LAMPIRAN

Lampiran 1. Hasil Wawancara Awal

Hari/Tanggal : 17 Januari 2024

Narasumber : Ida Komang Widhiarjaya, S.T.

Jabatan : Sekretaris UPA TIK Undiksha

Peneliti	:	Sejauh mana UPA TIK menilai pentingnya pelaksanaan manajemen risiko?
Narasumber	:	Sangat Penting untuk mengurangi risiko kegagalan sistem yang ada di Undiksha.
Peneliti	:	Apakah ada kebijakan khusus yang megatur tentang keamanan informasi?
Narasumber	:	Belum ada.
Peneliti	:	Bagaimana UPA TIK mengelola daftar inventarisasi aset untuk memastikan setiap aset memiliki dokumentasi yang lengkap, dan apakah setiap aset memiliki penanggung jawabnya?
Narasumber	:	Menggunakan sistem aset yang dikembangkan oleh UPA TIK dan digunakan di Undiksha.
Peneliti	:	Apakah UPA TIK pernah mengalami ancaman atau kerentanan yang terkait dengan aset, seperti kehilangan perangkat keras atau kehilangan data?
Narasumber	:	Pernah, contoh: kerusakan alat akibat dipinjam oleh mahasiswa. Untuk data pernah hilang, namun sudah ada
Peneliti	:	Bagaimana tindakan yang dilakukan UPA TIK selama ini dalam menanggulangi atau menghindari risiko yang mungkin terjadi?
Narasumber	:	Mencatat daftar risiko, menganalisis risiko, kemudian penilaian risiko, solusi yang diterapkan, dan terakhir pemantauan.
Peneliti	:	Apakah UPA TIK Undiksha pernah melakukan manajemen risiko?
Narasumber	:	Pernah.

Peneliti	:	Jika sudah, kerangka kerja apa yang digunakan untuk melakukan manajemen risiko?
Narasumber	:	Mengidentifikasi risiko, menganalisis risiko, kemudian penilaian risiko, solusi yang diterapkan, dan terakhir pemantauan.
Peneliti	:	Antara infrastruktur TI dengan sistem informasi aplikasi, manakah yang dianggap lebih berperan penting dalam mendukung kegiatan operasinal?
Narasumber	:	Sama-sama memiliki peranan penting, sehingga harus dapat terintegrasu dengan baik.
Peneliti	:	Secara spesifik, apasaja faktor-faktor yang pernah diidentifikasi sebagai ancaman terhadap keamanan informasi di lingkungan UPA TIK?
Narasumber	:	Kestabilan listrik internet, peralatan server
Peneliti	:	Bagaimana kondisi keamanan informasi pada UPA TIK Undiksha saat ini?
Narasumber	:	Saat ini masih perlu adanya perbaikan lebih baik, dan pemantauan berkelanjutan terhadap isu-isu keamanan
Penanya	:	Bagaimana rencana UPA TIK terkait dengan pendokumentasian terhadap standar keamanan informasi?
Narasumber	:	Membuat dokumentasi pemantauan keamanan jaringan dan sistem informasi.
Peneliti	:	Apakah ada pencatatan terkait insiden keamanan pada UPA TIK terkait dengan pendokumentasian terhadap standar keamanan informasi?
Narasumber	:	Ada, dicatat oleh tim Divisi Jaringan.
Peneliti	:	Apakah UPA TIK memiliki rencana kedepan untuk dapat meningkatkan sistem keamanan informasi?
Narasumber	:	Ada rencana untuk meningkatkan keamanan di bidang jaringan, yaitu dengan menambah *firewall*, dan di bidang SI dengan menambahkan *script security*.

BAGIAN V.
FORMULASI STRATEGI SI/TI

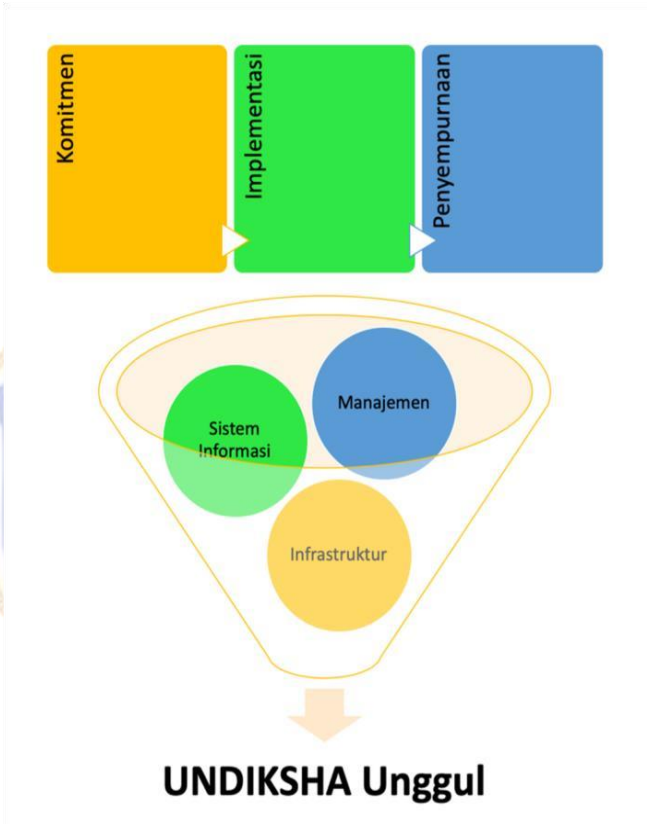
5.1 Deliverable Manajemen SI/TI

Manajemen Sistem Informasi/Teknologi Informasi (SI/TI) merupakan salah satu pilar penopang utama dalam mencapai tujuan bisnis Universitas Pendidikan Ganesha (UNDIKSHA). Seperti yang terlihat pada gambar di bawah ini. Manajemen SI/TI, Sistem Informasi, dan Infrastruktur TI merupakan penopang bagi berdiri kokohnya UNDIKSHA.

Pilar lainnya yang merupakan isi dari UNDIKSHA adalah Kurikulum, Proses Belajar Mengajar, Sarana dan Prasarana, Dunia Usaha dan Pranata Lembaga. Kesemuanya merupakan pilar utama dari UNDIKSHA. Pilar-pilar ini merupakan pengejawantahan dari karakteristik UNDIKSHA itu sendiri, sebagai entitas lembaga pendidikan yang harus melaksanakan Tri Dharma Perguruan Tinggi, dengan melakukan fungsi pendidikan, penelitian dan pengabdian kepada masyarakat. Juga sebagai entitas bisnis, yang bertujuan untuk menciptakan tenaga professional.

GAMBAR 5.1 PILAR-PILAR UTAMA UNDIKSHA

Manajemen SI/TI UNDIKSHA perlu melakukan proses “tata-ulang”. Proses tata ulang yang dimaksudkan disini adalah bagaimana menata kembali semua potensi yang telah ada, untuk disesuaikan dengan tujuan bisnis dari UNDIKSHA itu sendiri, dengan memperkuat strategi SI dan TI, guna menciptakan *competitive advantage* dan *key enabler* bagi UNDIKSHA.



GAMBAR 5.2 ARAH PERUBAHAN KE DEPAN UNDIKSHA

Proses penataan ulang ini, dimulai dengan memperkuat komitmen untuk melakukan perubahan. Isu penataan-ulang, bagi suatu pranata lembaga yang sudah cukup solid merupakan isu yang krusial. Penguatan komitmen dari pimpinan, pihak manajemen dan semua *stakeholder* yang terkait (termasuk diantaranya Senat Akademik) merupakan isu yang harus dimantapkan terlebih dahulu.

