

EVALUASI & AUDIT TI

# FINAL PROJECT



## **GROUP 06**

---

Muhammad Khotib - 05211540000061

Gregorius Yudistira Effendy - 05211540000125

Yasin Awwab - 05211540000127

## Bab 1

### Executive Summary

Institut Teknologi Sepuluh Nopember (ITS) merupakan salah satu perguruan tinggi terkemuka di Indonesia. Sebagai salah satu perguruan tinggi berbasis sains dan teknologi tertua di Indonesia, ITS menyediakan teknologi informasi untuk mendukung aktivitas-aktivitas yang berjalan didalamnya, seperti akademik, penelitian, dan pengabdian masyarakat. Untuk menjaga agar teknologi informasi yang ada tetap tersedia dan terjamin, maka dibutuhkan suatu badan yang bertugas untuk mengelola teknologi informasi tersebut.

Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) Institut Teknologi Sepuluh Nopember (ITS) Surabaya adalah sebuah badan yang memiliki wewenang untuk menyediakan dan mengelola layanan teknologi informasi yang ada di ITS, dimana layanan tersebut mendukung aktivitas akademik, penelitian, pengabdian masyarakat, serta manajerial ITS guna mencapai visi dan misinya. Untuk dapat memastikan bahwa layanan teknologi informasi yang ada di ITS tersedia dan dikelola dengan baik, perlu adanya suatu standar yang menjadi acuan dalam menentukan kebutuhan penetapan, penerapan, pemeliharaan dan peningkatan sistem manajemen keamanan informasi di ITS. Selain itu, juga perlu adanya standar yang berfungsi sebagai acuan dalam memilih kontrol pada proses penerapan sistem manajemen keamanan informasi. DPTSI dalam hal ini telah menggunakan kerangka kerja dan standar yang relevan, yaitu ISO/IEC 27001:2013 dalam menentukan kebutuhan penetapan, penerapan, pemeliharaan dan peningkatan sistem manajemen keamanan informasi, serta menggunakan ISO/IEC 27002:2013 dalam memilih kontrol pada proses penerapan sistem manajemen keamanan informasi. Namun dalam prakteknya, belum ada perangkat audit yang jelas yang dapat digunakan oleh DPTSI untuk memastikan bahwa seluruh kegiatan-kegiatan yang berlangsung di dalam DPTSI telah sesuai dengan standar yang telah digunakan. Oleh karena itu, diperlukan sebuah perangkat audit yang dapat digunakan DPTSI untuk memastikan kegiatan-kegiatan yang dilakukan telah sesuai dengan standar yang digunakan.

Dokumen proyek akhir ini bertujuan untuk memberikan sebuah perangkat audit yang dapat digunakan oleh DPTSI untuk memastikan standar ISO/IEC 27001:2013 telah benar-benar diterapkan. Perangkat audit ini menggunakan standar ISO/IEC27002:2013 dengan berfokus kepada audit berbasis resiko (*risk-based audit*). Harapannya dengan adanya perangkat audit ini, DPTSI dapat menerapkan standar dengan baik dan resiko-resiko yang dimiliki oleh DPTSI dapat dimitigasi, serta meminimalisir adanya *uncertainty* yang mungkin terjadi.

## Bab 2

### Pendahuluan

#### 1. Latar Belakang

Institut Teknologi Sepuluh Nopember (ITS) merupakan salah satu perguruan tinggi terkemuka di Indonesia. Sebagai salah satu perguruan tinggi berbasis sains dan teknologi tertua di Indonesia, ITS menyediakan teknologi informasi untuk mendukung aktivitas-aktivitas yang berjalan didalamnya, seperti akademik, penelitian, dan pengabdian masyarakat. Untuk menjaga agar teknologi informasi yang ada tetap tersedia dan terjamin, maka dibutuhkan suatu badan yang bertugas untuk mengelola teknologi informasi tersebut.

Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) Institut Teknologi Sepuluh Nopember (ITS) Surabaya adalah sebuah badan yang memiliki wewenang untuk menyediakan dan mengelola layanan teknologi informasi yang ada di ITS, dimana layanan tersebut mendukung aktivitas akademik, penelitian, pengabdian masyarakat, serta manajerial ITS guna mencapai visi dan misinya. Untuk dapat memastikan bahwa layanan teknologi informasi yang ada di ITS tersedia dan dikelola dengan baik, perlu adanya suatu standar yang menjadi acuan dalam menentukan kebutuhan penetapan, penerapan, pemeliharaan dan peningkatan sistem manajemen keamanan informasi di ITS. Selain itu, juga perlu adanya standar yang berfungsi sebagai acuan dalam memilih kontrol pada proses penerapan sistem manajemen keamanan informasi. DPTSI dalam hal ini telah menggunakan kerangka kerja dan standar yang relevan, yaitu ISO/IEC 27001:2013 dalam menentukan kebutuhan penetapan, penerapan, pemeliharaan dan peningkatan sistem manajemen keamanan informasi, serta menggunakan ISO/IEC 27002:2013 dalam memilih kontrol pada proses penerapan sistem manajemen keamanan informasi.

ISO/IEC 27001:2013 merupakan standar internasional yang menyediakan persyaratan untuk penetapan, penerapan, pemeliharaan, dan peningkatan sistem manajemen keamanan informasi. ISO/IEC 27001:2013 terdiri dari sistem manajemen keamanan informasi dalam mengamankan kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) informasi dengan menerapkan proses manajemen resiko. Sedangkan ISO/IEC 27002:2013 merupakan standar internasional yang dirancang bagi organisasi sebagai acuan dalam memilih kontrol pada proses penerapan sistem manajemen keamanan informasi berdasarkan ISO/IEC 27001.

Namun dalam prakteknya, belum ada perangkat audit yang jelas yang dapat digunakan oleh DPTSI untuk memastikan bahwa seluruh kegiatan-kegiatan yang berlangsung di dalam DPTSI telah sesuai dengan standar yang telah digunakan. Oleh karena itu, diperlukan sebuah perangkat audit yang dapat digunakan DPTSI untuk memastikan kegiatan-kegiatan yang dilakukan telah sesuai dengan standar yang digunakan.

## 2. Rumusan Masalah

Berdasarkan latar belakang yang telah dijabarkan, masalah yang hendak diselesaikan antara lain:

1. Apa saja resiko keamanan yang terjadi di DPTSI?
2. Apa saja kontrol yang dapat memitigasi resiko keamanan yang mungkin terjadi?
3. Bagaimana bentuk perangkat audit yang dapat digunakan untuk menerapkan kontrol-kontrol tersebut?

## 3. Tujuan

Berdasarkan latar belakang dan rumusan masalah, tugas akhir ini bertujuan untuk :

1. Mengetahui kontrol apa saja yang dapat dilakukan untuk memitigasi resiko yang ditemukan.
2. Menghasilkan perangkat audit yang dapat digunakan untuk memastikan bahwa kontrol-kontrol yang ditemukan dilaksanakan dengan baik.

## 4. Manfaat

Manfaat yang diharapkan didapat dari tugas akhir ini adalah:

1. DPTSI dapat menggunakan perangkat audit ini untuk memastikan bahwa aktivitas-aktivitas yang berjalan di DPTSI telah sesuai dengan standar ISO/IEC 27001 dan ISO/IEC 27002.
2. Dapat dijadikan rujukan untuk Pembuatan perangkat audit.

## 5. Ruang Lingkup

Ruang lingkup dalam pengerjaan tugas akhir ini adalah:

1. Berfokus kepada resiko-resiko dengan tingkat “Sedang” yang telah diidentifikasi oleh Alif Satria Perdana.
2. Standar yang digunakan adalah ISO/IEC 27002:2013.

## 6. Luaran

Luaran pengerjaan tugas akhir ini adalah dokumen perangkat audit berdasarkan kontrol-kontrol yang telah dipetakan untuk memitigasi suatu resiko.

### Bab 3

#### Control Mapping

No	Resiko	Penyebab	Sub-Clause	Kontrol	Implementation Guidance	Poin-Poin Kontrol
1	Sistem informasi/server tidak bisa diakses	Jaringan kabel pada sistem server terputus	11.2.4 Equipment Maintenance	Memastikan pemeliharaan atau perawatan terhadap aset untuk menjamin keberlangsungan ketersediaan dan keutuhannya.	<p>Panduan berikut untuk pemeliharaan peralatan harus dipertimbangkan:</p> <ul style="list-style-type: none"> <li>a) Peralatan harus dipelihara sesuai dengan interval dan spesifikasi layanan yang direkomendasikan oleh pemasok;</li> <li>b) Hanya personil perawatan yang berwenang yang harus melakukan perbaikan dan peralatan servis;</li> <li>c) Rekaman harus dijaga dari semua kesalahan yang dicurigai atau aktual, dan dari semua pemeliharaan preventif dan korektif;</li> <li>d) Kontrol yang sesuai harus dilaksanakan ketika peralatan dijadwalkan untuk pemeliharaan, dengan mempertimbangkan apakah pemeliharaan ini dilakukan oleh personel di lokasi atau di luar organisasi; bila perlu, informasi rahasia harus dibersihkan dari peralatan atau personil pemeliharaan harus cukup dibersihkan;</li> <li>e) Semua persyaratan perawatan yang diberlakukan oleh polis asuransi harus dipenuhi;</li> <li>f) Sebelum menempatkan peralatan kembali ke dalam operasi setelah pemeliharaannya, itu harus diperiksa untuk memastikan bahwa peralatan tidak rusak dan tidak berfungsi</li> </ul>	
				Memastikan kabel daya dan telekomunikasi yang	Panduan keamanan pemasangan kabel :	

