MODUL PRAKTIKUM

AUDIT SISTEM INFORMASI

Versi 2.0

Penyusun : Agus Salim, S.T., M.T.I.

Program Studi Sistem Informasi

Jurusan Teknik Informatika

Fakultas Teknologi Industri

Universitas Trisakti

2022

DAFTAR ISI

DAFTAR ISI 2

MODUL 1 : IT Assessment Berdasarkan COBIT 5 (Bagian 1) 5

Latihan 1.1. Melakukan IT Assessment Pada Proses EDM01..... 9

Latihan 1.2. Melakukan IT Assessment Pada Proses EDM02..... 10

Latihan 1.3. Melakukan IT Assessment Pada Proses EDM03..... 11

Latihan 1.4. Melakukan IT Assessment Pada Proses APO01. 12

Latihan 1.5. Melakukan IT Assessment Pada Proses APO02. 13

Latihan 1.6. Melakukan IT Assessment Pada Proses APO03. 14

Latihan 1.7. Melakukan IT Assessment Pada Proses APO05. 15

MODUL 2 : IT Assessment Berdasarkan COBIT 5 (Bagian 2) 16

Latihan 2.1. Melakukan IT Assessment Pada Proses APO07. 20

Latihan 2.2. Melakukan IT Assessment Pada Proses APO11. 21

Latihan 2.3. Melakukan IT Assessment Pada Proses APO12. 22

Latihan 2.4. Melakukan IT Assessment Pada Proses APO13. 23

Latihan 2.5. Melakukan IT Assessment Pada Proses BAI01. 24

Latihan 2.6. Melakukan IT Assessment Pada Proses APO03. 25

MODUL 3 : IT Assessment Berdasarkan COBIT 5 (Bagian 3) 26

Latihan 3.1. Melakukan IT Assessment Pada Proses BAI03. 31

Latihan 3.2. Melakukan IT Assessment Pada Proses BAI09. 33

Latihan 3.3. Melakukan IT Assessment Pada Proses DSS01. 34

Latihan 4.4. Melakukan IT Assessment Pada Proses DSS05. 35

Latihan 3.5. Melakukan IT Assessment Pada Proses DSS06. 36

Latihan 3.6. Melakukan IT Assessment Pada Proses MEA01. 37
Latihan 3.7. Melakukan IT Assessment Pada Proses MEA02. 38

MODUL 4 : Membuat Rencana Audit SI 40
Latihan 4.1. Membuat Rencana dan Jadwal Audit SI. 41
Latihan 4.2. Membuat Piagam Audit SI. 44

MODUL 5 : Audit Pada Komputer Bersistem Operasi Windows 46
Latihan 5.1. Melakukan audit pada *setup and general controls*. 48
Latihan 5.2. Melakukan audit pada layanan, aplikasi yang terinstal, dan *scheduled tasks*. 50
Latihan 5.3. Melakukan audit pada *account management* dan *password controls*. .51
Latihan 5.4. Melakukan audit pada *user rights* dan *security options*. 53
Latihan 5.5. Melakukan audit pada *network security and controls*. 54

MODUL 6 : Audit Pada Pusat Data, Jaringan, Internet, dan e-Commerce 56
Latihan 6.1. Melakukan audit pada lingkungan di sekitar pusat data. 58
Latihan 6.2. Melakukan audit pada *physical access control*. 59
Latihan 6.3. Melakukan audit pada *environmental control*. 60
Latihan 6.4. Melakukan audit pada *power continuity*. 61
Latihan 6.5. Melakukan audit pada sistem alarm. 63
Latihan 6.6. Melakukan audit pada sistem pemadaman api. 65
Latihan 6.7. Melakukan audit pada *surveillance system*. 66
Latihan 6.8. Melakukan audit pada operasional pusat data. 67
Latihan 6.9. Melakukan audit pada jaringan. 69
Latihan 6.10. Melakukan audit pada fasilitas internet. 72
Latihan 6.11. Melakukan audit pada e-Commerce. 74

MODUL 7 : Audit Untuk Sistem Manajemen Basis Data (DBMS) 76
Latihan 7.1. Melakukan audit pada *database permissions*. 78
Latihan 7.2. Melakukan audit pada *operating system security*. 80
Latihan 7.3. Melakukan audit pada *password strength and management features*. 81

Latihan 7.4. Melakukan audit pada *activity monitoring*. 82
Latihan 7.5. Melakukan audit pada *database encryption*..... 83
Latihan 7.6. Melakukan audit pada *database vulnerabilities, integrity, and patching process*. 84
Latihan 7.7. Melakukan audit pada fungsi DBA. 85
Latihan 7.8. Melakukan audit pada proses *backup* DB. 87
Latihan 7.9. Melakukan audit pada proses *restore* DB. 88

MODUL 8 : Audit Pencapaian Baseline Keamanan Informasi Berdasarkan ISO/IEC 27002 : 2005 (Bagian 1) 89
Latihan 8.1. Mengecek Area Domain A.5..... 94
Latihan 8.2. Mengecek Area Domain A.6..... 95
Latihan 8.3. Mengecek Area Domain A.7..... 97
Latihan 8.4. Mengecek Area Domain A.8..... 98
Latihan 8.5. Mengecek Area Domain A.9..... 100
Latihan 8.6. Mengecek Area Domain A.10..... 102

MODUL 9 : Audit Pencapaian Baseline Keamanan Informasi Berdasarkan ISO/IEC 27002 : 2005 (Bagian 2) 108
Latihan 9.1. Mengecek Area Domain A.11..... 112
Latihan 9.2. Mengecek Area Domain A.12..... 118
Latihan 9.3. Mengecek Area Domain A.13..... 122
Latihan 9.4. Mengecek Area Domain A.14..... 124
Latihan 9.5. Mengecek Area Domain A.15..... 126

MODUL 10 : Membuat Laporan Audit SI/TI Yang Lengkap..... 129
Latihan 10.1. Membuat laporan audit SI/TI secara sederhana..... 130

FORM UMPAN BALIK.....131

MODUL 1 : IT Assessment Berdasarkan COBIT 5 (Bagian 1)

Pokok Bahasan :

- Melakukan IT Assessment Berdasarkan COBIT 5 Pada Dimensi Proses EDM (ISM314.PRAK.2.0.0-01).
- Melakukan IT Assessment Berdasarkan COBIT 5 Pada Dimensi Proses APO (ISM314.PRAK.2.0.0-02).

Sub CPMK 6.1 : Mahasiswa mampu melakukan *IT assessment* berdasarkan COBIT 5 sebagai aktivitas pre-audit dalam praktikum.

No.	Deskripsi Tugas	Indikator Kinerja	Durasi (Menit)
1.1	Melakukan IT assessment pada proses EDM01.	Hasil IT assessment pada proses EDM01 berhasil ditentukan berdasarkan keterangan pada contoh kasus.	15
1.2	Melakukan IT assessment pada proses EDM02.	Hasil IT assessment pada proses EDM02 berhasil ditentukan berdasarkan keterangan pada contoh kasus.	15
1.3	Melakukan IT assessment pada proses EDM03.	Hasil IT assessment pada proses EDM03 berhasil ditentukan berdasarkan keterangan pada contoh kasus.	20
1.4	Melakukan IT assessment pada proses APO01.	Hasil IT assessment pada proses APO01 berhasil ditentukan berdasarkan keterangan pada contoh kasus.	30
1.5	Melakukan IT assessment pada proses APO02.	Hasil IT assessment pada proses APO02 berhasil ditentukan berdasarkan keterangan pada contoh kasus.	30
1.6	Melakukan IT assessment pada proses APO03.	Hasil IT assessment pada proses APO03 berhasil ditentukan berdasarkan keterangan pada contoh kasus.	30
1.7	Melakukan IT assessment pada proses APO05.	Hasil IT assessment pada proses APO05 berhasil ditentukan berdasarkan keterangan pada contoh kasus.	30
		TOTAL	**170**

TUGAS PENDAHULUAN

Untuk dapat menjalankan modul praktikum ini silahkan membaca artikel berikut :

1. COBIT Framework 5

DAFTAR PERTANYAAN

1. Proses apa saja yang terdapat pada dimensi proses EDM berdasarkan COBIT Framework 5 ?
2. Proses apa saja yang terdapat pada dimensi proses APO berdasarkan COBIT Framework 5 ?

TEORI SINGKAT

–

LAB SETUP

Untuk dapat menjalankan praktikum ini maka harus diketahui kondisi dan hasil pengumpulan bukti audit pada PT. XYZ.

EDM01 – Menjamin setting dan pemeliharaan pada kerangka kerja tata kelola.

Untuk dimensi proses EDM01, sebagai berikut :

- Sudah ada sistem tata kelola TI, tapi masih belum diimplementasikan, sehingga diberi nilai 20%.
- Belum ada arahan yang jelas terkait tata kelola TI sehingga diberi nilai 10%.
- Belum ada pihak yang memonitor tata kelola TI, sehingga diberi nilai 0%.

EDM02 – Menjamin pemberian manfaat.

Untuk dimensi proses EDM02, sebagai berikut :

- Sudah ada pihak yang ditugaskan untuk mengevaluasi manfaat TI di PT XYZ. Tetapi belum dijalankan dengan maksimal, sehingga diberi nilai 60%.
- Belum ada arahan terkait evaluasi manfaat TI di PT XYZ., sehingga diberi nilai 0%.
- Sudah ada pihak yang memonitor optmasi manfaat TI yaitu direktur PT. XYZ. Tetapi belum dapat memonitor secara optimal, sehingga diberi nilai 30%.

EDM03 – Menjamin optimasi risiko.

Untuk dimensi proses EDM03, sebagai berikut :

- Belum ada pihak yang ditugaskan untuk mengevaluasi pelaksanaan manajemen risiko TI di PT. XYZ, sehingga diberi nilai 0%.

- Belum ada arahan yang tegas terkait manajemen risiko TI di PT. XYZ, sehingga diberi nilai 0%.
- Belum ada pihak yang ditugaskan untuk memonitor pelaksanaan manajemen risiko TI di PT. XYZ, sehingga diberi nilai 0%.

APO01 – Mengelola kerangka kerja manajemen TI.

Untuk dimensi proses APO01, sebagai berikut :

- Sudah ada struktur organisasi di PT. XYZ, sehingga diberi nilai 100%.
- Sudah ada pemisahan tugas, wewenang, dan tanggung jawab unit kerja (divisi) di PT. XYZ, sehingga diberi nilai 100%.
- Motor penggerak perusahaan bersifat temporal dan tidak dapat memberikan motivasi secara penuh di PT. XYZ, sehingga diberi nilai 50%.
- Sudah ada pelaksanaan *briefing* dari pimpinan ke para kepala divisi terkait tujuan dan arah organisasi di PT. XYZ. Tapi belum didukung bukti yang valid, sehingga diberi nilai 70%.
- Fungsi TI dan struktur organisasi TI di PT. XYZ sudah dirumuskan. Tapi belum memiliki tugas yang jelas, sehingga diberi nilai 30%.
- Belum ada kepemilikan data dan informasi di PT. XYZ, sehingga diberi nilai 0%.
- Belum ada perbaikan proses organisasi secara kontinu di PT. XYZ, sehingga diberi nilai 0%.
- Kepatuhan terhadap regulasi belum sepenuhnya dijalankan oleh PT. XYZ, sehingga diberi nilai 60%.

APO02 – Mengelola strategi.

Untuk dimensi proses APO02, sebagai berikut :

- Belum ada pimpinan TI (CIO). Arahan TI organisasi di PT. XYZ belum jelas, sehingga diberi nilai 0%.
- Belum ada penilaian lingkungan, kapabilitas, dan kinerja TI di PT. XYZ, sehingga diberi nilai 0%.
- Belum ada target dari penilaian kapabilitas TI di PT. XYZ, sehingga diberi nilai 0%.
- Belum dilakukan analisis kesenjangan di PT. XYZ, sehingga diberi nilai 0%.
- Belum ada rencana strategis dan *IT roadmap* di PT. XYZ, sehingga diberi nilai 0%.
- Sudah ada diskusi dan pengarahan terkait TI di PT. XYZ. Tapi belum terkait aspek teknis dan belum mendetail, sehingga diberi nilai 40%.

APO03 – Mengelola arsitektur enterprise.

Untuk dimensi proses APO03, sebagai berikut :

- Visi dan misi TI PT. XYZ sedang dalam tahap perumusan, sehingga diberi nilai 10%.
- Arsitektur TI yang ada di PT. XYZ baru berupa arsitektur infrastruktur TI saja, sehingga diberi nilai 15%.
- Belum ada proses pemilihan peluang dan solusi bisnis berbasis TI untuk pengembangan PT. XYZ, sehingga diberi nilai 0%.
- Walaupun sudah ada arsitektur infrastruktur TI di PT. XYZ, tetapi belum diimplementasikan, sehingga diberi nilai 0%.
- Belum ada definisi dan dokumentasi resmi terkait layanan arsitektur TI di PT. XYZ, sehingga diberi nilai 0%.

APO05 – Mengelola portofolio.

Untuk dimensi proses APO05, sebagai berikut :

- Sudah ada rencana dan arahan untuk investasi TI di PT. XYZ, tapi belum mampu memberikan manfaat optimal, sehingga diberi nilai 30%.
- Sudah ada perencanaan dan akses terhadap sumber daya TI di PT. XYZ walaupun belum mampu memberikan manfaat optimal, sehingga diberi nilai 30%.
- Belum mampu merumuskan sumber pendanaan untuk belanja TI dengan benar dan mendetail di PT. XYZ, sehingga diberi nilai 60%.
- Belum ada portofolio invetasi TI di PT. XYZ, sehingga diberi nilai 0%.
- Tidak ada portofolio TI yang dapat dimonitor di PT. XYZ, sehingga diberi nilai 0%.
- Belum mampu mengelola pencapaian laba untuk belanja (pengadaan) TI di PT. XYZ, sehingga diberi nilai 60%.

Latihan 1.1. Melakukan IT Assessment Pada Proses EDM01.