Beberapa proses penataan-ulang yang dimaksud adalah:

1. Penguatan kelembagaan UPT. TIK.

Memperkuat kelembagaan UPT. TIK sebagai pusat pengelola sistem informasi tunggal UNDIKSHA. Struktur organisasi UPT. TIK harus memiliki pimpinan yang berlatar belakang ilmu komputer dan manajemen teknologi informasi. UPT. TIK harus memiliki sub unit Teknis dan Sub Unit Management. Sub Unit teknis bertanggung jawab untuk pengelolaan teknis sistem informasi yang dibangun dan dikembangkan UNDIKSHA. Staf Unit Teknis harus memiliki kompetensi dalam perancangan, pengembangan dan pemeliharaan sistem informasi, database, jaringan komputer dan implementasi teknologi informasi lainnya. Unit management merupakan staf yang memiliki kompetensi sebagai administrator. Misalnya admin jaringan, admin database, analis sistem, bisnis analis. Selain itu, sebaiknya terdapat juga *Chief Information Officer (CIO)* yang akan bertanggung jawab untuk mengarahkan pengelolaan yang dilakukan oleh Ketua UPT. TIK. UNDIKSHA. CIO UPT. TIK. UNDIKSHA dapat dijabat oleh Wakil Rektor I.

Secara umum, pekerjaan unit pengelola TIK di Undiksha dapat dikelompokkan dalam infrastruktur jaringan dan perangkat keras, perangkat lunak (yang merupakan bagian dari sistem informasi), help-desk, Multimedia dan Reserch & Development. Divisi pada unit pengelola TIK disusun berdasar kelompok tersebut. Untuk memastikan bahwa sarana TIK di Undiksha selalu dikembangkan sesuai dengan kemajuan teknologi di luar dan untuk menjamin bahwa kualitas layanan TIK sesuai standar tertentu. Di sini diusulkan untuk menambah satu divisi lagi yaitu Jaminan Kualitas & Keamanan.

2. *Policy Making.*

Perlu dibuat kebijakan dari Rektor mengenai pengelolaan, penggunaan, dan pemanfaatan IT dalam lingkungan UNDIKSHA. Kebijakan yang dimaksud diantaranya adalah *ownership* data dan infrastruktur, kebijakan menyangkut *security*, *maintainance* dan kontrol. Penguatan implementasi kebijakan harus dibarengi dengan control yang kuat dari pimpinan dan unit internal kontrol pada masingmasing unit bisnis.

Berdasarkan usulan penataan ulang yang telah dijelaskan diatas, maka akan muncul dampak/akibat dari penataan ulang tersebut, yaitu:

a. Munculnya resistensi akan perubahan yang akan dilakukan, baik terhadap struktural organisasi, kebijakan maupun budaya kerja.

b. Diperlukan suatu penyesuaian terhadap perubahan fungsional yang akan terjadi. Misalnya perubahan cara pelaporan yang lebih terintegrasi antar unit bisnis.

c. Pengintegrasian penggunaan sumber daya untuk mendukung sasaran bisnis yang akan dicapai.

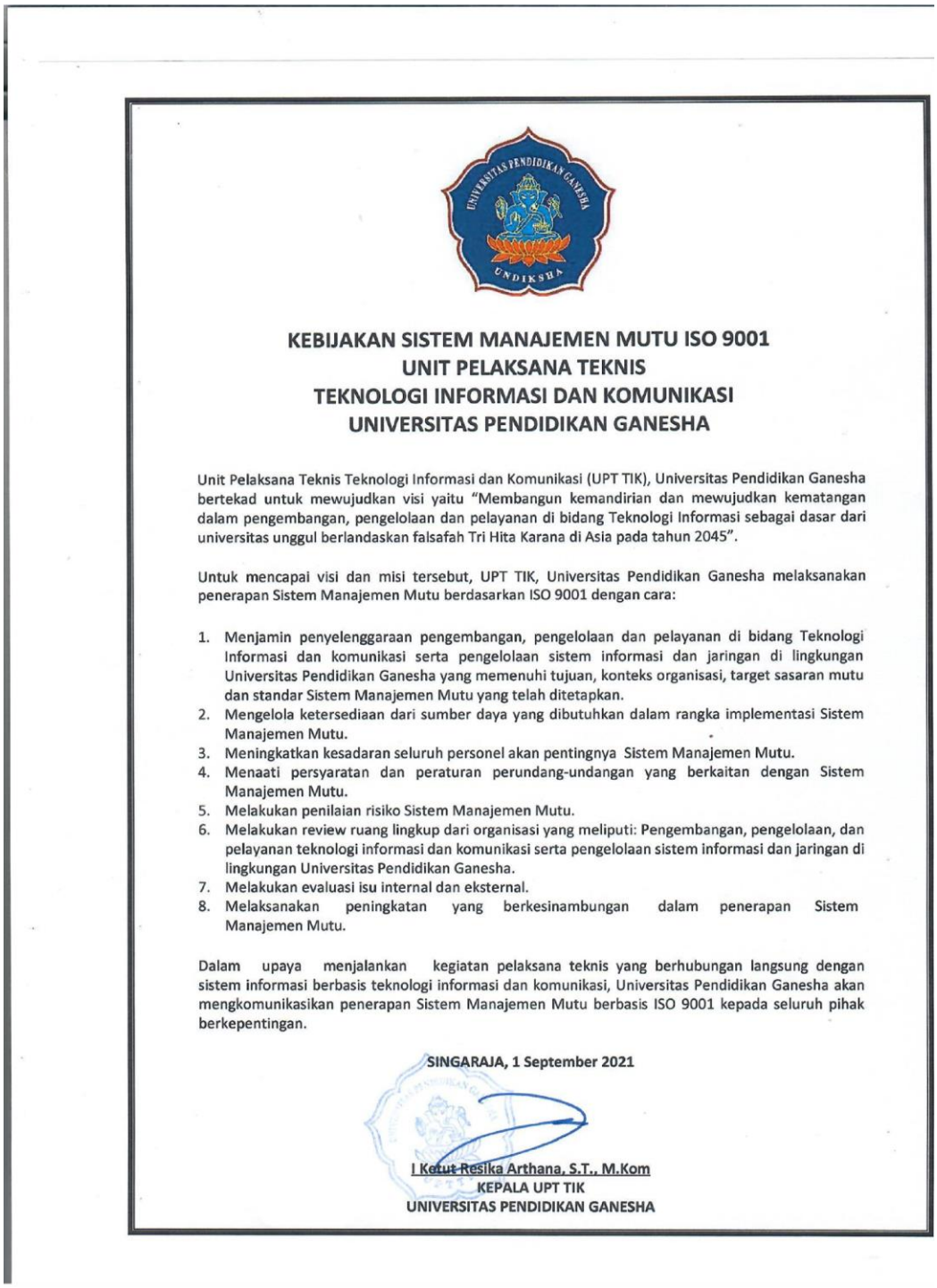
UNDIKSHA disarankan memiliki kebijakan umum maupun khusus di bidang TIK, yang tentunya tidak menyimpang dari visi dan misi dari Undiksha. Sebagai contoh, di bawah ini diberikan kebijakan umum sarana TIK untuk Undiksha sebagai berikut.

a. Manajemen informasi dan pemanfaatan sarana TIK tidak menyimpang danri ketentuan atau aturan-aturan yang berlaku di lingkungan PT dan regulasi pemerintah.

b. Sarana TIK disediakan bagi stakeholders di UNDIKSHA untuk memenuhi kebutuhan yang ada.

c. Sarana TIK dimanfaatkan untuk: (a) Mendukung penjaminan mutu, sehingga dimana dimungkinkan, semua keperluan informasi untuk penjaminan mutu harus disediakan, (b) Mendukung kegiatan Tri Dharma secara optimal, (c) Mendukung manajemen Universitas Pendidikan Ganesha secara optimal, dan (d) Memberikan layanan informasi yang memadai bagi masyarakat luar. Sarana TIK akan terus dikembangkan untuk mengikuti perkembangan teknologi dan mengoptimalkan pemanfaatannya, dengan demikian, SDM pengelola sarana TIK maupun pengguna sarana TIK juga akan terus dikembangkan.

Lampiran 3. Dokumen Kebijakan Yang Tersedia



KEBIJAKAN SISTEM MANAJEMEN MUTU ISO 9001
UNIT PELAKSANA TEKNIS
TEKNOLOGI INFORMASI DAN KOMUNIKASI
UNIVERSITAS PENDIDIKAN GANESHA

Unit Pelaksana Teknis Teknologi Informasi dan Komunikasi (UPT TIK), Universitas Pendidikan Ganesha bertekad untuk mewujudkan visi yaitu "Membangun kemandirian dan mewujudkan kematangan dalam pengembangan, pengelolaan dan pelayanan di bidang Teknologi Informasi sebagai dasar dari universitas unggul berlandaskan falsafah Tri Hita Karana di Asia pada tahun 2045".