			11.2.3 <i>Cabling security</i>	membawa data atau layanan informasi pendukung harus dilindungi dari intersepsi, interferensi atau kerusakan.	a) Jaringan listrik dan telekomunikasi harus berada di bawah tanah, jika memungkinkan, atau tunduk pada perlindungan alternatif yang memadai; b) Kabel harus dipisahkan dari kabel komunikasi untuk mencegah interferensi; c) Untuk kontrol sistem sensitif atau kritis lebih lanjut untuk dipertimbangkan termasuk: a. Pemasangan saluran berlapis baja dan ruangan atau kotak terkunci pada titik inspeksi dan terminasi b. Penggunaan perisai elektromagnetik untuk melindungi kabel; c. Inisiasi pembersihan teknis dan pemeriksaan fisik untuk perangkat yang tidak sah yang melekat pada kabel; d. Akses terkontrol untuk menambal panel dan ruang kabel	
			11.2.2 <i>Supporting Utilities</i>	Memastikan peralatan atau aset harus terbebas dari masalah listrik dan gangguan lainnya yang mengakibatkan kegagalan dalam aset pendukung	<i>Supporting Utilities</i> (misalnya listrik, telekomunikasi, pasokan air, gas, limbah, ventilasi, dan pendingin udara) harus: a) sesuai dengan spesifikasi pabrikan peralatan dan persyaratan hukum setempat; b) dinilai secara berkala untuk kapasitas mereka untuk memenuhi pertumbuhan bisnis dan interaksi dengan utilitas pendukung lainnya; c) diperiksa dan diuji secara teratur untuk memastikan fungsinya yang tepat; d) jika perlu, waspada untuk mendeteksi malfungsi; e) jika perlu, memiliki beberapa umpan dengan beragam perutean fisik.	
	Kapasitas <i>memory</i> tidak sanggup melayani akses	12.1.3 <i>Capacity management</i>	Kontrol yang memastikan penggunaan dari sumber daya	Persyaratan kapasitas harus diidentifikasi, dengan mempertimbangkan kekritisian bisnis dari sistem yang bersangkutan.	<ul style="list-style-type: none"><li>• Pengidentifikasian kapasitas</li><li>• Pengelolaan permintaan kapasitas</li></ul>	

		yang banyak sekaligus		haruslah dipantau, disesuaikan, dan proyeksi untuk kebutuhan kapasitas di masa yang akan datang untuk memastikan kinerja sistem sesuai dengan kebutuhan	<p>Penyetelan dan pemantauan sistem harus diterapkan untuk memastikan dan, bila perlu, meningkatkan ketersediaan dan efisiensi sistem.</p> <p>Kontrol detektif harus dilakukan untuk menunjukkan masalah pada waktunya.</p> <p>Proyeksi persyaratan kapasitas masa depan harus mempertimbangkan kebutuhan bisnis dan sistem baru serta tren saat ini dan yang diproyeksikan dalam kemampuan pemrosesan informasi organisasi.</p> <p>Perhatian khusus perlu diberikan pada sumber daya apa pun dengan waktu tunggu pengadaan yang lama atau biaya tinggi; oleh karena itu manajer harus memantau pemanfaatan sumber daya sistem kunci. Mereka harus mengidentifikasi tren dalam penggunaan, terutama dalam kaitannya dengan aplikasi bisnis atau alat manajemen sistem informasi. Manajer harus menggunakan informasi ini untuk mengidentifikasi dan menghindari potensi kemacetan dan ketergantungan pada personel kunci yang mungkin menjadi ancaman terhadap keamanan atau layanan sistem, dan merencanakan tindakan yang tepat.</p> <p>Menyediakan kapasitas yang memadai dapat dicapai dengan meningkatkan kapasitas atau dengan mengurangi permintaan. Contoh pengelolaan permintaan kapasitas meliputi:</p> <ul style="list-style-type: none"> <li>a) penghapusan data yang tidak terpakai (ruang disk);</li> <li>b) dekomisioning aplikasi, sistem, basis data atau lingkungan;</li> <li>c) mengoptimalkan proses dan jadwal batch;</li> <li>d) mengoptimalkan logika aplikasi atau kueri basis data;</li> <li>e) menolak atau membatasi bandwidth untuk layanan yang haus sumber daya jika ini bukan bisnis penting (misalnya streaming video).</li> </ul>	
2	Kerusakan perangkat keras	Tidak dilakukan <i>maintenance</i> dengan baik	11.2.4 <i>Equipment Maintenance</i>	Kontrol yang memastikan pemeliharaan atau perawatan terhadap	Panduan berikut untuk pemeliharaan peralatan harus dipertimbangkan:	

		terhadap perangkat		aset guna memastikan aset dapat digunakan dalam proses bisnis	<ul style="list-style-type: none"> <li>g) Peralatan harus dipelihara sesuai dengan interval dan spesifikasi layanan yang direkomendasikan oleh pemasok;</li> <li>h) Hanya personil perawatan yang berwenang yang harus melakukan perbaikan dan peralatan servis;</li> <li>i) Rekaman harus dijaga dari semua kesalahan yang dicurigai atau aktual, dan dari semua pemeliharaan preventif dan korektif;</li> <li>j) Kontrol yang sesuai harus dilaksanakan ketika peralatan dijadwalkan untuk pemeliharaan, dengan mempertimbangkan apakah pemeliharaan ini dilakukan oleh personel di lokasi atau di luar organisasi; bila perlu, informasi rahasia harus dibersihkan dari peralatan atau personil pemeliharaan harus cukup dibersihkan;</li> <li>k) Semua persyaratan perawatan yang diberlakukan oleh polis asuransi harus dipenuhi;</li> <li>l) Sebelum menempatkan peralatan kembali ke dalam operasi setelah pemeliharaannya, itu harus diperiksa untuk memastikan bahwa peralatan tidak rusak dan tidak berfungsi</li> </ul>	
		Ruangan yang tidak terkunci	<i>11.2.1 Equipment siting and protection</i>	Kontrol yang memastikan peralatan atau aset diletakkan dan dilindungi untuk mengurangi risiko dan ancaman dari lingkungan dan kemungkinan akses dari pihak yang tidak sah	<p>Panduan berikut harus dipertimbangkan untuk melindungi peralatan:</p> <ul style="list-style-type: none"> <li>a) Peralatan harus ditempatkan untuk meminimalkan akses yang tidak perlu ke area kerja;</li> <li>b) fasilitas pemrosesan informasi yang menangani data sensitif harus diposisikan dengan hati-hati untuk mengurangi risiko informasi yang dilihat oleh orang yang tidak berwenang selama penggunaannya;</li> <li>c) fasilitas penyimpanan harus diamankan untuk menghindari akses yang tidak sah;</li> <li>d) barang yang membutuhkan perlindungan khusus harus dijaga untuk mengurangi tingkat perlindungan umum yang diperlukan;</li> </ul>	



					<p>e) kontrol harus diadopsi untuk meminimalkan risiko potensi ancaman fisik dan lingkungan, misalnya pencurian, kebakaran, bahan peledak, asap, air (atau kegagalan pasokan air), debu, getaran, efek kimia, gangguan pasokan listrik, gangguan komunikasi, radiasi elektromagnetik dan vandalisme;</p> <p>f) pedoman untuk makan, minum dan merokok di dekat fasilitas pengolahan informasi harus ditetapkan;</p> <p>g) kondisi lingkungan, seperti suhu dan kelembaban, harus dipantau untuk kondisi yang dapat mempengaruhi operasi fasilitas pemrosesan informasi;</p> <p>h) proteksi petir harus diterapkan ke semua bangunan dan filter pelindung petir harus dipasang ke semua jalur daya dan komunikasi yang masuk;</p> <p>i) penggunaan metode perlindungan khusus, seperti membran keyboard, harus dipertimbangkan untuk peralatan di lingkungan industri;</p> <p>a) peralatan pengolahan informasi rahasia harus dilindungi untuk meminimalkan risiko kebocoran informasi karena emanasi elektromagnetik.</p>	
			<p><i>12.1.1 Documented operations procedures</i></p>	<p>Kontrol yang memastikan dokumentasi prosedur untuk setiap pengguna yang membutuhkan</p>	<p>Prosedur terdokumentasi harus disiapkan untuk kegiatan operasional yang terkait dengan pemrosesan informasi dan fasilitas komunikasi, seperti start-up komputer dan prosedur penutupan, pencadangan, pemeliharaan peralatan, penanganan media, ruang komputer dan manajemen penanganan surat dan keamanan.</p> <p>Prosedur operasi harus menentukan instruksi operasional, termasuk:</p> <p>a) Instalasi dan konfigurasi sistem; pengolahan dan penanganan informasi baik secara otomatis maupun manual; cadangan;</p>	<ul style="list-style-type: none"> <li>• Prosedur yang terdokumentasi harus disiapkan</li> <li>• Prosedur harus menentukan instruksi operasional</li> <li>• Prosedur operasi harus diperlakukan secara formal</li> </ul>

					<ul style="list-style-type: none"> <li>b) Persyaratan penjadwalan, termasuk interdependensi dengan sistem lain, awal pekerjaan paling awal dan waktu penyelesaian pekerjaan terbaru;</li> <li>c) Instruksi untuk menangani kesalahan atau kondisi luar biasa lainnya, yang mungkin timbul selama pelaksanaan pekerjaan, termasuk pembatasan penggunaan utilitas sistem;</li> <li>d) Kontak dukungan dan eskalasi termasuk kontak dukungan eksternal dalam hal kesulitan operasional atau teknis yang tidak terduga;</li> <li>e) Keluaran khusus dan instruksi penanganan media, seperti penggunaan alat tulis khusus atau pengelolaan output rahasia termasuk prosedur untuk pembuangan output dengan aman dari pekerjaan yang gagal (lihat 8.3 dan 11.2.7)</li> <li>f) Restart sistem dan prosedur pemulihan untuk digunakan jika terjadi kegagalan sistem; pengelolaan jejak audit dan informasi log sistem;</li> <li>g) Prosedur pemantauan.</li> </ul> <p>Prosedur operasi dan prosedur terdokumentasi untuk aktivitas sistem harus diperlakukan sebagai formal dokumen dan perubahan yang disahkan oleh manajemen. Dimana secara teknis layak, sistem informasi harus dikelola secara konsisten, menggunakan prosedur, alat, dan utilitas yang sama.</p>	
3	Server overheat	Pendingin ruangan server mati	11.2.2 Supporting Utilities	Memastikan peralatan atau aset harus terbebas dari masalah listrik dan gangguan lainnya yang mengakibatkan kegagalan dalam aset pendukung	<p><i>Supporting Utilities</i> (misalnya listrik, telekomunikasi, pasokan air, gas, limbah, ventilasi, dan pendingin udara) harus:</p> <ul style="list-style-type: none"> <li>f) sesuai dengan spesifikasi pabrikan peralatan dan persyaratan hukum setempat;</li> <li>g) dinilai secara berkala untuk kapasitas mereka untuk memenuhi pertumbuhan bisnis dan interaksi dengan utilitas pendukung lainnya;</li> </ul>	

