

Audit Checklist ISO 27001:2022 v.2.0

by Restia Moegiono, S.ST. {CEH|CHFI|ECSA|QRMO}

Komunitas Sadar SMKI (https://t.me/sadarsmki)

Kontribusi bisa diberikan melalui https://lynk.id/restiapriw/s/GP9WExY

Audit Checklist ISO 27001:2022

No.	Klausul/ Annex	Persyaratan ISO 27001:2022	Pertanyaan Audit	*Checklist*	Dokumentasi	Kesesuaian	PIC
4. Konteks Organisasi (*context of the organization*)							
1.	**4.1**	**Memahami organisasi dan konteksnya (understanding the organization and its context)**	a. Apakah sudah didokumentasikan masalah internal dan ekternal yang menjadi alasan diterapkannya SMKI? b. Apakah sudah didokumentasikan masalah internal dan eksternal yang dapat mempengaruhi kemampuan Perusahaan untuk mencapai hasil yang diharapkan dari SMKI?				
2.	**4.2**	**Memahami kebutuhan dan harapan pihak-pihak yang berkepentingan (*understanding the needs and expectations of interested parties*)**	Apakah sudah didokumentasikan pihak internal dan eksternal yang berkepentingan beserta kebutuhannya terhadap SMKI?				
3.	**4.3**	**Menentukan ruang lingkup sistem manajemen keamanan informasi (*determining the scope of the information security management system*)**	a. Apakah cakupan implementasi SMKI sudah dituliskan dalam suatu dokumen (misalnya pedoman?) b. Apakah dokumentasi (Misalnya surat ketetapan direksi, dsb.) mengenai cakupan sertifikasi sudah dibuat?				
4.	**4.4**	**Sistem manajemen keamanan informasi (*information security system management*)**	Apakah SMKI sudah dibangun, diimplementasikan, dipelihara, dan ditingkatkan secara berkelanjutan?				
5. Kepemimpinan (*leadership*)							

No.	Klausul/ Annex	Persyaratan ISO 27001:2022	Pertanyaan Audit	*Checklist*	Dokumentasi	Kesesuaian	PIC
5.	5.1	Kepemimpinan dan komitmen (*leadership and commitment*)	Komitmen manajemen puncak terhadap SMKI ditunjukkan dalam bentuk: a. Penetapan kebijakan SMKI; b. Penetapan sasaran SMKI; c. Penetapan tugas dan tanggung jawab SMKI; d. Mengkomunikasikan pentingnya implementasi SMKI; Apakah hal-hal tersebut sudah dilakukan?				
6.	5.2	Kebijakan (*policy*)	Apakah manajemen puncak sudah menetapkan dan mengkomunikasikan kebijakan SMKI?				
7.	5.3	Organisasi, peran, dan tanggung jawab (*organization, role and responsibility*)	Apakah manajemen puncak sudah memastikan peran dan tanggung jawab terkait koordinasi keamanan informasi sudah ditetapkan dan dikomunikasikan?				
6. Perencanaan (*planning*)							
8.	6.1.	Tindakan untuk mengatasi risiko dan peluang (*actions to address risks and opportunities*)	a. Apakah permasalahan internal dan eksternal, serta persyaratan pihak berkepentingan telah dipertimbangkan untuk menentukan risiko dan peluang yang perlu ditangani untuk memastikan bahwa SMKI mencapai hasilnya? b. Apakah tindakan untuk mengatasi risiko dan peluang telah direncanakan, dan diintegrasikan ke dalam proses SMKI, dan apakah tindakan tersebut dievaluasi efektivitasnya? c. Apakah proses penilaian risiko keamanan informasi yang menetapkan kriteria untuk melakukan penilaian risiko				

No.	Klausul/ Annex	Persyaratan ISO 27001:2022	Pertanyaan Audit	*Checklist*	Dokumentasi	Kesesuaian	PIC
			keamanan informasi, termasuk kriteria penerimaan risiko, telah ditetapkan? d. Apakah proses penilaian risiko keamanan informasi dapat diulangi dan apakah menghasilkan hasil yang konsisten, valid, dan dapat dibandingkan?				
9.	6.1.2	Penilaian risiko keamanan informasi (*information security risk assessment*)	a. Apakah proses penilaian risiko keamanan informasi mengidentifikasi risiko yang terkait dengan hilangnya kerahasiaan, integritas, dan ketersediaan informasi dalam lingkup SMKI, dan apakah pemilik risiko teridentifikasi? b. Apakah risiko keamanan informasi dianalisis untuk menilai kemungkinan realistis dan potensi konsekuensi yang akan terjadi, jika hal tersebut terjadi, dan apakah tingkat risiko telah ditentukan? c. Apakah risiko keamanan informasi dibandingkan dengan kriteria risiko yang ditetapkan dan diprioritaskan? d. Apakah informasi terdokumentasi tentang proses penilaian risiko keamanan informasi tersedia?				
10.	6.1.3	Perlakuan risiko keamanan informasi (*information security risk treatment*)	Apakah sudah dilakukan proses penanganan risiko (*risk treatment process*) dengan: a. Memilih opsi penanganan risiko yang sesuai?				

No.	Klausul/ Annex	Persyaratan ISO 27001:2022	Pertanyaan Audit	*Checklist*	Dokumentasi	Kesesuaian	PIC
			b. Menentukan semua kontrol yang diperlukan untuk mengimplementasikan opsi penanganan risiko yang dipilih? c. Membandingkan kontrol yang diperlukan dengan *Annex* A untuk memastikan tidak akan kontrol diperlukan yang dihilangkan? d. Membuat *Statement of Applicability* (SoA)? e. Memformulasikan rencana penanganan risiko (*risk treatment plan*)? f. Mendapatkan persetujuan dari pemilik risiko atas rencana penanganan risiko dan penerimaan atas risiko keamanan informasi yang bersifat residual?				
11.	6.2	Tujuan keamanan informasi dan perencanaan untuk mencapainya (*information security objectives and planning to achieve them*)	a. Apakah sudah ditetapkan sasaran keamanan informasi? b. Ketika melakukan perencanaan untuk mencapai sasaran keamanan informasi, apakah sudah ditentukan: 1) Apa yang akan dilakukan? 2) Sumber daya apa yang dibutuhkan? 3) Siapa yang akan bertanggung jawab? 4) Kapan sasaran akan dicapai? 5) Bagaimana hasilnya akan dievaluasi?				
12.	6.3	Perencanaan perubahan (*planning of changes*)	Apakah setiap perubahan pada SMKI telah direncanakan secara memadai				

No.	Klausul/ Annex	Persyaratan ISO 27001:2022	Pertanyaan Audit	*Checklist*	Dokumentasi	Kesesuaian	PIC
7. Dukungan (*support*)							
13.	7.1	Sumber daya (*resources*)	Apakah sumber daya yang diperlukan sudah ditentukan dan didukung untuk membangun, mengimplementasikan, memelihara, dan meningkatkan SMKI? (Misalnya ada mekanisme korporat *organization* planing berupa RAB/*annual planning*)				
14.	7.2	Kompetensi (*competence*)	a. Apakah sudah ditentukan kompetensi orang-orang yang melakukan pekerjaan terkait SMKI? b. Apakah sudah dipastikan orang-orang yang melakukan pekerjaan terkait SMKI memiliki kompetensi berdasarkan pendidikan, pelatihan, atau pengalaman? c. Apakah terdapat tindakan untuk memenuhi kompetensi yang diperlukan? (Misalnya mekanisme untuk analisis kebutuhan pelatihan) serta dilakukan evaluasi terhadap efektivitas tindakan yang diambil (Misalnya evaluasi keefektifan pelaksanaan *training*)? d. Apakah bukti kompetensi sudah terdokumentasikan?				
15.	7.3	Kesadaran (*awareness*)	a. Apakah sudah direncanakan program *security awareness* bagi personel internal dan eksternal? b. Apakah sudah dirangkum kebutuhan dan ekspektasi pada materi *security awareness*?				

No.	Klausul/ Annex	Persyaratan ISO 27001:2022	Pertanyaan Audit	*Checklist*	Dokumentasi	Kesesuaian	PIC
			c. Apakah sudah disiapkan rencana untuk menyampaikan materi *security awareness*? d. Apakah sudah dilakukan verifikasi pengetahuan dan pemahaman dari materi *security awareness*? e. Apakah sudah dilakukan verifikasi bahwa personel berlaku sesuai dengan materi *security awareness*?				
16.	7.4	Komunikasi (*communication*)	Apakah sudah ditetapkan sistem komunikasi terkait keamanan informasi yang mencakup: a. Apa saja hal-hal yang perlu dikomunikasikan? b. Kapan waktu terbaik untuk melakukan komunikasi? c. Siapa saja yang akan terlibat dalam aktivitas komunikasi? d. Siapa yang akan menginisiasi aktivitas komunikasi? e. Proses apa saja yang akan menginisiasi aktivitas komunikasi?				
17.	7.5	Informasi terdokumentasi (*documented information*)	Apakah informasi terdokumentasi yang dibutuhkan SMKI sudah tersedia?				
18.	7.5.2	Pembuatan dan pembaruan (*creating and updating*)	a. Apakah informasi yang terdokumentasi berada dalam format yang sesuai, dan apakah informasi tersebut telah diidentifikasi, ditinjau, dan disetujui kesesuaiannya? b. Apakah organisasi telah menetapkan konvensi penamaan termasuk (judul				

No.	Klausul/ Annex	Persyaratan ISO 27001:2022	Pertanyaan Audit	*Checklist*	Dokumentasi	Kesesuaian	PIC
			dokumen, tanggal, penulis & persetujuan)? c. Saat membuat dan memperbarui dokumen, apakah organisasi memastikan integritas dokumen dengan mencatat nomor versi dan persetujuan yang sesuai?				
19.	7.5.3	Pengendalian informasi terdokumentasi (*control of documented information*)	a. Apakah organisasi mempunyai proses untuk mengendalikan distribusi informasi terdokumentasi untuk memastikan informasi tersebut hanya tersedia bagi orang-orang yang dituju? b. Apakah organisasi melindungi informasi terdokumentasi dari hilangnya kerahasiaan, integritas dan ketersediaan? c. Apakah informasi yang terdokumentasi disimpan dengan benar dan dipelihara secara memadai agar dapat dibaca? d. Apakah organisasi telah mengidentifikasi dan mendokumentasikan dokumen yang berasal dari luar organisasi?				
8. Operasi (*operation*)							
20.	8.1	Perencanaan dan pengendalian operasional (*operational planning and control*)	a. Apakah sudah direncanakan, diimplementasikan, dan dikendalikan proses yang diperlukan untuk memenuhi kebutuhan keamanan informasi? b. Apakah informasi terdokumentasi sudah disimpan?				

