ASP4134 - Audit Sistem Informasi

Pertemuan V:
Information Systems Operation & Business Resillience

Confidential. Terbatas untuk mahasiswa PKN STAN

AGENDA

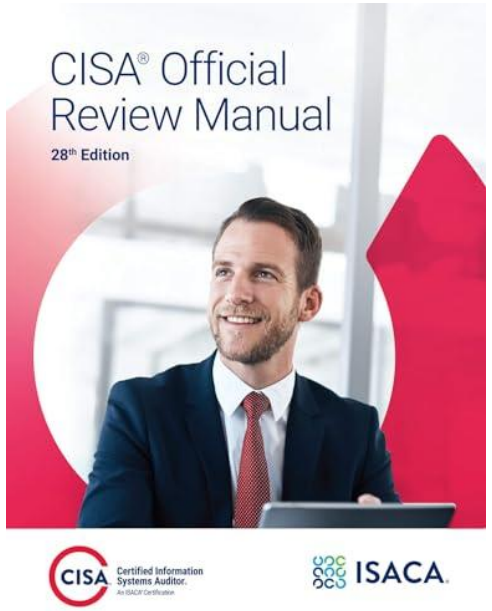
- Lecture: Auditing IT Operation

ASP4134 - Audit Sistem Informasi

Key objectives:

1. memahami kerangka **konsep audit tata kelola** teknologi informasi berdasarkan standar tata Kelola
2. menyusun **program audit tata kelola** sistem informasi
3. menyusun **laporan audit tata kelola** sistem informasi
4. melakukan **audit atas perolehan, pengembangan, dan implementasi sistem informasi**
5. melaksanakan **pengauditan atas pengoperasian dan pemeliharaan** atas sistem informasi  Here we are
6. melakukan **pengauditan atas keamanan informasi**
7. menggunakan **Teknik Audit Berbantuan Komputer** dalam pengujian pengendalian dan pengujian substantif
8. menjelaskan dampak kelemahan **pengendalian umum dan pengendalian aplikasi** terhadap peluang terjadinya kecurangan dan kesalahan saji pada laporan keuangan