					<p>h) diperiksa dan diuji secara teratur untuk memastikan fungsinya yang tepat;</p> <p>i) jika perlu, waspada untuk mendeteksi malfungsi;</p> <p>j) jika perlu, memiliki beberapa umpan dengan beragam perutean fisik.</p>	
4	Pembobolan sistem oleh pihak yang tidak bertanggung jawab	Penyalahgunaan wewenang	6.1.1 Information security roles and responsibilities	Memastikan semua tanggung jawab keamanan informasi harus didefinisikan dan dialokasikan	<p>Alokasi tanggung jawab keamanan informasi harus dilakukan sesuai dengan kebijakan keamanan informasi. Tanggung jawab untuk melindungi aset individu dan untuk melaksanakan proses keamanan informasi spesifik harus diidentifikasi. Tanggung jawab untuk kegiatan manajemen risiko keamanan informasi dan khususnya untuk penerimaan risiko residual harus ditentukan. Tanggung jawab ini harus dilengkapi, bila perlu, dengan panduan yang lebih rinci untuk situs tertentu dan fasilitas pemrosesan informasi. Tanggung jawab lokal untuk melindungi aset dan untuk melaksanakan proses keamanan spesifik harus ditentukan.</p> <p>Individu dengan tanggung jawab keamanan informasi yang dialokasikan dapat mendelegasikan tugas-tugas keamanan kepada orang lain. Namun demikian mereka tetap bertanggung jawab dan harus menentukan bahwa setiap tugas yang didelegasikan telah dilakukan dengan benar.</p> <p>Area di mana individu yang bertanggung jawab harus dinyatakan. Khususnya hal-hal berikut harus terjadi:</p> <ul style="list-style-type: none"> <li>a) Proses aset dan keamanan informasi harus diidentifikasi dan didefinisikan;</li> <li>b) Entitas yang bertanggung jawab untuk setiap aset atau proses keamanan informasi harus ditugaskan dan rincian tanggung jawab ini harus didokumentasikan;</li> <li>c) Tingkat otorisasi harus didefinisikan dan didokumentasikan;</li> <li>d) Untuk dapat memenuhi tanggung jawab di bidang keamanan informasi, individu yang ditunjuk harus kompeten di bidang tersebut</li> </ul>	<ul style="list-style-type: none"> <li>• Mengidentifikasi proses keamanan aset dan informasi</li> <li>• Menentukan penanggung jawab tiap keamanan aset dan informasi</li> <li>• Menentukan level otoritas</li> </ul>

					<p>dan diberikan kesempatan untuk mengikuti perkembangan terkini;</p> <p>e) Koordinasi dan pengawasan aspek keamanan informasi hubungan pemasok harus diidentifikasi dan didokumentasikan.</p>	
			<p><i>7.1.2 Term and conditions of employment</i></p>	<p>Mengatur perjanjian mengenai tanggung jawab pegawai, kontraktor, dan organisasi terhadap keamanan informasi</p>	<p>Kewajiban kontrak untuk karyawan atau kontraktor harus mencerminkan kebijakan organisasi untuk keamanan informasi selain klarifikasi dan menyatakan:</p> <ul style="list-style-type: none"> <li>a) Bahwa semua karyawan dan kontraktor yang diberi akses ke informasi rahasia harus menandatangani perjanjian kerahasiaan atau non-pengungkapan sebelum diberikan akses ke fasilitas pemrosesan informasi (lihat 13.2.4);</li> <li>b) Tanggung jawab dan hak hukum karyawan atau kontraktor, misalnya mengenai undang-undang hak cipta atau undang-undang perlindungan data (lihat 18.1.2 dan 18.1.4);</li> <li>c) Tanggung jawab untuk klasifikasi informasi dan manajemen aset organisasi yang terkait dengan informasi, fasilitas pemrosesan informasi dan layanan informasi yang ditangani oleh karyawan atau kontraktor (lihat Klausul 8);</li> <li>d) Tanggung jawab karyawan atau kontraktor untuk penanganan informasi yang diterima dari perusahaan lain atau pihak eksternal;</li> <li>e) Tindakan yang harus diambil jika karyawan atau kontraktor mengabaikan persyaratan keamanan organisasi (lihat 7.2.3).</li> </ul> <p>Peran dan tanggung jawab keamanan informasi harus dikomunikasikan kepada kandidat pekerjaan selama proses pra-kerja.</p> <p>Organisasi harus memastikan bahwa karyawan dan kontraktor menyetujui persyaratan dan ketentuan terkait keamanan informasi yang sesuai dengan sifat dan tingkat akses yang mereka miliki terhadap aset organisasi yang terkait dengan sistem dan layanan informasi.</p>	<ul style="list-style-type: none"> <li>• Mengidentifikasi pegawai dan kontraktor yang diberi akses</li> <li>• Pembuatan perjanjian mengenai tanggung jawab pegawai dan kontraktor</li> <li>• Pembuatan tindakan apabila ada pelanggaran</li> </ul>

					Apabila diperlukan, tanggung jawab yang terkandung dalam syarat dan ketentuan kerja harus berlanjut untuk jangka waktu tertentu setelah akhir pekerjaan (lihat 7.3).	
			7.2.2 Information security awareness, education, and training	Mengatur mengenai pendidikan dan pelatihan terhadap karyawan dan kontraktor mengenai keamanan informasi secara rutin sesuai dengan fungsi masing-masing.	<p>Program kesadaran keamanan informasi harus bertujuan untuk membuat karyawan dan, jika relevan, kontraktor menyadari tanggung jawab mereka untuk keamanan informasi dan sarana dimana tanggung jawab tersebut dilepaskan.</p> <p>Program kesadaran keamanan informasi harus ditetapkan sesuai dengan kebijakan keamanan informasi organisasi dan prosedur yang relevan, dengan mempertimbangkan informasi organisasi yang akan dilindungi dan kontrol yang telah diterapkan untuk melindungi informasi.</p> <p>Program penyadaran harus mencakup sejumlah kegiatan peningkatan kesadaran seperti kampanye (misalnya "hari keamanan informasi") dan menerbitkan buket atau buletin.</p> <p>Program kesadaran harus direncanakan dengan mempertimbangkan peran karyawan dalam organisasi, dan, jika relevan, harapan organisasi akan kesadaran kontraktor. Kegiatan dalam program kesadaran harus dijadwalkan dari waktu ke waktu, sebaiknya secara teratur, sehingga kegiatan diulang dan mencakup karyawan dan kontraktor baru. Program kesadaran juga harus diperbarui secara berkala agar tetap sejalan dengan kebijakan dan prosedur organisasi, dan harus dibangun berdasarkan pembelajaran dari insiden keamanan informasi.</p> <p>Pelatihan kesadaran harus dilakukan seperti yang disyaratkan oleh program kesadaran keamanan informasi organisasi. Pelatihan kesadaran dapat menggunakan media pengiriman yang berbeda termasuk pembelajaran berbasis kelas, jarak jauh,</p>	<ul style="list-style-type: none"> <li>• Pembuatan program kesadaran keamanan informasi</li> <li>• Penyesuaian program kesadaran keamanan informasi dengan fungsi pegawai di organisasi</li> <li>• Pengembangan lanjutan program kesadaran keamanan informasi</li> </ul>

					<p>berbasis web, serba cepat dan lain-lain.</p> <p>Pendidikan dan pelatihan keamanan informasi juga harus mencakup aspek-aspek umum seperti:</p> <ul style="list-style-type: none"> <li>a) Menyatakan komitmen manajemen terhadap keamanan informasi di seluruh organisasi;</li> <li>b) Kebutuhan untuk mengenal dan mematuhi peraturan dan kewajiban keamanan informasi yang berlaku, sebagaimana didefinisikan dalam kebijakan, standar, hukum, peraturan, kontrak, dan perjanjian;</li> <li>c) Pertanggungjawaban pribadi atas tindakan dan tidak adanya tindakan sendiri, dan tanggung jawab umum untuk mengamankan atau melindungi informasi milik organisasi dan pihak eksternal;</li> <li>d) Prosedur keamanan informasi dasar (seperti pelaporan insiden keamanan informasi) dan kontrol baseline (seperti keamanan kata sandi, kontrol malware dan meja yang jelas);</li> <li>e) Titik kontak dan sumber daya untuk informasi tambahan dan saran tentang masalah keamanan informasi, termasuk materi pendidikan dan pelatihan keamanan informasi lebih lanjut.</li> </ul> <p>Pendidikan dan pelatihan keamanan informasi harus dilakukan secara berkala. Pendidikan dan pelatihan awal berlaku bagi mereka yang beralih ke posisi atau peran baru dengan persyaratan keamanan informasi yang sangat berbeda, tidak hanya untuk pemula baru dan harus dilakukan sebelum peran menjadi aktif.</p> <p>Organisasi harus mengembangkan program pendidikan dan pelatihan untuk melakukan pendidikan dan pelatihan secara efektif. Program harus sejalan dengan kebijakan keamanan informasi organisasi dan prosedur yang relevan, dengan mempertimbangkan informasi organisasi</p>	
--	--	--	--	--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

			9.2.3 Management of privileged access rights	Memastikan alokasi dan penggunaan hak akses harus dibatasi dan dikontrol/ dikendalikan	<p>Alokasi hak akses istimewa harus dikontrol melalui proses otorisasi resmi sesuai dengan kebijakan kontrol akses yang relevan (lihat kontrol 9.1.1). Langkah-langkah berikut harus dipertimbangkan:</p> <ol style="list-style-type: none"> <li>hak akses istimewa yang terkait dengan setiap sistem atau proses, mis. sistem operasi, sistem manajemen basis data dan setiap aplikasi dan pengguna yang perlu dialokasikan harus diidentifikasi;</li> <li>hak akses istimewa harus dialokasikan kepada pengguna berdasarkan kebutuhan penggunaan dan atas dasar peristiwa demi peristiwa sesuai dengan kebijakan kontrol akses (lihat 9.1.1), yaitu berdasarkan persyaratan minimum untuk peran fungsional mereka;</li> <li>proses otorisasi dan catatan semua hak istimewa yang dialokasikan harus dipertahankan. Hak akses istimewa tidak boleh diberikan hingga proses otorisasi selesai;</li> <li>persyaratan untuk berakhirnya hak akses istimewa harus didefinisikan;</li> <li>hak akses istimewa harus ditetapkan ke ID pengguna yang berbeda dari yang digunakan untuk kegiatan bisnis biasa. Kegiatan bisnis biasa tidak boleh dilakukan dari ID istimewa;</li> <li>kompetensi pengguna dengan hak akses istimewa harus ditinjau secara berkala untuk memverifikasi apakah mereka sesuai dengan tugasnya;</li> <li>prosedur khusus harus ditetapkan dan dipelihara untuk menghindari penggunaan yang tidak sah dari ID pengguna administrasi generik, sesuai dengan kemampuan konfigurasi sistem;</li> <li>untuk ID pengguna administrasi generik, kerahasiaan informasi otentikasi rahasia harus dipertahankan ketika dibagikan (mis. mengubah kata sandi sering dan sesegera</li> </ol>	<ul style="list-style-type: none"> <li>Mengidentifikasi hak akses istimewa terkait sistem dan proses</li> <li>Penyesuaian hak akses dengan kebutuhan pengguna</li> <li>Pembuatan prosedur khusus agar tidak ada pelanggaran hak akses</li> <li>Penggantian kata sandi verifikasi secara berkala</li> </ul>
--	--	--	----------------------------------------------	----------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

