum tindakan darurat wajib diambil.
Single Loss Expectancy (SLE)	Total estimasi kerugian finansial yang timbul dari satu kali kejadian insiden tunggal, dihitung dengan rumus: SLE = AV x EF.
Threat (Ancaman)	Potensi penyebab terjadinya insiden yang tidak diinginkan yang dapat menimbulkan kerugian pada sistem informasi atau organisasi.
Three Lines Model	Model tata kelola organisasi modern (IIA 2020) yang membagi peran Lini 1 (Operasional), Lini 2 (Manajemen Risiko & Kepatuhan), dan Lini 3 (Audit Internal).
Vulnerability (Kerentanan)	Kelemahan atau celah pada aset, desain arsitektur, konfigurasi teknis, atau prosedur organisasi yang dapat dieksploitasi oleh ancaman.
Warm Site	Fasilitas pemulihan bencana yang sudah dilengkapi perangkat keras dan jaringan, namun memerlukan proses restore data cadangan sebelum dapat beroperasi penuh.

RUBRIK PENILAIAN & MATRIKS KORELASI TUGAS RPS (BOBOT TOTAL 100%)

Evaluasi pembelajaran Mata Kuliah Manajemen Risiko TI (Kode MK: 25136036) mengacu pada matriks penugasan resmi RPS Kurikulum 2025 ITATS:

1. Matriks Evaluasi Penugasan Terstruktur RPS (Bobot Total 100%)

	Komponen Penilaian RPS	Bobot	Indikator Penilaian & Artefak Tugas
1.	Kuis - Pemahaman Konsep Manajemen Risiko TI (SubCPMK 1 | M1-4)	5%	Mengukur pemahaman teoritis mengenai definisi risiko, taksonomi risiko TI, prinsip tata kelola, dan Three Lines of Defense.
2.	Resume Jurnal Ilmiah Standar Manajemen Risiko (SubCPMK 1 | M1-4)	5%	Kemampuan menelaah, merangkum, dan menganalisis artikel jurnal ilmiah bereputasi mengenai penerapan standar manajemen risiko TI.
3.	Resume Video Mitigasi Risiko Aset Informasi (SubCPMK 1 | M1-4)	5%	Kemampuan merangkum secara kritis langkah-langkah mitigasi risiko aset informasi dan praktik terbaik keamanan siber dari materi video studi kasus.
4.	Perancangan Risk Response Terhadap Analisa Risiko (SubCPMK 2, 4, 5)	20%	Kemampuan menyusun strategi mitigasi (opsi 4T), rencana aksi konkret, dan penetapan parameter kontinuitas sistem (BCP/DRP, RTO, RPO).
5.	Penerapan Manajemen Risiko TI dengan ISO 31000 (SubCPMK 3, 4, 5)	25%	Keterampilan mengimplementasikan 8 prinsip ISO 31000, integrasi kepemimpinan, dan siklus proses penilaian risiko enterprise.

Komponen Penilaian RPS	Bobot	Indikator Penilaian & Artefak Tugas
6. Manajemen Risiko Aset Informasi Berbasis ISO/IEC 27005 (SubCPMK 2, 3, 4, 5)	40%	Penguasaan komprehensif identifikasi aset CIA Triad, analisis kuantitatif ALE, penyusunan Risk Register lengkap, dan laporan evaluasi risiko akhir.

2. Skala Konversi Nilai & Standar Capaian Pembelajaran

Rentang Nilai & Huruf	Deskripsi Kualitatif Capaian
Sangat Baik (A: 85 - 100)	Penguasaan konsep sangat mendalam, analisis risiko kuantitatif (ALE/CBA) dan matriks 5x5 sangat akurat, dokumen Risk Register dan BCP/DRP tersusun profesional sesuai standar ISO 31000/27005.
Baik (B: 70 - 84)	Analisis risiko logis dan terstruktur, pemahaman standar ISO tepat, perhitungan SLE/ARO/ALE benar, dokumen penugasan lengkap.
Cukup (C: 55 - 69)	Konsep risiko dipahami secara umum, namun identifikasi kerentanan/ancaman kurang tajam atau perhitungan kuantitatif memiliki kekeliruan minor.
Kurang (D/E: < 55)	Gagal mengidentifikasi profil risiko aset secara memadai, tidak mampu menyusun Risk Register, atau tidak mengumpulkan laporan penugasan resmi RPS.

DAFTAR PUSTAKA UTAMA SESUAI RPS RESMI

International Organization for Standardization. (2018). ISO 31000:2018 – Risk management – Guidelines. Geneva: ISO. [Pustaka Utama RPS]

International Organization for Standardization. (2018). ISO/IEC 27005:2018 – Information technology – Security techniques – Information security risk management. Geneva: ISO. [Pustaka Utama RPS]

National Institute of Standards and Technology. (2012). NIST SP 800-30 Rev. 1: Guide for Conducting Risk Assessments. Gaithersburg, MD: NIST.

ISACA. (2019). COBIT 2019 Framework: Governance and Management Objectives (APO12 - Managed Risk). Rolling Meadows, IL: ISACA.

The Institute of Internal Auditors (IIA). (2020). The IIA's Three Lines Model: An update of the Three Lines of Defense. Lake Mary, FL: IIA.

International Organization for Standardization. (2019). ISO 22301:2019 – Security and resilience – Business continuity management systems – Requirements. Geneva: ISO.

PROFIL DOSEN PENGEMBANG RPS & PENGAMPU

Adib Pakarbudi, S.Kom., M.Kom.
Dosen Pengembang Rencana Pembelajaran Semester (RPS), Koordinator Rumpun Mata Kuliah Sistem Informasi, dan Dosen Pengampu Mata Kuliah Manajemen Risiko TI serta Manajemen Proses Bisnis pada Program Studi S1 Sistem Informasi, Fakultas Teknik Elektro dan Teknologi Informasi, Institut Teknologi Adhi Tama Surabaya (ITATS).

PANDUAN TATA KELOLA & MANAJEMEN RISIKO TEKNOLOGI INFORMASI ENTERPRISE

Buku modul ini menyajikan panduan terstruktur tata kelola dan manajemen risiko TI enterprise, mulai dari konsep Three Lines Model, integrasi standar ISO 31000:2018 & ISO/IEC 27005:2018, perlindungan keamanan CIA Triad, penyusunan Risk Register, analisis kualitatif matriks 5×5 hingga kuantitatif ALE, serta perancangan strategi mitigasi melalui Business Continuity Plan (BCP) dan Disaster Recovery Plan (DRP).

- Konsep Dasar Risiko TI & Model Three Lines of Defense
- Kerangka Kerja Standar Global: ISO 31000 & ISO/IEC 27005
- Risiko Keamanan Informasi (CIA Triad) & Risk Register
- Analisis Risiko: Kualitatif (Matriks 5×5) & Kuantitatif (ALE/CBA)
- Strategi Penanganan Risiko (4T) serta Perancangan BCP & DRP

IT Risk Analyst • IT Governance Officer • Information Security Specialist • IT Auditor

Diterbitkan oleh Program Studi S1 Sistem Informasi ITATS