No.	Klausul/ Annex	Persyaratan ISO 27001:2022	Pertanyaan Audit	*Checklist*	Dokumentasi	Kesesuaian	PIC
			c. Apakah perubahan sudah dikendalikan dan dampak sudah ditinjau? d. Apakah proses yang dikelola pihak luar (*outsource*) sudah ditentukan dan dikendalikan?				
21.	8.2	Penilaian risiko keamanan informasi (*information security risk assessment*)	a. Apakah dilaksanakan penilaian risiko pada waktu yang ditetapkan berdasarkan kriteria yang ditetapkan? b. Apakah informasi terdokumentasi dari hasil penilaian risiko keamanan informasi sudah dipelihara?				
22.	8.3	Perlakuan risiko keamanan informasi (*information security risk treatment*)	a. Apakah sudah diimplementasikan rencana penanganan risiko keamanan informasi? b. Apakah informasi terdokumentasi dari hasil penanganan risiko keamanan informasi sudah dipelihara?				
9. Evaluasi kinerja (*performance evaluation*)							
23.	9.1	Pemantauan, pengukuran, analisis, dan evaluasi (*monitoring, measurement, analysis and evaluation*)	a. Apakah performa keamanan informasi dan efektifitas SMKI sudah dievaluasi? b. Apakah sudah ditentukan: 1) Apa saja yang perlu dipantau dan diukur? 2) Apa metode untuk melakukan pemantauan, pengukuran, analisis, dan evaluasi? 3) Kapan pemantauan dan pengukuran harus dilakukan? 4) Siapa yang akan melakukan pemantauan dan pengukuran?				

No.	Klausul/ Annex	Persyaratan ISO 27001:2022	Pertanyaan Audit	*Checklist*	Dokumentasi	Kesesuaian	PIC
			5) Kapan hasil dari pemantauan dan pengukuran akan dianalisis dan dievaluasi? 6) Siapa yang akan melakukan analisis dan evaluasi terhadap hasil tersebut?				
24.	9.2	Audit internal (*internal audit*)	a. Apakah program audit sudah direncanakan, dibangun, diimplementasikan, dan dipelihara? b. Apakah sudah didefinisikan kriteria audit dan ruang lingkup untuk setiap audit? c. Apakah pemilihan auditor dan pelaksanaan audit sudah memastikan objektivitas dan ketidakberpihakan? d. Apakah hasil audit sudah dilaporkan ke pihak manajemen yang terkait? e. Apakah informasi terdokumentasi berupa bukti program audit dan hasil audit sudah dipelihara?				
25.	9.3	Tinjauan manajemen (*management review*)	Apakah tinjauan manajemen telah dilakukan pada periode waktu yang ditentukan?				
26.	9.3.2	Masukan pada tinjauan manajemen (*management review input*)	Apakah agenda dari tinjauan manajemen meliputi: a. Status dari tindakan pada tinjauan manajemen sebelumnya; b. Perubahan pada masalah internal dan eksternal yang relevan dengan SMKI; c. *Feedback* pada kinerja keamanan informasi; d. *Feedback* dari pihak yang terkait; e. Hasil dari penilaian risiko dan status dari rencana penanganan risiko;				

No.	Klausul/ Annex	Persyaratan ISO 27001:2022	Pertanyaan Audit	*Checklist*	Dokumentasi	Kesesuaian	PIC
			f. Peluang untuk melakukan peningkatan berkelanjutan.				
27.	9.3.3	Hasil tinjauan manajemen *management review result*	Apakah hasil dari tinjauan manajemen meliputi: a. Peluang untuk peningkatan berkelanjutan b. Perubahan SMKI				
10. Peningkatan (*improvement*)							
28.	10.1	*Continual improvement*	Apakah secara berkala sudah melakukan peningkatan pada kesesuaian, kecukupan, dan keefektifan SMKI?				
29.	10.2	*Nonconformity and corrective action when a nonconformity occurs*	Ketika ketidaksesuaian terjadi, maka apakah dilakukan hal-hal berikut: a. Bereaksi terhadap ketidaksesuaian; b. Mengevaluasi kebutuhan untuk menghilangkan penyebab dari ketidaksesuaian; c. Mengimplementasikan tindakan yang diperlukan; d. Meninjau efektivitas dari tindakan korektif yang dilakukan; e. Membuat perubahan pada SMKI jika diperlukan.				
5. Kontrol organisasi (*organizational control*)							
30.	5.1	Kebijakan untuk keamanan informasi (*policies for information security*)	Apakah kebijakan keamanan informasi sudah didefinisikan, ditetapkan oleh pihak manajemen, dipublikasikan, dan dikomunikasikan ke karyawan dan pihak eksternal terkait?				
31.	5.2	Peran dan tanggung jawab keamanan informasi	Apakah semua peran dan tanggung jawab di dalam keamanan informasi sudah didefinisikan dan dialokasikan?				

No.	Klausul/ Annex	Persyaratan ISO 27001:2022	Pertanyaan Audit	*Checklist*	Dokumentasi	Kesesuaian	PIC
		(*information security roles and responsibilities*)					
32.	5.3	Pemisahan tugas (*segregation of duties*)	Apakah telah dilakukan pemisahan tugas pada tugas dan area tanggung jawab yang mengalami konflik untuk mengurangi peluang terjadinya modifikasi tanpa otoritas atau tidak sengaja atau penyalahgunaan aset Perusahaan? (Misalnya dilakukan pemisahaan antara *software developer* & QC, dsb.)				
33.	5.4	Tangung jawab manajemen (*management responsibilities*)	a. Apakah manajemen menunjukkan dukungan terhadap kebijakan keamanan informasi, kebijakan spesifik topik, prosedur dan pengendalian keamanan informasi? b. Apakah manajemen memastikan bahwa personel mencapai tingkat kesadaran akan keamanan informasi yang relevan dengan peran dan tanggung jawab mereka dalam organisasi? c. Apakah manajemen memastikan bahwa personel diberikan sumber daya dan waktu perencanaan proyek yang memadai untuk menerapkan proses dan pengendalian terkait keamanan organisasi?				
34.	5.5	Kontak dengan pihak berwenang (*contact with authorities*)	Apakah sudah ditetapkan kapan dan oleh siapa, pihak berwenang akan dikontak dan bagaimana akan melaporkan insiden keamanan informasi dengan tepat?				
35.	5.6	Kontak dengan kelompok dengan kepentingan khusus (*contact with special interest groups*)	Apakah kontak dengan grup dengan minat khusus, atau keanggotaan pada forum spesialis keamanan atau asosiasi profesional sudah dipelihara?				

No.	Klausul/ Annex	Persyaratan ISO 27001:2022	Pertanyaan Audit	*Checklist*	Dokumentasi	Kesesuaian	PIC
36.	5.7	Intelijen ancaman (*threat intelligence*)	a. Apakah terdapat kebijakan/prosedur terdokumentasi yang menjelaskan proses pengumpulan, analisis, dan evaluasi informasi terkait ancaman keamanan informasi? b. Apakah program intelijen ancaman (*threat intelligence*) memastikan bahwa informasi yang dikumpulkan terkait ancaman keamanan informasi relevan, berwawasan luas, kontekstual, dan dapat ditindaklanjuti? c. Apakah program intelijen ancaman (*threat intelligence*) memiliki proses formal untuk mengidentifikasi, memeriksa dan memilih sumber ancaman keamanan informasi internal dan eksternal serta menganalisis informasi untuk memahami dampaknya terhadap organisasi?				
37.	5.8	Keamanan informasi pada manajemen proyek (*information security in project management*)	Apakah sudah keamanan informasi sudah diterapkan pada manajemen proyek? Terlepas dari tipe proyek yang dijalankan.				
38.	5.9	Inventarisasi informasi dan aset terkait lainnya (*inventory of information and other associated assets*)	a. Apakah terdapat inventarisasi seluruh aset yang terkait dengan informasi dan fasilitas pengolahan informasi? b. Apakah inventarisasi akurat dan selalu diperbarui? c. Apakah pemilik aset teridentifikasi dan ditandai ke seluruh aset?				