					mungkin ketika pengguna istimewa meninggalkan atau mengubah pekerjaan, mengkomunikasikannya di antara pengguna istimewa dengan mekanisme yang sesuai).	
			9.2.6 Removal or adjusment of access rights	Memastikan hak akses untuk semua karyawan dan pengguna eksternal terhadap informasi dan fasilitas pemrosesan informasi harus dihapus setelah pemutusan kerja, kontrak, atau perjanjian atau disesuaikan dengan perubahan	<ul style="list-style-type: none"> <li>a) Setelah penghentian, hak akses individu terhadap informasi dan aset yang terkait dengan fasilitas dan layanan pemrosesan informasi harus dihapus atau ditangguhkan. Ini akan menentukan apakah perlu untuk menghapus hak akses.</li> <li>b) Perubahan pekerjaan harus tercermin dalam penghapusan semua hak akses yang tidak disetujui untuk pekerjaan baru.</li> <li>c) Hak akses yang harus dihapus atau disesuaikan termasuk akses fisik dan logis. Penghapusan atau penyesuaian dapat dilakukan dengan penghapusan, pencabutan atau penggantian kunci, kartu identifikasi, fasilitas pemrosesan informasi atau langganan. Dokumentasi apa pun yang mengidentifikasi hak akses karyawan dan kontraktor harus mencerminkan penghapusan atau penyesuaian hak akses.</li> <li>d) Jika karyawan yang berangkat atau pengguna pihak eksternal mengetahui kata sandi untuk ID pengguna tetap aktif, ini harus diubah setelah penghentian atau perubahan pekerjaan, kontrak atau perjanjian.</li> <li>e) Hak akses untuk informasi dan aset yang terkait dengan fasilitas pemrosesan informasi harus dikurangi atau dihapus sebelum pekerjaan berakhir atau perubahan, tergantung pada evaluasi faktor risiko seperti: apakah penghentian atau perubahan diprakarsai oleh karyawan, pengguna pihak eksternal atau oleh manajemen, dan alasan untuk penghentian; tanggung jawab saat ini dari karyawan, pengguna pihak eksternal atau pengguna lainnya;</li> </ul>	<ul style="list-style-type: none"> <li>• Penghapusan dan Penangguhan Hak Akses Individu</li> <li>• Peninjauan Ulang Hak Akses Jika Terjadi Perubahan Pekerjaan</li> <li>• Penghapusan Hak Akses untuk Penghentian Pekerjaan</li> </ul>



			12.4.3 <i>Administrator and operator logs</i>	Memastikan aktivitas admin dan operator sistem harus dicatat dan dilindungi dan dilakukan peninjauan secara berkala	<i>Privileged user account</i> mungkin dapat memanipulasi log pada fasilitas pemrosesan informasi di bawah kendali langsung mereka, oleh karena itu perlu untuk melindungi dan tinjau log untuk menjaga akuntabilitas untuk <i>privileged users</i> .	<ul style="list-style-type: none"> <li>• Peninjauan log aktivitas dari <i>privileged users</i></li> </ul>
5	Server terserang virus/malware	Tidak dilakukan update <i>firewall</i> dan <i>antivirus</i> secara berkala	12.4.1 <i>Event logging</i>	Mengatur mengenai log kejadian yang merekam aktivitas pengguna, kesalahan, dan kejadian terkait keamanan informasi yang harus dibuat dan ditinjau secara berkala	<p>Log peristiwa harus berisi, bila relevan:</p> <ul style="list-style-type: none"> <li>a) ID pengguna;</li> <li>b) aktivitas sistem;</li> <li>c) tanggal, waktu, dan detail acara penting, mis. log-on dan log-off;</li> <li>d) identitas perangkat atau lokasi jika memungkinkan dan pengenalan sistem;</li> <li>e) catatan upaya akses sistem yang berhasil dan ditolak;</li> <li>f) catatan data yang berhasil dan ditolak dan upaya akses sumber daya lainnya;</li> <li>a) perubahan konfigurasi sistem;</li> <li>b) penggunaan hak istimewa;</li> <li>c) penggunaan utilitas sistem dan aplikasi;</li> <li>d) file yang diakses dan jenis akses;</li> <li>e) alamat dan protokol jaringan;</li> <li>f) alarm yang dibangkitkan oleh sistem kontrol akses;</li> <li>g) aktivasi dan de-aktivasi sistem perlindungan, seperti sistem anti-virus dan sistem deteksi intrusi;</li> <li>a) catatan transaksi yang dieksekusi oleh pengguna dalam aplikasi.</li> </ul> <p>Pencatatan kejadian menentukan fondasi untuk sistem pemantauan otomatis yang mampu menghasilkan laporan dan peringatan terkonsolidasi tentang keamanan sistem.</p>	<ul style="list-style-type: none"> <li>• Identifikasi log peristiwa</li> </ul>
6	Aktivitas tidak dapat terpantau	Maintenance perangkat yang kurang baik	11.2.4 <i>Equipment Maintenance</i>	Kontrol yang memastikan pemeliharaan atau perawatan terhadap aset guna	<p>Panduan berikut untuk pemeliharaan peralatan harus dipertimbangkan:</p> <ul style="list-style-type: none"> <li>m) Peralatan harus dipelihara sesuai dengan interval dan spesifikasi layanan yang direkomendasikan oleh pemasok;</li> </ul>	

				memastikan aset dapat digunakan dalam proses bisnis	<p>n) Hanya personil perawatan yang berwenang yang harus melakukan perbaikan dan peralatan servis;</p> <p>o) Rekaman harus dijaga dari semua kesalahan yang dicurigai atau aktual, dan dari semua pemeliharaan preventif dan korektif;</p> <p>p) Kontrol yang sesuai harus dilaksanakan ketika peralatan dijadwalkan untuk pemeliharaan, dengan mempertimbangkan apakah pemeliharaan ini dilakukan oleh personel di lokasi atau di luar organisasi; bila perlu, informasi rahasia harus dibersihkan dari peralatan atau personil pemeliharaan harus cukup dibersihkan;</p> <p>q) Semua persyaratan perawatan yang diberlakukan oleh polis asuransi harus dipenuhi;</p> <p>r) Sebelum menempatkan peralatan kembali ke dalam operasi setelah pemeliharaannya, itu harus diperiksa untuk memastikan bahwa peralatan tidak rusak dan tidak berfungsi</p>	
7	Data penting rusak/tidak dapat diakses	Data Corruption & Data Loss	12.3.1 <i>Information backup</i>	Menyalin <i>backup</i> dari informasi, perangkat lunak, dan sistem yang berjalan harus dilakukan dan diujicoba secara teratur sesuai dengan kebijakan <i>backup</i> yang berlaku.	<p>Kebijakan cadangan harus dibuat untuk menentukan persyaratan organisasi untuk mencadangkan informasi, perangkat lunak, dan sistem.</p> <p>Kebijakan cadangan harus menentukan persyaratan retensi dan perlindungan.</p> <p>Fasilitas pencadangan yang memadai harus disediakan untuk memastikan bahwa semua informasi penting dan perangkat lunak dapat dipulihkan setelah bencana atau kegagalan media.</p> <p>Saat merancang rencana cadangan, hal-hal berikut harus dipertimbangkan:</p> <p>a) catatan yang akurat dan lengkap dari salinan cadangan dan prosedur pemulihan terdokumentasi harus dibuat;</p> <p>b) cakupan (misalnya cadangan lengkap atau diferensial) dan frekuensi pencadangan harus</p>	<ul style="list-style-type: none"> <li>• Prosedur kebijakan pelaksanaan backup</li> <li>• Perencanaan backup</li> <li>• Pelaksanaan backup</li> </ul>

					<p>mencerminkan persyaratan bisnis organisasi, persyaratan keamanan informasi yang terlibat, dan kekritisan informasi untuk operasi organisasi yang berkelanjutan;</p> <p>c) backup harus disimpan di lokasi terpencil, pada jarak yang cukup untuk menghindari kerusakan dari bencana di situs utama;</p> <p>d) informasi cadangan harus diberikan tingkat perlindungan fisik dan lingkungan yang sesuai (lihat Klausul 11) konsisten dengan standar yang diterapkan di situs utama;</p> <p>e) media cadangan harus diuji secara teratur untuk memastikan bahwa mereka dapat diandalkan untuk penggunaan darurat bila diperlukan;</p> <p>f) ini harus dikombinasikan dengan tes prosedur restorasi dan diperiksa sesuai dengan waktu pemulihan yang diperlukan. Menguji kemampuan untuk memulihkan data cadangan harus dilakukan ke media pengujian khusus, bukan dengan menimpa media asli jika proses pencadangan atau pemulihan gagal dan menyebabkan kerusakan atau kehilangan data yang tidak dapat diperbaiki;</p> <p>g) dalam situasi di mana kerahasiaan penting, backup harus dilindungi dengan enkripsi.</p> <p>Prosedur operasional harus memantau pelaksanaan backup dan mengatasi kegagalan backup terjadwal untuk memastikan kelengkapan backup sesuai dengan kebijakan cadangan.</p> <p>Pengaturan cadangan untuk sistem dan layanan individual harus diuji secara teratur untuk memastikan bahwa mereka memenuhi persyaratan rencana kesinambungan bisnis. Dalam kasus sistem dan layanan penting, pengaturan cadangan harus mencakup semua sistem informasi, aplikasi dan data yang diperlukan untuk memulihkan sistem lengkap jika terjadi bencana.</p>	
--	--	--	--	--	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

					<p>Periode penyimpanan untuk informasi bisnis penting harus ditentukan, dengan mempertimbangkan apa pun persyaratan untuk salinan arsip untuk dipertahankan secara permanen.</p>	
		Kesalahan Konfigurasi	11.2.4 <i>Equipment Maintenance</i>	<p>Peralatan atau perlengkapan harus dipelihara dengan benar untuk menjamin keberlangsungan ketersediaan dan keutuhannya.</p>	<p>Panduan berikut untuk pemeliharaan peralatan harus dipertimbangkan:</p> <ul style="list-style-type: none"> <li>s) Peralatan harus dipelihara sesuai dengan interval dan spesifikasi layanan yang direkomendasikan oleh pemasok;</li> <li>t) Hanya personil perawatan yang berwenang yang harus melakukan perbaikan dan peralatan servis;</li> <li>u) Rekaman harus dijaga dari semua kesalahan yang dicurigai atau aktual, dan dari semua pemeliharaan preventif dan korektif;</li> <li>v) Kontrol yang sesuai harus dilaksanakan ketika peralatan dijadwalkan untuk pemeliharaan, dengan mempertimbangkan apakah pemeliharaan ini dilakukan oleh personel di lokasi atau di luar organisasi; bila perlu, informasi rahasia harus dibersihkan dari peralatan atau personil pemeliharaan harus cukup dibersihkan;</li> <li>w) Semua persyaratan perawatan yang diberlakukan oleh polis asuransi harus dipenuhi;</li> <li>x) Sebelum menempatkan peralatan kembali ke dalam operasi setelah pemeliharaannya, itu harus diperiksa untuk memastikan bahwa peralatan tidak rusak dan tidak berfungsi</li> </ul>	
			12.1.1 <i>Documented operations procedures</i>	<p>Prosedur operasional harus terdokumentasi dan tersedia bagi seluruh pengguna yang membutuhkan</p>	<p>Prosedur terdokumentasi harus disiapkan untuk kegiatan operasional yang terkait dengan pemrosesan informasi dan fasilitas komunikasi, seperti start-up komputer dan prosedur penutupan, pencadangan, pemeliharaan peralatan, penanganan media, ruang komputer dan manajemen penanganan surat dan keamanan.</p>	<ul style="list-style-type: none"> <li>• Prosedur yang terdokumentasi harus disiapkan</li> <li>• Prosedur harus menentukan instruksi operasional</li> </ul>