Untuk mencapai visi dan misi tersebut, UPT TIK, Universitas Pendidikan Ganesha melaksanakan penerapan Sistem Manajemen Mutu berdasarkan ISO 9001 dengan cara:

1. Menjamin penyelenggaraan pengembangan, pengelolaan dan pelayanan di bidang Teknologi Informasi dan komunikasi serta pengelolaan sistem informasi dan jaringan di lingkungan Universitas Pendidikan Ganesha yang memenuhi tujuan, konteks organisasi, target sasaran mutu dan standar Sistem Manajemen Mutu yang telah ditetapkan.
2. Mengelola ketersediaan dari sumber daya yang dibutuhkan dalam rangka implementasi Sistem Manajemen Mutu.
3. Meningkatkan kesadaran seluruh personel akan pentingnya Sistem Manajemen Mutu.
4. Menaati persyaratan dan peraturan perundang-undangan yang berkaitan dengan Sistem Manajemen Mutu.
5. Melakukan penilaian risiko Sistem Manajemen Mutu.
6. Melakukan review ruang lingkup dari organisasi yang meliputi: Pengembangan, pengelolaan, dan pelayanan teknologi informasi dan komunikasi serta pengelolaan sistem informasi dan jaringan di lingkungan Universitas Pendidikan Ganesha.
7. Melakukan evaluasi isu internal dan eksternal.
8. Melaksanakan peningkatan yang berkesinambungan dalam penerapan Sistem Manajemen Mutu.

Dalam upaya menjalankan kegiatan pelaksana teknis yang berhubungan langsung dengan sistem informasi berbasis teknologi informasi dan komunikasi, Universitas Pendidikan Ganesha akan mengkomunikasikan penerapan Sistem Manajemen Mutu berbasis ISO 9001 kepada seluruh pihak berkepentingan.

SINGARAJA, 1 September 2021

I Ketut Resika Arthana, S.T., M.Kom
KEPALA UPT TIK
UNIVERSITAS PENDIDIKAN GANESHA

Lampiran 4. Rancangan Uji Kebahasaan

1. Lembar kerja Evaluasi Kriteria Dampak

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	NILAI DAMPAK	PENGERTIAN	R	TR	
1	*Reputation*	Reputasi/Kepercayaan			
2	*Financial*	Keuangan			
3	*Productivity*	Produktifitas			
4	*Savety/Health*	Keamanan/Kesehatan			

2. Lembar Kerja Identifikasi Aset

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERTANYAAN	PENGERTIAN	R	TR	
1	*What system do people in your organization need to perform their jobs?*	Sistem apa yang dibutuhkan oleh orang-orang dalam organisasi Anda untuk menjalankan tugas mereka?			
2	*What information do people in your organization need to perform their jobs?*	Informasi apa yang dibutuhkan oleh orang-orang dalam organisasi Anda untuk melakukan pekerjaan mereka?			
3	*What application dan services do people in your organization need to perform their jobs?*	Aplikasi dan layanan apa yang dibutuhkan oleh orang-orang dalam organisasi Anda untuk melaksanakan pekerjaan mereka?			
4	*What other assets are closely related to these assets?*	Aset-aset lain apa yang terkait erat dengan asset ini?			

5	*Which people have a special skill or knowledge that is vital to your organization and would be difficult to replace?*	Siapa saja orang-orang yang memiliki keterampilan atau pengetahuan khusus yang sangat penting bagi organisasi Anda dan sulit untuk digantikan?			
6	*What are their special skills or knowledge?*	Apa keahlian atau pengetahuan khusus yang mereka miliki?			
7	*Which system do these people use?*	Sistem apa yang digunakan oleh orang-orang ini?			
8	*Which other assets do these people use? (i.e., information, services, and applications).*	Aset lain apa saja lainnya yang digunakan oleh orang-orang ini? (misalnya, informasi, layanan, dan aplikasi).			

3. Lembar Kerja Evaluasi Praktik Keamanan

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
1	*Saff members understand their security roles and responsinilities. This is documented and verified.*	Anggota staf memahami peran dan tanggung jawab keamanan mereka. Hal ini didokumentasikan dan diverifikasi.			
2	*There is adequate in-house expertise for all supported service, mechanism, and technologies (e.g., logging, monitoring, or encryption), including their secure operation. This is documented and verified.*	Terdapat keahlian internal yang memadai untuk semua layanan, dan teknologi yang didukung (misalnya, pencatatan, pemantauan, atau enkripsi), termasuk operasi yang aman. Hal ini didokumentasikan dan diverifikasi.			
3	*Security awareness, training, and periodic reminders are provided for all personnel. Staff*	Kesadaran akan keamanan, pelatihan, dan pengingat berkala disediakan untuk semua personil. Pemahaman staf			

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
	understanding is documented and conformance is periodically verified.	didokumentasikan dan kesesuaiannya diverifikasi secara berkala.			
4	*Staff members follow good security practice, such as:* *a. Securing information for which they are responsible* *b. Not divulging sensitive information to others (resistance to social engineering)* *c. Having adequate ability to use information technology hardware and software*	Anggota staf mengikuti praktik keamanan yang baik, seperti: a. Mengamankan informasi yang menjadi tanggung jawab mereka b. Tidak membocorkan informasi sensitif kepada orang lain (resistensi terhadap rekayasa sosial) c. Memiliki kemampuan yang memadai untuk menggunakan perangkat keras dan perangkat lunak teknologi informasi			

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
	d. Using good password practice *e. Understanding and following security policies and regulations* *f. Recognizing and reporting incidents*	d. Menggunakan praktik kata sandi yang baik e. Memahami dan mengikuti kebijakan dan peraturan keamanan f. Mengenali dan melaporkan insiden			
5	*The organization's business strategy routinely incorporate security considerations.*	Strategi bisnis organisasi secara rutin memasukkan pertimbangan keamanan.			
6	*Security strategies and policies take into consideration the organization's business strategies and goals.*	Strategi dan kebijakan keamanan mempertimbangkan strategi dan tujuan bisnis organisasi.			
7	*Security strategies, goals, and objectives are documented and*	Strategi, tujuan, dan sasaran keamanan didokumentasikan dan secara rutin			

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
	are routinely reviewed, updated, and communicated to the organization.	ditinjau, diperbarui dan dikomunikasikan kepada organisasi.			
8	*Management allocates sufficient funds and resources to information security activities.*	Manajemen mengalokasikan dana dan sumber daya yang cukup untuk kegiatan keamanan informasi.			
9	*Security roles and responsibilities are defined for all staff in the organization.*	Peran dan tanggung jawab keamanan ditetapkan untuk semua staf dalam organisasi.			
10	*All staff at all levels of responsibility implement their assigned roles and responsibility for information security.*	Semua staf di semua tingkat tanggung jawab melaksanakan peran dan tanggung jawab mereka untuk keamanan informasi.			
11	*There are documented procedures for authorizing and*	Terdapat prosedur yang terdokumentasi untuk mengesahkan dan mengawasi			

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
	overseeing all staff (including personnel from third party organizations) who work with sensitive information or who work in locations where the information resides.	semua staf (termasuk personil dari organisasi pihak ketiga) yang bekerja dengan informasi sensitif atau bekerja di lokasi tempat informasi tersebut berada).			
12	*The organization's hiring and termination practices for staff take information security issues into account.*	Praktik perekrutan dan pemberhentian staf mempertimbangkan masalah keamanan informasi			
13	*The organization manages information security risks, Including* *a. Assessing risks to information security*	Organisasi mengelola risiko keamanan informasi, termasuk: a. Menilai risiko terhadap keamanan informasi			

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
	b. Taking steps to mitigate information security risks	b. Mengambil langkah-langkah untuk mengurangi risiko keamanan informasi			
14	*Management receives and acts upon routine reports summarizing security-related information (e.g., audits, logs, risk and vulnerability assessments).*	Manajemen menerima dan menindaklanjuti laporan rutin yang merangkum informasi terkait keamanan (misalnya, audit, log, penilaian risiko dan kerentanan).			
15	*The organization has a comprehensive set of documented, current policies that are periodically reviewed and updated.*	Organisasi memiliki seperangkat kebijakan terdokumentasi yang komprehensif dan terkini yang ditinjau dan diperbarui secara berkala.			