Referensi

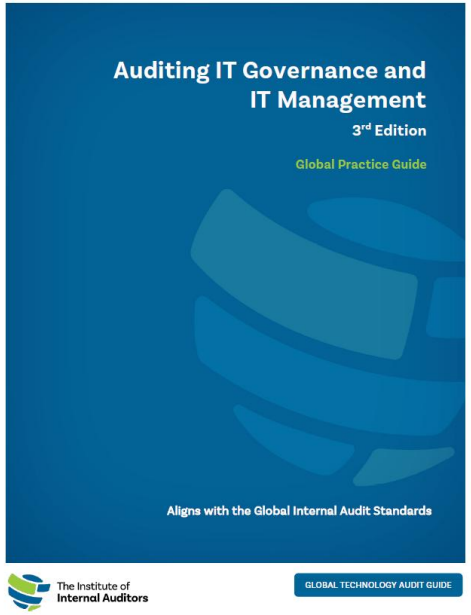


1

Useful references for this topic

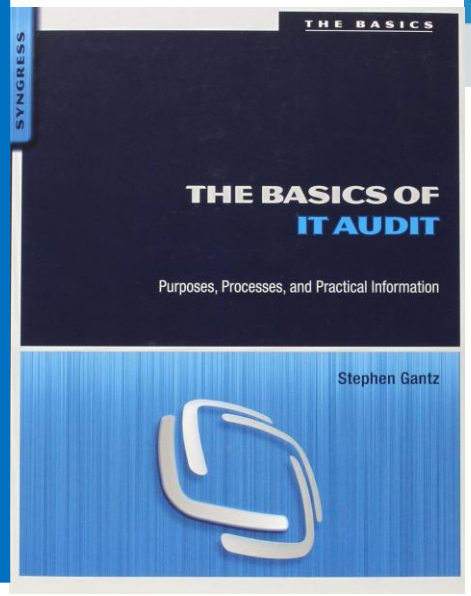
2

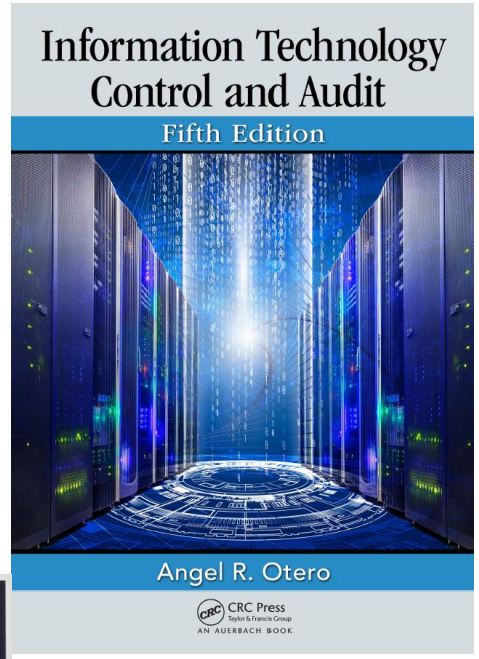




3

4





5

Information Systems Operations

1. IT Components

The most common elements in IT operations:

- **Infrastructure** – hardware, software , networks, data centers and cloud services
- **Network** – routers, switches, firewalls, load balancers, VPN concentrators, network cables and satellite communication equipment.
- **Applications and software** – OS, applications, database and middleware
- **System monitoring and management** – monitoring tools, log analysis, event management and proactive issue detection and resolution
- **Backup and disaster recovery** – reliable backup system, DRPs, and data replication
- **Virtualization and cloud computing** – IaaS, PaaS and SaaS
- **Documentation and knowledge management** – comprehensive documentation of IT systems, configurations and processes and effective knowledge management practices

1. IT Components – Risk & Control

Risiko	Pengendalian	Fokus Audit
• Kerusakan hardware (disk failure, overheating) • Bottleneck CPU/RAM/I/O • Single point of failure (SPOF) • Misconfiguration • Downtime pada perangkat jaringan • Cloud mismanagement (IAM salah konfigurasi)	• Redundancy • Preventive maintenance • Hardware replacement log • Monitoring 24/7 • Standard hardening guide • Standarisasi arsitektur. • Dokumentasi konfigurasi. • Asset inventory & CMDB.	• Kelengkapan inventaris aset TI (hardware/software). • Kontrol keamanan fisik & logis. • Dokumentasi konfigurasi. • Review CMDB dengan kondisi real

2. IT Asset Management

Mengelola aset TI sepanjang **life cycle** dari:

. pengadaan → penggunaan → perawatan → disposal .

The **first step in IT asset management** is the process of identifying and creating an **inventory of IT assets**.

Atribut penting:

- Owner, custodian
- Lokasi
- Klasifikasi keamanan
- Nilai bisnis
- Prioritas pemulihan
- Compliance (lisensi software)
- Status aset (aktif, rusak, retired)

2. IT Asset Management – Risk & Control

Risiko	Pengendalian	Fokus Audit
• Aset hilang/tidak tercatat -> risiko keamanan & finansial. • Software tanpa lisensi -> legal exposure. • Aset critical tidak di-maintain -> downtime. • Data tidak dihapus saat disposal -> data leakage.	• Register aset / CMDB. • Barcode/QR tagging. • Prosedur disposal (secure wipe, destruction). • Software Asset Management (SAM). • Periodic asset reconciliation.	• Cocokkan fisik perangkat vs CMDB. • Periksa lisensi software & bukti pembelian. • Periksa prosedur disposal & bukti pemusnahan. • Pastikan penetapan owner & kategori criticality.

3. Job Scheduling and Production Process Automation

Menjalankan proses rutin (batch) seperti: backup harian, batch payroll, data sync, report generation.

Advantages job scheduling software:

- Job information is set up only once, reducing reliance on operators and error probability.
- Job dependencies are defined so that if a job fails, subsequent jobs relying on its output will not be processed.
- Logs are maintained of all job successes and failures.
- Security over access to production data is available.
- The burden on manual tasks is reduced or eliminated.

Risiko	Pengendalian	Fokus Audit
• Job gagal -> data tidak sinkron. • Job dependency error -> hasil salah. • Operator menjalankan job manual tanpa kontrol.	• Tools job scheduler • Dependency mapping. • Logging job: success/failure. • Notifikasi otomatis jika gagal.	• Review job schedule & dependencia. • Analisa job failure log. • Cek siapa yang bisa trigger job manual. • Periksa SOP penanganan job failure.

4. System Interfaces

System interfaces allow **data output from one application** to be sent **as input to another** with little or no human interaction

Data transfers through system interfaces categories	Risks
System-to-system	can lead to pervasive errors if not corrected quickly.
Partner-to-partner	can expose confidential data to a third party or a cybersecurity vulnerability through a partner organization.
Person-to-person	human error, security exposure and repercussions from privacy issues that may not be caught in time.