Kode	Base Practices	Achievement Level			
		Not Achieved (N)	Partially Achieved (P)	Largely Achieved (L)	Fully Achieved (F)
		0% - 15%	15,01% - 50%	50,01% - 85%	85,01% - 100%
EDM01-BP1	*Evaluate the governance system.* Mengevaluasi sistem tata kelola.				
EDM01-BP2	*Direct the governance system.* Mengarahkan sistem tata kelola.				
EDM01-BP3	*Monitor the governance system.* Memonitor sistem tata kelola.				
Sub-total					
Total					
Rata-rata					

Latihan 1.2. Melakukan IT Assessment Pada Proses EDM02.

Kode	Base Practices	Achievement Level			
		Not Achieved (N)	Partially Achieved (P)	Largely Achieved (L)	Fully Achieved (F)
		0% - 15%	15,01% - 50%	50,01% - 85%	85,01% - 100%
EDM02-BP1	*Evaluate value optimisation.* Mengevaluasi optimasi manfaat.				
EDM02-BP2	*Direct value optimisation.* Mengarahkan optimasi manfaat.				
EDM02-BP3	*Monitor value optimisation.* Memonitor optimasi manfaat.				
Sub-total					
Total					
Rata-rata					

Latihan 1.3. Melakukan IT Assessment Pada Proses EDM03.

Kode	Base Practices	Achievement Level			
		Not Achieved (N)	Partially Achieved (P)	Largely Achieved (L)	Fully Achieved (F)
		0% - 15%	15,01% - 50%	50,01% - 85%	85,01% - 100%
EDM03-BP1	*Evaluate risk management.* Mengevaluasi manajemen risiko.				
EDM03-BP2	*Direct risk management.* Mengarahkan manajemen risiko.				
EDM03-BP3	*Monitor risk management.* Memonitor manajemen risiko.				
Sub-total					
Total					
Rata-rata					

Latihan 1.4. Melakukan IT Assessment Pada Proses APO01.

Kode	Base Practices	Achievement Level			
		Not Achieved (N)	Partially Achieved (P)	Largely Achieved (L)	Fully Achieved (F)
		0% - 15%	15,01% - 50%	50,01% - 85%	85,01% - 100%
APO01-BP1	*Define the organisational structure.* Mendefinisikan struktur organisasi.				
APO01-BP2	*Establish roles and responsibilities.* Membangun/menentukan peran dan tanggungjawab.				
APO01-BP3	*Maintain the enablers of the management system.* Memelihara motor penggerak untuk sistem manajemen.				
APO01-BP4	*Communicate management objectives and direction.* Mengkomunikasikan berbagai tujuan dan arahan manajemen.				
APO01-BP5	*Optimise the placement of the IT function.* Mengoptimasi posisi dari fungsi TI.				
APO01-BP6	*Define information (data) and system ownership.* Mendefinisikan kepemilikan informasi (data) dan sistem.				
APO01-BP7	*Manage continual improvement of processes.* Mengelola perbaikan proses secara kontinual.				
APO01-BP8	*Maintain compliance with policies and procedures.* Memelihara kepatuhan dengan berbagai kebijakan dan prosedur.				
Sub-total					
Total					
Rata-rata					

Latihan 1.5. Melakukan IT Assessment Pada Proses APO02.

Kode	Base Practices	Achievement Level			
		Not Achieved (N)	Partially Achieved (P)	Largely Achieved (L)	Fully Achieved (F)
		0% - 15%	15,01% - 50%	50,01% - 85%	85,01% - 100%
APO02-BP1	*Understand enterprise direction.* Memahami arahan *enterprise*.				
APO02-BP2	*Assess the current environment, capabilities and performance.* Menilai lingkungan, kapabilitas, dan kinerja saat ini.				
APO02-BP3	*Define the target IT capabilities.* Mendefinisikan berbagai kapabilitas TI dari target yang ada.				
APO02-BP4	*Conduct a gap analysis.* Melakukan analisis kesenjangan.				
APO02-BP5	*Define the strategic plan and road map.* Mendefinisikan rencana strategis dan *road map*.				
APO02-BP6	*Communicate the IT strategy and direction.* Mengkomunikasikan strategi dan arahan TI.				
Sub-total					
Total					
Rata-rata					

Latihan 1.6. Melakukan IT Assessment Pada Proses APO03.

Kode	Base Practices	Achievement Level			
		Not Achieved (N)	Partially Achieved (P)	Largely Achieved (L)	Fully Achieved (F)
		0% - 15%	15,01% - 50%	50,01% - 85%	85,01% - 100%
APO03-BP1	*Develop the enterprise architecture vision.* Membangun visi arsitektur *enterprise*.				
APO03-BP2	*Define reference architecture.* Mendefinisikan arsitektur referensi.				
APO03-BP3	*Select opportunities and solutions.* Memilih peluang dan solusi.				
APO03-BP4	*Define architecture implementation.* Mendefinisikan implementasi arsitektur.				
APO03-BP5	*Provide enterprise architecture services.* Menyediakan berbagai layanan arsitektur *enterprise*.				
Sub-total					
Total					
Rata-rata					

Latihan 1.7. Melakukan IT Assessment Pada Proses APO05.

Kode	Base Practices	Achievement Level			
		Not Achieved (N)	Partially Achieved (P)	Largely Achieved (L)	Fully Achieved (F)
		0% - 15%	15,01% - 50%	50,01% - 85%	85,01% - 100%
APO05-BP1	*Establish the target investment mix.* Membangun kombinasi investasi pada target.				
APO05-BP2	*Determine the availability and sources of funds.* Menentukan ketersediaan dan sumber daya dari pendanaan.				
APO05-BP3	*Evaluate and select programmes to fund.* Mengevaluasi dan memilih program untuk pendanaan.				
APO05-BP4	*Monitor, optimise and report on investment portfolio performance.* Memonitor, mengoptimasi, dan melaporkan kinerja portofolio investasi.				
APO05-BP5	*Maintain portfolios.* Memelihara berbagai portofolio.				
APO05-BP6	*Manage benefits achievement.* Mengelola pencapaian keuntungan.				
Sub-total					
Total					
Rata-rata					

MODUL 2 : IT Assessment Berdasarkan COBIT 5 (Bagian 2)

Pokok Bahasan :

- Melakukan IT Assessment Berdasarkan COBIT 5 Pada Dimensi Proses APO (ISM314.PRAK.2.0.0-02).
- Melakukan IT Assessment Berdasarkan COBIT 5 Pada Dimensi Proses BAI (ISM314.PRAK.2.0.0-03).

Sub CPMK 6.1 : Mahasiswa mampu melakukan *IT assessment* berdasarkan COBIT 5 sebagai aktivitas pre-audit dalam praktikum.

No.	Deskripsi Tugas	Indikator Kinerja	Durasi (Menit)
2.1	Melakukan IT assessment pada proses APO07.	Hasil IT assessment pada proses APO07 berhasil ditentukan berdasarkan keterangan pada contoh kasus.	30
2.2	Melakukan IT assessment pada proses APO11.	Hasil IT assessment pada proses APO11 berhasil ditentukan berdasarkan keterangan pada contoh kasus.	30
2.3	Melakukan IT assessment pada proses APO12.	Hasil IT assessment pada proses APO12 berhasil ditentukan berdasarkan keterangan pada contoh kasus.	20
2.4	Melakukan IT assessment pada proses APO13.	Hasil IT assessment pada proses APO13 berhasil ditentukan berdasarkan keterangan pada contoh kasus.	30
2.5	Melakukan IT assessment pada proses BAI01.	Hasil IT assessment pada proses BAI01 berhasil ditentukan berdasarkan keterangan pada contoh kasus.	30
2.6	Melakukan IT assessment pada proses BAI02.	Hasil IT assessment pada proses BAI02 berhasil ditentukan berdasarkan keterangan pada contoh kasus.	30
		TOTAL	**170**

TUGAS PENDAHULUAN

Untuk dapat menjalankan modul praktikum ini silahkan membaca artikel berikut :

1. COBIT Framework 5

DAFTAR PERTANYAAN

1. Proses apa saja yang terdapat pada dimensi proses APO berdasarkan COBIT Framework 5 ?
2. Proses apa saja yang terdapat pada dimensi proses BAI berdasarkan COBIT Framework 5 ?

TEORI SINGKAT

–

LAB SETUP

Untuk dapat menjalankan praktikum ini maka harus diketahui kondisi dan hasil pengumpulan bukti audit pada PT. XYZ.

APO07 – Mengelola sumber daya manusia (SDM).

Untuk dimensi proses APO07, sebagai berikut :

- Sudah ada penempatan staf sesuai kebutuhan dan keahliannya, tapi masih belum diimplementasikan dengan tepat, sehingga diberi nilai 70%.
- Staf TI yang penting belum mampu diidentifikasi dengan tepat, sehingga diberi nilai 30%.
- Beberapa staf sudah mulai dikirimkan untuk pengikuti pengembangan kompetensi dan pelatihan, sehingga diberi nilai 40%.
- Sudah ada evaluasi kinerja untuk sebagian besar karyawan per tahun, sehingga diberi nilai 80%.
- Perusahaan belum mampu menentukan berapa orang yang dibutuhkan untuk menjadi staf TI dan staf non-TI dengan tepat, sehingga diberi nilai 25%.
- Perusahan sudah mampu mengelola staf yang dikontrak dari awal penerimaan hingga pemutusan/pemberhentian kontrak, sehingga diberi nilai 100%.

APO11 – Mengelola kualitas.

Untuk dimensi proses APO11, sebagai berikut :

- Belum ada manajemen mutu yang diterapkan di perusahaan, sehingga diberi nilai 60%.
- Sudah ada pendefinisian terkait mutu dan standar yang digunakan perusahaan, sehingga diberi nilai 70%.
- Manajemen mutu belum sepenuhnya difokuskan pada pelanggan, sehingga diberi nilai 70%.
- Belum ada pengawasan terkait implementasi manajemen mutu di perusahaan, sehingga diberi nilai 0%.
- Manajemen mutu belum diintegrasikan ke berbagai proses bisnis yang berhubungan dengan kayanan yang diberikan ke pelanggan, sehingga diberi nilai 0%.
- Sudah ada evaluasi dan perbaikan berkelanjutan, tetapi hasil perbaikan belum terlihat, sehingga diberi nilai 50%.

APO12 – Mengelola risiko.

Untuk dimensi proses APO12, sebagai berikut :

- Perusahaan sudah sadar akan kebutuhan data, pengumpulan data, dan pengelompokkan data, sehingga diberi nilai 90%.
- Analisis risiko bisnis dan TI masih dilakukan secara *ad hoc* setelah terjadi insiden, sehingga diberi nilai 20%.
- Belum ada perumusan *risk profile* yang mungkin dialami oleh perusahaan, sehingga diberi nilai 0%.
- Belum ada strategi atau tindakan untuk mengubah risiko, sehingga diberi nilai 0%.
- Perusahaan belum merumuskan portofolio untuk manajemen risiko bisnis dan TI organisasi, sehingga diberi nilai 0%.
- Perusahaan belum mampu merespon risiko dengan tepat karena belum diantisipasi, sehingga diberi nilai 20%.

APO13 – Mengelola keamanan.

Untuk dimensi proses APO13, sebagai berikut :

- Perusahaan belum memiliki sebuah sistem manajemen keamanan informasi, sehingga diberi nilai 0%.
- Perusahaan belum dapat menangani risiko terkait insiden keamanan informasi yang terjadi dengan tepat, sehingga diberi nilai 20%.
- Belum ada aktivitas pengawasan terhadap pelaksanaan ISMS (*Information Security Management System*), sehingga diberi nilai 0%.

BAI01 – Mengelola program dan proyek.

Untuk dimensi proses BAI01, sebagai berikut :

- Perusahaan sudah memiliki ketentuan dan prosedur (SOP) terkait manajemen proyek dan program kerja organisasi, sehingga diberi nilai 100%.
- Belum semua unit kerja di perusahan dapat memberikan ide atau inisiatif terkait program kerja organisasi, sehingga diberi nilai 70%.
- Belum semua karyawan menyadari perlunya pendekatan dan *engagement* dengan pelanggan terkait perumusan program kerja, sehingga diberi nilai 60%.
- Sebagian unit kerja sudah mampu merencanakan program kerja yang dibuatnya, tetapi belum tentu dapat menjalankannya dengan baik, sehingga diberi nilai 80%.
- Sebagian unit kerja sudah mampu dan menjalankan program kerja yang dibuatnya, tetapi belum mampu mengawasinya dengan baik, sehingga diberi nilai 60%.
- Unit kerja belum mampu sepenuhnya melaporkan pelaksanaan program kerjanya, sehingga diberi nilai 75%.
- Hanya sebagian kecil unit kerja yang mampu menginisiasi proyek ke dalam sebuah ide untuk program kerja, sehingga diberi nilai 30%.

BAI02 – Mengelola definisi prasyarat.

Untuk dimensi proses BAI02, sebagai berikut :

- Perusahaan belum sepenuhnya dapat menentukan dan meng-*update* prasyarat fungsional dan teknis untuk kebutuhan bisnisnya, sehingga diberi nilai 70%.
- Studi atau pengecekan kelayakan tidak selalu dilakukan untuk semua proyek atau solusi bisnis atau TI, sehingga diberi nilai 60%.
- Belum ada pengelolaan risiko bisnis dan TI dari berbagai prasyarat yang dibutuhkan untuk bisnis, sehingga diberi nilai 0%.
- Belum ada persetujuan atas penentuan prasyarat dan solusi bisnis-TI walau sudah dikonfirmasi oleh pimpinan unit, sehingga diberi nilai 50%.

Latihan 2.1. Melakukan IT Assessment Pada Proses APO07.