No.	Klausul/ Annex	Persyaratan ISO 27001:2022	Pertanyaan Audit	*Checklist*	Dokumentasi	Kesesuaian	PIC
			d. Apakah inventarisasi aset diperbarui pada saat aset diperoleh, dinonaktifkan, atau dilepaskan?				
39.	5.10	Penggunaan informasi dan aset terkait lainnya dapat diterima (*acceptable use of information and other associated assets*)	a. Apakah terdapat kebijakan mengenai penggunaan informasi, aset informasi dan fasilitas pemrosesan informasi yang dapat diterima? (Misalnya hal-hal yang boleh/tidak boleh terkait penggunaan komputer, notebook, internet, *email*, jaringan komputer, *portable devices*, dsb.) b. Apakah kebijakan tersebut sudah diidentifikasi, didokumentasikan dan diimplementasikan?				
40.	5.11	Pengembalian aset (*return of assets*)	Apakah terdapat kebijakan mengenai kewajiban karyawan dan pihak ketiga untuk mengembalikan semua aset Perusahaan yang digunakan setelah pemutusan hubungan kerja, kontrak, atau perjanjian? Misalnya, penggunaan laptop, *smartphone* milik Perusahaan.				
41.	5.12	Klasifikasi informasi (*classification of information*)	a. Apakah terdapat kebijakan tentang klasifikasi informasi berdasarkan persyaratan hukum, nilai, kekritisan dan sensitivitas terhadap pengungkapan atau modifikasi yang tidak sah? b. Apakah informasi-informasi sudah diklasifikasikan berdasarkan kebijakan klasifikasi informasi?				
42.	5.13	Pelabelan informasi (*labelling of information*)	Apakah terdapat prosedur tentang pelabelan informasi yang dikembangkan dan diimplementasikan sesuai dengan skema klasifikasi informasi?				

No.	Klausul/ Annex	Persyaratan ISO 27001:2022	Pertanyaan Audit	*Checklist*	Dokumentasi	Kesesuaian	PIC
43.	5.14	Pertukaran informasi (*information transfer*)	a. Apakah kebijakan, prosedur dan kontrol untuk pertukaran informasi sudah ada untuk melindungi transfer informasi melalui penggunaan semua jenis fasilitas komunikasi? b. Apakah perjanjian sudah mengatur tentang pertukaran informasi bisnis yang aman antara Perusahaan dan pihak eksternal?				
44.	5.15	Kontrol akses (*access control*)	a. Apakah terdapat kebijakan/prosedur terdokumentasi yang menjelaskan proses pengelolaan akses logis dan fisik terhadap informasi, aset, dan aset pemrosesan informasi? b. Apakah kebijakan didasarkan pada kebutuhan bisnis? c. Apakah kebijakan dikomunikasikan dengan tepat? d. Apakah manajemen akses mencakup prinsip "perlu diketahui" dan "perlu digunakan" untuk mengelola akses logis dan fisik terhadap informasi, aset, dan fasilitas pemrosesan informasi?				
45.	5.16	Manajemen identitas (*identity management*)	a. Apakah karyawan diberikan ID unik untuk mengakses informasi, aset, dan fasilitas pemrosesan informasi? b. ID/Akun pengguna bersama hanya diotorisasi bila diperlukan untuk tujuan bisnis dan setelah mendapat persetujuan?				

No.	Klausul/ Annex	Persyaratan ISO 27001:2022	Pertanyaan Audit	*Checklist*	Dokumentasi	Kesesuaian	PIC
			c. Apakah Identitas dihapus/dinonaktifkan ketika tidak diperlukan lagi?				
46.	5.17	Informasi autentikasi (*authentication information*)	a. Apakah pengguna diminta untuk mengikuti prosedur tentang penggunaan informasi otentikasi rahasia (misalnya *password*)? b. Apakah penggunaan *password* dari penguna dipantau untuk mengetahui kesesuaiannya terhadap kebijakan manajemen *password*?				
47.	5.18	Hak akses (*access rights*)	a. Apakah hak yang dinilai diberikan dengan mempertimbangkan kebutuhan bisnis serta peran dan tanggung jawab individu? b. Apakah prinsip pemisahan tugas dipertimbangkan saat memberikan hak akses? c. adalah persetujuan yang sesuai yang diambil dari pemilik aset/informasi untuk penyediaan atau pencabutan hak akses? d. Apakah ada frekuensi yang telah ditentukan untuk meninjau hak akses? e. Apakah hak akses diubah setelah perubahan peran pekerjaan atau pemutusan hubungan kerja?				
48.	5.19	Keamanan informasi dalam hubungan pemasok (*information security in supplier relationships*)	a. Apakah terdapat kebijakan/prosedur terdokumentasi yang menjelaskan proses untuk mengelola risiko keamanan informasi yang terkait dengan				

No.	Klausul/ Annex	Persyaratan ISO 27001:2022	Pertanyaan Audit	*Checklist*	Dokumentasi	Kesesuaian	PIC
			penggunaan produk atau layanan pemasok? b. Apakah vendor/pemasok dievaluasi sesuai dengan persyaratan organisasi untuk keamanan informasi? c. Apakah proses ditetapkan untuk menangani insiden dan kemungkinan yang terkait dengan produk dan layanan pemasok? d. Apakah pemasok/vendor dilengkapi dengan persyaratan keamanan yang terdokumentasi? e. Apakah akses pemasok/vendor terhadap aset informasi & infrastruktur dikendalikan dan dipantau?				
49.	5.20	Mengatasi keamanan informasi dalam perjanjian pemasok (*addressing information security within supplier agreements*)	Apakah semua persyaratan keamanan informasi yang relevan sudah ditetapkan dan disepakati dengan setiap pemasok yang dapat mengakses, memproses, menyimpan, mengkomunikasikan, atau menyediakan komponen infrastruktur TI untuk informasi Perusahaan?				
50.	5.21	Mengelola keamanan informasi dalam rantai pasokan TIK (*managing information security in the information and communication technology supply chain*)	Apakah perjanjian pemasok mencakup persyaratan untuk mengatasi keamanan informasi dalam rantai pasokan layanan & produk?				
51.	5.22	Memantau, meninjau, dan mengubah manajemen layanan pemasok (*monitoring, review and change management of*	a. Apakah terdapat kebijakan/prosedur terdokumentasi yang menjelaskan proses untuk menjaga tingkat keamanan informasi dan pemberian				

No.	Klausul/ Annex	Persyaratan ISO 27001:2022	Pertanyaan Audit	*Checklist*	Dokumentasi	Kesesuaian	PIC
		supplier services)	layanan yang disepakati sejalan dengan perjanjian pemasok? b. Apakah SLA (*Service Level Agreement*) ditetapkan untuk semua penyedia layanan? c. Apakah ada pemeriksaan berkala yang dilakukan untuk memastikan pemasok memberikan tingkat layanan yang disepakati kepada organisasi.?				
52.	5.23	Keamanan informasi untuk penggunaan layanan *cloud* (*information security for use of cloud service*)	a. Apakah terdapat kebijakan/prosedur terdokumentasi yang menjelaskan proses pengelolaan keamanan informasi untuk penggunaan layanan *cloud* dalam organisasi? b. Apakah peran dan tanggung jawab terkait penggunaan dan pengelolaan layanan *cloud* telah ditentukan? c. Apakah ada proses yang ditetapkan untuk mendapatkan jaminan atas kontrol keamanan informasi yang diterapkan oleh penyedia layanan *cloud*? d. Apakah terdapat proses yang ditetapkan untuk menangani insiden keamanan informasi yang terjadi sehubungan dengan penggunaan layanan *cloud*?				
53.	5.24	Perencanaan dan persiapan manajemen insiden keamanan informasi (*information security incident management planning and preparation*)	a. Apakah terdapat kebijakan/prosedur terdokumentasi yang menjelaskan proses respons yang cepat, efektif, konsisten dan teratur terhadap insiden keamanan informasi?				

No.	Klausul/ Annex	Persyaratan ISO 27001:2022	Pertanyaan Audit	*Checklist*	Dokumentasi	Kesesuaian	PIC
			b. Apakah ada proses untuk melaporkan kelemahan keamanan informasi yang teridentifikasi? c. Apakah proses ini dikomunikasikan kepada seluruh karyawan dan pihak berkepentingan sebagaimana berlaku? d. Apakah anggota tim manajemen insiden diberikan pelatihan yang sesuai untuk mengelola insiden? e. Apakah rencana tanggap insiden diuji secara berkala?				
54.	5.25	Penilaian dan keputusan pada peristiwa keamanan informasi (*assessment and decision on information security events*)	a. Apakah ada proses untuk memastikan kejadian keamanan informasi dinilai dan diklasifikasikan dengan benar? b. Apakah ada proses untuk mengkategorikan dan memprioritaskan insiden berdasarkan dampaknya?				
55.	5.26	Tanggap insiden keamanan informasi (*response to information security incidents*)	a. Apakah ada proses yang ditetapkan untuk merespons insiden keamanan informasi? b. Apakah ada jadwal respons yang terdokumentasi untuk semua kategori insiden? c. Apakah ada proses untuk memahami dan menganalisis akar penyebab insiden tersebut? d. Apakah tindakan yang diambil untuk memitigasi insiden tersebut efektif?				
56.	5.27	Belajar dari insiden keamanan informasi	Apakah pengetahuan yang diperoleh dari menganalisis dan menyelesaikan insiden keamanan informasi sudah digunakan				