Mekanisme pertukaran data antar sistem:

- API
- ETL
- File transfer (SFTP, batch file)
- Message queue

4. System Interfaces – Risk & Control

Risiko	Pengendalian	Fokus Audit
• Mapping data salah -> data corruption. • File transfer tidak enkripsi -> data leakage. • Gagal transfer -> incomplete transactions.	• Validasi data inbound/outbound. • Enkripsi (TLS/SFTP). • Error handling & retry mechanism. • Audit trail interface.	• Periksa error log & retry report. • Pastikan enkripsi aktif untuk transfer luar organisasi. • Uji kesesuaian data antar sistem (sampling reconciliation).

5. End-User Computing (EUC) & Shadow IT

- **EUC:** aplikasi yang dibuat user (spreadsheet makro, Access DB). End-user computing (EUC) refers to **the ability of end users (who typically are not programmers) to design and implement their own application or information system** using computer software products.

- **Shadow IT:** penggunaan aplikasi cloud/apps tanpa persetujuan TI.

Risiko	Pengendalian	Fokus Audit
• Tidak ada testing → hasil salah. • Tidak ada backup → hilang. • Mengandung informasi sensitif tanpa kontrol. • Kepatuhan regulasi gagal (misal data pribadi).	• Registrasi EUC. • Data classification policy. • Review berkala & risk assessment. • Shadow IT policy & centralized procurement.	• Identifikasi EUC di unit bisnis. • Review spreadsheet yang digunakan untuk laporan kritikal. • Cek penggunaan aplikasi tanpa izin (scan network). • Cek apakah EUC memiliki backup & kontrol akses.

6. System Availability & Capacity Governance

System Availability & Capacity Governance mencakup seluruh proses, mekanisme, arsitektur, dan aktivitas yang memastikan **sistem TI tersedia secara konsisten**, serta memiliki **kapasitas yang cukup dan optimal** untuk memenuhi kebutuhan bisnis saat ini dan masa depan.

- **Availability Management:** fokus ke **kemampuan sistem untuk tetap beroperasi** sesuai target SLA.
  - Monitoring Uptime/Downtime
  - High Availability (HA) Architecture
  - Failover & Recovery Mechanisms
  - Service Level Agreement (SLA) Availability
  - Maintenance Windows

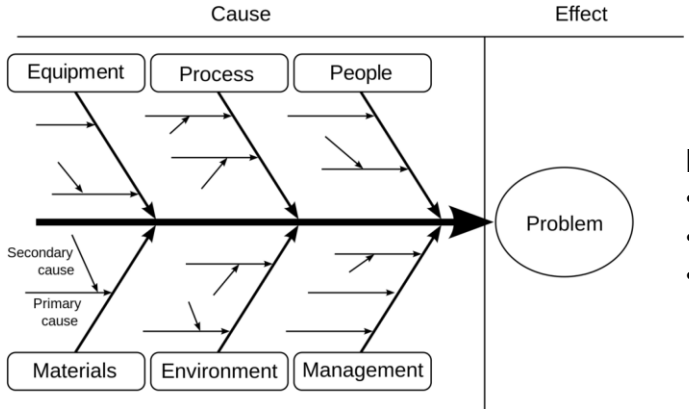
- **Capacity Management:** berfokus pada kemampuan sistem dalam menangani **beban kerja.**
  - Resource Utilization Monitoring
  - Performance Threshold & Alert
  - Workload Forecasting (Forecasting Pertumbuhan)
  - Scalability Planning
  - Capacity Planning Documentation
  - Resource Optimization

6. IT Asset Management – Risk & Control

Risiko	Pengendalian	Fokus Audit
A. Risiko Availability • Downtime sistem → layanan berhenti → kerugian finansial. • Gangguan layanan menyebabkan reputasi buruk. • Kegagalan failover → kehilangan transaksi. • Planned maintenance tidak terjadwal → mengganggu operasi kritis. **B. Risiko Capacity** • Kapasitas CPU/memori tidak mencukupi → aplikasi lambat atau hang. • Storage penuh → transaksi gagal, data tidak tersimpan. • Latency tinggi → user experience menurun. • Ketidakmampuan memenuhi pertumbuhan bisnis → layanan tidak scalable.	**A. Kontrol untuk Availability** • Arsitektur high availability (HA) • Redundansi komponen kritis • Load balancer • Failover automatic • Monitoring uptime 24/7 • SOP pemeliharaan & maintenance window • Tracking SLA & reporting otomatis **B. Kontrol untuk Capacity** • Monitoring kapasitas secara real-time • Threshold alert (warning & critical) • Capacity planning & forecasting tahunan • Resource optimization tools • VM auto-scaling (cloud) • Storage expansion plan	**A. Tujuan Audit Availability** • Ketersediaan sistem memenuhi kebutuhan bisnis dan SLA • Mekanisme failover bekerja • Efektivitas uptime efektif untuk mendeteksi gangguan • Availability metrics dilaporkan secara konsisten **B. Tujuan Audit Capacity** • Memastikan kapasitas sumber daya TI mencukupi untuk melayani beban kerja • Memastikan perencanaan kapasitas jangka panjang berdasarkan analisis kebutuhan • Memastikan pemanfaatan sumber daya optimal (tidak overutilized atau underutilized).