Kode	Base Practices	Achievement Level			
		Not Achieved (N)	Partially Achieved (P)	Largely Achieved (L)	Fully Achieved (F)
		0% - 15%	15,01% - 50%	50,01% - 85%	85,01% - 100%
APO07-BP1	*Maintain adequate and appropriate staffing.* Memelihara penempatan staf yang memadai dan sesuai.				
APO07-BP2	*Identify key IT personnel.* Mengidentifikasi personel TI yang penting.				
APO07-BP3	*Maintain the skills and competencies of personnel.* Memelihara berbagai keahlian dan kompetensi dari personel.				
APO07-BP4	*Evaluate employee job performance.* Mengevaluasi kinerja dari pekerjaan karyawan.				
APO07-BP5	*Plan and track the usage of IT and business human resources.* Merencanakan dan melacak penggunaan berbagai SDM TI dan bisnis.				
APO07-BP6	*Manage contract staff.* Mengelola staf yang dikontrak.				
Sub-total					
Total					
Rata-rata					

Latihan 2.2. Melakukan IT Assessment Pada Proses APO11.

Kode	Base Practices	Achievement Level			
		Not Achieved (N)	Partially Achieved (P)	Largely Achieved (L)	Fully Achieved (F)
		0% - 15%	15,01% - 50%	50,01% - 85%	85,01% - 100%
APO11-BP1	*Establish a quality management system (QMS).* Membangun sebuah sistem manajemen mutu (QMS).				
APO11-BP2	*Define and manage quality standards, practices and procedures.* Mendefinisikan dan mengelola berbagai standar, praktik, dan prosedur terkait mutu.				
APO11-BP3	*Focus quality management on customers.* Memfokuskan manajemen mutu pada pelanggan.				
APO11-BP4	*Perform quality monitoring, control and reviews.* Melakukan pengawasan, kontrol, dan pengkajian mutu.				
APO11-BP5	*Integrate quality management into solutions for development and service delivery.* Mengintegrasikan manajemen mutu ke dalam berbagai solusi untuk pengembangan dan pemberian layanan				
APO11-BP6	*Maintain continuous improvement.* Memelihara perbaikan yang berkelanjutan.				
Sub-total					
Total					
Rata-rata					

Latihan 2.3. Melakukan IT Assessment Pada Proses APO12.

Kode	Base Practices	Achievement Level			
		Not Achieved (N)	Partially Achieved (P)	Largely Achieved (L)	Fully Achieved (F)
		0% - 15%	15,01% - 50%	50,01% - 85%	85,01% - 100%
APO12-BP1	*Collect data.* Mengumpulkan data.				
APO12-BP2	*Analyse risk.* Menganalisa risiko.				
APO12-BP3	*Maintain a risk profile.* Memelihara sebuah *risk profile*.				
APO12-BP4	*Articulate risk.* Mengubah risiko.				
APO12-BP5	*Define a risk management action portfolio.* Mendefinisikan sebuah portofolio tindakan manajemen risiko.				
APO12-BP6	*Respond to risk.* Merespon risiko.				
	Sub-total				
				Total	
				Rata-rata	

Latihan 2.4. Melakukan IT Assessment Pada Proses APO13.

Kode	Base Practices	Achievement Level			
		Not Achieved (N)	Partially Achieved (P)	Largely Achieved (L)	Fully Achieved (F)
		0% - 15%	15,01% - 50%	50,01% - 85%	85,01% - 100%
APO13-BP1	*Establish and maintain an information security management system (ISMS).* Membangun dan memelihara sebuah sistem manajemen keamanan informasi (ISMS).				
APO13-BP2	*Define and manage an information security risk treatment plan.* Mendefinisikan dan mengelola sebuah rencana *risk treatment* keamanan informasi.				
APO13-BP3	*Monitor and review the ISMS.* Memonitor dan mengkaji ISMS.				
Sub-total					
Total					
Rata-rata					

Latihan 2.5. Melakukan IT Assessment Pada Proses BAI01.

Kode	Base Practices	Achievement Level			
		Not Achieved (N)	Partially Achieved (P)	Largely Achieved (L)	Fully Achieved (F)
		0% - 15%	15,01% - 50%	50,01% - 85%	85,01% - 100%
BAI01-BP1	*Maintain a standard approach for programme and project management.* Memelihara sebuah pendekatan yang standar untuk program dan manajemen proyek.				
BAI01-BP2	*Initiate a programme.* Menginisiasi sebuah program.				
BAI01-BP3	*Manage stakeholder engagement.* Mengelola *engagement* dengan pemangku kepentingan.				
BAI01-BP4	*Develop and maintain the programme plan.* Membangun dan memelihara rencana program.				
BAI01-BP5	*Launch and execute the programme.* Meluncurkan dan menjalankan program.				
BAI01-BP6	*Monitor, control and report on the programme outcomes.* Memonitor, mengontrol, dan melaporkan *outcome* dari program.				
BAI01-BP7	*Start up and initiate projects within a programme.* Memulai dan menginisiasi berbagai proyek ke dalam sebuah program.				
Sub-total					
Total					
Rata-rata					

Latihan 2.6. Melakukan IT Assessment Pada Proses APO03.

Kode	Base Practices	Achievement Level			
		Not Achieved (N)	Partially Achieved (P)	Largely Achieved (L)	Fully Achieved (F)
		0% - 15%	15,01% - 50%	50,01% - 85%	85,01% - 100%
BAI02-BP1	*Define and maintain business functional and technical requirements.* Mendefinisikan dan memelihara berbagai prasyarat fungsional dan teknis pada bisnis.				
BAI02-BP2	*Perform a feasibility study and formulate alternative solutions.* Melakukan sebuah studi kelayakan dan memformulasikan berbagai solusi alternatif.				
BAI02-BP3	*Manage requirements risk.* Mengelola risiko dari prasyarat.				
BAI02-BP4	*Obtain approval of requirements and solutions.* Memperoleh persetujuan atas berbagai prasyarat dan solusi.				
Sub-total					
Total					
Rata-rata					

MODUL 3 : IT Assessment Berdasarkan COBIT 5 (Bagian 3)

Pokok Bahasan :

- Melakukan IT Assessment Berdasarkan COBIT 5 Pada Dimensi Proses BAI (ISM314.PRAK.2.0.0-03).
- Melakukan IT Assessment Berdasarkan COBIT 5 Pada Dimensi Proses DSS (ISM314.PRAK.2.0.0-04).
- Melakukan IT Assessment Berdasarkan COBIT 5 Pada Dimensi Proses MEA (ISM314.PRAK.2.0.0-05).

Sub CPMK 6.1 : Mahasiswa mampu melakukan *IT assessment* berdasarkan COBIT 5 sebagai aktivitas pre-audit dalam praktikum.

No.	Deskripsi Tugas	Indikator Kinerja	Durasi (Menit)
3.1	Melakukan IT assessment pada proses BAI03.	Hasil IT assessment pada proses BAI03 berhasil ditentukan berdasarkan keterangan pada contoh kasus.	30
3.2	Melakukan IT assessment pada proses BAI09.	Hasil IT assessment pada proses BAI09 berhasil ditentukan berdasarkan keterangan pada contoh kasus.	30
3.3	Melakukan IT assessment pada proses DSS01.	Hasil IT assessment pada proses DSS01 berhasil ditentukan berdasarkan keterangan pada contoh kasus.	20
3.4	Melakukan IT assessment pada proses DSS05.	Hasil IT assessment pada proses DSS05 berhasil ditentukan berdasarkan keterangan pada contoh kasus.	30
3.5	Melakukan IT assessment pada proses DSS06.	Hasil IT assessment pada proses DSS06 berhasil ditentukan berdasarkan keterangan pada contoh kasus.	20
3.6	Melakukan IT assessment pada proses MEA01.	Hasil IT assessment pada proses MEA01 berhasil ditentukan berdasarkan keterangan pada contoh kasus.	20
3.7	Melakukan IT assessment pada	Hasil IT assessment pada proses	20

	proses MEA02.	MEA02 berhasil ditentukan berdasarkan keterangan pada contoh kasus.	
		TOTAL	**170**

TUGAS PENDAHULUAN

Untuk dapat menjalankan modul praktikum ini silahkan membaca artikel berikut :

1. COBIT Framework 5

DAFTAR PERTANYAAN

1. Proses apa saja yang terdapat pada dimensi proses BAI berdasarkan COBIT Framework 5 ?
2. Proses apa saja yang terdapat pada dimensi proses DSS berdasarkan COBIT Framework 5 ?
3. Proses apa saja yang terdapat pada dimensi proses MEA berdasarkan COBIT Framework 5 ?

TEORI SINGKAT

–

LAB SETUP

Untuk dapat menjalankan praktikum ini maka harus diketahui kondisi dan hasil pengumpulan bukti audit pada PT. XYZ.

BAI03 – Mengelola identifikasi dan pengembangan solusi.

Untuk dimensi proses BAI03, sebagai berikut :

- Belum ada desain solusi TI yang betul-betul *high-level*, sehingga diberi nilai 25%.
- Belum ada desain dari berbagai komponen solusi TI yang mendetail, sehingga diberi nilai 0%.
- Tidak ada pengembangan berbagai komponen untuk solusi TI, sehingga diberi nilai 0%.
- Sudah dilakukan pengadaan untuk sebagain komponen solusi TI, sehingga diberi nilai 60%.
- Perusahaan belum sepenuhnya mampu membangun berbagai solusi TI, sehingga diberi nilai 50%.
- Belum dijalankannya prosedur penjaminan mutu (QA), sehingga diberi nilai 0%.

- Aktivitas pengujian atas solusi TI belum dipersiapkan dengan matang dan belum ada prosedurnya, sehingga diberi nilai 20%.
- Belum dijalankan sepenuhnya aktivitas pengujian atas solusi TI, sehingga diberi nilai 30%.
- Jika terdapat perubahan pada prasyarat terkait solusi TI, perusahaan belum mampu mengelolanya sama sekali, sehingga diberi nilai 0%.
- Belum ada proses pemutakhiran dan pemeliharaan solusi TI, sehingga diberi nilai 0%.
- Layanan TI belum diindentifikasi dengan cermat dan portofolio layanan TI belum dirumuskan dengan baik, sehingga diberi nilai 50%.

BAI09 – Mengelola aset.

Untuk dimensi proses BAI09, sebagai berikut :

- Perusahaan belum mendata berbagai aset TI organisasi dengan lengkap, sehingga diberi nilai 70%.
- Perusahaan belum mampu mengelola aset-aset kritikal dengan tepat, sehingga diberi nilai 40%.
- Perusahaan belum memahami siklus hidup aset dan belum mampu mengelolanya, sehingga diberi nilai 0%.
- Perusahaan belum mampu sepenuhnya mengoptimalkan biaya aset TI, sehingga diberi nilai 50%.
- Perusahaan belum mampu mengelola license yang dibutuhkan Divisi TI organisasi, sehingga diberi nilai 30%.

DSS01 – Mengelola operasional.

Untuk dimensi proses DSS01, sebagai berikut :

- Perusahaan belum menjalankan berbagai prosedur operasional dengan benar, sehingga diberi nilai 40%.
- Perusahaan belum mampu mengelola layanan TI yang dialihdayakan, sehingga diberi nilai 10%.
- Perusahaan belum dapat memonitor infrastruktur TI dengan benar, sehingga diberi nilai 60%.
- Perusahaan belum mampu sepenuhnya mengelola lingkungan sekitar, sehingga diberi nilai 80%.
- Perusahaan belum mampu sepenuhnya mengelola berbagai fasilitas operasional dan strategis, sehingga diberi nilai 60%.

DSS05 – Mengelola layanan keamanan.

Untuk dimensi proses DSS05, sebagai berikut :

- Belum seluruh perangkat komputer dan server terlindungi dari malware, sehingga diberi nilai 75%.
- Sudah ada pengelolaan jaringan tapi belum sesuai prosedur keamanan informasi, sehingga diberi nilai 50%.
- Belum ada pengelolaan endpoint, sehingga diberi nilai 0%.
- Belum ada IDM (Identity Management), sehingga diberi nilai 0%.
- Belum ada pengelolaan akses fisik terhadap aset TI dengan baik, sehingga diberi nilai 40%.
- Belum ada prosedur pengelolaan dokumen dan peralatan TI yang sensitif, sehingga diberi nilai 0%.
- Pengawasan terhadap infrastruktur TI masih bersifat insidentil, sehingga diberi nilai 20%.

DSS06 – Mengelola kontrol atas proses bisnis.

Untuk dimensi proses DSS06, sebagai berikut :

- Belum ada penyelarasan berbagai aktivitas kontrol yang melekat pada proses bisnis dengan tujuan organisasi, sehingga diberi nilai 0%.
- Belum ada pengawasan yang cukup terhadap pemrosesan informasi pada sistem, sehingga diberi nilai 30%.
- Belum ada pengelolaan peran, tanggung jawab, hak akses, dan level otoritas secara penuh, sehingga diberi nilai 60%.
- Belum ada pihak yang menangani *error* dan eksepsi, sehingga diberi nilai 0%.
- Belum ada penjaminan pelacakan dari peristiwa dan akuntabilitas informasi, sehingga diberi nilai 0%.
- Berbagai aset informasi belum dapat diamankan dengan memadai, sehingga diberi nilai 60%.

MEA01 – Memonitor, mengevaluasi, dan menilai kinerja dan kesesuaian.

Untuk dimensi proses MEA01, sebagai berikut :

- Belum ada metode yang digunakan untuk pengawasan secara intensif, sehingga diberi nilai 30%.
- Belum ditetapkan target kinerja dan kesesuaian dengan standar TI, sehingga diberi nilai 0%.
- Belum ada aktivitas pengumpulan dan pemprosesan data kinerja dan kesesuaian dengan standar TI, sehingga diberi nilai 0%.
- Belum ada aktivitas analisa dan pelaporan kinerja TI, sehingga diberi nilai 0%.
- Belum ada implementasi dari tindakan perbaikan, sehingga diberi nilai 0%.

MEA02 – Memonitor, mengevaluasi, dan menilai sistem kontrol internal.

Untuk dimensi proses MEA02, sebagai berikut :

- Belum ada pengawasan secara penuh terhadap berbagai kontrol internal di perusahaan, sehingga diberi nilai 60%.
- Belum ada pengkajian terhadap efektivitas kontrol atas proses bisnis, sehingga diberi nilai 0%.
- Belum pernah dilakukan *self-assessment* atas kontrol, sehingga diberi nilai 0%.
- Belum pernah dilakukan identifikasi dan pelaporan kekurangan atas kontrol, sehingga diberi nilai 0%.
- Belum ada penyedia penjaminan (asuransi) bersifat independen dan memiliki kualifikasi, sehingga diberi nilai 0%.
- Belum ada perencanaan atas berbagai inisiatif untuk penjaminan (asuransi), sehingga diberi nilai 0%.
- Belum ada penentuan berbagai inisiastif atas penjaminan (asuransi), sehingga diberi nilai 0%.
- Belum dijalankannya berbagai inisiatif atas penjaminan (asuransi), sehingga diberi nilai 0%.