No.	Klausul/ Annex	Persyaratan ISO 27001:2022	Pertanyaan Audit	*Checklist*	Dokumentasi	Kesesuaian	PIC
		(*learning from information security incidents*)	untuk mengurangi kemungkinan atau dampak insiden di masa depan?				
57.	5.28	Pengumpulan bukti (*collection of evidence*)	Apakah prosedur untuk identifikasi, pengumpulan, akuisisi dan pelestarian informasi yang dapat berfungsi sebagai bukti (*evidence*) sudah ditentukan dan diterapkan?				
58.	5.29	Keamanan informasi selama gangguan (*information security during disruption*)	a. Apakah ada kebijakan/prosedur terdokumentasi yang menjelaskan proses untuk melindungi informasi dan aset terkait lainnya selama gangguan? b. Apakah ada proses untuk mempertahankan kontrol keamanan informasi yang ada selama gangguan?				
59.	5.30	Kesiapan TIK untuk kelangsungan bisnis (*ICT readiness for business continuity*)	a. Apakah terdapat kebijakan/prosedur terdokumentasi untuk memastikan ketersediaan informasi organisasi dan aset terkait lainnya selama gangguan? b. Apakah keamanan informasi termasuk dalam rencana kesinambungan organisasi (*business continuity plans*)? c. Apakah fasilitas pemrosesan informasi mempunyai redundansi yang cukup untuk memenuhi persyaratan ketersediaan organisasi? d. Apakah organisasi menguji rencana kesinambungannya secara berkala?				
60.	5.31	Persyaratan hukum, undang-undang, peraturan dan kontrak (*legal, statutory, regulatory and contractual requirements*)	a. Apakah terdapat proses untuk memastikan kepatuhan terhadap persyaratan hukum, undang-undang, peraturan, dan kontrak terkait keamanan informasi?				

No.	Klausul/ Annex	Persyaratan ISO 27001:2022	Pertanyaan Audit	*Checklist*	Dokumentasi	Kesesuaian	PIC
			b. Apakah tanggung jawab diberikan kepada individu untuk mengelola persyaratan hukum, undang-undang, peraturan dan kontrak terkait dengan keamanan informasi? c. Apakah tindakan yang diambil untuk memenuhi persyaratan hukum, undang-undang, peraturan dan kontrak terkait keamanan informasi ditinjau untuk memeriksa efektivitasnya?				
61.	5.32	Hak kekayaan intelektual (*intellectual property rights*)	Apakah prosedur yang tepat sudah diterapkan untuk memastikan kepatuhan dengan persyaratan legislatif, peraturan dan kontrak yang terkait dengan hak kekayaan intelektual dan penggunaan produk perangkat lunak berpemilik?				
62.	5.33	Perlindungan rekaman (*protection of records*)	Apakah catatan (*records*) sudah dilindungi dari kerugian, penghancuran, pemalsuan, akses tidak sah dan pelepasan yang tidak sah, sesuai dengan persyaratan legislasi, peraturan, kontrak dan bisnis?				
63.	5.34	Privasi dan perlindungan data pribadi (*privacy and protection of personal identifiable information/ PII)*	a. Apakah terdapat proses untuk memastikan kepatuhan terhadap persyaratan hukum, undang-undang, peraturan, dan kontrak terkait dengan aspek keamanan informasi dalam pelindungan data pribadi? b. Apakah proses tersebut dikomunikasikan kepada semua pihak berkepentingan terkait yang terlibat dalam pemrosesan data pribadi?				
64.	5.35	Tinjauan independen pada keamanan informasi	Apakah pengelolaan keamanan informasi dan implementasinya (sasaran, tujuan,				

No.	Klausul/ Annex	Persyaratan ISO 27001:2022	Pertanyaan Audit	*Checklist*	Dokumentasi	Kesesuaian	PIC
		Independent review of information security	kontrol, kebijakan, proses dan prosedur untuk keamanan informasi) sudah ditinjau secara independen pada interval yang direncanakan atau ketika perubahan signifikan terjadi?				
65.	5.36	Kepatuhan terhadap kebijakan, aturan, dan standar keamanan informasi (*compliance with policies, rules and standards for information security*)	Apakah pihak manajemen sudah meninjau secara teratur tentang kepatuhan pemrosesan informasi dan prosedur dalam bidang tanggung jawabnya dengan kebijakan keamanan, standar, dan persyaratan keamanan lainnya yang sesuai?				
66.	5.37	prosedur operasional yang terdokumentasi (*documented operating procedures*)	Apakah prosedur operasional terkait aktifitas/proses (secara umum) sudah didokumentasikan dan tersedia untuk semua pengguna yang membutuhkannya?				
6. Kontrol personel (*people controls*)							
67.	6.1	*Screening*	a. Apakah ada proses penyaringan untuk penerimaan staf penuh waktu, paruh waktu, dan sementara? b. Apakah pemeriksaan verifikasi latar belakang dilakukan terhadap semua calon pekerja baru? c. Apakah proses verifikasi latar belakang mempertimbangkan pemeriksaan pengalaman profesional, kualifikasi akademis, verifikasi identitas independen, verifikasi catatan kriminal, dan tinjauan kredit? d. Apakah pemeriksaan tersebut mematuhi undang-undang, peraturan, dan etika yang relevan?				

No.	Klausul/ Annex	Persyaratan ISO 27001:2022	Pertanyaan Audit	*Checklist*	Dokumentasi	Kesesuaian	PIC
68.	6.2	Syarat dan ketentuan kerja (*terms and conditions of employment*)	a. Apakah ada syarat dan ketentuan kerja formal yang didokumentasikan dan dikomunikasikan kepada semua staf penuh waktu, paruh waktu, dan sementara sebelum masuk kerja? b. Apakah syarat dan ketentuan kerja mencakup kebijakan keamanan informasi organisasi dan kebijakan spesifik topik yang relevan. c. Apakah syarat dan ketentuan kerja mencakup tanggung jawab dan hak hukum seperti undang-undang hak cipta atau undang-undang perlindungan data? d. Apakah syarat dan ketentuan kerja mencakup tanggung jawab penanganan informasi yang diterima dari pihak yang berkepentingan? e. Apakah syarat dan ketentuan kerja mencakup tindakan yang harus diambil jika personel mengabaikan persyaratan keamanan organisasi?				
69.	6.3	Kesadaran keamanan informasi, pendidikan dan pelatihan (*information security awareness, education and training*)	a. Apakah semua karyawan, kontraktor, dan pengguna pihak ketiga menjalani pelatihan kesadaran keamanan secara berkala sesuai dengan peran dan fungsinya dalam organisasi? b. Apakah program kesadaran keamanan informasi mencakup kebijakan keamanan informasi dan kebijakan, standar, undang-undang, undang-undang, peraturan, kontrak, dan perjanjian spesifik topik?				

No.	Klausul/ Annex	Persyaratan ISO 27001:2022	Pertanyaan Audit	*Checklist*	Dokumentasi	Kesesuaian	PIC
			c. Apakah program kesadaran keamanan informasi mencakup akuntabilitas pribadi atas tindakan dan kelambanan seseorang, dan tanggung jawab umum terhadap pengamanan atau perlindungan informasi milik organisasi dan pihak yang berkepentingan? d. Apakah organisasi mempunyai proses formal untuk mengakses efektivitas program kesadaran keamanan informasi dengan memastikan bahwa semua karyawan mengikuti kuis?				
70.	6.4	Proses disipliner (*disciplinary process*)	a. Apakah ada proses disipliner formal yang memungkinkan organisasi mengambil tindakan terhadap karyawan yang melakukan pelanggaran keamanan informasi? b. Apakah proses disipliner formal disetujui oleh manajemen puncak? c. Apakah proses disipliner formal dikomunikasikan kepada seluruh karyawan? d. Apakah proses pendisiplinan formal mempertimbangkan faktor-faktor seperti: 1) Sifat (siapa, apa, kapan, bagaimana) dan tingkat keparahan pelanggaran serta konsekuensinya 2) Apakah pelanggaran tersebut disengaja (berbahaya) atau tidak disengaja (tidak disengaja) 3) Apakah ini merupakan pelanggaran pertama atau pelanggaran berulang				

No.	Klausul/ Annex	Persyaratan ISO 27001:2022	Pertanyaan Audit	*Checklist*	Dokumentasi	Kesesuaian	PIC
			4) Apakah pelanggarnya telah dilatih dengan baik atau tidak				
71.	6.5	Tanggung jawab setelah pemutusan hubungan kerja atau perubahan pekerjaan (*responsibilities after termination or change of employment*)	a. Apakah proses pemberhentian karyawan menentukan tanggung jawab dan tugas keamanan informasi yang akan tetap berlaku setelah pemutusan hubungan kerja atau perubahan peran pekerjaan untuk semua staf penuh waktu, paruh waktu, dan sementara? b. Apakah tanggung jawab dan tugas yang tetap berlaku setelah pemutusan hubungan kerja atau kontrak termasuk dalam syarat dan ketentuan kerja, kontrak atau perjanjian individu?				
72.	6.6	Perjanjian kerahasiaan atau non-pengungkapan (*confidentiality or non-disclosure agreements*)	a. Apakah staf penuh waktu, paruh waktu, dan sementara diharuskan menandatangani perjanjian kerahasiaan atau kerahasiaan sebelum diberikan akses terhadap informasi rahasia organisasi dan aset terkait lainnya? b. Apakah perjanjian kerahasiaan atau kerahasiaan mencakup: 1) Definisi informasi yang harus dilindungi. 2) Keabsahan perjanjian. 3) Kepemilikan informasi, rahasia dagang dan kekayaan intelektual. 4) Persyaratan informasi dikembalikan atau dimusnahkan pada saat pengakhiran perjanjian.				