7. Problem Management

Fishbone/Ishikawa Cause-and-effect Diagrams



Metode Lain:
- 5 Whys
- Fault-tree analysis
- Log & event correlation

Objective

Problem Management
- Reduce the number and/or severity of incidents.
- Improve the quality of service of an IS organization.

Incident Management
- React to issues as they arise.
- Return the affected process back to normal service quickly.
- Minimize business impacts of incidents.

Jenis Incident
- **Service outage**: sistem mati total
- **Degradation**: slow response
- **Security incident**: malware, brute force, unauthorized access
- **Capacity incident**: CPU 100%, disk penuh
- **Network incident**: link putus, routing error

Detection → **Recording / Logging** → **Classification & Prioritization** → **Assignment / Dispatching** → **Investigation & Diagnosis** → Resolution & Recovery → **Closure** → **Escalation**

7. IT Asset Management – Risk & Control

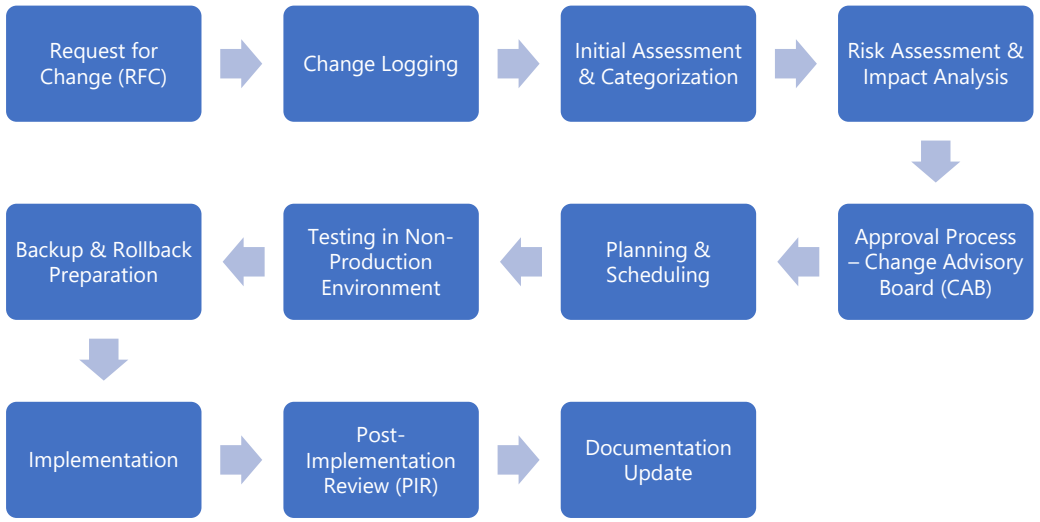
Risiko	Pengendalian	Fokus Audit
• Insiden berulang. • Incident tidak dicatat → tidak dianalisis. • Prioritas salah → delay penanganan.	• Incident ticketing system. • SLA response & resolution time. • Problem management & KEDB. • RCA tools: fishbone, 5 Whys.	• Memastikan insiden ditangani cepat, terdokumentasi, dan sesuai SLA. • Memastikan problem management mencegah terulangnya insiden. • Memastikan proses peningkatan layanan berjalan berdasarkan analisa insiden.

8. Change, Configuration & Patch Management

Tujuan memastikan bahwa:

- Perubahan pada sistem dilakukan **terkendali**,
- Konfigurasi sistem **tercatat dan akurat**,
- Patch keamanan dan perbaikan software **diterapkan secara efektif**.