					<p>Prosedur operasi harus menentukan instruksi operasional, termasuk:</p> <ul style="list-style-type: none"> <li>h) Instalasi dan konfigurasi sistem; pengolahan dan penanganan informasi baik secara otomatis maupun manual; cadangan;</li> <li>i) Persyaratan penjadwalan, termasuk interdependensi dengan sistem lain, awal pekerjaan paling awal dan waktu penyelesaian pekerjaan terbaru;</li> <li>j) Instruksi untuk menangani kesalahan atau kondisi luar biasa lainnya, yang mungkin timbul selama pelaksanaan pekerjaan, termasuk pembatasan penggunaan utilitas sistem;</li> <li>k) Kontak dukungan dan eskalasi termasuk kontak dukungan eksternal dalam hal kesulitan operasional atau teknis yang tidak terduga;</li> <li>l) Keluaran khusus dan instruksi penanganan media, seperti penggunaan alat tulis khusus atau pengelolaan output rahasia termasuk prosedur untuk pembuangan output dengan aman dari pekerjaan yang gagal (lihat 8.3 dan 11.2.7)</li> <li>m) Restart sistem dan prosedur pemulihan untuk digunakan jika terjadi kegagalan sistem; pengelolaan jejak audit dan informasi log sistem;</li> <li>n) Prosedur pemantauan.</li> </ul> <p>Prosedur operasi dan prosedur terdokumentasi untuk aktivitas sistem harus diperlakukan sebagai formal dokumen dan perubahan yang disahkan oleh manajemen. Dimana secara teknis layak, sistem informasi harus dikelola secara konsisten, menggunakan prosedur, alat, dan utilitas yang sama.</p>	<ul style="list-style-type: none"> <li>• Prosedur operasi harus diperlakukan secara formal</li> </ul>
--	--	--	--	--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------

			12.4.1 <i>Event logging</i>	Mengatur mengenai log kejadian yang merekam aktivitas pengguna, kesalahan, dan kejadian terkait keamanan informasi yang harus dibuat dan ditinjau secara berkala	Log peristiwa harus berisi, bila relevan: <ul style="list-style-type: none"><li>g) ID pengguna;</li><li>h) aktivitas sistem;</li><li>i) tanggal, waktu, dan detail acara penting, mis. log-on dan log-off;</li><li>j) identitas perangkat atau lokasi jika memungkinkan dan pengenalan sistem;</li><li>k) catatan upaya akses sistem yang berhasil dan ditolak;</li><li>l) catatan data yang berhasil dan ditolak dan upaya akses sumber daya lainnya;</li><li>h) perubahan konfigurasi sistem;</li><li>i) penggunaan hak istimewa;</li><li>j) penggunaan utilitas sistem dan aplikasi;</li><li>k) file yang diakses dan jenis akses;</li><li>l) alamat dan protokol jaringan;</li><li>m) alarm yang dibangkitkan oleh sistem kontrol akses;</li><li>n) aktivasi dan de-aktivasi sistem perlindungan, seperti sistem anti-virus dan sistem deteksi intrusi;</li><li>b) catatan transaksi yang dieksekusi oleh pengguna dalam aplikasi.</li></ul> <p>Pencatatan kejadian menentukan fondasi untuk sistem pemantauan otomatis yang mampu menghasilkan laporan dan peringatan terkonsolidasi tentang keamanan sistem.</p>	<ul style="list-style-type: none"><li>Identifikasi log peristiwa</li></ul>
	Cyber crime	10.1.1 <i>Policy on the use of cryptographic controls</i>	Memastikan bahwa kebijakan penggunaan kriptografi sebagai upaya untuk pengamanan informasi telah ada dan telah terimplementasi.	Ketika membuat sebuah kebijakan penggunaan kriptografi, hal-hal ini perlu dipertimbangkan: <ul style="list-style-type: none"><li>a) Pendekatan manajemen dalam penggunaan kontrol kriptografi, termasuk prinsip-prinsip umum mengenai informasi bisnis apa yang harus diproteksi.</li><li>b) Berdasarkan Penilaian resiko, level proteksi yang dibutuhkan harus diidentifikasi meliputi tipe, kekuatan, dan kualitas dari algoritma enkripsi yang dibutuhkan</li></ul>		

					<p>c) Penggunaan enkripsi untuk proteksi informasi yang dibawa oleh media mobile dan perangkat yang dapat dilepas.</p> <p>d) pendekatan manajemen kunci, termasuk metode untuk menangani perlindungan kunci kriptografi dan pemulihan informasi terenkripsi dalam kasus kehilangan, kerusakan atau kerusakan kunci</p> <p>e) peran dan tanggung jawab, mis. siapa yang bertanggung jawab untuk:</p> <ol style="list-style-type: none"> <li>the implementation of the policy;</li> <li>the key management, including key generation (see 10.1.2);</li> </ol> <p>f) standar yang akan diadopsi untuk implementasi yang efektif di seluruh organisasi (solusi mana yang digunakan untuk proses bisnis)</p> <p>g) dampak penggunaan informasi terenkripsi pada kontrol yang bergantung pada pemeriksaan konten (mis. deteksi virus)</p>	
8	Kecelakaan kerja	Pegawai yang lalai	7.1.1 Screening	Memeriksa verifikasi latar belakang pada semua kandidat untuk pekerjaan harus dilakukan sesuai dengan hukum, peraturan dan etika yang relevan dan harus proporsional dengan persyaratan bisnis, klasifikasi informasi yang akan diakses dan risiko yang dirasakan	<p>Verifikasi harus mempertimbangkan semua privasi yang relevan, perlindungan informasi identitas pribadi dan peraturan berbasis pekerjaan, dan harus, jika diizinkan, termasuk yang berikut:</p> <ol style="list-style-type: none"> <li>ketersediaan referensi karakter yang memuaskan, misalnya satu bisnis dan satu pribadi;</li> <li>verifikasi (untuk kelengkapan dan akurasi) dari daftar riwayat hidup pemohon;</li> <li>konfirmasi kualifikasi akademik dan profesional yang diklaim;</li> <li>verifikasi identitas independen (paspor atau dokumen serupa);</li> <li>verifikasi yang lebih rinci, seperti peninjauan ulang kredit atau tinjauan catatan kriminal.</li> </ol>	<ul style="list-style-type: none"> <li>Pemeriksaan berkas</li> <li>Menyeleksi kemampuan sesuai dengan permintaan</li> <li>Melakukan seleksi tingkat lanjut terhadap tanggungan dan latar belakang serta karakter</li> </ul>

					<p>Ketika seorang individu dipekerjakan untuk peran keamanan informasi tertentu, organisasi harus memastikan kandidat:</p> <ul style="list-style-type: none"> <li>a) memiliki kompetensi yang diperlukan untuk melakukan peran keamanan;</li> <li>b) dapat dipercaya untuk mengambil peran, terutama jika perannya sangat penting untuk organisasi.</li> </ul> <p>Di mana pekerjaan, baik pada penunjukan awal atau pada promosi, melibatkan orang yang memiliki akses ke fasilitas pemrosesan informasi, dan, khususnya, jika ini menangani informasi rahasia, mis. informasi keuangan atau informasi yang sangat rahasia, organisasi juga harus mempertimbangkan lebih lanjut, verifikasi yang lebih rinci.</p> <p>Prosedur harus menetapkan kriteria dan batasan untuk ulasan verifikasi, mis. yang memenuhi syarat untuk menyaring orang dan bagaimana, kapan dan mengapa pemeriksaan verifikasi dilakukan.</p> <p>Proses penyaringan juga harus dipastikan untuk kontraktor. Dalam kasus ini, perjanjian antara organisasi dan kontraktor harus menetapkan tanggung jawab untuk melakukan penyaringan dan prosedur pemberitahuan yang perlu diikuti jika skrining belum selesai atau jika hasilnya memberikan alasan untuk keraguan atau kekhawatiran.</p> <p>Informasi tentang semua kandidat yang dipertimbangkan untuk posisi dalam organisasi harus dikumpulkan dan ditangani sesuai dengan undang-undang yang sesuai yang ada di yurisdiksi yang relevan. Tergantung pada undang-undang yang berlaku, para</p>	
--	--	--	--	--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--



					kandidat harus diberitahu sebelumnya tentang kegiatan skrining.	
9	Social engineering	Pegawai yang lalai	7.1.2 Terms and Condition of Employment	Mengatur perjanjian mengenai tanggung jawab pegawai, kontraktor, dan organisasi terhadap keamanan informasi	<p>Kewajiban kontrak untuk karyawan atau kontraktor harus mencerminkan kebijakan organisasi untuk keamanan informasi selain klarifikasi dan menyatakan:</p> <ul style="list-style-type: none"> <li>a) Bahwa semua karyawan dan kontraktor yang diberi akses ke informasi rahasia harus menandatangani perjanjian kerahasiaan atau non-pengungkapan sebelum diberikan akses ke fasilitas pemrosesan informasi (lihat 13.2.4);</li> <li>b) Tanggung jawab dan hak hukum karyawan atau kontraktor, misalnya mengenai undang-undang hak cipta atau undang-undang perlindungan data (lihat 18.1.2 dan 18.1.4);</li> <li>c) Tanggung jawab untuk klasifikasi informasi dan manajemen aset organisasi yang terkait dengan informasi, fasilitas pemrosesan informasi dan layanan informasi yang ditangani oleh karyawan atau kontraktor (lihat Klausul 8);</li> <li>d) Tanggung jawab karyawan atau kontraktor untuk penanganan informasi yang diterima dari perusahaan lain atau pihak eksternal;</li> <li>e) Tindakan yang harus diambil jika karyawan atau kontraktor mengabaikan persyaratan keamanan organisasi (lihat 7.2.3).</li> <li>f) Peran dan tanggung jawab keamanan informasi harus dikomunikasikan kepada kandidat pekerjaan selama proses pra-kerja. Organisasi harus memastikan bahwa karyawan dan kontraktor menyetujui persyaratan dan ketentuan terkait keamanan informasi yang sesuai dengan sifat dan tingkat akses yang mereka miliki terhadap aset organisasi yang terkait dengan sistem dan layanan informasi. Apabila diperlukan, tanggung jawab yang terkandung dalam syarat dan ketentuan kerja</li> </ul>	