No.	Klausul/ Annex	Persyaratan ISO 27001:2022	Pertanyaan Audit	*Checklist*	Dokumentasi	Kesesuaian	PIC
73.	6.7	Bekerja jarak jauh (*remote working*)	a. Apakah ada kebijakan formal yang mencakup persyaratan keamanan informasi yang memungkinkan personel bekerja dan mengakses informasi organisasi dari jarak jauh? b. Apakah kebijakan kerja jarak jauh disetujui oleh manajemen puncak? c. Apakah kebijakan kerja jarak jauh dikomunikasikan kepada seluruh staf penuh waktu, paruh waktu, dan sementara yang bekerja jarak jauh? d. Apakah kebijakan kerja jarak jauh mempertimbangkan persyaratan keamanan fisik? e. Apakah kebijakan kerja jarak jauh mempertimbangkan lokasi kerja jarak jauh seperti lemari arsip yang dapat dikunci, transportasi yang aman antar lokasi dan aturan untuk akses jarak jauh, meja kerja yang bersih, pencetakan dan pembuangan informasi? f. Apakah kebijakan kerja jarak jauh mempertimbangkan persyaratan keamanan komunikasi? g. Apakah kebijakan kerja jarak jauh mempertimbangkan ancaman akses tidak sah terhadap informasi atau sumber daya dari orang lain di tempat umum? h. Apakah kebijakan kerja jarak jauh mempertimbangkan penggunaan langkah-langkah keamanan, seperti				

No.	Klausul/ Annex	Persyaratan ISO 27001:2022	Pertanyaan Audit	*Checklist*	Dokumentasi	Kesesuaian	PIC
			firewall dan perlindungan terhadap malware?				
74.	6.8	Pelaporan peristiwa keamanan informasi (*information security event reporting*)	a. Apakah semua staf penuh waktu, paruh waktu, dan sementara disadarkan akan tanggung jawab mereka untuk melaporkan kejadian keamanan informasi? b. Apakah semua staf penuh waktu, paruh waktu, dan sementara mengetahui prosedur pelaporan keamanan informasi? c. Apakah semua staf penuh waktu, paruh waktu, dan sementara mengetahui rincian kontak komunikasi dan media komunikasi untuk melaporkan kejadian keamanan informasi?				
7. Kontrol fisik (*physical controls*)							
75.	7.1	Perimeter keamanan fisik (*physical security perimeters*)	a. Apakah ada batasan keamanan yang ditetapkan? b. Apakah area informasi yang sensitif atau kritis dipisahkan dan dikontrol dengan tepat? c. Apakah organisasi telah menerapkan perimeter yang baik secara fisik untuk bangunan atau lokasi yang memuatnya?				
76.	7.2	Entri fisik (*physical entry*)	a. Apakah organisasi telah menetapkan proses formal untuk pengelolaan hak akses terhadap wilayah fisik? b. Apakah prosesnya mencakup penyediaan, peninjauan berkala,				

No.	Klausul/ Annex	Persyaratan ISO 27001:2022	Pertanyaan Audit	*Checklist*	Dokumentasi	Kesesuaian	PIC
			pembaruan, dan pencabutan otorisasi akses fisik? c. apakah ada proses untuk memelihara dan memantau buku catatan fisik atau jejak audit elektronik dari semua akses fisik? d. Apakah mekanisme autentikasi yang memadai seperti kartu akses, biometrik, atau autentikasi dua faktor seperti kartu akses dan PIN rahasia diterapkan untuk akses fisik ke fasilitas pemrosesan informasi? e. Apakah ada proses formal untuk mengelola akses pengunjung? f. Apakah pengunjung diberikan Visitor Badge yang membedakannya dengan karyawan? g. Apakah catatan pengunjung disimpan termasuk tanggal, waktu masuk, waktu keluar, tujuan kunjungan dan personel yang mengizinkan pengunjung masuk? h. Apakah pengunjung diverifikasi identitasnya dengan memeriksa KTP atau kartu identitas perusahaan? i. Apakah pengunjung didampingi oleh personal organisasi dan diantar ke seluruh tempat dalam organisasi? j. Apakah pintu pengiriman dan pemuatan internal dan eksternal sudah diamankan dengan baik? k. Apakah pengiriman yang masuk diperiksa dan diperiksa apakah ada				

No.	Klausul/ Annex	Persyaratan ISO 27001:2022	Pertanyaan Audit	*Checklist*	Dokumentasi	Kesesuaian	PIC
			bahan peledak, bahan kimia atau bahan berbahaya lainnya sebelum dipindahkan dari area pengiriman dan pemuatan? l. Apakah pengiriman masuk didaftarkan sesuai dengan prosedur manajemen aset? m. Apakah pengiriman yang masuk diperiksa apakah ada gangguan atau campur tangan.				
77.	7.3	Pengamanan kantor, ruangan dan fasilitas (*securing offices, rooms and facilities*0	a. Apakah kantor, ruangan, dan fasilitas pemrosesan informasi penting ditempatkan untuk mencegah akses yang tidak sah? b. Apakah pengendalian diterapkan pada fasilitas proses penting untuk mencegah informasi atau aktivitas rahasia terlihat dan terdengar dari luar?				
78.	7.4	Pemantauan keamanan fisik (*physical security monitoring*)	a. Apakah lokasi fisik organisasi dipantau oleh sistem pengawasan, penjaga keamanan, atau *alarm* penyusup? b. Apakah titik masuk dan keluar fasilitas pemrosesan informasi penting dilengkapi dengan sistem pemantauan video? c. Apakah akses terhadap sistem pemantauan video/CCTV dibatasi hanya untuk personel yang berwenang? d. Apakah pemantauan video/rekaman CCTV disimpan sesuai organisasi dan persyaratan hukum?				

No.	Klausul/ Annex	Persyaratan ISO 27001:2022	Pertanyaan Audit	*Checklist*	Dokumentasi	Kesesuaian	PIC
79.	7.5	Perlindungan dari ancaman fisik dan lingkungan (*protecting against physical and environmental threats*)	a. Apakah fasilitas pemrosesan informasi penting terlindungi dari ancaman fisik dan lingkungan? b. Apakah pengendalian yang memadai diterapkan untuk melindungi personel dan aset dari kebakaran, banjir, lonjakan arus listrik, petir, bahan peledak, dll?				
80.	7.6	Bekerja dalam area yang aman (*working in secure areas*)	a. Apakah personel mengetahui keberadaan area aman? b. Kegiatan di dalam wilayah aman dikomunikasikan hanya kepada personel yang berwenang berdasarkan kebutuhan untuk mengetahuinya? c. Apakah area aman diperiksa secara berkala untuk mengidentifikasi area yang kosong? d. Apakah ada kontrol untuk membatasi peralatan fotografi, video, audio, atau rekaman lainnya, seperti kamera di perangkat pengguna *end user*, kecuali diizinkan di dalam area aman?				
81.	7.7	*Clear desk and clear screen*	a. Apakah organisasi sudah menetapkan kebijakan formal *clear desk* dan *clear screen*? b. Apakah kebijakan *clear desk* dan *clear screen* disetujui oleh manajemen puncak? c. Apakah kebijakan *clear desk* dan *clear screen* dikomunikasikan kepada semua staf penuh waktu, paruh waktu, dan sementara?				

No.	Klausul/ Annex	Persyaratan ISO 27001:2022	Pertanyaan Audit	*Checklist*	Dokumentasi	Kesesuaian	PIC
			d. Apakah kebijakan *clear desk* dan *clear screen* mencakup persyaratan untuk melindungi perangkat titik akhir pengguna dengan kunci atau cara keamanan lainnya saat tidak digunakan atau tanpa pengawasan? e. Apakah kebijakan *clear desk* dan *clear screen* mencakup persyaratan untuk mengonfigurasi perangkat pengguna *end user* dengan *screen saver* yang aman setelah periode tidak aktif tertentu? f. Apakah kebijakan *clear desk* dan *clear screen* mencakup persyaratan penggunaan printer dengan fungsi otentikasi? g. Apakah kebijakan *clear desk* dan *clear screen* mencakup persyaratan untuk menyimpan dokumen secara aman dan media penyimpanan yang dapat dipindahkan yang berisi informasi sensitif? h. Apakah kebijakan *clear desk* dan *clear screen* mencakup persyaratan untuk menghapus informasi sensitif atau penting pada papan tulis dan jenis tampilan lainnya ketika tidak lagi diperlukan?				
82.	7.8	Penempatan dan perlindungan peralatan (*equipment siting and protection*)	a. Apakah peralatan yang menangani data sensitif ditempatkan secara memadai untuk mengurangi risiko informasi dilihat oleh orang yang tidak berwenang selama penggunaannya?				