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
16	*There us a documented process for management of security policies, including* *a. Creation* *b. Administration (including periodic reviews and updates)* *c. Communication*	Terdapat proses yang terdokumentasi untuk pengelolaan kebijakan keamanan termasuk a. Penciptaan b. Administrasi (termasuk tinjauan dan pembaruan berkala) c. Komunikasi			
17	*The organization has a documented process for evaluating and ensuring compliance with information security policies, applicable laws and regulations, and insurance requirements.*	Organisasi memiliki proses yang terdokumentasi untuk mengevaluasi dan memastikan kepatuhan terhadap kebijakan keamanan informasi, hukum dan peraturan yang berlaku, dan persyaratan asuransi.			

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
18	*The organization uniformly enforce its security policies.*	Organisasi secara kompak menerapkan kebijakan keamanannya.			
19	*The organization has policies and procedures for protecting information when working with external organizations (e.g., third parties, collaborators, subcontractors, or partners), including* *a. Protecting information belonging to other organizations* *b. Understanding the security policies and procedures of external organizations*	Organisasi memiliki kebijakan dan prosedur untuk melindungi informasi ketika bekerja dengan organisasi eksternal (misalnya, pihak ketiga, kolaborator, subkontraktor, atau mitra), termasuk; a. Melindungi informasi milik organisasi lain b. Memahami kebijakan dan prosedur keamanan organisasi eksternal c. Mengakhiri akses informasi ke personil eksternal yang diberhentikan			

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
	c. *Ending access to information by terminated external personel*				
20	*The organization documents information protection requirements and explicitly communicates them to all appropriate third parties.*	Organisasi mendokumentasikan persyaratan perlindungan informasi dan secara eksplisit mengkomunikasikannya kepada semua pihak ketiga yang sesuai.			
21	*The organization has formal mechanisms for verifying that all third-party organizations, outsourced security services, mechanisms, and technologies meet its needs and requirements.*	Organisasi memiliki mekanisme formal untuk memverifikasi bahwa semua organisasi pihak ketiga, layanan keamanan yang dialihdayakan, mekanisme, dan teknologi memenuhi kebutuhan dan persyaratannya.			

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
22	*The organization has policies and procedures for collaborating with all third-party organizations that* *a. Provide security awareness and training services* *b. develop security policies for the organization* *c. develop contingency plans for the organization*	Organisasi memiliki kebijakan dan prosedur untuk berkolaborasi dengan semua organisasi pihak ketiga a. Menyediakan layanan pelatihan dan kesadaran keamanan b. Mengembangkah kebijakan keamanan untuk organisasi c. Mengembangkan rencana kontinjensi untuk organisasi			
23	*An analysis of operations, applications, and data criticality has been performed.*	Analisis operasi, aplikasi, dan kekritisan data telah dilakukan.			

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
24	*The organization has documented, reviewed, and tested* *a. Contingency plan(s) for responding to emergencies* *b. Disaster recovery plan(s)* *c. Business continuity or emergency operation plans.*	Organisasi telah mendokumentasikan, menunjau, dan menguji a. Rencana kontinjensi untuk menanggapi keadaan darurat b. Rencana pemulihan bencana c. Kelangsungan rencana operasi darurat			
25	*The contingency, disaster recovery, and business continuity plans consider physical and electronic access requirements and controls.*	Rencana kontinjensi, pemulihan bencana, dan kelangsungan operasi mempertimbangkan persyaratan dan control akses fisik dan elektronik.			
26	*All staff are*	Semua staf semestinya			

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
	a. Aware of the contingency, disaster recovery, and business continuity plans *b. understand and are able to carry out their responsibilities*	a. Mengetahui rencana kontinjensi, pemulihan bencana, dan kelangsungan operasional b. Memahami dan mampu melaksanakan tanggung jawab mereka.			
27	*Facility security plans and procedures for safeguarding the premises, buildings, and any restricted areas are documented and tested.*	Rencana dan prosedur keamanan fasilitas untuk melindungi tempat, bangunan, dan area terlarang didokumentasikan dan diuji.			
28	*There are documented policies and procedures for managing visitors.*	Terdapat kebijakan dan prosedur yang terdokumentasi untuk mengelola pengunjung.			

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
29	*There are documented policies and procedures for controlling physical access to work areas and hardware (computers, communication devices, etc.) and software media.*	Terdapat kebijakan dan prosedur yang terdokumentasi untuk mengendalikan akses fisik ke area kerja dan perangkat keras (komputer, perangkat komunikasi, dll.) dan media perangkat lunak.			
30	*Workstations and other components that allow access to sensitive information are physically safeguarded to prevent unauthorized access.*	Lingkungan kerja dan komponen lain yang memungkinkan akses ke informasi sensitif dilindungi secara fisik untuk mencegah akses yang tidak sah.			
31	*Maintenance records are kept to document the repairs and modifications of a facility's physical components.*	Catatan pemeliharaan disimpan untuk mendokumentasikan perbaikan dan modifikasi komponen fisik fasilitas.			

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
32	*An individual's or group's actions, with respect to all physically controlled media, can be accounted for.*	Tindakan individu atau kelompok, sehubungan dengan semua media dikontrol secara fisik, dapat dipertanggungjawabkan.			
33	*Audit and monitoring records are routinely examined for anomalies, and corrective action is taken as needed.*	Catatan audit dan pemantauan secara rutin diperiksa untuk mengetahui adanya anomali, dan tindakan kolektif diambil sesuai kebutuhan.			
34	*There are documented and tested security plan(s) for safeguarding the systems and networks.*	Ada rencana keamanan yang terdokumentasikan dan teruji untuk melindungi sistem dan jaringan.			
35	*Sensitive information is protected by secure storage (e.g., backups stored off site,*	Informasi sensitif dilindungi oleh penyimpanan yang aman (misalnya,			

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
	discard process for sensitive information).	cadangan disimpan di luar lokasi, proses pembuangan informasi sensitif).			
36	*The integrity of installed software is regularly verified.*	Integritas perangkat lunak yang terinstal diverifikasi secara teratur.			
37	*All systems are up to date with respect to revisions, patches, and recommendations in security advisories.*	Semua sistem selalu diperbarui sehubungan dengan revisi, pembaruan, dan rekomendasi dalam saran keamanan.			
38	*There is a documented and tested data backup plan for backups of both software and data. All staff understand their responsibilities under the backup plans.*	Ada rencana pencadangan data yang terdokumentasi dan teruji untuk pencadangan perangkat lunak dan data. Semua staf memahami tanggung jawab mereka di bawah rencana pencadangan.			

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
39	*Changes to IT hardware and software are planned, controlled, and documented.*	Perubahan pada perangkat keras dan perangkat lunak TI direncanakan, dikontrol, dan didokumentasikan.			
40	*IT staff members follow procedures when issuing, changing, and terminating users' passwords, accounts, and privileges.* a. *Unique user identification is required for all information system users, including third party users* b. *Default accounts and default passwords have*	Anggota staf TI mengikuti prosedur saat menerbitkan, mengubah, dan menghentikan kata sandi, akun, dan hak istimewa pengguna. a. Identifikasi pengguna yang unik diperlukan untuk semua pengguna sistem informasi, termasuk pengguna pihak ketiga. b. Akun bawaan dan kata sandi bawaan telah dihapus dari sistem.			