					harus berlanjut untuk jangka waktu tertentu setelah akhir pekerjaan (lihat 7.3).	
10	Pencurian data	Pegawai yang lalai	7.1.2 Terms and Condition of Employment	Mengatur perjanjian mengenai tanggung jawab pegawai, kontraktor, dan organisasi terhadap keamanan informasi	<p>Kewajiban kontrak untuk karyawan atau kontraktor harus mencerminkan kebijakan organisasi untuk keamanan informasi selain klarifikasi dan menyatakan:</p> <ul style="list-style-type: none"> <li>a) Bahwa semua karyawan dan kontraktor yang diberi akses ke informasi rahasia harus menandatangani perjanjian kerahasiaan atau non-pengungkapan sebelum diberikan akses ke fasilitas pemrosesan informasi (lihat 13.2.4);</li> <li>b) Tanggung jawab dan hak hukum karyawan atau kontraktor, misalnya mengenai undang-undang hak cipta atau undang-undang perlindungan data (lihat 18.1.2 dan 18.1.4);</li> <li>c) Tanggung jawab untuk klasifikasi informasi dan manajemen aset organisasi yang terkait dengan informasi, fasilitas pemrosesan informasi dan layanan informasi yang ditangani oleh karyawan atau kontraktor (lihat Klausul 8);</li> <li>d) Tanggung jawab karyawan atau kontraktor untuk penanganan informasi yang diterima dari perusahaan lain atau pihak eksternal;</li> <li>e) Tindakan yang harus diambil jika karyawan atau kontraktor mengabaikan persyaratan keamanan organisasi (lihat 7.2.3).</li> </ul> <p>Peran dan tanggung jawab keamanan informasi harus dikomunikasikan kepada kandidat pekerjaan selama proses pra-kerja.</p> <p>Organisasi harus memastikan bahwa karyawan dan kontraktor menyetujui persyaratan dan ketentuan terkait keamanan informasi yang sesuai dengan sifat dan tingkat akses yang mereka miliki terhadap aset organisasi yang terkait dengan sistem dan layanan informasi.</p> <p>Apabila diperlukan, tanggung jawab yang terkandung dalam syarat dan ketentuan kerja harus berlanjut untuk jangka waktu tertentu setelah akhir pekerjaan (lihat 7.3).</p>	



Table Control Mapping

No	Sub-Clause	Control Objective	Justifikasi
1	6.1.1 <i>Information security roles and responsibilities</i>	Memastikan semua tanggung jawab keamanan informasi harus didefinisikan dan dialokasikan	Diambil berdasarkan pemetaan yang dilakukan oleh Mas Alif
2	7.1.1 <i>Screening</i>	Memeriksa verifikasi latar belakang pada semua kandidat untuk pekerjaan harus dilakukan sesuai dengan hukum, peraturan dan etika yang relevan dan harus proporsional dengan persyaratan bisnis, klasifikasi informasi yang akan diakses dan risiko yang dirasakan	Diambil berdasarkan pemetaan yang dilakukan oleh Mas Alif
3	7.1.2 <i>Term and conditions of employment</i>	Mengatur perjanjian mengenai tanggung jawab pegawai, kontraktor, dan organisasi terhadap keamanan informasi	Diambil berdasarkan pemetaan yang dilakukan oleh Mas Alif
4	7.2.2 <i>Information security awareness, education, and training</i>	Mengatur mengenai pendidikan dan pelatihan terhadap karyawan dan kontraktor mengenai keamanan informasi secara rutin sesuai dengan fungsi masing-masing	Diambil berdasarkan pemetaan yang dilakukan oleh Mas Alif
5	9.2.3 <i>Management of privileged access rights</i>	Memastikan alokasi dan penggunaan hak akses harus dibatasi dan dikontrol/ dikendalikan	Diambil berdasarkan pemetaan yang dilakukan oleh Mas Alif
6	9.2.6 <i>Removal or adjustment of access rights</i>	Memastikan hak akses untuk semua karyawan dan pengguna eksternal terhadap informasi dan fasilitas pemrosesan informasi harus dihapus setelah pemutusan kerja, kontrak, atau perjanjian atau disesuaikan dengan perubahan	Diambil berdasarkan pemetaan yang dilakukan oleh Mas Alif
7	10.1.1 <i>Policy on the use of cryptographic controls</i>	Memastikan bahwa kebijakan penggunaan kriptografi sebagai upaya untuk pengamanan informasi telah ada dan telah terimplementasi.	Diambil berdasarkan pemetaan yang dilakukan oleh Mas Alif
8	11.2.1 <i>Equipment siting and protection</i>	Memastikan bahwa peralatan telah ditempatkan pada tempat yang tepat dan diproteksi untuk mengurangi resiko yang diakibatkan oleh ancaman bencana alam serta kesempatan untuk akses yang tidak sah.	Diambil berdasarkan pemetaan yang dilakukan oleh Mas Alif
9	11.2.2 <i>Supporting Utilities</i>	Memastikan bahwa peralatan telah terproteksi dari kegagalan energi dan gangguan lainnya yang disebabkan oleh kegagalan pada peralatan pendukung	Diambil berdasarkan pemetaan yang dilakukan oleh Mas Alif

10	11.2.3 <i>Cabling security</i>	Memastikan bahwa kabel-kabel tenaga dan telekomunikasi yang membawa data atau informasi pendukung layanan telah terproteksi dari penyadapan, gangguan, dan kerusakan	Diambil berdasarkan pemetaan yang dilakukan oleh Mas Alif
11	11.2.4 <i>Equipment Maintenance</i>	Memastikan bahwa peralatan telah terawat dengan benar untuk menjamin keberlangsungan integritas dan ketersediaannya.	Diambil berdasarkan pemetaan yang dilakukan oleh Mas Alif
12	12.1.1 <i>Documented operations procedures</i>	Memastikan dokumentasi prosedur untuk setiap pengguna yang membutuhkan	Diambil berdasarkan pemetaan yang dilakukan oleh Mas Alif
13	12.1.3 <i>Capacity management</i>	Memastikan penggunaan dari sumber daya haruslah dipantau, disesuaikan, dan proyeksi untuk kebutuhan kapasitas di masa yang akan datang untuk memastikan kinerja sistem sesuai dengan kebutuhan	Diambil berdasarkan pemetaan yang dilakukan oleh Mas Alif
14	12.3.1 <i>Information backup</i>	Memastikan salinan dari cadangan informasi, perangkat lunak, dan gambar sistem harus dilakukan dan diuji secara berkala sesuai dengan kebijakan yang berlaku	Diambil berdasarkan pemetaan yang dilakukan oleh Mas Alif
15	12.4.1 <i>Event logging</i>	Mengatur mengenai log kejadian yang merekam aktivitas pengguna, kesalahan, dan kejadian terkait keamanan informasi yang harus dibuat dan ditinjau secara berkala	Diambil berdasarkan pemetaan yang dilakukan oleh Mas Alif
16	12.4.3 <i>Administrator and operator logs</i>	Memastikan aktivitas admin dan operator sistem harus dicatat dan dilindungi dan dilakukan peninjauan secara berkala	Diambil berdasarkan pemetaan yang dilakukan oleh Mas Alif

## Bab 4

### Audit Program

	Perangkat Audit							
	Memastikan semua tanggung jawab keamanan informasi harus didefinisikan dan dialokasikan							
	Tanggal Audit		Auditor		Auditee			
Poin-Poin Kontrol	Prosedur	Tipe Kontrol	Checklist	Yes	No	Parsial	Expected Evidence	
Mengidentifikasi proses keamanan aset dan informasi	Auditor mengecek identifikasi pada kewanan aset dan informasi	<i>Compliance</i>	Apakah terdapat proses identifikasi keamanan aset?				Dokumen proses identifikasi keamanan aset	
		<i>Compliance</i>	Apakah terdapat proses identifikasi keamanan informasi?				Dokumen proses identifikasi keamanan informasi	
		<i>Substantive</i>	Apakah identifikasi yang dilakukan telah menyeluruh?				List aset dan keamann infromasi	
Menentukan penannggung jawab tiap keamanan aset dan informasi	Auditor mengecek penanggung jawab tiap aset	<i>Compliance</i>	Apakah tiap aset memiliki penanggung jawab?				Dokumen penanggung jawab aset	
		<i>Substantive</i>	Apakah penanggung jawab berkompeten dibidang aset terkait?				Dokumen penanggung jawab aset	
Menentukan level otoritas	Auditor mengecek tiap asset memiliki level otoritas tertentu bagi penanggung jawab	<i>Compliance</i>	Apakah tiap penanggung jawab memiliki hak akses otoritas ?				Dokumen penanggung jawab aset, dokumen hak otoritas	
		<i>Substantive</i>	Apakah hak akses otoritas sesuai dengan masing masing aset?				Dokumen penanggung jawab aset, dokumen hak otoritas	

Bukti/Temuan			Opini	
Rekomendasi			Auditor	Auditee

	Perangkat Audit							
	Memeriksa verifikasi latar belakang pada semua kandidat untuk pekerjaan harus dilakukan sesuai dengan hukum, peraturan dan etika yang relevan dan harus proporsional dengan persyaratan bisnis, klasifikasi informasi yang akan diakses dan risiko yang dirasakan							
	Tanggal Audit		Auditor		Auditee			
Poin-Poin Kontrol	Prosedur	Tipe Kontrol	Checklist	Yes	No	Parsial	Expected Evidence	
Pemeriksaan berkas	Auditor mengecek kandidat memiliki sertifikat pendukung?	<i>Compliance</i>	Apakah kandidat memiliki sertifikat pendidikan yang resmi?				Dokumen daftar berkas rekrutmen	
		<i>Compliance</i>	Apakah kandidat memiliki sertifikat keahlian?				Dokumen daftar berkas rekrutmen	
	Auditor mengecek adanya dokumen data diri pada kandidat	<i>Compliance</i>	Apakah kandidat memiliki daftar riwayat hidup yang lengkap?				Dokumen daftar berkas rekrutmen	
		<i>Compliance</i>	Apakah kandidat memiliki kartu tanda penduduk atau passport?				Dokumen daftar berkas rekrutmen	
Menyeleksi kemampuan sesuai dengan permintaan	Auditor mengecek asal Pendidikan kandidat	<i>Compliance</i>	Apakah kandidat berasal dari bidang Pendidikan yang relevan dengan bidang pekerjaan?				Dokumen daftar berkas rekrutmen	
	Auditor mengecek adanya ujian kemampuan	<i>Compliance</i>	Apakah terdapat test kemampuan untuk para kandidat?				Dokumen hasil test kandidat	
		<i>Substantive</i>	Apakah kandidat mampu melewati test kemampuan?				Dokumen hasil test kandidat	
Melakukan seleksi tingkat lanjut terhadap tanggungan dan latar belakang serta karakter	Auditor mengecek kelayakan seleksi berkas pendukung dan tanggungan kandidat	<i>Compliance</i>	Apakah tiap kandidat telah melengkapi berkas?				Dokumen daftar berkas rekrutmen	
		<i>Compliance</i>	Apakah kandidat tidak memiliki tanggungan yang belum diselesaikan?				Dokumen daftar berkas rekrutmen, dokumen tanggungan kandidat	
		<i>Substantive</i>	Apakah semua berkas telah terverifikasi oleh pihak terkait?				Dokumen daftar berkas rekrutmen, dokumen verifikasi berkas kandidat	