Latihan 3.1. Melakukan IT Assessment Pada Proses BAI03.

Kode	Base Practices	Achievement Level			
		Not Achieved (N)	Partially Achieved (P)	Largely Achieved (L)	Fully Achieved (F)
		0% - 15%	15,01% - 50%	50,01% - 85%	85,01% - 100%
BAI03-BP1	*Design high-level solutions.* Mendesain solusi yang *high-level*.				
BAI03-BP2	*Design detailed solution components.* Mendesain berbagai komponen solusi yang mendetail.				
BAI03-BP3	*Develop solution components.* Mengembangkan berbagai komponen untuk solusi.				
BAI03-BP4	*Procure solution components.* Melakukan pengadaan untuk berbagai komponen solusi.				
BAI03-BP5	*Build solutions.* Membangun berbagai solusi.				
BAI03-BP6	*Perform quality assurance (QA).* Melakukan penjaminan mutu (QA).				
BAI03-BP7	*Prepare for solution testing.* Mempersiapkan untuk pengujian atas solusi.				
BAI03-BP8	*Execute solution testing.* Menjalankan pengujian atas solusi.				
BAI03-BP9	*Manage changes to requirements.* Mengelola berbagai perubahan pada prasyarat.				
BAI03-BP10	*Maintain solutions.* Memelihara berbagai solusi.				
BAI03-BP11	*Define IT services and maintain the service portfolio.* Mendefinisikan berbagai layanan TI dan memelihara				

	portofolio layanan.				
Sub-total					
Total					
Rata-rata					

Latihan 3.2. Melakukan IT Assessment Pada Proses BAI09.

Kode	Base Practices	Achievement Level			
		Not Achieved (N)	Partially Achieved (P)	Largely Achieved (L)	Fully Achieved (F)
		0% - 15%	15,01% - 50%	50,01% - 85%	85,01% - 100%
BAI09-BP1	*Identify and record current assets.* Mengidentifikasi dan merekam berbagai aset saat ini.				
BAI09-BP2	*Manage critical assets.* Mengelola berbagai aset kritikal.				
BAI09-BP3	*Manage the asset life cycle.* Mengelola siklus hidup aset.				
BAI09-BP4	*Optimise asset costs.* Mengoptimasi berbagai biaya aset.				
BAI09-BP5	*Manage licences.* Mengelola berbagai *license*.				
Sub-total					
Total					
Rata-rata					

Latihan 3.3. Melakukan IT Assessment Pada Proses DSS01.

Kode	Base Practices	Achievement Level			
		Not Achieved (N)	Partially Achieved (P)	Largely Achieved (L)	Fully Achieved (F)
		0% - 15%	15,01% - 50%	50,01% - 85%	85,01% - 100%
DSS01-BP1	*Perform operational procedures.* Menjalankan berbagai prosedur operasional.				
DSS01-BP2	*Manage outsourced IT services.* Mengelola berbagai layanan TI yang dialihdayakan.				
DSS01-BP3	*Monitor IT infrastructure.* Memonitor infrastruktur TI.				
DSS01-BP4	*Manage the environment.* Mengelola lingkungan sekitar.				
DSS01-BP5	*Manage facilities.* Mengelola berbagai fasilitas.				
Sub-total					
Total					
Rata-rata					

Latihan 4.4. Melakukan IT Assessment Pada Proses DSS05.

Kode	Base Practices	Achievement Level			
		Not Achieved (N)	Partially Achieved (P)	Largely Achieved (L)	Fully Achieved (F)
		0% - 15%	15,01% - 50%	50,01% - 85%	85,01% - 100%
DSS05-BP1	*Protect against malware.* Perlindungan terhadap *malware*.				
DSS05-BP2	*Manage network and connectivity security.* Mengelola keamanan jaringan dan konektivitas.				
DSS05-BP3	*Manage endpoint security.* Mengelola keamanan *endpoint*.				
DSS05-BP4	*Manage user identity and logical access.* Mengelola identitas dan *logical access* pengguna.				
DSS05-BP5	*Manage physical access to IT assets.* Mengelola akses fisik terhadap aset TI.				
DSS05-BP6	*Manage sensitive documents and output devices.* Mengelola dokumen dan peralatan *output* yang sensitif.				
DSS05-BP7	*Monitor the infrastructure for security-related events.* Mengawasi infrastruktur untuk berbagai peristiwa terkait keamanan.				
	Sub-total				
				Total	
				Rata-rata	

Latihan 3.5. Melakukan IT Assessment Pada Proses DSS06.

Kode	Base Practices	Achievement Level			
		Not Achieved (N)	Partially Achieved (P)	Largely Achieved (L)	Fully Achieved (F)
		0% - 15%	15,01% - 50%	50,01% - 85%	85,01% - 100%
DSS06-BP1	*Align control activities embedded in business processes with enterprise objectives.* Menyelaraskan berbagai aktivitas kontrol yang melekat pada proses bisnis dengan tujuan organisasi.				
DSS06-BP2	*Control the processing of information.* Mengontrol pemrosesan informasi.				
DSS06-BP3	*Manage roles, responsibilities, access privileges and levels of authority.* Mengelola peran, tanggung jawab, hak akses, dan level otoritas.				
DSS06-BP4	*Manage errors and exceptions.* Mengelola *error* dan eksepsi.				
DSS06-BP5	*Ensure traceability of Information events and accountabilities.* Menjamin pelacakan dari peristiwa dan akuntabilitas informasi.				
DSS06-BP6	*Secure information assets.* Mengamankan berbagai aset informasi.				
Sub-total					
Total					
Rata-rata					

Latihan 3.6. Melakukan IT Assessment Pada Proses MEA01.

Kode	Base Practices	Achievement Level			
		Not Achieved (N)	Partially Achieved (P)	Largely Achieved (L)	Fully Achieved (F)
		0% - 15%	15,01% - 50%	50,01% - 85%	85,01% - 100%
MEA01-BP1	*Establish a monitoring approach.* Membangun sebuah pendekatan untuk pengawasan.				
MEA01-BP2	*Set performance and conformance targets.* Menentukan target kinerja dan kesesuaian.				
MEA01-BP3	*Collect and process performance and conformance data.* Mengumpulkan dan memproses data kinerja dan kesesuaian.				
MEA01-BP4	*Analyse and report performance.* Menganalisa dan melaporkan kinerja.				
MEA01-BP5	*Ensure the implementation of corrective actions.* Memastikan implementasi dari tindakan perbaikan.				
	Sub-total				
				Total	
				Rata-rata	

Latihan 3.7. Melakukan IT Assessment Pada Proses MEA02.

Kode	Base Practices	Achievement Level			
		Not Achieved (N)	Partially Achieved (P)	Largely Achieved (L)	Fully Achieved (F)
		0% - 15%	15,01% - 50%	50,01% - 85%	85,01% - 100%
MEA02-BP1	*Monitor internal controls.* Mengawasi berbagai kontrol internal.				
MEA02-BP2	*Review business process controls effectiveness.* Mengkaji efektivitas kontrol atas proses bisnis.				
MEA02-BP3	*Perform control self-assessments.* Melakukan *self-assessment* atas kontrol.				
MEA02-BP4	*Identify and report control deficiencies.* Mengidentifikasi dan melaporkan kekurangan atas kontrol.				
MEA02-BP5	*Ensure that assurance providers are independent and qualified.* Memastikan bahwa penyedia penjaminan (asuransi) bersifat independen dan memiliki kualifikasi.				
MEA02-BP6	*Plan assurance initiatives.* Merencanakan berbagai inisiatif untuk penjaminan (asuransi).				
MEA02-BP7	*Scope assurance initiatives.* Menentukan berbagai inisiastif atas penjaminan (asuransi).				
MEA02-BP8	*Execute assurance initiatives.* Menjalankan berbagai inisiatif atas penjaminan (asuransi).				
	Sub-total				
				Total	

Rata-rata	

MODUL 4 : Membuat Rencana Audit SI

Pokok Bahasan :

- Membuat Rencana Audit SI (ISM314.PRAK.2.0.0-06).
- Membuat Piagam Audit SI (ISM314.PRAK.2.0.0-07).

Sub CPMK 7.1 : Mahasiswa mampu membuat skenario audit SI dan piagam audit dalam praktikum.

No.	Deskripsi Tugas	Indikator Kinerja	Durasi (Menit)
4.1	Membuat Rencana dan Jadwal Audit SI.	Rencana dan jadwal audit SI berhasil dirumuskan berdasarkan keterangan pada contoh kasus.	50
4.2	Membuat Piagam Audit SI.	Piagam audit SI berhasil dirumuskan berdasarkan keterangan pada contoh kasus.	120
		TOTAL	**170**

TUGAS PENDAHULUAN

Untuk dapat menjalankan modul praktikum ini silahkan membaca artikel berikut :

1. Perencanaan audit SI
2. Piagam audit SI

DAFTAR PERTANYAAN

–

TEORI SINGKAT

–

LAB SETUP

Untuk dapat menjalankan praktikum ini maka harus diketahui kondisi dan hasil pengumpulan bukti audit pada PT. XYZ.

Latihan 4.1. Membuat Rencana dan Jadwal Audit SI.

No	Nama Kegiatan	PIC	Bulan 1				Bulan 2				Bulan 3			
			1	2	3	4	1	2	3	4	1	2	3	4
1.	Pengecekan awal proses bisnis saat ini.													
2.	Pengecekan awal kondisi SI/TI saat ini.													
3.	Pengecekan terhadap regulasi.													
4.	Pengecekan pada Divisi Personalia.													
5.	Pengecekan pada Divisi Inventori dan Gudang.													
6.	Pengecekan pada Divisi Produksi.													
7.	Pengecekan pada Divisi Penjualan dan Marketing.													
8.	Pengecekan pada Divisi TI.													
9.	Pengecekan pada *Software*.													
	a. Aplikasi/Sistem A													
	b. Aplikasi/Sistem B													
	c. Aplikasi/Sistem C													
	d. Aplikasi/Sistem D													
	e. Aplikasi/Sistem D													
	f. KMS													
	g. AI dan Expert System													
	h. Database													
10.	Pengecekan pada infrastruktur TI.													
	a. Server A													

	b. Server B													
	c. Server B													
	d. Server D													
	e. Komputer client													
	f. SMTP													
	g. FTP													
	h. Firewall													
	i. Jaringan / akses internet													
	j. VPN													
	k. Hub / switch / access point													
	l. Mekanisme keamanan data dan informasi													
11.	Kontrak dengan vendor terkait layanan pihak ketiga (*third party*).													
12.	Pengecekan pada prosedur, tata kelola, dan kebijakan TI.													
13.	Pengujian terhadap kebenaran bukti audit.													
14.	Pengujian terhadap kesesuaian dengan standar dan *best practise*.													
15.	Pengujian substantif.													
16.	Penilaian terhadap bukti audit.													
17.	Perumusan rekomendasi audit.													
18.	Penyusunan laporan audit TI ringkas (*summary*).													
19.	Penyusunan laporan audit TI detail.													

20.	Penyerahan laporan audit TI kepada pimpinan auditi.													

Latihan 4.2. Membuat Piagam Audit SI.

Latar Belakang :

Struktur Organisasi :

Tujuan audit :

Otoritas :

Tanggung jawab auditor terhadap aktivitas audit SI :

Tanggung jawab auditi terhadap aktivitas audit SI :

Standar dan etika yang digunakan dalam audit SI :

MODUL 5 : Audit Pada Komputer Bersistem Operasi Windows

Pokok Bahasan :

- Melakukan Audit Pada Operasional Komputer (ISM314.PRAK.2.0.0-08).

Sub CPMK 6.2 : Mahasiswa mampu melakukan audit SI pada *hardware*, *software*, dan komponen pendukung SI lainnya dalam praktikum.

No.	Deskripsi Tugas	Indikator Kinerja	Durasi (Menit)
5.1	Melakukan audit pada *setup and general controls*.	Audit pada *setup and general controls* berhasil dilakukan berdasarkan keterangan pada contoh kasus.	60
5.2	Melakukan audit pada layanan, aplikasi yang terinstal, dan *scheduled tasks*.	Audit pada layanan, aplikasi yang terinstal, dan *scheduled tasks* berhasil dilakukan berdasarkan keterangan pada contoh kasus.	15
5.3	Melakukan audit pada *account management* dan *password controls*.	Audit pada *account management* dan *password controls* berhasil dilakukan berdasarkan keterangan pada contoh kasus.	60
5.4	Melakukan audit pada *user rights* dan *security options*.	Audit pada *user rights* dan *secyrity options* berhasil dilakukan berdasarkan keterangan pada contoh kasus.	15
5.5	Melakukan audit pada *network security and controls*.	Audit pada *network security and controls* berhasil dilakukan berdasarkan keterangan pada contoh kasus.	20
		TOTAL	**170**

TUGAS PENDAHULUAN

Untuk dapat menjalankan modul praktikum ini silahkan membaca artikel berikut :

1. Audit pada komputer bersistem operasi Windows.

DAFTAR PERTANYAAN

–

TEORI SINGKAT

–

LAB SETUP

Untuk dapat menjalankan modul praktikum ini, gunakan komputer / notebook Anda yang bersistem operasi Windows.

Latihan 5.1. Melakukan audit pada *setup and general controls*.