Change Lifecycle:



Configuration Management

- Configuration Item identification, baseline
- Configuration Management Database
- Dependency mapping
- Avoid configuration drift

Patch Management

- Patch identification
- Assessment
- Testing, deployment, verification
- Compliance reporting

8. Change, Configuration & Patch Management – Risk & Control

Risiko	Pengendalian	Fokus Audit
• Perubahan tanpa approval. • Patch gagal • Konfigurasi tidak terdokumentasi	• Change Advisory Board (CAB). • UAT hasil testing. • Rollback plan. • CMDB update otomatis.	• Memastikan Change Request mendapatkan approval, testing evidence. • Review patch compliance report. • Review configuration baseline vs real. • Cek segregasi tugas developer vs operator.

9. Operational Log Management

The purpose of operational log management is to **ensure the availability, integrity and confidentiality of log data**, which play a crucial role in IT operations, security and compliance.



Log Management Cycle

Log Types				
Event log Server log System log	Access log Change log Availability log	Resource log Threat log Database log	Error log Firewall log Operating system log	Application log Access control log

Risiko	Pengendalian	Fokus Audit
• Log tidak lengkap • Log dihapus/dimodifikasi • Tidak ada alert → insiden terlambat.	• Centralized logging. • Retention policy (regulatory compliance). • Integrity check.	• Memastikan log mendukung deteksi insiden & forensik. • Memastikan log akurat, lengkap, terjaga integritasnya. • Memastikan log retention sesuai standar keamanan & regulasi.

10. IT Service Level Management

Service Level Management (SLM) adalah proses untuk memastikan bahwa TI memberikan layanan **sesuai kebutuhan bisnis** dan **sesuai SLA** yang telah disepakati.

- **Service Level Agreement (SLA)** = Perjanjian formal antara TI dan pelanggan (internal atau eksternal)
  - Definisi layanan: apa yang disediakan TI.
  - Service hours: jam layanan (24/7, jam kerja saja, dsb.)
  - Availability target (misal 99.90%).Performance metrics: response time, throughput.Incident response & resolution time.
  - Capacity & scalability commitments.
  - Security requirements: enkripsi, akses, audit log.
  - Backup & recovery commitments (RTO/RPO).
  - Reporting: frekuensi dan format laporan SLA.
  - Penalties / consequences jika SLA tidak tercapai (jika vendor).

- **Operational Level Agreement (OLA)** = Perjanjian internal antar unit TI untuk mendukung SLA.
  - Contoh: Network Team (99.99% uptime), DBA Team (Restore <30 menit)

Risiko	Pengendalian	Fokus Audit
• SLA tidak realistis. • Vendor tidak deliver sesuai kontrak. • KPI tidak dimonitor.	• SLA agreement dengan bisnis/vendor. • Dashboard SLA. • Monthly service performance review.	• Bandingkan SLA vs actual metrics. • Periksa laporan monthly service review. • Review kontrak vendor.

11. Database Management

Database Management memastikan bahwa **data yang tersimpan dalam DBMS dapat diakses, diproses, dikelola, diamankan, dan dipulihkan** secara efektif.

Lingkup:
- Database Administration
- Database Architecture & Design
- Access Control & Security
- Database Backup & Recovery
- High Availability, Replication & Clustering
- Monitoring, Logging & Audit Trail

Tujuan
- Database optimal
- Akses terkontrol & aman
- Backup & Pemulihan terjamin
- Monitoring efektif
- Integritas data terjaga
- Ketersediaan maksimal.



Risiko	Pengendalian	Fokus Audit
• Akses DBA disalahgunakan → manipulasi data. • Data corrupt tanpa backup. • Kinerja DB buruk → pengaruh ke bisnis.	• Segregasi tugas. • DB backup & restore test. • Hardening DB. • Database auditing.	• Review hak akses DBA. • Verifikasi backup DB & uji restore. • Review DB audit log. • Review parameter keamanan (hardening).