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
	been removed from systems.				
41	*Only necessary services are running on systems – all unnecessary services have been removed.*	Hanya layanan yang diperlukan yang dijalankan pada sistem - semua layanan yang tidak perlu dihapus.			
42	*Tools and mechanisms for secure system and network administration are used, and are routinely reviewed and updated or replaced.*	Alat dan mekanisme untuk administrasi sistem dan jaringan yang aman digunakan, dan secara rutin ditinjau dan diperbarui atau diganti.			
43	*System and network monitoring and auditing tools are routinely used by the organization. Unusual activity is dealt with*	Alat-alat pemantauan dan audit sistem dan jaringan secara rutin digunakan oleh organisasi. Aktivitas yang tidak biasa			

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
	according to the appropriate policy or procedure.	ditangani sesuai dengan kebijakan atau prosedur yang berlaku.			
44	*Firewall and other security components are periodically audited for compliance with policy.*	*Firewall* dan komponen keamanan lainnya diaudit secara berkala untuk memastikan kepatuhan terhadap kebijakan.			
45	*Appropriate access controls and user authentication (e.g., file permissions, network configuration) consistent with policy are used to restrict user access to information, sensitive systems, specific applications and services, and network connections.*	Kontrol akses yang tepat dan autentikasi pengguna (misalnya, izin file, konfigurasi jaringan) yang sesuai dengan kebijakan digunakan untuk membatasi akses pengguna ke informasi, sistem yang sensitif, aplikasi dan layanan tertentu, dan koneksi jaringan.			

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
46	*There are documented policies and procedures to establish and terminate the right of access to information for both individuals and groups.*	Terdapat kebijakan dan prosedur yang terdokumentasi untuk menetapkan dan mengakhiri hak akses terhadap informasi bagi individu maupun kelompok.			
47	*Methods or mechanisms are provided to ensure that sensitive information has not been accessed, altered, or destroyed in an unauthorized manner. Methods or mechanisms are periodically reviewed and verified.*	Metode atau mekanisme disediakan untuk memastikan bahwa informasi sensitif tidak diakses, diubah, atau dihancurkan dengan cara yang tidak sah. Metode atau mekanisme ditinjau dan diverifikasi secara berkala.			

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
48	*There is a documented set of procedures for managing vulnerabilities, including* a. *Selecting vulnerability evaluation tools, checklists, and scripts* b. *Keeping up to date with known vulnerability types and attack methods* c. *Reviewing sources of information on vulnerability announcements, security alerts, and notices*	Terdapat serangkaian prosedur terdokumentasi untuk mengelola kerentanan, termasuk a. Memilih alat evaluasi terentanan, data periksa, dan skrip b. Selalu mengikuti perkembangan jenis kerentanan dan metode serangan yang diketahui c. Meninjau sumber informasi tentang pengumuman kerentanan, peringatan keamanan, dan permberitahuan d. Mengidentifikasi komponen infrastruktur yang akan dievaluasi e. Penjadwalan untuk evaluasi kerentanan			

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
	d. *Identifying infrastructure components to be evaluated* e. *Scheduling of vulnerability evaluations* f. *Interpreting and responding to the evaluation results* g. *Maintaining secure storage and disposition of vulnerability data*	f. Menafsirkan dan menganggapi hasil evaluasi g. Menjaga penyimpanan dan disposisi data kerentanan yang aman.			
49	*Vulnerability management procedures are followed and are periodically reviewed and updated.*	Prosedur manajemen kerentanan diikuti dan ditinjau serta diperbarui secara berkala.			

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
50	*Technology vulnerability assessments are performed on a periodic basis, and vulnerabilities are addressed when they are identified.*	Penilaian kerentanan teknologi dilakukan secara berkala, dan kerentanan diatasi ketika teridentifikasi.			
51	*Appropriate security controls are used to protect sensitive information while in storage and during transmission (e.g., data encryption, public key infrastructure, virtual private network technology).*	Kontrol keamanan yang tepat digunakan untuk melindungi informasi sensitif saat berada dalam penyimpanan dan selama transmisi (misalnya, enkripsi data, infrastruktur kunci publik, teknologi jaringan pribadi virtual).			
52	*Encrypted protocols are used when remotely managing systems, routers, and firewalls.*	Protokol terenkripsi digunakan ketika mengelola sistem, *router*, dan *firewall* dari jarak jauh.			

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
53	*System architecture and design for new and revised systems include considerations for* a. *Security strategies, policies, and procedures* b. *History of security compromises* c. *Results of security risk assessments*	Arsitektur dan desain sistem untuk sistem baru dan sistem yang direvisi mencakup pertimbangan untuk: a. Strategi, kebijakan, dan prosedur keamanan b. Riwayat kompromi keamanan c. Hasil penilaian risiko keamanan			
54	*The organization has up-to-date diagrams that show the enterprise-wide security architecture and network topology.*	Organisasi memiliki diagram terkini yang menunjukkan arsitektur keamanan di seluruh perusahaan topologi jaringan.			

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
55	*Documented procedures exist for identifying, reporting, and responding to suspected security incidents and violations.*	Terdapat prosedur yang terdokumentasi untuk mengidentifikasi, melaporkan, dan menanggapi dugaan insiden dan pelanggaran keamanan.			
56	*Incident management procedures are periodically tested, verified, and updated.*	Prosedur manajemen insiden diuji, diverifikasi, dan diperbarui secara berkala.			
57	*There are documented policies and procedures for working with law enforcement agencies.*	Terdapat kebijakan dan prosedur yang terdokumentasi untuk bekerja dama dengan lembaga penegak hukum.			

4. Lembar Kerja Pemilihan Aset Kritis

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERTANYAAN	PENGERTIAN	R	TR	
1	*Which assets would have a large adverse impact on the organization if* *a. They are disclosed to unauthorized people?* *b. They are modified without authorization?* *c. They are lost destroyed?* *d. Access to them is interrupted?*	Aset mana yang akan memiliki dampak buruk yang besar pada organisasi jika a. Informasi tersebut dibocorkan kepada pihak yang tidak berwenang? b. Informasi tersebut diubah tanpa otorisasi? c. Informasi tersebut hilang atau hancur? d. Akses terhadap informasi tersebut terputus?			

5. Lembar Kerja Informasi Aset Kritis Untuk Informasi, Sistem, Aplikasi, dan Orang

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERTANYAAN	PENGERTIAN	R	TR	
1	*What is the critical Information, system, application, and people?*	Apa arti dari informasi kritis, sistem, aplikasi, dan orang?			
2	*Why is this information, system, application, and people critical to the organization?*	Mengapa informasi, sistem, aplikasi, dan orang penting bagi organisasi?			
3	*Which assets are related to this information, syetem, application, and people?* *a. Information* *b. System* *c. Application* *d. Human/People* *e. Other*	Aset apa saja yang terkait dengan informasi, sistem, aplikasi, dan orang? a. Informasi b. Sistem c. Aplikasi d. Orang e. Lainnya			

4	*What are the security requirements for this information? (Hint: Focus on what the security requirements should be for this information,system, application, and people, not what they currently are).* *a. Confidentiality (Only authorized personnel can view…)* *b. Integrity (Only authorized personnel can modify …)* *c. Availability (…must be available for personnel to perform their jobs. Unavailability cannot exceed … hour(s) per every … hours.* *d. Other*	Apa saja kebutuhan keamanan untuk informasi ini? (Petunjuk: Fokus pada persyaratan keamanan yang seharusnya untuk informasi, sistem, aplikasi, dan orang ini, bukan yang ada pada persyaratan keamanan saat ini). a. Kerahasiaan (hanya personil yang berwenang yang dapat melihat …) b. Integritas (hanya personil yang berwenang yang dapat memodifikasi …) c. Ketersediaan (… harus tersedia bagi personil untuk melakukan pekerjaannya. Ketidaktersediaan tidak boleh melebihi … jam per setiap … jam. d. Lainnya			

5	*Which security requirement is most important for this information, system, application, and people?* *a. Confidentiality* *b. Integrity* *c. Avalilability* *d. Other*	Persyaratan keamanan manakah yang paling penting untuk informasi, sistem, aplikasi, dan orang ini? a. Kerahasiaan b. Integritas c. Ketersediaan d. Lainnya			

Keterangan:

1. R: Relevan
2. TR: Tidak Relevan

Lampiran 5. Hasil Uji Kebahasaan Penguji Ahli 1

HASIL UJI KEBAHASAAN OLEH AHLI
DALAM RANGKA PENELITIAN ANALISIS MANAJEMEN RISIKO KEAMANAN INFORMASI MENGGUNAKAN OCTAVE-S DAN ISO 27001:2022 PADA UNIT PENUNJANG AKADEMIK TEKNOLOGI INFORMASI DAN KOMUNIKASI (UPA TIK) UNIVERSITAS PENDIDIKAN GANESHA.