No.	Prosedur	Hasil
1.	Dapatkan sistem informasi dan versi *service pack* dan bandingkan dengan prasyarat kebijakan.	
2.	Tentukan apakah server/komputer yang sedang dijalankan menggunakan *firewall* (dalam bentuk *hardware* atau *software*).	
3.	Tentukan apakah server/komputer yang sedang digunakan menggunakan program antivirus.	
4.	Pastikan bahwa seluruh *patch* yang telah disetujui terinstal di setiap server/komputer.	
5.	Tentukan apakah server/komputer yang sedang digunakan menjalankan solusi manajemen *patch.*	

6.	**Kaji dan verifikasi informasi *startup* melalui perintah : msconfig atau dengan menggunakan *tools* lain.**	

Latihan 5.2. Melakukan audit pada layanan, aplikasi yang terinstal, dan *scheduled tasks*.

No.	Prosedur	Hasil
1.	Tentukan layanan apa saja yang dijalankan pada sistem operasi, validasi kebutuhannya dengan *system administrator.*	
2.	Pastikan bahwa hanya aplikasi yang telah disetujui terinstal pada setiap server/komputer.	
3.	Pastikan bahwa hanya *scheduled task* yang telah disetujui untuk dijalankan.	

Latihan 5.3. Melakukan audit pada *account management* dan *password controls*.

No.	Prosedur	Hasil
1.	Mengkaji dan mengevaluasi prosedur untuk pembuatan *user account* dan memastikan bahwa *account* dibuat hanya untuk keperluan bisnis yang sah.	
2.	Memastikan bahwa seluruh *user* dibuat pada level domain dan terhubung ke dalam *active directory.*	
3.	Mengkaji dan mengevaluasi kegunaan *group* dan menentukan batasan-nya.	
4.	Mengkaji dan mengevaluasi kekuatan dari *system password.*	

5.	**Mengevaluasi penggunaan *password control* pada server/komputer (masa berlaku *password*, panjang, kompleksitas, *history*, dan kebijakan *lockout*).**	

Latihan 5.4. Melakukan audit pada *user rights* dan *security options*.

No.	Prosedur	Hasil
1.	Mengkaji dan mengevaluasi penggunaan *user right* dan *security option* yang berlaku pada elemen tersebut dalam *security policy setting.*	

Latihan 5.5. Melakukan audit pada *network security and controls*.

No.	Prosedur	Hasil
1.	Mengkaji dan mengevaluasi penggunaan dan kebutuhan untuk *remote access* (*RAS connection*, FTP, telnet, SSH, VPN, dan metode lainya).	
2.	Memastikan bahwa sebuah *banner* peringatan yang sah ditampilkan ketika terhubung ke sistem.	
3.	Mencari dan mengevaluasi penggunaan *share on the host.*	
4.	Memastikan bahwa dapat diaudit untuk setiap kebijakan keamanan organisasi.	

5.	**Mengkaji dan mengevaluasi prosedur bagi *system administrator* untuk memonitor keadaan keamanan pada sistem.**	
6.	**Ketika mengaudit lingkungan yang besar, tentukan apakah telah ada standar yang dibangun untuk sistem baru dan apakah *baseline* telah sesuai dengan *setting* keamanan.**	
7.	**Menjalankan tahapan audit pada pusat data dan *disaster recovery.***	

MODUL 6 : Audit Pada Pusat Data, Jaringan, Internet, dan e-Commerce

Pokok Bahasan :

- Melakukan Audit Pada Operasional Komputer (ISM314.PRAK.2.0.0-08).

Sub CPMK 6.2 : Mahasiswa mampu melakukan audit SI pada *hardware*, *software*, dan komponen pendukung SI lainnya dalam praktikum.

No.	Deskripsi Tugas	Indikator Kinerja	Durasi (Menit)
6.1	Melakukan audit pada lingkungan di sekitar pusat data.	Audit pada lingkungan di sekitar pusat data berhasil dilakukan berdasarkan keterangan pada contoh kasus.	10
6.2	Melakukan audit pada *physical access control.*	Audit pada *physical access control* berhasil dilakukan berdasarkan keterangan pada contoh kasus.	10
6.3	Melakukan audit pada *environmental control.*	Audit pada *environmental control* berhasil dilakukan berdasarkan keterangan pada contoh kasus.	15
6.4	Melakukan audit pada *power continuity.*	Audit pada *power continuity* berhasil dilakukan berdasarkan keterangan pada contoh kasus.	20
6.5	Melakukan audit pada sistem alarm.	Audit pada sistem alarm berhasil dilakukan berdasarkan keterangan pada contoh kasus.	20
6.6	Melakukan audit pada sistem pemadaman api.	Audit pada sistem pemadaman api berhasil dilakukan berdasarkan keterangan pada contoh kasus.	10
6.7	Melakukan audit pada	Audit pada *surveillance*	10

	surveillance system.	*system* berhasil dilakukan berdasarkan keterangan pada contoh kasus.	
6.8	Melakukan audit pada operasional pusat data.	Audit pada operasional pusat data berhasil dilakukan berdasarkan keterangan pada contoh kasus.	25
6.9	Melakukan audit pada jaringan.	Audit pada jaringan berhasil dilakukan berdasarkan keterangan pada contoh kasus.	20
6.10	Melakukan audit pada fasilitas internet.	Audit audit pada fasilitas internet berhasil dilakukan berdasarkan keterangan pada contoh kasus.	15
6.11	Melakukan audit pada e-Commerce.	Audit pada e-Commerce berhasil dilakukan berdasarkan keterangan pada contoh kasus.	15
		TOTAL	**170**

TUGAS PENDAHULUAN

Untuk dapat menjalankan modul praktikum ini silahkan membaca artikel berikut :

1. Audit pada pusat data.

DAFTAR PERTANYAAN

–

TEORI SINGKAT

–

LAB SETUP

Untuk dapat menjalankan modul praktikum ini, Anda harus mengobservasi *data center*.

–

Latihan 6.1. Melakukan audit pada lingkungan di sekitar pusat data.

No.	Prosedur	Hasil
1.	**Mengkaji penerangan eksterior, building orientation, rambu-rambu, and karakteristik lingkungan sekitar pada *data center* untuk mengidentifikasi fasilitas yang beresiko.**	
2.	**Meneliti lokasi *data center* untuk bahaya di sekitar dan menentukan jarak menuju layanan darurat.**	

Latihan 6.2. Melakukan audit pada *physical access control*.

No.	Prosedur	Hasil
1.	Mengkaji pintu luar dan dinding untuk menentukan apakah sudah cukup melindungi fasilitas *data center.*	
2.	Mengevaluasi peralatan otentikasi fisik untuk menentukan apakah telah mencukupi untuk keadaan tertentu.	
3.	Mengkaji *log* penjagaan keamanan gedung dan dokumentasi lainnya untuk mengevaluasi efektivitas dari fungsi staf keamanan.	
4.	Memverifikasi bahwa beberapa area tertentu telah memiliki keamanan yang cukup.	

Latihan 6.3. Melakukan audit pada *environmental control*.

No.	Prosedur	Hasil
1.	**Memverifikasi bahwa sistem pemanas, ventilasi, dan *air-conditioning* menjaga suhu agar tetap konstan di dalam *data center.***	
2.	**Mengevaluasi penggunaan perisai elektronik pada *data center* untuk memverifikasi bahwa emisi radio tidak mempengaruhi sistem komputer atau emisi sistem tidak dapat digunakan untuk memperoleh akses tak terotorisasi atas informasi sensitif.**	

Latihan 6.4. Melakukan audit pada *power continuity*.

No.	Prosedur	Hasil
1.	Menentukan apakah *data center* memiliki sumber daya listrik cadangan.	
2.	Memverifikasi bahwa sudah ada '*ground to earth*' untuk melindungi sistem komputer.	
3.	Menjamin daya listrik terkondisi untuk mencegah kehilangan data.	
4.	Memverifikasi bahwa *battery backup systems* telah tersedia untuk mengantisipasi *black-outs* dan *brown-outs.*	
5.	Menjamin bahwa generator terlindungi dari kehilangan daya dan bekerja di kondisi yang baik.	

Latihan 6.5. Melakukan audit pada sistem alarm.

No.	Prosedur	Hasil
1.	Menjamin bahwa sebuah *burglar alarm* melindungi *data center* dari gangguan fisik.	
2.	Memverifikasi bahwa *fire alarm* melindungi *data center* dari resiko kebakaran.	
3.	Memverifikasi bahwa *water alarm* dikonfigurasi untuk mendeteksi genangan air di beberapa area yang beresiko tinggi di *data center.*	
4.	Memverifikasi bahwa *humidity alarm* dikonfigurasi untuk memberitahukan staf *data center* atas kondisi kelembaban yang rendah atau tinggi.	
5.	Mengkaji konsol pengawasan alarm dan pelaporan alarm untuk memverifikasi bahwa	

	alarm telah dimonitor secara kontinu oleh staf.	

Latihan 6.6. Melakukan audit pada sistem pemadaman api.

No.	Prosedur	Hasil
1.	Menjamin bahwa konstruksi bangunan *data center* memiliki pemadam kebakaran	
2.	Menjamin staf *data center* dilatih untuk penanganan material dan penyimpanan berbahaya dan sudah ada prosedur yang memadai	
3.	Memverifikasi bahwa pemadam api ditempatkan di setiap 50 kaki di dalam *data center* dan dipelihara dengan baik	
4.	Menjamin bahwa sistem pemadaman api melindungi *data center* dari kebakaran	

Latihan 6.7. Melakukan audit pada *surveillance system*.

No.	Prosedur	Hasil
1.	**Memverifikasi sistem keamanan dirancang dan beroperasi dengan baik.**	

Latihan 6.8. Melakukan audit pada operasional pusat data.

No.	Prosedur	Hasil
1.	Menjamin bahwa prosedur kontrol akses fisik komprehensif dan dijalankan oleh petugas keamanan.	
2.	Mengkaji prosedur pengawasan fasilitas untuk menjamin bahwa kondisi alarm dalam keadaan baik.	
3.	Memverifikasi bahwa pengawasan atas jaringan, sistem operasi, dan aplikasi menyediakan informasi yang cukup untuk mengidentifikasi berbagai masalah potensial.	
4.	Menjamin bahwa peran dan tanggung jawab dari staf *data center* telah dirumuskan dengan baik.	
5.	Memverifikasi bahwa kewajiban dan fungsi kerja dari staf *data center* telah dipisahkan dengan baik.	
6.	Menjamin bahwa prosedur respon darurat diarahkan untuk mengantisipasi ancaman	

	tertentu.	
7.	**Memverifikasi bahwa sistem dan peralatan pada fasilitas *data center* dipelihara dengan baik.**	
8.	**Menjamin bahwa staf *data center* dilatih dengan tepat untuk menunjukkan fungsi kerjanya.**	
9.	**Menjamin bahwa kapasitas *data center* direncanakan untuk menghindari kerugian yang tidak penting.**	
10.	**Memverifikasi bahwa prosedur sudah ada untuk menjamin keamanan penyimpanan dan pembuangan media elektronik.**	

Latihan 6.9. Melakukan audit pada jaringan.

No.	Prosedur	Hasil
1.	Memverifikasi kebijakan dan prosedur keamanan jariangan.	
2.	Memverifikasi sistem antivirus.	
3.	Memverifikasi *firewall* dan hasil *firewall setting.*	
4.	Memverifikasi *network log.*	
5.	Memverifikasi pemonitoran jaringan.	
6.	Memverifikasi sistem deteksi gangguan pada jaringan.	

7.	**Memverifikasi pengendalian terhadap serangan DOS (*Denial of Service*) atau DDOS (*Distributed Denial of Service*).**	
8.	**Memverifikasi enkripsi *user ID* dan *password* pada jaringan.**	
9.	**Memverifikasi hak akses dan *role* pada jaringan.**	
10.	**Memeriksa VPN (*Virtual Private Network*).**	
11.	**Memverifikasi DRP.**	
12.	**Memverifikasi respon terhadap insiden pada jaringan.**	

13.	**Memverifikasi eksposur kegagalan peralatan.**	

Latihan 6.10. Melakukan audit pada fasilitas internet.

No.	Prosedur	Hasil
1.	Memeriksa apakah kebijakan dan prosedur internet telah memenuhi standar keamanan informasi.	
2.	Memverifikasi *public key encryption.*	
3.	Memverifikasi *CA* (*Certificate Authentication*) dan *digital signature.*	
4.	Memeriksa keamanan *website* yang dikunjungi oleh *user.*	
5.	Memeriksa *history* gangguan / insiden pada internet.	
6.	Memeriksa SLA vendor penyedia jasa internet dengan kinerja vendor selama ini.	

Latihan 6.11. Melakukan audit pada e-Commerce.

No.	Prosedur	Hasil
1.	**Memverifikasi keamanan dan integritas berbagai transaksi *e-commerce* dengan menetapkan bahwa pengendalian dapat :** – Mendeteksi dan memperbaiki pesan yang hilang karena adanya kegagalan dalam perlengkapan. – Mencegah dan mendeteksi akses tidak sah dari internal dan internet. – Membuat data yang berhasil didapat oleh pelaku penipuan menjadi tidak berguna.	
2.	**Memverifikasi bahwa berbagai prosedur pembuatan *backup* telah cukup untuk menjaga integritas dan keamanan fisik basis data serta berbagai *file* lainnya yang berhubungan dengan jaringan tersebut.**	
3.	**Memeriksa bahwa semua transaksi EDI diotorisasi, divalidasi, dan sesuai dengan perjanjian kemitraan dagang**	
4.	**Memeriksa bahwa tidak ada perusahaan yang secara tidak sah mengakses berbagai *recors* dalam basis data.**	
5.	**Memeriksa bahwa mitra dagang yang sah hanya**	

	memiliki akses ke hanya data yang diotorisasi.	
6.	**Memeriksa bahwa terdapat pengendalian yang memadai untuk memastikan adanya jejak audit yang lengkap untuk semua transaksi yang melibatkan EDI.**	

MODUL 7 : Audit Untuk Sistem Manajemen Basis Data (DBMS)

Pokok Bahasan :

- Melakukan Audit Pada Operasional Komputer (ISM314.PRAK.2.0.0-08).

Sub CPMK 6.2 : Mahasiswa mampu melakukan audit SI pada *hardware*, *software*, dan komponen pendukung SI lainnya dalam praktikum.