Business Resilience

1. Business Impact Analysis (BIA)

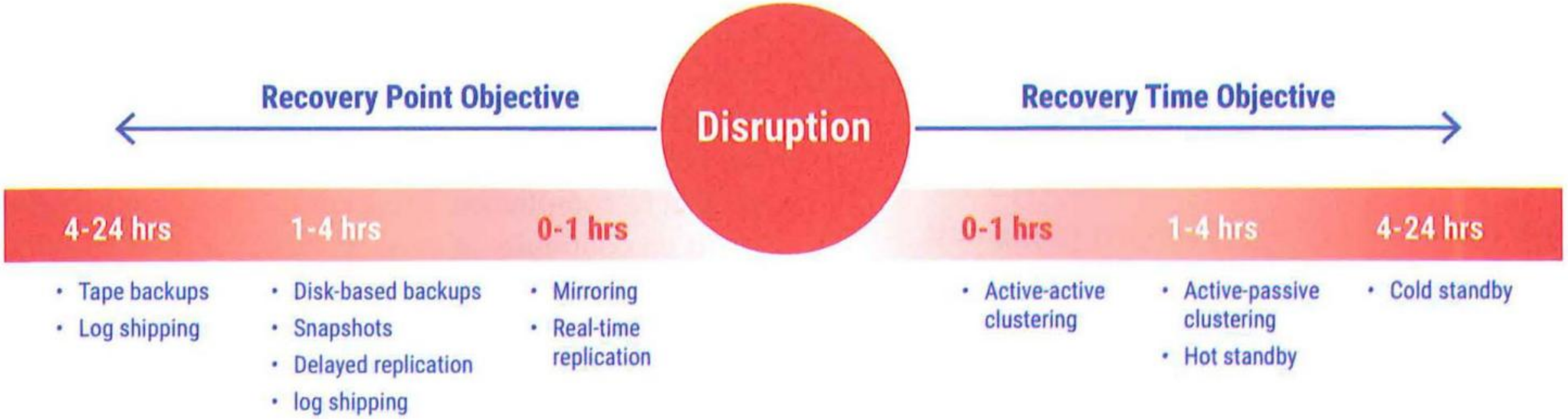
Business Impact Analysis (BIA) menentukan:

- Proses bisnis mana yang kritikal
- Dampak apa jika terjadi gangguan
- Recovery Point Objective (seberapa banyak data yang boleh hilang) & Recovery Time Objective (berapa lama sistem dapat diterima untuk down) yang harus dipenuhi
- Prioritas pemulihan layanan
- Dasar penyusunan BCP dan DRP

BIA adalah proses sistematis untuk **mengidentifikasi prioritas pemulihan**, **menilai dampak bisnis**, dan **menentukan kebutuhan keberlanjutan operasi** jika terjadi gangguan.

Risiko	Pengendalian	Fokus Audit
• Prioritas pemulihan salah → sistem penting tidak segera dipulihkan. • RTO/RPO tidak realistis → DRP gagal dijalankan. • Dampak bisnis tidak terkelola → kerugian finansial & reputasi. • Ketergantungan tidak terlihat → gangguan berantai. • BCP/DRP tidak efektif karena tidak berbasis analisis yang benar	• Metodologi BIA yang terdokumentasi dengan jelas. • Dokumentasi proses bisnis & dampaknya. • RTO & RPO disetujui manajemen. • Review BIA secara berkala (misal tiap tahun). • Integrasi dengan BCP dan DRP.	• Proses bisnis kritikal telah diidentifikasi secara akurat. • Dampak gangguan dinilai secara objektif dan konsisten. • RTO dan RPO sesuai kebutuhan bisnis dan mampu didukung oleh TI. • Ketergantungan proses & sistem terdokumentasi dengan benar. • Hasil BIA digunakan untuk menyusun BCP & DRP. • BIA diperbaharui secara berkala dan relevan dengan kondisi terbaru

Figure 4.40—Relationship Between RTO and RPO



2. System dan Operational Resilience

System & Operational Resilience memastikan bahwa:

- Sistem **tetap berjalan** meski ada gangguan,
- Operasi TI **tidak mudah terganggu**,
- Layanan dapat **pulih cepat**,
- Risiko downtime **diminimalkan**,
- SLA **dapat dipenuhi secara konsisten**.

System dan Operational Resilience adalah kemampuan sistem TI dan proses operasional untuk **tetap berjalan**, **meminimalkan gangguan**, serta **pulih dengan cepat** jika terjadi insiden.