Penguji Ahli

Nama	:	Gede Arna Jude Saskara, S.T., M.T.
Instansi	:	UPA TIK Undiksha.
Jabatan	:	Kepala Divisi Jaringan, Infrastruktur & Keamanan.
NIP	:	199105152020121003

Hasil Uji:

1.

Singaraja, 29 Agustus 2024

Penguji Ahli,

Gede Arna Jude Saskara, S.T., M.T.
NIP. 199105152020121003

Peneliti,

Hardiyanti Rohmania
NIM. 2015091018

1. **Lembar Kerja Kriteria Evaluasi Dampak**

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	NILAI DAMPAK	PENGERTIAN	R	TR	
1	*Reputation*	Reputasi/Kepercayaan	✓		
2	*Financial*	Keuangan	✓		
3	*Productivity*	Produktifitas	✓		
4	*Savety/Health*	Keamanan/Keselamatan	✓		

2. **Lembar Kerja Identifikasi Aset**

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERTANYAAN	PENGERTIAN	R	TR	
1	*What system do people in your organization need to perform their jobs?*	Sistem apa yang dibutuhkan oleh orang-orang dalam organisasi Anda untuk menjalankan tugas mereka?	✓		
2	*What information do people in your organization need to perform their jobs?*	Informasi apa yang dibutuhkan oleh orang-orang di organisasi Anda untuk melakukan pekerjaan mereka?	✓		

3	*What application dan services do people in your organization need to perform their jobs?*	Aplikasi dan layanan apa yang dibutuhkan oleh orang-orang di organisasi Anda untuk melaksanakan pekerjaan mereka?	✓		
4	*What other assets are closely related to these assets?*	Aset-aset lain apa yang terkait erat dengan asset ini?	✓		
5	*Which people have a special skill or knowledge that is vital to your organization and would be difficult to replace?*	Siapa saja orang-orang yang memiliki keterampilan atau pengetahuan khusus yang sangat penting bagi organisasi Anda dan sulit untuk digantikan?	✓		
6	*What are their special skills or knowledge?*	Apa keahlian atau pengetahuan khusus yang mereka miliki?	✓		
7	*Which system do these people use?*	Sistem apa yang digunakan oleh orang-orang ini?	✓		
8	*Which other assets do these people use? (i.e., information, services, and applications).*	Aset apa saja lainnya yang digunakan oleh orang-orang ini? (misalnya, informasi, layanan, dan aplikasi).	✓		

3. Lembar Kerja Praktik Keamanan

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
1	*Saff members understand their security roles and responsinilities. This is documented and verified.*	Anggota staf memahami peran dan tanggung jawab keamanan mereka. Hal ini didokumentasikan dan diverifikasi.	✓		
2	*There is adequate in-house expertise for all supported service, mechanism, and technologies (e.g., logging, monitoring, or encryption), including their secure operation. This is documented and verified.*	Terdapat keahlian internal yang memadai untuk semua layanan, dan teknologi yang didukung (misalnya, pencatatan, pemantauan, atau enkripsi), termasuk operasi yang aman. Hal ini didokumentasikan dan diverifikasi.	✓		
3	*Security awareness, training, and periodic reminders are provided for all personnel. Staff understanding is documented and conformance is periodically verified.*	Kesadaran akan keamanan, pelatihan, dan pengingat berkala disediakan untuk semua personel. Pemahaman staf didokumentasikan dan kesesuaiannya diverifikasi secara berkala.	✓		

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
4	*Staff members follow good security practice, such as:* *a. Securing information for which they are responsible* *b. Not divulging sensitive information to others (resistance to social engineering)* *c. Having adequate ability to use information technology hardware and software* *d. Using good password practice* *e. Understanding and following security policies and regulations*	Anggota staf mengikuti praktik keamanan yang baik, seperti: a. Mengamankan informasi yang menjadi tanggung jawab mereka b. Tidak membocorkan informasi sensitif kepada orang lain (resistensi terhadap rekayasa sosial) c. Memiliki kemampuan yang memadai untuk menggunakan perangkat keras dan perangkat lunak teknologi informasi d. Menggunakan praktik kata sandi yang baik e. Memahami dan mengikuti kebijakan dan peraturan keamanan	✓		

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
	f. Recognizing and reporting incidents	f. Mengenali dan melaporkan insiden			
5	*The organization's business strategy routinely incorporate security considerations.*	Strategi bisnis organisasi secara rutin memasukkan pertimbangan keamanan.	✓		
6	*Security strategies and policies take into consideration the organization's business strategies and goals.*	Strategi dan kebijakan keamanan mempertimbangkan strategi dan tujuan bisnis organisasi.	✓		
7	*Security strategies, goals, and objectives are documented and are routinely reviewed, updated, and communicated to the organization.*	Strategi, tujuan, dan sasaran keamanan didokumentasikan dan secara rutin ditinjau, diperbarui dan dikomunikasikan kepada organisasi.	✓		
8	*Management allocates sufficient funds and resources to information security activities.*	Manajemen mengalokasikan dana dan sumber daya yang cukup untuk kegiatan keamanan informasi.	✓		

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
9	*Security roles and responsibilities are defined for all staff in the organization.*	Peran dan tanggung jawab keamanan ditetapkan untuk semua staf dalam organisasi.	✓		
10	*All staff at all levels of responsibility implement their assigned roles and responsibility for information security.*	Semua staf di semua tingkat tanggung jawab melaksanakan peran dan tanggung jawab mereka untuk keamanan informasi.	✓		
11	*There are documented procedures for authorizing and overseeing all staff (including personnel from third party organizations) who work with sensitive information or who work in locations where the information resides.*	Terdapat prosedur terdokumentasi untuk mengesahkan dan mengawasi semua staf (termasuk personil dari organisasi pihak ketiga) yang bekerja dengan infrmasi sensitif atau bekerja di lokasi tempat informasi tersebut berada).			
12	*The organization's hiring and termination practices for staff*	Praktik perekrutan dan pemberhentian staf mempertimbangkan masalah keamanan informasi	✓		

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
	take information security issues into account.				
13	*The organization manages information security risks, Including* *a. Assessing risks to information security* *b. Taking steps to mitigate information security risks*	Organisasi mengelola risiko keamanan informasi, termasuk; a. Menilai risiko terhadap keamanan informasi b. Mengambil langkah-langkah untuk mengurangi risiko keamanan informasi	✓		
14	*Management receives and acts upon routine reports summarizing security-related information (e.g., audits, logs, risk and vulnerability assessments).*	Manajemen menerima dan menindaklanjuti laporan rutin yang merangkum informasi terkait keamanan (misalnya, audit, log,penilaian risiko dan kerentanan).	✓		
15	*The organization has a comprehensive set of*	Organisasi memiliki seperangkat kebijakan terdokumentasi yang	✓		

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
	documented, current policies that are periodically reviewed and updated.	komprehensif dan terkini yang ditinjau dan diperbarui secara berkala.			
16	*There us a documented process for management of security policies, including* *a. Creation* *b. Administration (including periodic reviews and updates)* *c. Communication*	Terdapat proses yang terdokumentasi untuk pengelolaan kebijakan keamanan termasuk a. Penciptaan b. Administrasi (termasuk tinjauan dan pembaruan berkala) c. Komunikasi	✓		
17	*The organization has a documented process for evaluating and ensuring compliance with information security policies, applicable laws and regulations, and insurance requirements.*	Organisasi memiliki proses yang terdokumentasi untuk mengevaluasi dan memastikan kepatuhan terhadap kebijakan keamanan informasi, hukum dan peraturan yang berlaku, dan persyaratan asuransi.	✓		