No.	Deskripsi Tugas	Indikator Kinerja	Durasi (Menit)
7.1	Melakukan audit pada *database permissions*.	Audit pada *database permission*berhasil dilakukan berdasarkan keterangan pada contoh kasus.	20
7.2	Melakukan audit pada *operating system security*.	Audit pada *operating system security* berhasil dilakukan berdasarkan keterangan pada contoh kasus.	15
7.3	Melakukan audit pada *password strength and management features*.	Audit pada *password strength and management features* berhasil dilakukan berdasarkan keterangan pada contoh kasus.	15
7.4	Melakukan audit pada *activity monitoring*.	Audit audit pada *activity monitoring* berhasil dilakukan berdasarkan keterangan pada contoh kasus.	10
7.5	Melakukan audit pada *database encryption*.	Audit audit pada *database encryption* berhasil dilakukan berdasarkan keterangan pada contoh kasus.	15
7.6	Melakukan audit pada *database vulnerabilities, integrity, and patching process*.	Audit audit pada *database vulnerabilities, integrity, and patching process* berhasil dilakukan berdasarkan keterangan pada contoh kasus.	20
7.7	Melakukan audit pada fungsi	Audit pada fungsi DBA berhasil	35

	DBA.	dilakukan berdasarkan keterangan pada contoh kasus.	
7.8	Melakukan audit pada proses *backup* DB.	Audit pada proses *backup* DB berhasil dilakukan berdasarkan keterangan pada contoh kasus.	25
7.9	Melakukan audit pada proses *restore* DB.	Audit pada proses *restore* DB berhasil dilakukan berdasarkan keterangan pada contoh kasus.	15
		TOTAL	**170**

TUGAS PENDAHULUAN

Untuk dapat menjalankan modul praktikum ini silahkan membaca artikel berikut :

1. Audit pada DBMS

DAFTAR PERTANYAAN

_

TEORI SINGKAT

_

LAB SETUP

Untuk dapat menjalankan praktikum ini, maka harus diketahui kondisi dan hasil pengumpulan bukti audit pada PT. XYZ.

Latihan 7.1. Melakukan audit pada *database permissions*.

No.	Prosedur	Hasil
1.	Memverifikasi bahwa *database permission* diberikan atau dijalankan dengan tepat untuk level otorisasi yang dibutuhkan.	
2.	Mengkaji *database permission* yang diberikan kepada individu, di luar *group* atau *role.*	
3.	Memastikan bahwa *database permission* tidak secara implisit diberikan dengan tidak tepat	
4.	Mengkaji *dynamic SQL* yang dieksekusi dalam *store procedure.*	
5.	Memastikan bahwa *low-level acess* pada data tabel diimplementasikan dengan tepat.	
6.	Menjalankan PUBLIC *permission* yang tidak dibutuhkan.	

Latihan 7.2. Melakukan audit pada *operating system security*.

No.	Prosedur	Hasil
1.	**Membatasi akses pada sistem operasi.**	
2.	**Membatasi *permission* pada *directory* di mana *database* terinstal.**	
3.	**Membatasi *permission* pada *registry key* yang digunakan oleh *database.***	

Latihan 7.3. Melakukan audit pada *password strength and management features*.

No.	Prosedur	Hasil
1.	Memeriksa *default user name* dan *password.*	
2.	Memeriksa untuk *password* yang dapat ditebak dengan mudah.	
3.	Memeriksa bahwa *pasword management capabilities* telah berjalan.	

Latihan 7.4. Melakukan audit pada *activity monitoring*.

No.	Prosedur	Hasil
1.	Memeriksa bahwa kegiatan audit terlaksana dan termonitor dengan baik.	

Latihan 7.5. Melakukan audit pada *database encryption*.

No.	Prosedur	Hasil
1.	Memverifikasi bahwa *network encryption* dijalankan.	
2.	Memverifikasi bahwa enkripsi data dijalankan jika dibutuhkan.	

Latihan 7.6. Melakukan audit pada *database vulnerabilities, integrity, and patching process*.

No.	Prosedur	Hasil
1.	Memverifikasi bahwa *patch* terbaru untuk *database* telah terinstal.	
2.	Memverifikasi bahwa *database* sedang menggunakan versi yang terus menerus didukung oleh vendor.	
3.	Memverifikasi bahwa berbagai kebijakan dan prosedur telah ditempatkan untuk mengidentifikasi ketika sebuah *patch* dirilis dan dan menjalankan *patch.*	
4.	Memeriksa integritas dari *database* dengan cara mencari *root kit*, virus, *backdoor*, dan *trojan horse.*	

Latihan 7.7. Melakukan audit pada fungsi DBA.

No.	Prosedur	Hasil
1.	**Memeriksa fungsi DBA : Perencanaan basis data** • Mengembangkan strategi basis data organisasi. • Mendefinisikan lingkungan basis data. • Mendefinisikan persyaratan basis data. • Mengembangkan kamus data.	
2.	**Memeriksa fungsi DBA : Desain** • Merancang skema DB. • Merancang tampilan penguna eksternal. • Merancang tampilan internal DB. • Merancang pengendali DB.	
3.	**Memeriksa fungsi DBA : Implementasi** • Menentukan kebijakan akses. • Mengimplementasikan pengendalian keamanan. • Menentukan prosedur pengujian. • Menetapkan standar pemrograman.	
4.	**Memeriksa fungsi DBA : Operasi dan pemeliharaan** • Mengevaluasi kinerja DB. • Mengatur kembali DB sesuai permintaan kebutuhan pengguna (*optimizing*).	
5.	**Memeriksa fungsi DBA : Perubahan dan pertumbuhan** • Merencanakan perubahan dan pertumbuhan data.	

	• Mengevaluasi teknologi baru.	

Latihan 7.8. Melakukan audit pada proses *backup* DB.

No.	Prosedur	Hasil
1.	Memeriksa cadangan *file* secara berurutan (GPC – *Grand Parent-Parent-Children*)	
2.	Memeriksa *file transaksi backup*	
3.	Memeriksa *file akses secara langsung*	
4.	Memeriksa penyimpanan di tempat lain	

Latihan 7.9. Melakukan audit pada proses *restore* DB.

No.	Prosedur	Hasil
1.	**Memverifikasi bahwa cadangan dibuat secara rutin dan mengawasi terjadinya *restore* DB tanpa banyak proses lainnya.**	
2.	**Mengecek *error* yang terjadi selama proses *restore* DB.**	

MODUL 8 : Audit Pencapaian Baseline Keamanan Informasi Berdasarkan ISO/IEC 27002 : 2005 (Bagian 1)

Pokok Bahasan :

- Melakukan Audit Keamanan Informasi Berdasarkan Standar dan *Best Practise* (ISM314.PRAK.2.0.0-09).

Sub CPMK 6.3 : Mahasiswa mampu melakukan identifikasi kebutuhan keamanan SI dan mengecek celah keamanan SI berdasarkan ISO/IEC 27002 : 2005 dalam praktikum.

No.	Deskripsi Tugas	Indikator Kinerja	Durasi (Menit)
8.1	Mengecek Area Domain A.5.	Pengecekan area domain A.5 berhasil dilakukan berdasarkan keterangan pada contoh kasus.	15
8.2	Mengecek Area Domain A.6.	Pengecekan area domain A.6 berhasil dilakukan berdasarkan keterangan pada contoh kasus.	45
8.3	Mengecek Area Domain A.7.	Pengecekan area domain A.7 berhasil dilakukan berdasarkan keterangan pada contoh kasus.	20
8.4	Mengecek Area Domain A.8.	Pengecekan area domain A.8 berhasil dilakukan berdasarkan keterangan pada contoh kasus.	25
8.5	Mengecek Area Domain A.9.	Pengecekan area domain A.9 berhasil dilakukan berdasarkan keterangan pada contoh kasus.	25
8.6	Mengecek Area Domain A.10.	Pengecekan area domain A.10 berhasil dilakukan berdasarkan keterangan	40

		pada contoh kasus.	
		TOTAL	**170**

TUGAS PENDAHULUAN

Untuk dapat menjalankan modul praktikum ini silahkan membaca artikel berikut :

1. Audit berdasarkan risiko SI berdasarkan ISO/IEC 27002 : 2005.

DAFTAR PERTANYAAN

–

TEORI SINGKAT

–

LAB SETUP

Untuk dapat menjalankan praktikum ini, maka harus diketahui kondisi dan hasil pengumpulan bukti audit pada PT. XYZ, sebagai berikut :

- Dokumen kebijakan keamanan informasi sudah ada, tapi belum disosialisasikan ke seluruh staf / karyawan.
- Peninjauan kebijakan keamanan informasi belum pernah dilakukan.
- Komitmen manajemen terhadap keamanan informasi sudah ada, tapi belum didukung oleh seluruh staf / karyawan .
- Koordinasi keamanan informasi sudah dilakukan antara pihak manajemen puncak dengan para kepala divisi.
- Tanggung jawab keamanan informasi sudah dialokasikan ke para staf terpilih.
- Proses otorisasi untuk berbagai fasilitas pemrosesan informasi sudah ditentukan, tetapi belum dijalankan sesuai dengan rencana.
- Perjanjian terkait kerahasiaan belum pernah dibuat dan dijalankan.
- Kontak dengan pihak otoritas terkait sudah dilakukan beberapa kali dalam kurun waktu setahun terakhir.
- Kontak dengan kelompok kepentingan tertentu belum pernah dilakukan.
- Peninjauan keamanan informasi yang independen belum pernah dilakukan.
- Identifikasi risiko terkait pihak eksternal belum pernah dilakukan.
- Penempatan keamanan ketika berhubungan dengan pelanggan belum pernah direncanakan.
- Penempatan keamanan di dalam perjanjian dengan pihak eksternal belum pernah direncanakan.

- Penginventorian aset sudah dilakukan oleh pihak manajemen melalui *Asset Management System*.
- Kepemilikan aset sudah dilakukan dan dipetakan untuk setiap divisi.
- Persetujuan penggunaan aset masih dalam tahap pembahasan bersama seluruh divisi.
- Petunjuk klasifikasi informasi sudah ada.
- Pelabelan dan penanganan informasi sudah dilakukan.
- Peran dan tanggung jawab karyawan telah dirumuskan dan disahkan oleh pihak manajemen.
- Prosedur pemilihan karyawan baru telah dirumuskan dan disahkan oleh pihak manajemen.
- Syarat dan kondisi diterima bekerja baru telah dirumuskan dan disahkan oleh pihak manajemen.
- Tanggung jawab manajemen selama karyawan bekerja telah dirumuskan dan disahkan oleh pihak manajemen.
- Kesadaran, edukasi, dan pelatihan terkait keamanan informasi telah dilakukan secara berkala (bulanan).
- Proses penertiban / pendisiplinan telah dirumuskan dan disahkan oleh pihak manajemen melalui pemberian *reward* dan *punishment*.
- Tanggung jawab pemberhentian karyawan telah dirumuskan dan disahkan oleh pihak manajemen.
- Prosedur pengembalian aset dari karyawan yang diberhentikan / pensiun telah dirumuskan dan disahkan oleh pihak manajemen.
- Prosedur penghapusan hak akses dari karyawan yang diberhentikan / pensiun telah dirumuskan dan disahkan oleh pihak manajemen.
- Batasan keamanan fisik pada area yang aman telah ditentukan oleh pihak manajemen.
- Kontrol masuk secara fisik pada area yang aman telah ditentukan oleh pihak manajemen.
- Prosedur pengamanan kantor, ruangan, dan fasilitas telah dirumuskan dan disahkan oleh pihak manajemen.
- Prosedur perlindungan terhadap ancaman eksternal dan lingkungan telah dirumuskan dan disahkan oleh pihak manajemen.
- Kepastian bekerja dalam area yang aman telah ditentukan oleh pihak manajemen.
- Area untuk akses publik, pengantaran, dan pemuatan telah ditentukan oleh pihak manajemen.
- Prosedur penempatan dan perlindungan atas perlengkapan telah dirumuskan dan disahkan oleh pihak manajemen.

- Peralatan pendukung telah disiapkan dan ditempatkan di tempat-tempat tertentu.
- Pengamanan kabel telah dilakukan.
- Prosedur pemeliharaan peralatan telah dirumuskan dan disahkan oleh pihak manajemen.
- Keamanan peralatan di lokasi telah dilakukan oleh pihak keamanan.
- Prosedur keamanan pembuangan atau penggunaan kembali atas peralatan yang ada telah dirumuskan dan disahkan oleh pihak manajemen.
- Prosedur pemindahan properti telah dirumuskan dan disahkan oleh pihak manajemen.
- Prosedur operasional telah terdokumentasi.
- Manajemen perubahan belum dirumuskan oleh pihak manajemen.
- Pemisahan kewenangan / tugas telah dilakukan melalui sop.
- Pemisahan antara fasilitas pengembangan, pengujian, dan operasional telah dilakukan.
- Pemberian layanan oleh pihak ketiga telah dilakukan.
- Pengawasan dan peninjauan layanan pihak ketiga dilakukan setiap akhir kontrak kerjasama.
- Pengelolaan perubahan pada layanan pihak ketiga telah dilakukan oleh divisi ti.
- Manajemen kapasitas sistem belum dirumuskan.
- Prosedur penerimaan sistem baru atau ter-*update* telah dirumuskan dan disahkan oleh pihak manajemen.
- Prosedur kontrol atas kode berbahaya telah dirumuskan dan disahkan oleh pihak manajemen.
- Prosedur kontrol atas kode yang bersifat *mobile* berbahaya telah dirumuskan dan disahkan oleh pihak manajemen.
- Prosedur *back-up* informasi telah dirumuskan dan disahkan oleh pihak manajemen.
- Prosedur kontrol jaringan telah dirumuskan dan disahkan oleh pihak manajemen.
- Prosedur keamanan layanan pada jaringan telah dirumuskan dan disahkan oleh pihak manajemen.
- Manajemen media *removable* telah dirumuskan dan disahkan oleh pihak manajemen.
- Prosedur pembuangan media telah dirumuskan dan disahkan oleh pihak manajemen.
- Prosedur penanganan informasi telah dirumuskan dan disahkan oleh pihak manajemen.