Bukti/Temuan			Opini	
Rekomendasi			Auditor	Auditee

	Perangkat Audit							
	Mengatur perjanjian mengenai tanggung jawab pegawai, kontraktor, dan organisasi terhadap keamanan informasi							
	Tanggal Audit		Auditor		Auditee			
Poin-Poin Kontrol	Prosedur	Tipe Kontrol	Checklist	Yes	No	Parsial	Expected Evidence	
Mengidentifikasi pegawai dan kontraktor yang diberi akses	Auditor mengecek tentang hak akses pada user	<i>Compliance</i>	Apakah pegawai dan kontraktor yang terlibat memiliki hak akses?				Dokumen pegawai dan kontraktor yang terlibat, Dokumen hak akses	
		<i>Substantive</i>	Apakah hak akses yang diberikan sesuai dengan kebutuhan dan batasan tiap pegawai dan kontraktor?				Dokumen kebutuhan tiap pegawai dan kontraktor, dokumen hak akses	
Pembuatan perjanjian mengenai tanggung jawab pegawai dan kontraktor	Auditor mengecek terdapat perjanjian mengenai tanggung jawab atas hak akses	<i>Compliance</i>	Apakah terdapat perjanjian mengenai tanggung jawab pegawai dan kontraktor atas asset dan keamanan informasi?				Dokumen daftar perjanjian tanggung jawab	
Pembuatan tindakan apabila ada pelanggaran	Auditor mengecek adanya tindakan tegas untuk pelanggaran	<i>Compliance</i>	Apakah ada tindakan tegas apabila terdapat pegawai atau kontraktor yang melanggar perjanjian?				Dokumen daftar sanksi	
		<i>Compliance</i>	Apakah tindakan tersebut tertulis, konsisten dan dijalankan?				Dokumen daftar sanksi	

Bukti/Temuan			Opini	
Rekomendasi			Auditor	Auditee


	Perangkat Audit						
	Mengatur mengenai pendidikan dan pelatihan terhadap karyawan dan kontraktor mengenai keamanan informasi secara rutin sesuai dengan fungsi masing-masing.						
	Tanggal Audit		Auditor		Auditee		
Poin-Poin Kontrol	Prosedur	Tipe Kontrol	Checklist	Yes	No	Parsial	Expected Evidence
Pembuatan program kesadaran keamanan informasi	Auditor mengecek adanya program kesadaran keamanan informasi	Compliance	Apakah telah dibuat program kesadaran keamanan informasi?				Dokumen daftar kegiatan kesadaran keamanan informasi
		Compliance	Apakah pegawai yang berganti posisi mendapatkan program serupa khusus posisi tersebut?				Dokumen daftar kegiatan kesadaran keamanan informasi, dokumen daftar pegawai yang berganti posisi
		Substantive	Apakah program yang dibuat telah dijalankan secara rutin?				Dokumentasi program kesadaran keamanan informasi
Penyesuaian program kesadaran keamanan informasi dengan fungsi pegawai di organisasi	Auditor mengecek kesesuaian program kesadaran keamanan informasi dengan pegawai	Substantive	Apakah program kesadaran keamanan informasi telah sesuai dengan fungsi pegawai di organisasi?				Dokumen bidang program kesadaran keamanan informasi, Dokumen fungsi pegawaai
Pengembangan lanjutan program kesadaran keamanan informasi	Auditor mengecek adanya kegiatan pasca pelatihan	Compliance	Apakah terdapat kegiatan pasca pelatihan yang menerapkan hasil dari program kesadaran tersebut?				Dokumentasi Program pasca pelatihan
	Auditor mengecek program kesadaran keamanan informasi berlanjut	Compliance	Apakah program kesadaran keamanan informasi berlanjut secara rutin dan terdapat peningkatan kualitas pada kesadaran para pegawai?				DOKumentasi program kesadaran kemanan informasi, dokumen

							perencanaan program kesadaran kemanan informasi
Bukti/Temuan				Opini			
Rekomendasi				Auditor		Auditee	

	Perangkat Audit							
	Memastikan alokasi dan penggunaan hak akses harus dibatasi dan dikontrol/ dikendalikan							
	Tanggal Audit		Auditor		Auditee			
Poin-Poin Kontrol	Prosedur	Tipe Kontrol	Checklist	Yes	No	Parsial	Expected Evidence	
Mengidentifikasi hak akses istimewa terkait sistem dan proses	Auditor mengecek hak istimewa untuk asset	<i>Compliance</i>	Apakah ada hak istimewa untuk asset istimewa dan tidak ada yang bias mengakses selain yang memiliki hak akses?				Dokumen hak akses istimewa, riwayat akses aset	
Penyesuaian hak akses dengan kebutuhan pengguna	Auditor mengecek hak akses istimewa tepat sasaran	<i>Substantive</i>	Apakah hak akses istimewa tepat sasaran bagi pengguna yang membutuhkan?				Dokumen daftar hak akses istimewa, dokumen kebutuhan pengguna	
		<i>Substantive</i>	Apakah user biasa tidak dapat mengakses asset istimewa?				Dokumen daftar hak akses istimewa, riwayat akses	
		<i>Substantive</i>	Apakah hak akses telah sesuai dengan kebutuhan pengguna?				Dokumen daftar hak akses istimewa, daftar kebutuhan pengguna	
Pembuatan prosedur khusus agar tidak ada pelanggaran hak akses	Auditor mengecek adanya sanksi tertulis untuk yang melanggar	<i>Compliance</i>	Apakah ada aturan tertulis mengenai pelanggaran?				Dokumen sanksi bagi pelanggaran	
		<i>Substantive</i>	Apakah pelanggaran diberikan sanksi tegas?				Riwayat pelanggaran dan sanksi yang diberikan	
	Auditor mengecek rutinitas penggantian kata sandi	<i>Compliance</i>	Apakah kata sandi diperbarui secara berkala untuk menghindari peretasan hak akses?				Riwayat penggantian kata sandi	
Bukti/Temuan				Opini				

Rekomendasi			Auditor	Auditee

	Perangkat Audit							
	Memastikan hak akses untuk semua karyawan dan pengguna eksternal terhadap informasi dan fasilitas pemrosesan informasi harus dihapus setelah pemutusan kerja, kontrak, atau perjanjian atau disesuaikan dengan perubahan							
	Tanggal Audit		Auditor		Auditee			
Poin-Poin Kontrol	Prosedur	Tipe Kontrol	Checklist	Yes	No	Parsial	Expected Evidence	
Penghapusan dan Penangguhan Hak Akses Individu	Auditor mengecek ketersediaan prosedur penghapusan atau penangguhan hak akses	Compliance	Apakah terdapat prosedur penghapusan atau penangguhan hak akses pada perusahaan?				Prosedur Hak Akses	
	Auditor melakukan pengecekan terhadap fasilitas, layanan serta hak akses yang diberikan kepada karyawan pada tiap departemen yang berjalan di perusahaan.	Compliance	Apakah fasilitas, layanan, dan hak akses pada setiap departemen telah sesuai dengan prosedur?				List fasilitas, layanan, dan Hak Akses	
	Auditor melakukan pengecekan terhadap history perubahan pekerjaan karyawan	Substantive	Berapakah jumlah karyawan yang berubah pekerjaannya?				Data karyawan	
	Auditor melakukan pengecekan terhadap jumlah hak akses yang masih aktif pada karyawan yang telah berubah pekerjaannya.	Substantive	Apakah terdapat hak akses yang masih aktif pada karyawan yang telah berubah pekerjaannya?				Log perubahan hak akses	
Peninjauan Ulang Hak Akses Jika Terjadi Perubahan Pekerjaan	Auditor melakukan pengecekan terhadap prosedur peninjauan ulang hak akses yang ada pada perusahaan?	Compliance	Apakah terdapat prosedur peninjauan ulang hak akses ?				Prosedur peninjauan ulang hak akses	
	Auditor melakukan pengecekan terhadap dokumen dan data history terkait dengan peninjauan ulang hak akses.	Substantive	Apakah aktifitas peninjauan hak akses selalu dilakukan di perusahaan sesuai dengan prosedur?				Log aktivitas peninjauan	
Penghapusan Hak Akses untuk Penghentian Pekerjaan	Auditor melakukan pengecekan terhadap prosedur penghapusan hak akses pada penghentian pekerjaan	Compliance	Apakah terdapat prosedur penghapusan hak akses pada kasus penghentian pekerjaan?				Prosedur penghapusan hak akses	
	Auditor melakukan pengecekan terhadap pemberlakuan prosedur penghapusan hak akses	Compliance	Apakah prosedur telah diterapkan dengan baik di perusahaan?				Log penerapan prosedur	
	Auditor melakukan pengecekan terhadap akun-akun yang dapat mengakses informasi penting pada perusahaan	Substantive	Apakah terdapat akun yang masih aktif yang dimiliki karyawan yang telah keluar dari perusahaan?				List akun yang ada di perusahaan	



Bukti/Temuan				Opini			
Rekomendasi				Auditor		Auditee	

	Perangkat Audit								
	Memastikan bahwa kebijakan penggunaan kriptografi sebagai upaya untuk pengamanan informasi telah ada dan telah terimplementasi.								
	Tanggal Audit			Auditor			Auditee		
Poin-Poin Kontrol	Prosedur		Tipe Kontrol	Checklist	Yes	No	Parsial	Expected Evidence	
Ketersediaan Kebijakan Penggunaan Kriptografi	Auditor mengecek ada tidaknya kebijakan penggunaan kriptografi		Compliance	Apakah kebijakan penggunaan kriptografi telah sesuai dengan kebutuhan perusahaan?				Dokumen kebijakan penggunaan kriptografi	
	Auditor melakukan pengecekan terhadap kontrol kriptografi yang ada pada kebijakan		Substantive	Apakah informasi-informasi bisnis yang perlu diproteksi telah diidentifikasi?				Dokumen informasi bisnis yang harus terproteksi.	
			Substantive	Apakah informasi bisnis yang teridentifikasi telah diberikan kontrol kriptografi?				Dokumen informasi bisnis yang harus terproteksi.	
	Auditor melakukan pengecekan terhadap tingkat proteksi kriptografi yang digunakan		Compliance	Apakah ada klasifikasi tingkatan proteksi kriptografi?				Dokumen Kebijakan penggunaan kriptografi.	
Implementasi Kebijakan Penggunaan Kriptografi	Auditor melakukan pengecekan terhadap implementasi kebijakan penggunaan kriptografi		Compliance	Apakah kebijakan implementasi telah memiliki penanggungjawab?				Dokumen kebijakan penggunaan kriptografi.	
	Auditor melakukan pengecekan terhadap metode implementasi yang dilakukan		Substantive	Apakah mekanisme atau metode perlindungan kunci kriptografi dan pemulihan kriptografi telah sesuai dengan kebijakan?				Dokumen Kebijakan, Log pelaksanaan kebijakan.	
Bukti/Temuan					Opini				
Rekomendasi					Auditor			Auditee	