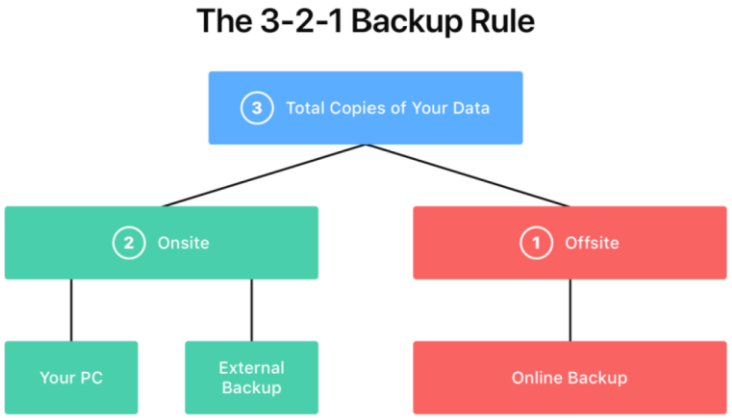
Risiko	Pengendalian	Fokus Audit
• Terjadi **downtime berkepanjangan** akibat tidak ada failover. • Kegagalan komponen menyebabkan **gangguan total layanan**. • Tidak mampu memenuhi SLA ketersediaan. • Sistem tidak sanggup menangani beban • Insiden kecil dapat berkembang menjadi **insiden besar**. • Ketergantungan pada vendor dapat menyebabkan **keterlambatan pemulihan**.	**Kontrol Teknis** • Redundancy server, database, dan network • Auto-failover configuration • Resource monitoring & alerting **Kontrol Operasional** • SOP penanganan insiden • Change control untuk menghindari gangguan • Uji failover secara periodik	Auditor ingin memastikan bahwa: • Sistem memiliki mekanisme ketahanan • Tidak ada Single Point of Failure (SPOF) • Proses operasi TI stabil dan tetap berjalan meskipun terjadi gangguan pada komponen tertentu • Failover & pemulihan telah diuji secara berkala • Vendor dan pihak ketiga mendukung ketahanan layanan

3. Data Backup, Storage, and Restoration

Backup & restoration bertujuan memastikan data **tetap tersedia**, **tidak hilang**, dan **dapat dipulihkan** jika terjadi insiden seperti kegagalan sistem, human error, atau serangan siber.

Tipe Penyimpanan

- **Onsite storage** (NAS, disk array, tape)
- **Offsite storage** (data center sekunder, vault)
- **Cloud backup** (S3, Azure Blob, Glacier)
- **Air-gapped storage** (diputus dari jaringan untuk mencegah ransomware)



Jenis Backup

- **Full Backup:** menyalin semua data.
- **Incremental Backup:** menyalin data yang berubah sejak backup terakhir.
- **Differential Backup:** menyalin data yang berubah sejak full backup terakhir.
- **Snapshot Backup:** snapshot storage / VM untuk pemulihan cepat.

Kriteria Penyimpanan Backup

- Keamanan (enkripsi)
- Durability & redundancy
- Aksesibilitas saat darurat
- Retention period sesuai regulasi

Prinsip Restorasi

- Restore harus **benar-benar diuji** (restore test).
- Waktu pemulihan harus sesuai RTO.
- Integritas data harus terjaga setelah pemulihan.

3. Data Backup, Storage, and Restoration – Risk & Control

Risiko	Pengendalian	Fokus Audit
• **Kehilangan data permanen** • **Gagal memulihkan layanan** saat terjadi insiden • **Downtime berkepanjangan** → kerugian finansial • **Backup tidak valid / korup** • **Data breach** kalau backup tidak dienkripsi • **Ketidakpatuhan regulasi**, misalnya retensi data	• Backup terotomasi dan dimonitor • Enkripsi dan kontrol akses backup • Penyimpanan backup yang aman • Restore test rutin • Dokumentasi dan kebijakan yang jelas	Memastikan: • Backup berjalan konsisten dan mencakup data penting. • Backup disimpan dengan aman dan sesuai kebijakan retensi. • Proses restore dapat dilakukan dan mendukung RTO/RPO. • Integritas backup terjamin dan rutin diuji. • Kontrol keamanan melindungi backup dari akses tidak sah. • Backup & restore memenuhi persyaratan regulasi dan standar internal

4. Business Continuity Plan (BCP)

BCP adalah rencana menyeluruh yang memastikan **bisnis tetap dapat berjalan** ketika terjadi gangguan besar, misalnya kegagalan sistem TI, bencana alam, gangguan listrik, serangan siber, atau kejadian operasional lain.



Hal yang dilakukan:

- Identifikasi proses kritikal berdasarkan Bussiness Impact Analysis (BIA)
- Workaround manual jika sistem TI gagal.
- Prioritas layanan yang harus dipertahankan minimal
- Menentukan sumber daya minimum yang dibutuhkan untuk tetap beroperasi
- Mengatur tindakan organisasi: pembagian peran, alur eskalasi dan komunikasi
- Activation, Execution, and Return-to-Normal Plan