- Prosedur keamanan dokumentasi sistem telah dirumuskan dan disahkan oleh pihak manajemen.
- Kebijakan dan Prosedur Pertukaran Informasi telah dirumuskan dan disahkan oleh pihak manajemen.
- Perjanjian pertukaran informasi telah dirumuskan dan disahkan oleh pihak manajemen.
- Prosedur media fisik yang singgah belum dirumuskan oleh pihak manajemen.
- Prosedur pengiriman pesan elektronik belum dirumuskan oleh pihak manajemen.
- Prosedur sistem informasi bisnis telah dirumuskan dan disahkan oleh pihak manajemen.
- Prosedur e-commerce belum dirumuskan oleh pihak manajemen.
- Prosedur transaksi *on-line* belum dirumuskan oleh pihak manajemen.
- Prosedur pembuatan *log* audit belum dirumuskan oleh pihak manajemen.
- Prosedur pemantauan penggunaan sistem belum dirumuskan oleh pihak manajemen.
- Prosedur perlindungan untuk informasi pada *log* belum dirumuskan oleh pihak manajemen.
- *Log* administrator dan operator belum dirumuskan oleh pihak manajemen.
- Prosedur pembuatan *log* untuk kesalahan belum dirumuskan oleh pihak manajemen.
- Sinkronisasi waktu untuk pemantauan belum dirumuskan oleh pihak manajemen.

Latihan 8.1. Mengecek Area Domain A.5.

Komponen Yang Dikontrol		*Control Item*		Keterangan
A.5.1	**Kebijakan Keamanan Informasi**	A.5.1.1	Dokumen Kebijakan Keamanan Informasi	
		A.5.1.2	Peninjauan Kebijakan Keamanan Informasi	

Latihan 8.2. Mengecek Area Domain A.6.

Komponen Yang Dikontrol		*Control Item*		Keterangan
A.6.1	**Organisasi Internal**	A.6.1.1	Komitmen Manajemen Terhadap Keamanan Informasi	
		A.6.1.2	Koordinasi Keamanan Informasi	
		A.6.1.3	Alokasi Tanggung Jawab Keamanan Informasi	
		A.6.1.4	Proses Otorisasi Untuk Berbagai Fasilitas Pemrosesan Informasi	
		A.6.1.5	Perjanjian Terkait Kerahasiaan	
		A.6.1.6	Kontak Dengan Pihak Otoritas	
		A.6.1.7	Kontak Dengan Kelompok Kepentingan Tertentu	

		A.6.1.8	Peninjauan Keamanan Informasi Yang Independen	
A.6.2	**Pihak Eksternal**	A.6.2.1	Identifikasi Risiko Terkait Pihak Eksternal	
		A.6.2.2	Penempatan Keamanan Ketika Berhubungan Dengan Pelanggan	
		A.6.2.3	Penempatan Keamanan Di Dalam perjanjian Dengan Pihak Eksternal	

Latihan 8.3. Mengecek Area Domain A.7.

Komponen Yang Dikontrol		*Control Item*		Keterangan
A.7.1	**Tanggung Jawab Atas Aset**	A.7.1.1	Penginventorian Aset	
		A.7.1.2	Kepemilikan Aset	
		A.7.1.3	Persetujuan Penggunaan Aset	
A.7.2	**Klasifikasi Informasi**	A.7.2.1	Petunjuk Klasifikasi	
		A.7.2.2	Pelabelan dan Penanganan Informasi	

Latihan 8.4. Mengecek Area Domain A.8.

Komponen Yang Dikontrol		*Control Item*		Keterangan
A.8.1	**Sebelum Karyawan Diterima Bekerja**	A.8.1.1	Peran dan Tanggung Jawab	
		A.8.1.2	Pemilihan	
		A.8.1.3	Syarat dan Kondisi Diterima Bekerja	
A.8.2	**Selama Karyawan Diterima Bekerja**	A.8.2.1	Tanggung Jawab Manajemen	
		A.8.2.2	Kesadaran, Edukasi, dan Pelatihan Terkait Keamanan Informasi	
		A.8.2.3	Proses Penertiban / Pendisiplinan	
A.8.3	**Pemberhentian atau Pergantian Karyawan**	A.8.3.1	Tanggung Jawab Pemberhentian	

		A.8.3.2	Pengembalian Aset	
		A.8.3.3	Penghapusan Hak Akses	

Latihan 8.5. Mengecek Area Domain A.9.

Komponen Yang Dikontrol		*Control Item*		Keterangan
A.9.1	**Area Yang Aman**	A.9.1.1	Batasan Keamanan Fisik	
		A.9.1.2	Kontrol Masuk Secara Fisik	
		A.9.1.3	Pengamanan Kantor, Ruangan, dan Fasilitas	
		A.9.1.4	Perlindungan Terhadap Ancaman Eksternal dan Lingkungan	
		A.9.1.5	Bekerja Dalam Area Yang Aman	
		A.9.1.6	Area Untuk Akses Publik, Pengantaran, dan Pemuatan	
A.9.2	**Keamanan Perlengkapan**	A.9.2.1	Penempatan dan	

			Perlindungan Atas Perlengkapan	
		A.9.2.2	Peralatan Pendukung	
		A.9.2.3	Pengamanan Kabel	
		A.9.2.4	Pemeliharaan Peralatan	
		A.9.2.5	Keamanan Peralatan Di Lokasi	
		A.9.2.6	Keamanan Pembuangan atau Penggunaan Kembali Atas Peralatan Yang Ada	
		A.9.2.7	Pemindahan Properti	

Latihan 8.6. Mengecek Area Domain A.10.

Komponen Yang Dikontrol		*Control Item*		Keterangan
A.10.1	**Prosedur dan Tanggung Jawab Operasional**	A.10.1.1	Prosedur Operasional Terdokumentasi	
		A.10.1.2	Manajemen Perubahan	
		A.10.1.3	Pemisahan Kewenangan / Tugas	
		A.10.1.4	Pemisahan Antara Fasilitas Pengembangan, Pengujian, dan Operasional	
A.10.2	**Manajemen Pemberian Layanan Oleh Pihak Ketiga**	A.10.2.1	Pemberian Layanan	
		A.10.2.2	Pengawasan dan Peninjauan Layanan Pihak	

			Ketiga	
		A.10.2.3	Pengelolaan Perubahan Pada Layanan Pihak Ketiga	
A.10.3	**Perencanaan dan Penerimaan Sistem**	A.10.3.1	Manajemen Kapasitas	
		A.10.3.2	Penerimaan Sistem	
A.10.4	**Perlindungan Terhadap Kode Yang Berbahaya dan Bersifat *Mobile***	A.10.4.1	Kontrol Atas Kode Berbahaya	
		A.10.4.2	Kontrol Atas Kode Yang Bersifat *Mobile*	
A.10.5	***Back-up***	A.10.5.1	*Back-up* Informasi	

A.10.6	**Manajemen Keamanan Jaringan**	A.10.6.1	Kontrol Jaringan	
		A.10.6.2	Keamanan Layanan Pada Jaringan	
A.10.7	**Penanganan Media**	A.10.7.1	Manajemen Media *Removable*	
		A.10.7.2	Pembuangan Media	
		A.10.7.3	Prosedur Penanganan Informasi	
		A.10.7.4	Keamanan Dokumentasi Sistem	

A.10.8	**Pertukaran Informasi**	A.10.8.1	Kebijakan dan Prosedur Pertukaran Informasi	
		A.10.8.2	Perjanjian Pertukaran	
		A.10.8.3	Media Fisik Yang Singgah	
		A.10.8.4	Pengiriman Pesan Elektronik	
		A.10.8.5	Sistem Informasi Bisnis	
A.10.9	**Layanan e-Commerce**	A.10.9.1	e-Commerce	

		A.10.9.2	Transaksi *On-line*	
		A.10.9.3	Informasi yang Tersedia Bagi Publik	
A.10.10	**Pemantauan**	A.10.10.1	Pembuatan *Log* Audit	
		A.10.10.2	Pemantauan Penggunaan Sistem	
		A.10.10.3	Perlindungan Untuk Informasi Pada *Log*	
		A.10.10.4	*Log* Administrator dan Operator	

		A.10.10.5	Pembuatan *Log* Untuk Kesalahan	
		A.10.10.6	Sinkronisasi Waktu	

MODUL 9 : Audit Pencapaian Baseline Keamanan Informasi Berdasarkan ISO/IEC 27002 : 2005 (Bagian 2)

Pokok Bahasan :

- Melakukan Audit Keamanan Informasi Berdasarkan Standar dan *Best Practise* (ISM314.PRAK.2.0.0-09).

Sub CPMK 6.3 : Mahasiswa mampu melakukan identifikasi kebutuhan keamanan SI dan mengecek celah keamanan SI berdasarkan ISO/IEC 27002 : 2005 dalam praktikum.

No.	Deskripsi Tugas	Indikator Kinerja	Durasi (Menit)
9.1	Mengecek Area Domain A.11	Pengecekan area domain A.11 berhasil dilakukan berdasarkan keterangan pada contoh kasus.	50
9.2	Mengecek Area Domain A.12	Pengecekan area domain A.12 berhasil dilakukan berdasarkan keterangan pada contoh kasus.	50
9.3	Mengecek Area Domain A.13	Pengecekan area domain A.13 berhasil dilakukan berdasarkan keterangan pada contoh kasus.	25
9.4	Mengecek Area Domain A.14	Pengecekan area domain A.14 berhasil dilakukan berdasarkan keterangan pada contoh kasus.	15
9.5	Mengecek Area Domain A.15	Pengecekan area domain A.10 berhasil dilakukan berdasarkan keterangan pada contoh kasus.	30
		TOTAL	**170**

TUGAS PENDAHULUAN

Untuk dapat menjalankan modul praktikum ini silahkan membaca artikel berikut :

1. Audit berdasarkan risiko SI berdasarkan ISO/IEC 27002 : 2005.

DAFTAR PERTANYAAN

–

TEORI SINGKAT

–

LAB SETUP

Untuk dapat menjalankan praktikum ini, maka harus diketahui kondisi dan hasil pengumpulan bukti audit pada PT. XYZ, sebagai berikut :

- Kebijakan pengendalian akses sudah dirumuskan dan disahkan oleh pihak manajemen.
- Prosedur registrasi pengguna sudah dirumuskan dan dijalankan.
- Manajemen hak akses sudah sudah dirumuskan dan dijalankan.
- Manajemen *password* pengguna sudah sudah dirumuskan dan dijalankan.
- Peninjauan hak akses pengguna belum sudah dirumuskan.
- Prosedur penggunaan *password* sudah dirumuskan dan dijalankan.
- Prosedur perlengkapan milik pengguna yang tidak diawasi belum dirumuskan.
- Kebijakan meja dan layar tampilan yang bersih sudah dirumuskan dan dijalankan.
- Kebijakan untuk penggunaan layanan pada jaringan sudah dirumuskan dan dijalankan.
- Prosedur otentikasi pengguna untuk koneksi eksternal sudah dirumuskan dan dijalankan.
- Prosedur identifikasi peralatan dalam jaringan sudah dirumuskan dan dijalankan.
- Prosedur perlindungan atas *port* yang didiagnostik dan dikonfigurasi secara *remote* belu dirumuskan.
- Prosedur pemisahan dalam jaringan sudah dirumuskan dan dijalankan.
- Prosedur pengendalian koneksi pada jaringan sudah dirumuskan dan dijalankan.
- Prosedur pengendalian *routing* jaringan sudah dirumuskan dan dijalankan.
- Prosedur *log-on* yang aman sudah dirumuskan dan dijalankan.

- Prosedur prosedur identifikasi dan otentikasi pengguna sudah dirumuskan dan dijalankan.
- Sistem manajemen *password* sudah diimplementasikan.
- Prosedur penggunaan program utilitas milik sistem belum dirumuskan.
- Prosedur *session time-out* belum dirumuskan.
- Prosedur pembatasan waktu koneksi sudah dirumuskan dan dijalankan.
- Prosedur pembatasan akses informasi sudah dirumuskan dan dijalankan.
- Prosedur isolasi sistem yang sensistif belum dirumuskan.
- Prosedur komputasi dan komunikasi secara *mobile* sudah dirumuskan dan dijalankan.
- Prosedur *teleworking* belum dirumuskan.
- Prosedur analisis dan spesifikasi kebutuhan keamanan si belum dirumuskan.
- Prosedur validasi data *input* / masukan si sudah dirumuskan dan dijalankan.
- Prosedur pengendalian atas proses internal si sudah dirumuskan dan dijalankan.
- Prosedur integritas / kelengkapan pesan dalam si sudah dirumuskan dan dijalankan.
- Prosedur validasi data *output* / keluaran si sudah dirumuskan dan dijalankan.
- Kebijakan terkait penggunaan kontrol secara kriptografi sudah dirumuskan dan dijalankan.
- Penentuan karyawan inti belum dilakukan.
- Prosedur pengendalian *software* operasional sudah dirumuskan dan dijalankan.
- Prosedur perlindungan atas data pengujian sistem sudah dirumuskan dan dijalankan.
- Prosedur pengendalian akses terhadap *source code* program sudah dirumuskan dan dijalankan.
- Prosedur pengendalian perubahan belum dirumuskan.
- Prosedur peninjauan teknis pada aplikasi setelah perubahan sistem operasi sudah dirumuskan dan dijalankan.
- Prosedur pembatasan pada perubahan paket perangkat lunak sudah dirumuskan dan dijalankan.
- Prosedur kebocoran informasi sudah dirumuskan dan dijalankan.
- Prosedur pengembangan perangkat lunak *outsourcing* belum dirumuskan.
- Prosedur pengendalian atas kerentanan teknis belum dirumuskan.
- Mekanisme pelaporan kejadian terkait keamanan informasi sudah dirumuskan dan dijalankan.