	Perangkat Audit							
	Prosedur operasional harus terdokumentasi dan tersedia bagi seluruh pengguna yang membutuhkan							
	Tanggal Audit		Auditor		Auditee			
Poin-Poin Kontrol	Prosedur	Tipe Kontrol	Checklist	Yes	No	Parsial	Expected Evidence	
Prosedur yang terdokumentasi harus disiapkan	Auditor memastikan bahwa sudah terdapat prosedur operasional yang terdokumentasi	Compliance	Apakah prosedur yang telah terdokumentasi mencakup keseluruhan operasional dari prosedur tersebut?				Dokumen prosedur operasional	
	Auditor mengecek sistematika prosedur operasional	Compliance	Apakah sistematika yang telah dibuat sesuai dengan prosedur operasional yang berlaku?				Dokumen prosedur operasional	
	Auditor mengecek setiap tahap dalam list prosedur operasional yang ada	Compliance	Apakah terdapat tahap yang tidak sesuai dengan kondisi operasional?				Dokumen prosedur operasional	
Prosedur harus sesuai instruksi operasional	Auditor mengecek dokumen prosedur	Subtative	Apakah sudah sesuai dengan instruksi operasional?				Dokumen prosedur operasional	
	Auditor mengecek instalasi dan konfigurasi sistem	Subtative	Apakah terdapat instalasi atau konfigurasi yang tidak sesuai dengan sistem?				Dokumen prosedur operasional	
	Auditor mengecek penjadwalan pekerjaan	Subtative	Apakah terdapat penjadwalan yang saling bertentangan, atau tidak jelas, dan kurang lengkap?				Dokumen prosedur operasional	
	Auditor mengecek instruksi untuk menangani kesalahan	Compliance	Apakah instruksi yang telah dibuat benar-benar dapat menangani kesalahan?				Dokumen prosedur operasional	
	Auditor mengidentifikasi prosedur pemantauan	Compliance	Apakah terdapat prosedur pemantauan yang masih belum tercantum?				Dokumen prosedur operasional	
Prosedur operasi harus diperlakukan secara formal	Auditor mengecek perubahan yang dilakukan manajemen	Subtative	Apakah terdapat perubahan yang tidak diketahui oleh manajemen?				Dokumen prosedur operasional	
	Auditor mengecek pengelolaan sistem informasi	Subtative	Apakah sistem informasi sudah dikelola secara konsisten?				Dokumen prosedur operasional	
Bukti/Temuan			Opini					

Rekomendasi			Auditor	Auditee

	Perangkat Audit							
	Kontrol yang memastikan penggunaan dari sumber daya haruslah dipantau, disesuaikan, dan proyeksi untuk kebutuhan kapasitas di masa yang akan datang untuk memastikan kinerja sistem sesuai dengan kebutuhan							
	Tanggal Audit		Auditor		Auditee			
Poin-Poin Kontrol	Prosedur	Tipe Kontrol	Checklist	Yes	No	Parsial	Expected Evidence	
Pengidentifikasian kapasitas	Auditor melakukan identifikasi kapasitas	Substantive	Apakah kapasitas sudah sepadan dengan kekritisan bisnis dari sistem yang bersangkutan?				Dokumen kapasitas sistem	
	Auditor melakukan analisis proyeksi kapasitas masa depan	Substantive	Apakah proyeksi masa depan sudah mempertimbangkan kebutuhan bisnis dan sistem baru yang tren saat ini?				Capacity Management Plan	
	Auditor melakukan analisis rencana tindakan dalam menghindari kebergantungan yang mengakibatkan munculnya suatu ancaman	Substantive	Apakah pihak manajemen sudah merencanakan tindakan yang tepat untuk menghindari potensi kebergantungan saat ini?				Capacity Management Plan	
	Auditor melakukan identifikasi kapasitas	Compliance	Apakah pihak manajemen sudah menyediakan kapasitas yang memadai?				Dokumen kapasitas sistem	
Pengelolaan permintaan kapasitas	Auditor mengecek data yang tidak terpakai	Compliance	Apakah sudah melakukan penghapusan data yang tidak terpakai?				Dokumen kapasitas sistem	
	Auditor mengidentifikasi kategori kegiatan untuk memutuskan tindakan penolakan atau pembatasan bandwidth layanan	Compliance	Apakah kegiatannya termasuk ke dalam kategori kegiatan yang sangat penting/krusial?				Dokumen kapasitas sistem	
	Auditor mengecek optimalisasi logika aplikasi	Substantive	Apakah logika aplikasi dari suatu basis data sudah optimal?				Dokumen kapasitas sistem	
Bukti/Temuan					Opini			
Rekomendasi		Auditor			Auditee			

--	--	--	--	--

	Perangkat Audit								
	Menyalin backup dari informasi, perangkat lunak, dan sistem yang berjalan harus dilakukan dan diujicoba secara teratur sesuai dengan kebijakan backup yang berlaku.								
	Tanggal Audit			Auditor			Auditee		
Poin-Poin Kontrol	Prosedur	Tipe Kontrol	Checklist	Yes	No	Parsial	Expected Evidence		
Prosedur kebijakan pelaksanaan backup	Auditor mengecek ketersediaan kebijakan pelaksanaan backup	Compliance	Apakah kebijakan pelaksanaan backup telah sesuai dengan kebijakan keamanan sistem saat ini?				Dokumen backup system		
	Auditor mengidentifikasi kebijakan pelaksanaan backup	Subtative	Apakah kebijakan pelaksanaan backup sudah mewakili persyaratan organisasi untuk retensi dan perlindungan?				Dokumen backup system		
	Auditor menganalisis fasilitas pencadangan	Subtative	Apakah seluruh fasilitas pencadangan memadai jika terjadi insiden kedepannya?				Dokumen backup system		
Perencanaan backup	Auditor menganalisis perencanaan backup kedepannya	Compliance	Apakah perencanaan backup sudah mempertimbangkan cakupan dan frekuensi pencadangan?				Backup management plan		
	Auditor menganalisis tempat perencanaan backup kedepannya	Subtative	Apakah perencanaan backup sudah mempertimbangkan lokasi penyimpanan pencadangan?				Backup management plan		
	Auditor menganalisis kondisi media backup cadangan	Compliance	Apakah media backup cadangan diuji secara teratur?				Backup management plan		
	Auditor menganalisis sistem keamanan backup	Compliance	Apakah backup dilindungi dengan bantuan enkripsi?				Backup management plan		
Pelaksanaan backup	Auditor melakukan uji backup termasuk cadangan backup	Subtative	Apakah uji yang dilakukan ditemukan kegagalan dalam melakukan backup maupun cadangan backup?				Backup activity		
	Auditor melakukan analisis mengenai periode dilakukan backup	Compliance	Apakah periode backup yang ditentukan telah sesuai dengan kebutuhan penyimpanan data saat ini?				Backup activity		
Bukti/Temuan						Opini			



Rekomendasi			Auditor	Auditee

	Perangkat Audit							
	Mengatur mengenai log kejadian yang merekam aktivitas pengguna, kesalahan, dan kejadian terkait keamanan informasi yang harus dibuat dan ditinjau secara berkala							
	Tanggal Audit		Auditor		Auditee			
Poin-Poin Kontrol	Prosedur	Tipe Kontrol	Checklist	Yes	No	Parsial	Expected Evidence	
Identifikasi log peristiwa	Auditor mengidentifikasi isi dari dokumen log event yang ada	Compliance	Apakah terdapat pencatatan keterangan hasil apakah diterima atau ditolak?				Dokumen log event	
	Auditor mengidentifikasi isi dari dokumen konfigurasi log event yang ada	Compliance	Apakah terdapat dokumen perubahan konfigurasi sistem				Dokumen change request	
	Auditor mengidentifikasi isi dari dokumen log aktivitas user	Compliance	Apakah log event berisi seluruh kegiatan yang sudah ditetapkan?				Dokumen log event	
	Auditor mengidentifikasi isi dari dokumen log keamanan sistem user	Compliance	Apakah terdapat history aktivasi dan deaktivasi sistem perlindungan?				Dokumen log event	
	Auditor mengidentifikasi isi dari dokumen log transaksi setiap user	Compliance	Apakah terdapat history pencatatan transaksi oleh pengguna?				Dokumen log event	
	Auditor mengidentifikasi isi dari dokumen log mengenai GPS dan data personal user	Substantive	Apakah terdapat pendeteksian lokasi dan identitas perangkat?				Dokumen log event	
Bukti/Temuan				Opini				
Rekomendasi				Auditor		Auditee		

	Perangkat Audit								
	Memastikan aktivitas admin dan operator sistem harus dicatat dan dilindungi dan dilakukan peninjauan secara berkala								
	Tanggal Audit			Auditor			Auditee		
Poin-Poin Kontrol	Prosedur		Tipe Kontrol	Checklist		Yes	No	Parsial	Expected Evidence
Peninjauan log aktivitas dari <i>privileged users</i>	Auditor mengecek ketersediaan log dari user account		Compliance	Apakah log mencatat setiap kegiatan dari user account?					Dokumen log user account
	Auditor mengecek pembagian hak istimewa user		Compliance	Apakah ada hak istimewa dari user yang tidak sesuai?					Dokumen log user account
	Auditor menganalisis sistem dari aktivitas user account		Subtantine	Apakah terdapat aktivitas dari user account yang melanggar peraturan?					Dokumen log user account
	Auditor melakukan pengujian log dan sistem dari user account		Subtantine	Apakah dari hasil uji log dan sistem memiliki kekurangan?					Dokumen log user account
Bukti/Temuan					Opini				
Rekomendasi					Auditor			Auditee	

## Bab 5

### Pembagian Tugas

No	NRP	Nama	Pembagian Tugas
1	05211540000061	Muhammad Khotib	<ul style="list-style-type: none"> <li>- Ruang Lingkup</li> <li>- Luaran</li> <li>- List Resiko dan kontrol dari TA Mas Alif</li> <li>- Membuat perangkat audit dari tabel Control Mapping nomor 1 hingga 5</li> </ul>
2	05211540000125	Gregorius Yudistira E	<ul style="list-style-type: none"> <li>- Executive Summary</li> <li>- Latar Belakang</li> <li>- Membuat pemetaan kontrol terhadap resiko nomor 6 hingga 10.</li> <li>- Membuat list Control Objective</li> <li>- Membuat perangkat audit dari tabel Control Mapping nomor 6 hingga 11</li> </ul>
3	05211540000127	Yasin Awwab	<ul style="list-style-type: none"> <li>- Rumusan Masalah</li> </ul>

			<ul style="list-style-type: none"> <li>- Tujuan</li> <li>- Manfaat</li> <li>- Membuat pemetaan kontrol terhadap resiko nomor 1 hingga 5</li> <li>- Membuat perangkat audit dari tabel Control Mapping nomor 12 hingga 16</li> </ul>
--	--	--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------