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
18	*The organization uniformly enforce its security policies.*	Organisasi secara kompak menerapkan kebijakan keamanannya.	✓		
19	*The organization has policies and procedures for protecting information when working with external organizations ((e.g., third parties, collaborators, subcontractors, or partners), including* *a. Protecting information belonging to other organizations* *b. Understanding the security policies and procedures of external organizations* *c. Ending access to information by*	Organisasi memiliki kebijakan dan prosedur untuk melindungi informasi ketika bekerja dengan organisasi eksternal (misalnya, pihak ketiga, kolaborator, subskontraktor, atau mitra), termasuk; a. Melindungi informasi milik organisasi lain b. Memahami kebijakan dan prosedur keamanan organisasi eksternal c. Mengakhiri akses ke informasi oleh personel eksternal yang diberhentikan	✓		

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
	terminated external personel				
20	*The organization documents information protection requirements and explicitly communicates them to all appropriate third parties.*	Organisasi mendokumentasikan persyaratan perlindungan informasi dan secara eksplisit mengkomunikasikannya kepada semua pihak ketiga yang sesuai.	✓		
21	*The organization has formal mechanisms for verifying that all third-party organizations, outsourced security services, mechanisms, and technologies meet its needs and requirements.*	Organisasi memiliki mekanisme formal untuk memverifikasi bahwa semua organisasi pihak ketiga, layanan keamanan yang dialihdayakan, mekanisme, dan teknologi memenuhi kebutuhan dan persyaratannya.	✓		
22	*The organization has policies and procedures for collaborating with all third-party organizations that*	Organisasi memiliki kebijakan dan prosedur untuk berkolaborasi dengan semua organisasi pihak ketiga a. Menyediakan layanan pelatihan dan kesadaran keamanan	✓		

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
	a. *Provide security awareness and training services* b. *develop security policies for the organization* c. *develop contingency plans for the organization*	b. Mengembangkah kebijakan keamanan untuk organisasi c. Mengembangkan rencana kontinjensi untuk organisasi	✓		
23	*An analysis of operations, applications, and data criticality has been performed.*	Analisis operasi, aplikasi, dan kekritisan data telah dilakukan.	✓		
24	*The organization has documented, reviewed, and tested* a. *Contingency plan(s) for responding to emergencies* b. *Disaster recovery plan(s)*	Organisasi telah mendokumentasikan, menunjau, dan menguji a. Rencana kontinjensi untuk menanggapi keadaan darurat b. Rencana pemulihan bencana c. Kelangsungan rencana operasi darurat	✓		

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
	c. *Business continuity or emergency operation plans.*				
25	*The contingency, disaster recovery, and business continuity plans consider physical and electronic access requirements and controls.*	Rencana kontinjensi, pemulihan bencana, dan kelangsungan operasi mempertimbangkan persyaratan dan control akses fisik dan elektronik.	✓		
26	*All staff are* a. *Aware of the contingency, disaster recovery, and business continuity plans* b. *understand and are able to carry out their responsibilities*	Semua staf adalah a. Mengetahui rencana kontinjensi, pemulihan bencana, dan kelangsungan operasional b. Memahami dan mampu melaksanakan tanggung jawab mereka.	✓		
27	*Facility security plans and procedures for safeguarding the*	Rencana dan prosedur keamanan fasilitas untuk melindungi tempat, bangunan, dan	✓		

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
	premises, buildings, and any restricted areas are documented and tested.	area terlarang didokumentasikan dan diuji.			
28	*There are documented policies and procedures for managing visitors.*	Terdapat kebijakan dan prosedur yang terdokumentasi untuk mengelola pengunjung.	✓		
29	*There are documented policies and procedures for controlling physical access to work areas and hardware (computers, communication devices, etc.) and software media.*	Terdapat kebijakan dan prosedur yang terdokumentasi untuk mengendalikan akses fisik ke area kerja dan perangkat keras (komputer, perangkat komunikasi, dll) dan media perangkat lunak.	✓		
30	*Workstations and other components that allow access to sensitive information are physically safeguarded to prevent unauthorized access.*	Lingkungan kerja dan komponen lain yang memungkinkan akses ke informasi sensitive dilindungi secara fisik untuk mencegah akses yang tidak sah.	✓		

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
31	*Maintenance records are kept to document the repairs and modifications of a facility's physical components.*	Catatan pemeliharaan disimpan untuk mendokumentasikan perbaikan dan modifikasi komponen fisik fasilitas.	✓		
32	*An individual's or group's actions, with respect to all physically controlled media, can be accounted for.*	Tindakan individu atau kelompok, sehubungan dengan semua media dikontrol secara fisik, dapat dipertanggungjawabkan.	✓		
33	*Audit and monitoring records are routinely examined for anomalies, and corrective action is taken as needed.*	Catatan audit dan pemantauan secara rutin diperiksa untuk mengetahui adanya animali, dan tindakan kolektif diambil sesuai kebutuhan.	✓		
34	*There are documented and tested security plan(s) for safeguarding the systems and networks.*	Ada rencana keamanan yang didokumentasi dan teruji untuk melindungi sistem dan jaringan.	✓		
35	*Sensitive information is protected by secure storage*	Informasi sensitif dilindungi oleh penyimpanan yang aman (missal,	✓		

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
	(e.g., backups stored off site, discard process for sensitive information).	cadangan disimpan diluar lokasi, proses pembuangan informasi sensitive).			
36	*The integrity of installed software is regularly verified.*	Integritas perangkat lunak yang terinstal diverifikasi secara teratur.	✓		
37	*All systems are up to date with respect to revisions, patches, and recommendations in security advisories.*	Semua sistem selalu diperbarui sehubunga dengan revisi, tambalan, dan rekomendasi dalam saran keamanan.	✓		
38	*There is a documented and tested data backup plan for backups of both software and data. All staff understand their responsibilities under the backup plans.*	Ada rencana pencadangan data yang terdokumentasi dan teruji untuk pencadangan perangkat lunak dan data. Semua staf memahami tanggung jawab mereka di bawah rencana pencadangan.	✓		
39	*Changes to IT hardware and software are planned, controlled, and documented.*	Perubahan pada perangkat keras dan perangkat lunakTI direncanakan, dikontrol, dan didokumentasikan.	✓		

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
40	*IT staff members follow procedures when issuing, changing, and terminating users' passwords, accounts, and privileges.* a. *Unique user identification is required for all information system users, including third party users* b. *Default accounts and default passwords have been removed from systems.*	Anggota staf TI mengikuti prosedur saat menerbitkan, mengubah, dan mengehentikan kata sandi, akun, dan hak istimewa pengguna. a. Identifikasi pengguna yang unik diperlukan untuk semua pengguna sistem informasi, termasuk pengguna pihak ketiga. b. Aku defaukt dan kata sandi default telah dihapus dari sistem.	✓		
41	*Only necessary services are running on systems – all unnecessary services have been removed.*	Hanya layanan yang diperlukan yang berjalan pada sistem-semua layanan yang tidak perlu dihapus.	✓		

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
42	*Tools and mechanisms for secure system and network administration are used, and are routinely reviewed and updated or replaced.*	Alat dan mekanisme untuk administrasi sistem dan jaringan yang aman digunakan, dan secara rutin ditinjau dan diperbarui atau diganti.	✓		
43	*System and network monitoring and auditing tools are routinely used by the organization. Unusual activity is dealt with according to the appropriate policy or procedure.*	Alat-alat pemantauan dan audit sistem dan jaringan secara rutin digunakan oleh organisasi. Aktivitas yang tidak biasa ditangani sesuai dengan kebijakan atau prosedur yang berlaku.	✓		
44	*Firewall and other security components are periodically audited for compliance with policy.*	Firewall dan komponen keamanan lainnya diaudit secara berkala untuk memastikan kepatuhan terhadap kebijakan.	✓		
45	*Appropriate access controls and user authentication (e.g., file permissions, network*	Kontrol akses yang tepat dan autentikasi pengguna (misalnya, izin file, konfigurasi jaringan) yang sesuai dengan kebijakan	✓		