No.	Klausul/ Annex	Persyaratan ISO 27001:2022	Pertanyaan Audit	*Checklist*	Dokumentasi	Kesesuaian	PIC
			b. Apakah peralatan ditempatkan secara memadai untuk melindungi terhadap ancaman fisik dan lingkungan? c. Apakah organisasi telah menetapkan pedoman makan, minum, dan merokok di dekat fasilitas pemrosesan informasi? d. Apakah ada pengendalian untuk memantau kondisi lingkungan, seperti suhu dan kelembapan di sekitar?				
83.	7.9	Keamanan aset di luar lokasi (*security of assets off-premises*)	a. Apakah organisasi telah menetapkan proses formal untuk perlindungan perangkat yang menyimpan atau memproses informasi di luar lokasi organisasi? b. Apakah personel disadarkan akan pedoman penanganan aset organisasi di luar lokasi? c. Apakah log disimpan untuk peralatan pelacakan yang dibawa ke luar organisasi? d. Apakah pengendalian diterapkan untuk melacak lokasi aset dan menghapus perangkat dari jarak jauh?				
84.	7.10	Media penyimpanan (*storage media*)	a. Apakah organisasi telah menetapkan proses formal untuk mengelola media penyimpanan yang dapat dipindahkan? b. Apakah kebijakan media yang dapat dipindahkan disetujui oleh manajemen puncak? c. Apakah kebijakan media lepasan dikomunikasikan kepada semua staf				

No.	Klausul/ Annex	Persyaratan ISO 27001:2022	Pertanyaan Audit	*Checklist*	Dokumentasi	Kesesuaian	PIC
			penuh waktu, paruh waktu, dan sementara? d. Apakah kebijakan media penyimpanan yang dapat dilepas mempertimbangkan persyaratan untuk membatasi penggunaan media penyimpanan yang dapat dilepas hanya untuk personel yang berwenang berdasarkan kebutuhan? e. Apakah kebijakan media penyimpanan lepasan mempertimbangkan persyaratan untuk mengelola inventaris media penyimpanan lepasan? f. Apakah kebijakan media penyimpanan yang dapat dilepas mempertimbangkan persyaratan untuk memelihara log audit untuk membawa media penyimpanan yang dapat dipindahkan ke luar organisasi? g. Apakah kebijakan media penyimpanan lepasan mempertimbangkan persyaratan untuk menyimpan media penyimpanan lepasan dengan perlindungan yang memadai? h. Apakah kebijakan media penyimpanan yang dapat dipindahkan mempertimbangkan persyaratan penggunaan teknik kriptografi untuk mengamankan/melindungi data dalam media penyimpanan yang dapat dipindahkan? i. Apakah kebijakan media penyimpanan yang dapat dilepas mempertimbangkan				

No.	Klausul/ Annex	Persyaratan ISO 27001:2022	Pertanyaan Audit	*Checklist*	Dokumentasi	Kesesuaian	PIC
			persyaratan untuk mengaktifkan slot USB atau kartu SD hanya pada sistem yang memerlukan basis?				
85.	7.11	Utilitas pendukung (*supporting utilities*)	a. Apakah peralatan pendukung utilitas dikonfigurasi, dioperasikan dan dipelihara sesuai dengan spesifikasi pabrikan terkait? b. Apakah ada proses untuk mengelola kebutuhan kapasitas utilitas pendukung? c. Apakah peralatan pendukung utilitas diperiksa dan diuji secara berkala untuk memastikan berfungsi dengan baik? d. Apakah saklar dan katup darurat untuk memutus aliran listrik, air, gas atau utilitas lainnya diterapkan? e. Apakah organisasi mempunyai penerangan dan komunikasi darurat yang memadai?				
86.	7.12	Keamanan kabel (*cabling security*)	a. Apakah jalur listrik dan telekomunikasi menjadi fasilitas pemrosesan informasi jika memungkinkan disalurkan ke bawah tanah atau dilengkapi dengan perlindungan yang memadai seperti pelindung kabel lantai atau tiang listrik? b. Apakah kabel listrik dan kabel telekomunikasi dipisahkan untuk mencegah interferensi? c. Apakah kabel diberi label pada setiap ujungnya dengan rincian sumber dan tujuan yang memadai untuk				

No.	Klausul/ Annex	Persyaratan ISO 27001:2022	Pertanyaan Audit	*Checklist*	Dokumentasi	Kesesuaian	PIC
			memungkinkan identifikasi fisik dan inspeksi kabel?				
87.	7.13	Pemeliharaan peralatan (*equipment maintenance*)	a. Apakah peralatan dirawat sesuai dengan frekuensi dan spesifikasi servis yang direkomendasikan pemasok? b. Apakah organisasi memastikan hanya personel pemeliharaan resmi yang melakukan perbaikan dan pemeliharaan peralatan? c. Apakah ada proses untuk mengawasi personel pemeliharaan saat melakukan pemeliharaan di lokasi? d. Apakah ada proses untuk mengotorisasi dan mengendalikan akses untuk pemeliharaan jarak jauh? e. Apakah ada proses pemeriksaan peralatan sebelum dioperasikan kembali setelah pemeliharaan, untuk memastikan peralatan tidak mengalami kerusakan dan berfungsi dengan baik?				
88.	7.14	Pembuangan atau penggunaan kembali peralatan secara aman (*secure disposal or re-use of equipment*)	a. Apakah organisasi sudah menetapkan proses formal untuk pembuangan dan penggunaan kembali peralatan/aset secara aman? b. Apakah organisasi memastikan untuk menghancurkan atau menghapus data di perangkat penyimpanan secara fisik sebelum dibuang? c. Apakah organisasi memastikan untuk menghapus label dan tanda yang mengidentifikasi organisasi atau				

No.	Klausul/ Annex	Persyaratan ISO 27001:2022	Pertanyaan Audit	*Checklist*	Dokumentasi	Kesesuaian	PIC
			menunjukkan klasifikasi, pemilik, sistem atau jaringan sebelum dibuang?				
8. Kontrol teknologi (*technological controls*)							
89.	8.1	Perangkat pengguna *end point (user end point devices*)	a. Apakah kebijakan perangkat seluler ada dan disetujui? b. Detail inventaris perangkat seluler yang terdaftar? c. Apakah dokumen kebijakan mengatasi risiko tambahan penggunaan perangkat seluler (misalnya pencurian perangkat, penggunaan hotspot Wi-Fi terbuka? d. Apakah organisasi mempunyai kontrol akses dan perlindungan malware untuk perangkat seluler? e. Apakah organisasi melakukan pencadangan perangkat seluler secara rutin? f. Apakah ada proses pendaftaran perangkat titik akhir pengguna? g. Apakah ada batasan instalasi perangkat lunak pada perangkat titik akhir pengguna? h. Apakah ada kontrol penonaktifan, penghapusan, atau penguncian jarak jauh yang diterapkan pada perangkat titik akhir pengguna? i. Apakah port USB dinonaktifkan pada perangkat titik akhir pengguna?				
90.	8.2	Hak akses istimewa (*privileged access rights*)	a. Apa kriteria yang organisasi Anda rencanakan agar pengguna diberi hak akses?				

No.	Klausul/ Annex	Persyaratan ISO 27001:2022	Pertanyaan Audit	*Checklist*	Dokumentasi	Kesesuaian	PIC
			b. Bagaimana Anda mengotorisasi dan mencatat hak akses serta mempertahankannya? c. Apakah ada kebijakan kontrol akses? d. Bagaimana cara organisasi memberi tahu karyawannya tentang akses istimewa yang diberikan kepada mereka? e. Terdapat prosedur untuk mencegah penggunaan ID generik tanpa izin f. Apakah organisasi menentukan ketentuan berakhirnya akses hak istimewa? g. Apakah ada proses untuk meninjau hak akses istimewa yang diberikan kepada pengguna? h. Seberapa sering tinjauan akses dilakukan?				
91.	8.3	Pembatasan akses informasi (*information access restriction*)	a. Apakah Anda memastikan bahwa informasi sensitif dijaga kerahasiaannya, dan tidak ada orang yang tidak berwenang yang dapat mengakses informasi tersebut? b. Apakah organisasi telah menetapkan, memelihara, dan mengendalikan data apa saja yang dapat diakses oleh siapa? c. Apakah kontrol organisasi yang diidentifikasi akan memiliki akses mana (*read,write,delete,execute*)? d. Di manakah organisasi menyediakan kontrol akses fisik/logis untuk				

No.	Klausul/ Annex	Persyaratan ISO 27001:2022	Pertanyaan Audit	*Checklist*	Dokumentasi	Kesesuaian	PIC
			mengisolasi sistem, aplikasi, dan data sensitif?				
92.	8.4	Akses ke kode sumber (*access to source code*)	a. Apakah organisasi mengelola akses ke kode sumber program dan perpustakaannya sesuai dengan prosedur yang ditetapkan. b. Apakah pemberian dan pencabutan akses baca/tulis didasarkan pada kebutuhan? c. Apakah organisasi Anda memastikan bahwa pengembang hanya memiliki akses kode sumber melalui alat pengembang yang memiliki otorisasi yang sesuai? d. Apakah organisasi Anda menyimpan log audit semua akses dan semua perubahan yang dilakukan pada kode sumber?				
93.	8.5	Autentikasi secara aman (*secure authentication*)	a. Apakah organisasi Anda memastikan bahwa tidak ada informasi rahasia yang ditampilkan sebelum proses *login* berhasil diselesaikan? b. Apakah organisasi Anda menampilkan pemberitahuan/peringatan umum bahwa sistem hanya boleh diakses oleh pengguna yang berwenang? c. Apakah ada batasan tertentu pada upaya *login* yang gagal? d. Apakah suatu prosedur ditetapkan untuk mengangkat masalah keamanan? e. Apakah *password* ditutupi?				