- Mekanisme pelaporan kelemahan terkait keamanan sudah dirumuskan dan dijalankan.
- Tanggung jawab dan prosedur manajemen insiden dan perbaikan terkait keamanan informasi sudah dirumuskan dan dijalankan.
- Proses pembelajaran dari insiden terkait keamanan informasi dijalankan.
- Pengumpulan bukti terkait keamanan informasi sudah dirumuskan dan dijalankan.
- Aspek keamanan informasi sudah dimasukkan ke dalam proses manajemen kontinuitas bisnis.
- Kontinuitas bisnis dan penilaian resiko sudah dilakukan.
- Pengembangan dan pelaksanaan rencana kontinuitas termasuk keamanan informasi sudah dilakukan.
- Kerangka kerja perencanaan kontinuitas bisnis belum dirumuskan.
- Pengujian, pemeliharaan, dan penilaian kembali dari rencana kontinuitas bisnis belum dilakukan.
- Identifikasi peraturan yang berlaku sudah dilakukan secara berkala (bulanan).
- Aspek hak kekayaan intelektual (hki) sudah diperhatikan.
- Perlindungan atas *record* organisasi sudah dilakukan.
- Perlindungan data dan privasi informasi personal sudah dilakukan.
- Pencegahan atas penyalahgunaan fasilitas pengolahan informasi belum sepenuhnya dilakukan, yaitu pada divisi pemasaran dan divisi inventori.
- Regulasi atas pengendalian secara kriptografi belum dijalankan.
- Kepatuhan dengan kebijakan dan standar keamanan belum dilakukan speenuhnya.
- Pengecekan kepatuhan teknis belum pernah dilakukan.
- Pengendalian audit sistem informasi belum dilakukan.
- Perlindungan atas perangkat audit sistem informasi belum dilakukan.

Latihan 9.1. Mengecek Area Domain A.11.

Komponen Yang Dikontrol		*Control Item*		Keterangan
A.11.1	**Kebutuhan Bisnis Akan Pengendalian Akses**	A.11.1.1	Kebijakan Pengendalian Akses	
A.11.2	**Manajemen Akses Pengguna**	A.11.2.1	Registrasi Pengguna	
		A.11.2.2	Manajemen Hak Akses	
		A.11.2.3	Manajemen *Password* Pengguna	
		A.11.2.4	Peninjauan Hak Akses Pengguna	
A.11.3	**Tanggung Jawab Pengguna**	A.11.3.1	Penggunaan *Password*	

		A.11.3.2	Perlengkapan Milik Pengguna Yang Tidak Diawasi	
		A.11.3.3	Kebijakan Meja dan Layar Tampilan Yang Bersih	
A.11.4	**Pengendalian Akses Jaringan**	A.11.4.1	Kebijakan Untuk Penggunaan Layanan Pada Jaringan	
		A.11.4.2	Otentikasi Pengguna Untuk Koneksi Eksternal	
		A.11.4.3	Identifikasi Peralatan Dalam Jaringan	

		A.11.4.4	Perlindungan Atas *Port* Yang Didiagnostik dan Dikonfigurasi Secara *Remote*	
		A.11.4.5	Pemisahan Dalam Jaringan	
		A.11.4.6	Pengendalian Koneksi Pada Jaringan	
		A.11.4.7	Pengendalian *Routing* Jaringan	

A.11.5	**Pengendalian Akses Pada Sistem Operasi**	A.11.5.1	Prosedur *Log-on* Yang Aman	
		A.11.5.2	Identifikasi dan Otentikasi Pengguna	
		A.11.5.3	Sistem Manajemen *Password*	
		A.11.5.4	Penggunaan Program Utilitas Milik Sistem	

		A.11.5.5	*Session Time-out*	
		A.11.5.6	Pembatasan Waktu Koneksi	
A.11.6	**Pengendalian Akses Terhadap Aplikasi dan Informasi.**	A.11.6.1	Pembatasan Akses Informasi	
		A.11.6.2	Isolasi Sistem Yang Sensistif	
A.11.7	**Komputasi *Mobile* dan *Teleworking***	A.11.7.1	Komputasi dan Komunikasi Secara *Mobile*	

		A.11.7.2	*Teleworking*	

Latihan 9.2. Mengecek Area Domain A.12.

Komponen Yang Dikontrol		*Control Item*		Keterangan
A.12.1	**Kebutuhan Keamanan Pada Sistem Informasi**	A.12.1.1	Analisis dan Spesifikasi Kebutuhan Keamanan	
A.12.2	**Proses Perbaikan Dalam Aplikasi**	A.12.2.1	Validasi Data *Input* / Masukan	
		A.12.2.2	Pengendalian atas proses internal	
		A.12.2.3	Integritas / Kelengkapan Pesan	
		A.12.2.4	Validasi Data *Output* / Keluaran	
A.12.3	**Pengendalian Secara Kriptografi**	A.12.3.1	Kebijakan Terkait Penggunaan Kontrol	

			Secara Kriptografi	
		A.12.3.2	Karyawan Inti	
A.12.4	**Keamanan Sistem *File***	A.12.4.1	Pengendalian *Software* Operasional	
		A.12.4.2	Perlindungan Atas Data Pengujian Sistem	
		A.12.4.3	Pengendalian Akses Terhadap *Source Code* Program	
A.12.5	**Keamanan Dalam Proses Pengembangan Dan Pemberian Dukungan**	A.12.5.1	Prosedur Pengendalian Perubahan	

		A.12.5.2	Tinjauan Teknis Pada Aplikasi Setelah Perubahan Sistem Operasi	
		A.12.5.3	Pembatasan Pada Perubahan Paket Perangkat Lunak	
		A.12.5.4	Kebocoran Informasi	
		A.12.5.5	Pengembangan Perangkat Lunak *Outsourcing*	
A.12.6	**Manajemen Terkait Kerentanan Teknis**	A.12.6.1	Pengendalian Atas Kerentanan Teknis	

Latihan 9.3. Mengecek Area Domain A.13.

Komponen Yang Dikontrol		*Control Item*		Keterangan
A.13.1	**Pelaporan Atas Kejadian dan Kelemahan Terkait Keamanan Informasi**	A.13.1.1	Pelaporan Kejadian Terkait Keamanan Informasi	
		A.13.1.2	Pelaporan Kelemahan terkait Keamanan	
A.13.2	**Manajemen Insiden dan Perbaikan Terkait Keamanan Informasi**	A.13.2.1	Tanggung Jawab dan Prosedur	
		A.13.2.2	Pembelajaran Dari Insiden Terkait Keamanan Informasi	
		A.13.2.3	Pengumpulan Bukti	

Latihan 9.4. Mengecek Area Domain A.14.

Komponen Yang Dikontrol		*Control Item*		Keterangan
A.14.1	**Aspek Keamanan Informasi Pada Manajemen Kontinuitas Bisnis**	A.14.1.1	Memasukkan Keamanan Informasi Ke Dalam Proses Manajemen Kontinuitas Bisnis	
		A.14.1.2	Kontinuitas Bisnis dan Penilaian Resiko	
		A.14.1.3	Pengembangan dan Pelaksanaan Rencana Kontinuitas Termasuk Keamanan Informasi	
		A.14.1.4	Kerangka Kerja Perencanaan Kontinuitas Bisnis	

		A.14.1.5	Pengujian, Pemeliharaan, dan Penilaian Kembali Dari Rencana Kontinuitas Bisnis	

Latihan 9.5. Mengecek Area Domain A.15.

Komponen Yang Dikontrol		*Control Item*		Keterangan
A.15.1	**Kepatuhan Dengan Persyaratan Hukum**	A.15.1.1	Identifikasi Peraturan Yang Berlaku	
		A.15.1.2	Hak Kekayaan Intelektual (HKI)	
		A.15.1.3	Perlindungan Atas *Record* Organisasi	
		A.15.1.4	Perlindungan Data dan Privasi Informasi Personal	
		A.15.1.5	Pencegahan Atas Penyalahgunaan Fasilitas Pengolahan Informasi	

		A.15.1.6	Regulasi Atas Pengendalian Secara Kriptografi	
A.15.2	**Kepatuhan Dengan Kebijakan dan Standar Keamanan, dan Kepatuhan Teknis**	A.15.2.1	Kepatuhan Dengan Kebijakan dan Standar Keamanan	
		A.15.2.2	Pengecekan Kepatuhan Teknis	
A.15.3	**Organisasi**	A.15.3.1	Pengendalian Audit Sistem Informasi	

		A.15.3.2	Perlindungan Atas Perangkat Audit Sistem Informasi	

MODUL 10 : Membuat Laporan Audit SI/TI Yang Lengkap

Pokok Bahasan :

– Melakukan Laporan Audit SI Sederhana (ISM314.PRAK.2.0.0-10).

Sub CPMK 8.1 : Mahasiswa mampu membuat laporan audit sistem informasi secara sederhana dalam praktikum.

No.	Deskripsi Tugas	Indikator Kinerja	Durasi (Menit)
10.1	Membuat laporan audit SI/TI secara sederhana.	Laporan audit SI/TI secara sederhana berhasil dilakukan berdasarkan keterangan pada contoh kasus.	170
		TOTAL	**170**

TUGAS PENDAHULUAN

Untuk dapat menjalankan modul praktikum ini silahkan membaca artikel berikut :

1. Pembuatan laporan audit SI.

DAFTAR PERTANYAAN

–

TEORI SINGKAT

–

LAB SETUP

–

Latihan 10.1. Membuat laporan audit SI/TI secara sederhana.

Struktur Dokumen Audit SI/TI

BAB I PENDAHULUAN
1.1 Latar Belakang
1.2 Tujuan Audit SI
1.3 Ruang Lingkup Audit SI
1.4 Sistematika Laporan Audit SI

BAB II PROFIL AUDITI
2.1 Visi-Misi-Tujuan Organisasi
2.2 Struktur Organisasi
2.3 Proses Bisnis

BAB III PERSIAPAN AUDIT SI
3.1 Tim Auditor
3.2 Tim Auditi
3.3 Otoritas
3.4 Tanggung Jawab Auditor Terhadap Aktivitas Audit SI
3.5 Tanggung Jawab Auditi Terhadap Aktivitas Audit SI
3.6 Standar dan Etika Yang Digunakan Dalam Audit SI
3.7 Jadwal dan Rencana Pelaksanaan Audit SI
3.8 Metodologi / Pendekatan / Tools Yang Digunakan
3.9 Peran Pihak Auditor Eksternal

BAB IV PELAKSANAAN AUDIT SI
4.1 Hasil Audit Berdasarkan COBIT 5
4.2 Hasil Audit Keamanan Informasi Berdasarkan ISO/IEC 27002 : 2005
4.3 Rekomendasi Audit SI
4.4 Pihak Yang Berhak Mendapatkan Hasil Audit SI

BAB V PENUTUP
5.1 Kesimpulan Audit SI
5.2 Penutupan

<Untuk laporan audit SI, silahkan kerjakan di lembar berikutnya>

FORM UMPAN BALIK

Modul	Tingkat Kesulitan	Tingkat Ketertarikan	Waktu Penyelesaian (menit)
Modul 1 : IT Assessment Berdasarkan COBIT 5 (Bagian 1)	☐ Sangat Mudah ☐ Mudah ☐ Biasa ☐ Sulit ☐ Sangat Sulit	☐ Tidak Tertarik ☐ Cukup Tertarik ☐ Tertarik ☐ Sangat Tertarik	170
Modul 2 : IT Assessment Berdasarkan COBIT 5 (Bagian 2)	☐ Sangat Mudah ☐ Mudah ☐ Biasa ☐ Sulit ☐ Sangat Sulit	☐ Tidak Tertarik ☐ Cukup Tertarik ☐ Tertarik ☐ Sangat Tertarik	170
Modul 3 : IT Assessment Berdasarkan COBIT 5 (Bagian 3)	☐ Sangat Mudah ☐ Mudah ☐ Biasa ☐ Sulit ☐ Sangat Sulit	☐ Tidak Tertarik ☐ Cukup Tertarik ☐ Tertarik ☐ Sangat Tertarik	170
Modul 4 : Membuat Rencana Audit SI	☐ Sangat Mudah ☐ Mudah ☐ Biasa ☐ Sulit ☐ Sangat Sulit	☐ Tidak Tertarik ☐ Cukup Tertarik ☐ Tertarik ☐ Sangat Tertarik	170

Modul 5 : Audit Pada Komputer Bersistem Operasi Windows	☐ Sangat Mudah ☐ Mudah ☐ Biasa ☐ Sulit ☐ Sangat Sulit	☐ Tidak Tertarik ☐ Cukup Tertarik ☐ Tertarik ☐ Sangat Tertarik	170
Modul 6 : Audit Pada Pusat Data, Jaringan, Internet, dan e-Commerce	☐ Sangat Mudah ☐ Mudah ☐ Biasa ☐ Sulit ☐ Sangat Sulit	☐ Tidak Tertarik ☐ Cukup Tertarik ☐ Tertarik ☐ Sangat Tertarik	170
Modul 7 : Audit Untuk Sistem Manajemen Basis Data (DBMS)	☐ Sangat Mudah ☐ Mudah ☐ Biasa ☐ Sulit ☐ Sangat Sulit	☐ Tidak Tertarik ☐ Cukup Tertarik ☐ Tertarik ☐ Sangat Tertarik	170
Modul 8 : Audit Pencapaian Baseline Keamanan Informasi Berdasarkan ISO/IEC 27002 : 2005 (Bagian 1)	☐ Sangat Mudah ☐ Mudah ☐ Biasa ☐ Sulit ☐ Sangat Sulit	☐ Tidak Tertarik ☐ Cukup Tertarik ☐ Tertarik ☐ Sangat Tertarik	170
Modul 9 : Audit Pencapaian Baseline Keamanan Informasi Berdasarkan ISO/IEC 27002 : 2005 (Bagian 2)	☐ Sangat Mudah ☐ Mudah ☐ Biasa ☐ Sulit ☐ Sangat Sulit	☐ Tidak Tertarik ☐ Cukup Tertarik ☐ Tertarik ☐ Sangat Tertarik	170

Modul 10 : Membuat Laporan Audit SI/TI Yang Lengkap	☐ Sangat Mudah ☐ Mudah ☐ Biasa ☐ Sulit ☐ Sangat Sulit	☐ Tidak Tertarik ☐ Cukup Tertarik ☐ Tertarik ☐ Sangat Tertarik	170

Saran / Masukan :