Risiko	Pengendalian	Fokus Audit
• Bisnis berhenti total saat terjadi gangguan. • Kerugian finansial meningkat karena lambat merespons insiden. • Ketidakmampuan memberikan layanan publik/pelanggan. • Ketergantungan berbahaya pada satu lokasi atau satu sistem TI. • Reputasi rusak karena respons lambat. • Tidak memenuhi kewajiban regulasi.	• Dokumen BCP yang lengkap dan disetujui manajemen. • Latihan BCP rutin (tabletop exercise atau simulasi). • Prosedur komunikasi krisis yang jelas. • Workaround operasional siap dijalankan. • BCP diperbarui secara berkala mengikuti hasil BIA & perubahan lingkungan.	Auditor ingin memastikan: • BCP ada, lengkap, dan sesuai BIA. • BCP dapat menjaga kelangsungan fungsi bisnis kritikal selama gangguan. • BCP selalu diperbarui sesuai perubahan proses bisnis atau teknologi.

5. Disaster Recovery Plans (DRPs)

DRP adalah rencana teknis untuk **memulihkan sistem TI, data, dan infrastruktur** setelah terjadi gangguan besar (disaster).
Jika BCP berfokus pada **kelangsungan proses bisnis**, maka **DRP berfokus pada pemulihan TI**.

Pemulihan melalui:

- Pemulihan sistem sesuai prioritas BIA
- Backup & restore yang andal
- Recovery site (hot/warm/cold/cloud)
- Runbook teknis yang jelas
- Pengujian berkala

Jenis recovery site:

- **Hot Site**: siap pakai, data direplikasi real-time (pemulihan cepat).
- **Warm Site**: infrastruktur siap, data perlu restore (pemulihan sedang).
- **Cold Site**: hanya ruang fisik (pemulihan lama).
- **Cloud DR**: failover ke cloud secara otomatis/semi otomatis.

Jenis pengujian DRP::

- Tabletop exercise (diskusi skenario)
- Simulation test (uji sebagian sistem)
- Full failover test (uji pemulihan penuh ke site cadangan)

5. Disaster Recovery Plans (DRPs) – Risk & Control

Risiko	Pengendalian	Fokus Audit
• Sistem TI tidak dapat dipulihkan → bisnis tidak dapat beroperasi. • Kehilangan data melebihi RPO → kerugian signifikan. • Pemulihan lambat → SLA dan kewajiban bisnis tidak terpenuhi. • Gangguan kecil berubah menjadi bencana besar karena tidak ada panduan teknis. • DRP tidak up-to-date → runbook tidak sesuai dengan sistem terkini.	• Dokumen DRP lengkap & mutakhir, mencakup sistem, urutan pemulihan, dan recovery site. • Backup & restore berjalan sesuai RTO/RPO. • DRP test rutin untuk memastikan rencana dapat dijalankan. • Recovery site tersedia & siap digunakan. • Akses & kredensial darurat dikelola dengan aman.	Auditor ingin memastikan bahwa: • DRP mampu memulihkan sistem TI kritikal dalam waktu yang ditentukan (RTO). • DRP mendukung pemulihan data sesuai toleransi kehilangan data (RPO). • Recovery site dan infrastruktur pendukung siap digunakan saat bencana. • Backup valid dan benar-benar dapat digunakan untuk pemulihan. • DRP diuji secara berkala, dan hasilnya digunakan untuk perbaikan. • Dokumen DRP diperbarui mengikuti perubahan sistem dan arsitektur TI.

TUGAS PERTEMUAN V - Ransomware di Pusat Data Nasional

Background:
https://www.bbc.com/indonesia/articles/cxee2985jrvo

Pusat Data Nasional (PDN) merupakan fasilitas yang digunakan untuk menampung berbagai sistem layanan publik dari banyak instansi pemerintah, seperti imigrasi, kesehatan, dan layanan administrasi lainnya.
Pada tanggal **20 Juni 2024**, terjadi gangguan besar pada PDN yang menyebabkan layanan publik **mengalami downtime berkepanjangan**, termasuk layanan **keimigrasian** sehingga proses keberangkatan dan kedatangan penumpang di bandara terganggu.

Tugas:
- Buatkan ringkasan insiden
- Sebutkan **4–5 risiko utama** yang muncul dalam insiden PDN
- Sebutkan **3–5 pengendalian** yang relevan
- **Evaluasi BCP & DRP: mengapa tidak berjalan?**
- Untuk layanan kritikal seperti imigrasi: berapa **RTO & RPO** beserta alasannya?
- Berikan **5 rekomendasi audit**

Kelompok lakukan secara randomisasi, misalnya menggunakan: https://www.randomlists.com/team-generator
Dikumpulkan oleh masing-masing mahasiswa di:
https://forms.gle/sKZJDPoxRFqoGQ156