No.	Klausul/ Annex	Persyaratan ISO 27001:2022	Pertanyaan Audit	*Checklist*	Dokumentasi	Kesesuaian	PIC
			f. Apakah *password* dienkripsi sebelum dikirimkan? g. Apakah ada waktu istirahat sesi untuk keluar dari sesi yang tidak aktif? h. Apakah pengguna diwajibkan mengubah *password* saat pertama kali *login*? i. Apakah akun dan *password default* vendor diubah?				
94.	8.6	Manajemen kapasitas (*capacity management*)	a. Apakah ada proses untuk mengelola kebutuhan kapasitas semua sistem berdasarkan proses bisnis dan kekritisan proses? b. Apakah ada proses untuk mengidentifikasi kebutuhan kapasitas yang diharapkan di masa depan? c. Apakah ada pengendalian detektif yang diterapkan untuk menunjukkan masalah dan memberi tahu administrator? d. Apakah organisasi mengikuti praktik retensi dan menghapus data absolut?				
95.	8.7	Perlindungan terhadap *malware* (*protection against malware*)	a. Apakah organisasi Anda membuat kebijakan formal untuk mengelola Malware? b. Apakah solusi *anti-malware* diterapkan pada semua sistem? c. Apakah solusi *anti-malware* dikonfigurasi untuk melakukan pemindaian berkala? d. Apakah solusi *anti-malware* dikonfigurasi untuk mendapatkan pembaruan tanda tangan secara rutin?				

No.	Klausul/ Annex	Persyaratan ISO 27001:2022	Pertanyaan Audit	*Checklist*	Dokumentasi	Kesesuaian	PIC
			e. Apakah solusi *anti-malware* dikonfigurasi untuk mengirimkan peringatan kepada administrator sistem setelah mengidentifikasi malware? f. Apakah ada proses untuk mendeteksi situs web berbahaya?				
96.	8.8	Manajemen kerentanan teknis (*management of technical vulnerabilities*)	a. Apakah peran dan tanggung jawab terkait pemantauan kerentanan, penilaian risiko kerentanan, dan patching sudah ditetapkan? b. Apakah cakupan dan frekuensi penilaian kerentanan teknis sudah ditentukan? c. Apakah ada proses untuk menilai kerentanan sebagai *critical, high, medium* dan *low*? d. Apakah jadwal remediasi ditentukan sesuai dengan peringkat kerentanan? e. Apakah ada proses formal untuk menginstal patch guna memulihkan kerentanan? f. Apakah kita menguji dan mengevaluasi *patch* sebelum diinstal?				
97.	8.9	Manajemen konfigurasi (*configuration management*)	a. Apakah organisasi memiliki kebijakan dan prosedur untuk mendokumentasikan konfigurasi perangkat keras, perangkat lunak, dan perangkat jaringan? b. Apakah ada peran dan kepemilikan yang tepat yang diberikan kepada individu untuk mengelola konfigurasi pada perangkat?				

No.	Klausul/ Annex	Persyaratan ISO 27001:2022	Pertanyaan Audit	*Checklist*	Dokumentasi	Kesesuaian	PIC
			c. Apakah organisasi mengikuti pola standar untuk *hardening* perangkat keras dan perangkat lunak? d. Apakah organisasi mempunyai mekanisme yang tepat untuk meninjau sistem, pembaruan (*update*) perangkat keras secara berkala, dan ancaman keamanan apa pun saat ini untuk memastikan kinerja optimal?				
98.	8.10	Penghapusan informasi (*information deletion*)	a. Apakah organisasi Anda memiliki kebijakan yang mencakup aktivitas pemeliharaan terkait penghapusan dan pemusnahan data dan atau aset TI (termasuk penggunaan perangkat lunak khusus dan hubungan dengan vendor yang berspesialisasi dalam penghapusan data dan perangkat)? b. Apakah organisasi secara rutin mengidentifikasi data yang tidak lagi digunakan dan perlu dihapus untuk mencegah akses tidak sah atau penyalahgunaan? c. Saat mempekerjakan vendor penghapusan khusus, apakah cukup bukti yang diperoleh (melalui dokumentasi) bahwa penghapusan telah dilakukan?				
99.	8.11	Penyamaran data (*data masking*)	a. Apakah organisasi mempunyai kebijakan dan prosedur untuk memastikan anonimisasi atau pseudonimisasi data untuk perlindungan data sesuai dengan persyaratan hukum dan peraturan?				

No.	Klausul/ Annex	Persyaratan ISO 27001:2022	Pertanyaan Audit	*Checklist*	Dokumentasi	Kesesuaian	PIC
			b. Ada proses untuk mengetahui bagaimana data yang disamarkan diakses? c. Apakah kebijakan dan prosedur penyamaran data (*data masking*) mencakup persyaratan berikut? 1) Menerapkan teknik penyamaran untuk mengekspos hanya jumlah data sesedikit mungkin dari data yang digunakan. 2) Atas permintaan subjek data, data tertentu mungkin disembunyikan dan akses staf ke bagian terkait dibatasi hanya untuk personel tertentu. 3) Membangun prosedur penyamaran data sesuai dengan persyaratan hukum dan peraturan. 4) Pseudonimisasi memerlukan penggunaan algoritma untuk membuka data yang disamarkan dan harus tetap aman				
100.	8.12	Pencegahan kebocoran data (*data leakage prevention*)	a. Apakah organisasi sudah menetapkan prosedur untuk mengurangi risiko kebocoran data dari *email*, transfer *file* masuk atau keluar, dan perangkat USB? b. Apakah organisasi telah menetapkan langkah-langkah yang tepat untuk memastikan data diatur sesuai dengan standar industri untuk menetapkan tingkat risiko yang berbeda? c. Apakah organisasi telah menyiapkan metode otorisasi yang tepat?				

No.	Klausul/ Annex	Persyaratan ISO 27001:2022	Pertanyaan Audit	*Checklist*	Dokumentasi	Kesesuaian	PIC
			d. Apakah data yang dicadangkan dan semua data sensitif dienkripsi? e. Apakah organisasi telah menerapkan langkah-langkah keamanan *gateway* dan retensi kebocoran untuk melindungi terhadap pengaruh eksternal? f. Apakah organisasi sudah mengidentifikasi saluran pemantauan untuk mengidentifikasi kebocoran data?				
101.	8.13	Pencadangan informasi (*information backup*)	a. Apakah organisasi telah menyetujui kebijakan dan prosedur untuk mengelola cadangan data pada perangkat, media penyimpanan, cloud, DB, dan server? b. Seberapa sering server dan data konfigurasi dicadangkan? c. Apakah data yang dicadangkan dipulihkan dan diperiksa secara berkala? d. Apakah hasil restorasi dicatat? e. Apakah rencana pencadangan diperbarui secara berkala? f. Apakah organisasi sudah menentukan frekuensi pengujian restorasi cadangan?				
102.	8.14	Redundansi pada fasilitas pemrosesan informasi (*redundancy of information processing facilities*)	a. Apakah organisasi mempunyai kebijakan dan prosedur untuk memastikan data yang diproses melalui teknologi TIK, fasilitas fisik, perangkat lunak diduplikasi untuk memastikan ketersediaan jika terjadi gangguan? b. Apakah organisasi telah mempertimbangkan lokasi yang berbeda secara geografis ketika melakukan				

No.	Klausul/ Annex	Persyaratan ISO 27001:2022	Pertanyaan Audit	*Checklist*	Dokumentasi	Kesesuaian	PIC
			outsourcing layanan data (fasilitas penyimpanan file/pusat data)? c. Apakah redundansi diterapkan pada semua sistem untuk memastikan ketersediaan fasilitas pemrosesan informasi?				
103.	8.15	*Logging*	a. Apakah Anda memiliki proses untuk meninjau log audit keamanan secara tepat waktu dan bertindak terhadap ancaman? b. Apakah log peristiwa yang sesuai dipelihara dan ditinjau secara berkala? c. Apakah fasilitas logging terlindungi dari gangguan dan akses tidak sah? d. Apakah aktivitas admin sistem/operator dicatat dan ditinjau secara berkala? e. Apakah layanan NTP disebarkan dan sistem disinkronkan dengan layanan NTP? f. Apakah arsip *log* dipelihara? g. Bagaimana pengumpulan *log* dari berbagai jaringan, perangkat keamanan, *server*, DB, sistem identitas, dan aplikasi dikelola?				
104.	8.16	Kegiatan pemantauan (*monitoring activities*)	a. Apakah terdapat kebijakan dan prosedur untuk mencurigai adanya kejadian yang harus dilaporkan kepada personel terkait untuk menjaga integritas jaringan dan meningkatkan kelangsungan bisnis? b. Apakah organisasi telah menetapkan *baseline* kondisi kerja normal untuk				

No.	Klausul/ Annex	Persyaratan ISO 27001:2022	Pertanyaan Audit	*Checklist*	Dokumentasi	Kesesuaian	PIC
			mengidentifikasi anomali dalam jaringan?				
105.	8.17	Sinkronisasi jam (*clock synchronization*)	a. Apakah organisasi sudah mengidentifikasi sumber waktu yang memiliki reputasi baik? b. Apakah semua perangkat disinkronkan dengan server NTP yang dihosting di organisasi? c. Apakah ada proses untuk membatasi akses ke data waktu di organisasi? d. Apakah ada proses untuk mengidentifikasi dan memantau semua perubahan pada sistem NTP?				
106.	8.18	Penggunaan program utilitas istimewa (*use of privileged utility programs*)	a. Apakah organisasi telah menetapkan daftar program utilitas? b. Apakah organisasi mempunyai prosedur untuk mengidentifikasi, mengotorisasi dan mengautentikasi penggunaan program utilitas? c. Apakah program utilitas ad hoc digunakan? Jika ya, apakah proses persetujuannya sama? d. Bagaimana detail pencatatan untuk program utilitas?				
107.	8.19	Instalasi perangkat lunak pada sistem operasional (*installation of software on operational systems*)	a. Ada kebijakan dan prosedur untuk instalasi perangkat lunak dan peningkatan perangkat lunak yang sudah ada? b. Daftar perangkat lunak yang masuk daftar putih yang disetujui oleh				

No.	Klausul/ Annex	Persyaratan ISO 27001:2022	Pertanyaan Audit	*Checklist*	Dokumentasi	Kesesuaian	PIC
			manajemen untuk digunakan dalam organisasi? c. Log audit disimpan untuk perubahan yang dilakukan? d. Ubah prosedur manajemen, kebijakan untuk menginstal/meningkatkan perangkat lunak baru? e. Contoh tiket manajemen perubahan yang diajukan untuk instalasi dan peningkatan perangkat lunak tersebut?				
108.	8.20	Keamanan jaringan (*networks security*)	a. Apakah organisasi mempunyai salinan diagram jaringan yang disetujui? b. Inventaris aset jaringan untuk organisasi? c. Apakah pencatatan dan pemantauan peralatan jaringan sudah ada? d. Detail penyimpanan file konfigurasi jaringan dan cadangannya? e. Kontrol enkripsi apa yang diterapkan untuk data saat transit? f. Apakah ada prosedur untuk mengautentikasi perangkat jaringan?				
109.	8.21	Keamanan pada layanan jaringan (*security of network services*)	a. Ada kebijakan dan prosedur untuk manajemen keamanan jaringan? b. Prosedur untuk memperbarui atau mem-*patch* OS pada perangkat jaringan? c. Detail individu yang disetujui yang dapat melakukan perubahan pada jaringan? d. Detail SIEM, DLP. SOAR, IDS, IPS diimplementasikan?				

No.	Klausul/ Annex	Persyaratan ISO 27001:2022	Pertanyaan Audit	*Checklist*	Dokumentasi	Kesesuaian	PIC
			e. Apakah ada prosedur untuk mengakses perangkat jaringan?				
110.	8.22	Pemisahan jaringan (*segregation of networks*)	a. Kontrol keamanan apa yang diterapkan untuk memastikan pemisahan akses untuk lingkungan produksi, pengujian, dan pengembangan? b. Bagaimana jaringan tersegmentasi dan bagaimana akses dipantau ke berbagai segmen jaringan?				
111.	8.23	Pemfilteran *web* (*web filtering*)	a. Apakah aturan pemfilteran *web* diterapkan untuk mengizinkan akses ke situs *web* tertentu saja? b. Apakah terdapat daftar situs web/kategori konten berisiko tinggi yang disetujui? c. Apakah kontrol diterapkan untuk memblokir pengunduhan konten berbahaya (misalnya *web proxy*, *email gateway*, modul anti-phishing, EDR?				
112.	8.24	Penggunaan kriptografi (*use of cryptography*)	a. Apakah organisasi sudah mempunyai kebijakan kriptografi? b. Bagaimana kunci kriptografi diakses, disimpan, dan dilindungi? c. Apakah inventarisasi kunci kriptografi dan sertifikat yang digunakan terpelihara? d. Apakah ada proses yang ditentukan untuk menentukan kekuatan kunci enkripsi dan algoritma enkripsi? e. Apakah periode kripto ditentukan untuk semua kunci enkripsi?				

No.	Klausul/ Annex	Persyaratan ISO 27001:2022	Pertanyaan Audit	*Checklist*	Dokumentasi	Kesesuaian	PIC
113.	8.25	Siklus hidup pengembangan yang aman (*secure development life cycle*)	a. Apakah organisasi mempunyai kebijakan pengembangan aplikasi yang aman? b. Apakah persyaratan keamanan dipertimbangkan dalam semua tahap pembangunan? c. Apakah ada pedoman pengkodean aman yang digunakan untuk pengembangan? d. Apakah organisasi memiliki repositori *source code* yang aman? e. Apakah organisasi mempertahankan pengendalian versi pada *source code*?				
114.	8.26	Kebutuhan keamanan aplikasi (*application security requirements*)	a. Apakah ada proses untuk memastikan mengidentifikasi semua persyaratan keamanan informasi saat mengembangkan atau memperoleh aplikasi? b. Apakah persyaratan hukum, undang-undang dan peraturan dipertimbangkan selama pengembangan aplikasi? c. Apakah persyaratan privasi dipertimbangkan selama pengembangan aplikasi?				
115.	8.27	Prinsip rekayasa dan arsitektur sistem yang aman (*secure system architecture and engineering principles*)	a. Apakah terdapat standar terdokumentasi dan bukti untuk rekayasa sistem yang aman dan arsitektur sistem? b. Apakah pedoman *secure engineering* mencakup hal berikut: 1) Metode autentikasi pengguna 2) Panduan kontrol sesi yang aman 3) Prosedur sanitasi dan validasi data				

No.	Klausul/ Annex	Persyaratan ISO 27001:2022	Pertanyaan Audit	*Checklist*	Dokumentasi	Kesesuaian	PIC
			4) Langkah-langkah keamanan untuk melindungi aset dan sistem informasi dari ancaman yang diketahui 5) Langkah-langkah keamanan dianalisis kemampuannya untuk mengidentifikasi, menghilangkan dan merespons ancaman keamanan 6) Bagaimana dan di mana tindakan pengamanan akan diterapkan c. Apakah terdapat prosedur untuk memvalidasi praktik, standar penyedia layanan/pihak ketiga agar sejalan dengan protokol rekayasa yang aman?				
116.	8.28	Pengkodean yang aman (*secure coding*)	a. Apakah terdapat kebijakan dan prosedur tentang *secure development*? b. Apakah terdapat proses untuk menilai ancaman dan kerentanan? c. Apakah terdapat *tools* untuk pengembangan *secure code*? d. Apakah terdapat laporan tinjauan *secure code*, SAST,DAST? e. Apakah tim pengembangan dilatih secara rutin mengenai ancaman siber? f. Apakah *secure* mempertimbangkan poin-poin berikut? a. Detail pada *attack surface* b. OWASP Top 10 Vulnerabilities				
117.	8.29	Pengujian keamanan pada pengembangan dan penerimaan (*security testing in development*	a. Apakah autentikasi pengguna, pembatasan akses dan penggunaan teknik kriptografi diuji?				

No.	Klausul/ Annex	Persyaratan ISO 27001:2022	Pertanyaan Audit	*Checklist*	Dokumentasi	Kesesuaian	PIC
		and acceptance)	b. Apakah organisasi menguji konfigurasi aman OS, *firewall*, dan komponen lainnya? c. Apakah organisasi telah menetapkan, mendokumentasikan, dan menerapkan rencana pengujian? d. Apakah organisasi yang melaksanakan *vulnerability assessment*, jika ya, frekuensi dan laporannya sama? e. Apakah organisasi tersebut melakukan *penetration testing*, jika ya frekuensi dan laporannya sama? f. Apakah organisasi menguji keamanan DB?				
118.	8.30	Pengembangan yang dialihdayakan (*outsourced development*)	a. Apakah perizinan, kepemilikan kode, dan HKI terkait dengan pengembangan yang dialihdayakan sudah ada? b. Apakah organisasi memiliki persyaratan kontrak untuk praktik desain, pengkodean, dan pengujian yang aman c. Apakah ketentuan untuk pemodelan ancaman dipertimbangkan oleh pengembang eksternal? d. Apakah UAT sudah selesai dan disetujui e. Rincian perangkat lunak ESCROW sudah ada f. Rincian organisasi yang melakukan audit terhadap pihak ketiga sudah ada?				
119.	8.31	Pemisahan pada lingkungan pengembangan, pengujian dan produksi (*separation*	a. Apakah organisasi memiliki lingkungan terpisah untuk aplikasi (pengembangan, pengujian, dan produksi)?				

No.	Klausul/ Annex	Persyaratan ISO 27001:2022	Pertanyaan Audit	*Checklist*	Dokumentasi	Kesesuaian	PIC
		of development, test and production environments)	b. Akses daftar kontrol untuk setiap lingkungan dan tinjauannya? c. Proses manajemen akses pengguna hak istimewa ada? d. Apakah *patch* dan manajemen *backup* sudah ada? e. Apakah terdapat laporan rinci VAPT? f. Apakah terdapat detail keamanan aplikasi web?				
120.	8.32	Manajemen *perubahan (change management*)	a. Apakah organisasi mempunyai kebijakan dan prosedur manajemen perubahan? b. Apakah ada proses permintaan perubahan formal? c. Apakah penilaian dampak perubahan, pengujian dan rencana roll back ditetapkan untuk semua perubahan? d. Apakah perubahan disetujui sebelum diterapkan? e. Apakah ada proses untuk mengelola perubahan darurat?				
121.	8.33	Informasi pengujian (*test information*)	a. Apakah organisasi menerapkan prosedur kontrol akses yang sama pada lingkungan pengujian dan produksi? b. Detail persetujuan jika data produk dimasukkan ke lingkungan pengujian? c. Contoh data yang digunakan dalam lingkungan pengujian, pengembangan, dan produksi? d. Apakah organisasi telah menetapkan proses dan pedoman pengelolaan data?				

No.	Klausul/ Annex	Persyaratan ISO 27001:2022	Pertanyaan Audit	*Checklist*	Dokumentasi	Kesesuaian	PIC
112.	8.34	Perlindungan sistem informasi selama pengujian audit (*protection of information systems during audit testing*)	a. Apakah organisasi mempunyai rencana audit dan jaminan sistem? b. Daftar semua undang-undang dan peraturan privasi? c. Detail kalender audit dan laporan audit terkini? d. Ada prosedur untuk melindungi data pribadi? e. Catatan kesadaran pengguna tentang operasi sistem yang melibatkan pribadi?				