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
	configuration) consistent with policy are used to restrict user access to information, sensitive systems, specific applications and services, and network connections.	digunakan untuk membatasi akses pengguna ke informasi, sistem yang sensitif, aplikasi dan layanan tertentu, dan koneksi jaringan.			
46	*There are documented policies and procedures to establish and terminate the right of access to information for both individuals and groups.*	Terdapat kebijakan dan prosedur yang terdokumentasi untuk menetapkan dan mengakhiri hak akses terhadap informasi baik untuk individu maupun kelompok.	✓		
47	*Methods or mechanisms are provided to ensure that sensitive information has not been accessed, altered, or destroyed in an unauthorized manner. Methods or mechanisms are*	Metode atau mekanisme disediakan untuk memastikan bahwa informasi sensitif tidak diakses, diubah, atau dihancurkan dengan cara yang tidak sah. Metode atau mekanisme ditinjau dan diverifikasi secara berkala.	✓		

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
	periodically reviewed and verified.				
48	*There is a documented set of procedures for managing vulnerabilities, including* a. *Selecting vulnerability evaluation tools, checklists, and scripts* b. *Keeping up to date with known vulnerability types and attack methods* c. *Reviewing sources of information on vulnerability announcements, security alerts, and notices*	Terdapat serangkaian prosedur terdokumentasi untuk mengelola kerentanan, termasuk a. Memilih alat evaluasi terentanan, data periksa, dan skrip. b. Selalu mengikuti perkembangan jenis kerentanan dan metode serangan yang diketahui. c. Meninjau sumber informasi tentang pengumuman kerentanan, peringatan keamanan, dan permberitahuan. d. Mengidentifikasi komponen infrastruktur yang akan dievaluasi e. Penjadwalan evaluasi kerentanan.	✓		

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
	d. *Identifying infrastructure components to be evaluated* e. *Scheduling of vulnerability evaluations* f. *Interpreting and responding to the evaluation results* g. *Maintaining secure storage and disposition of vulnerability data*	f. Menafsirkan dan menganggapi hasil evaluasi. g. Menjaga penyimpanan dan disposisi data kerentanan yang aman.	✓		
49	*Vulnerability management procedures are followed and are periodically reviewed and updated.*	Prosedur manajemen kerentanan diikuti dan ditinjau serta diperbarui secara berkala.	✓		
50	*Technology vulnerability assessments are performed on a periodic basis, and*	Penilaian kerentanan teknologi dilakukan secara berkala, dan kerentanan diatasi ketika teridentifikasi.	✓		

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
	vulnerabilities are addressed when they are identified.				
51	*Appropriate security controls are used to protect sensitive information while in storage and during transmission (e.g., data encryption, public key infrastructure, virtual private network technology).*	Kontrol keamanan yang tepat digunakan untuk melindungi informasi sensitif saat berada dalam penyimpanan dan selama transmisi (misalnya, enkripsi data, infrastruktur kunci public, teknologi jaringan pribadi virtual).	✓		
52	*Encrypted protocols are used when remotely managing systems, routers, and firewalls.*	Protokol terenkripsi digunakan ketika mengelola sistem, router, dan firewall dari jarak jauh.	✓		
53	*System architecture and design for new and revised systems include considerations for* a. *Security strategies, policies, and procedures*	Arsitektur dan desain sistem untuk sistem baru dan sistem yang direvisi mencakup pertimbangan untuk: a. Strategi, kebijakan, dan prosedur keamanan b. Riwayat kompromi keamanan	✓		

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
	b. *History of security compromises* c. *Results of security risk assessments*	c. Hasil penilaian risiko keamanan	✓		
54	*The organization has up-to-date diagrams that show the enterprise-wide security architecture and network topology.*	Organisasi memiliki diagram terkini yang menunjukkan arsitektur keamanan di seluruh perusahaan topologi jaringan.	✓		
55	*Documented procedures exist for identifying, reporting, and responding to suspected security incidents and violations.*	Terdapat prosedur yang terdokumentasi untuk mengidentifikasi, melaporkan, dan menanggapi dugaan insiden dan pelanggaran keamanan.	✓		
56	*Incident management procedures are periodically tested, verified, and updated.*	Prosedur manajemen insiden diuji, diverifikasi, dan diperbarui secara berkala.	✓		

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
57	*There are documented policies and procedures for working with law enforcement agencies.*	Terdapat kebijakan dan prosedur yang terdokumentasi untuk bekerja dama dengan lembaga penegak hukum.	✓		

4. Lembar Kerja Pemilihan Aset Kritis

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERTANYAAN	PENGERTIAN	R	TR	
1	*Which assets would have a large adverse impact on the organization if* *a. They are disclosed to unauthorized people?* *b. They are modified without authorization?* *c. They are lost destroyed?*	Aset mana yang akan memiliki dampak buruk yang besar pada organisasi jika a. Informasi tersebut dibocorkan kepada pihak yang tidak berwenang? b. Informasi tersebut diubah tanpa otorsasi?	✓		

	d. Access to them is interrupted?	c. Informasi tersebut hilang atau hancur? d. Akses terhadap informasi tersebut terputus?			

5. Lembar Kerja Informasi Aset Kritis Untuk Informasi, Sistem, Aplikasi, dan Orang

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERTANYAAN	PENGERTIAN	R	TR	
1	*What is the critical Information, system, application, and people?*	Apa informasi, sistem, aplikasi, dan orang yang kritis?	✓		
2	*Why is this information, system, application, and people critical to the organization?*	Mengapa informasi, sistem, aplikasi, dan orang penting bagi organisasi?	✓		
3	*Which assets are related to this information, syetem, application, and people?* *a. Information* *b. System* *c. Application*	Aset apa saja yang terkait dengan informasi, sistem, aplikasi, dan orang? a. Informasi b. Sistem c. Aplikasi d. Orang	✓		

	d. Other	e. Lainnya			
4	*What are the security requirements for this information? (Hint: Focus on what the security requirements should be for this information,system, application, and people, not what they currently are).* *a. Confidentiality (Only authorized personnel can view...)* *b. Integrity (Only authorized personnel can modify ...)* *c. Availability (... must be available for personnel to perform their jobs. Unavailability cannot exceed ... hour(s) per every ... hours.* *d. Other*	Apa kebutuhan untuk informasi ini? (Petunjuk: Fokus pada persyaratan keamanan yang seharusnya untuk informasi, sistem, aplikasi, dan orang ini, bukan yang ada pada persyaratan keamanan saat ini). a. Kerahasiaan (hanya personel yang berwenang yang dapat melihat ...) b. Integritas (hanya personel yang berwenang yang dapat memodifikasi ...) c. Ketersediaan (... harus tersedia bagi personel untuk melakukan pekerjaannya. Ketidaktersediaan tidak boleh melebihi ... jam per setiap ... jam. d. Lainnya	✓		

5	*Which security requirement is most important for this information, system, application, and people?* *a. Confidentiality* *b. Integrity* *c. Avalilability* *d. Other*	Persyaratan keamanan manakah yang paling penting untuk informasi, sistem, aplikasi, dan orang ini? a. Kerahasiaan b. Integritas c. Ketersediaan d. Lainnya	✓		

Keterangan:

1. R: Relevan
2. TR: Tidak Relevan

HASIL UJI KEBAHASAAN OLEH AHLI
DALAM RANGKA PENELITIAN ANALISIS MANAJEMEN RISIKO KEAMANAN INFORMASI MENGGUNAKAN OCTAVE-S DAN ISO 27001:2022 PADA UNIT PENUNJANG AKADEMIK TEKNOLOGI INFORMASI DAN KOMUNIKASI (UPA TIK) UNIVERSITAS PENDIDIKAN GANESHA.

Penguji Ahli

Nama	:	Gede Arna Jude Saskara, S.T., M.T.
Instansi	:	UPA TIK Undiksha.
Jabatan	:	Kepala Divisi Jaringan, Infrastruktur & Keamanan.
NIP	:	199105152020121003

Hasil Uji:

1.

Singaraja, 29 Agustus 2024

Penguji Ahli,

Gede Arna Jude Saskara, S.T., M.T.
NIP. 199105152020121003

Peneliti,

Hardiyanti Rohmania
NIM. 2015091018

1. **Lembar Kerja Kriteria Evaluasi Dampak**

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	NILAI DAMPAK	PENGERTIAN	R	TR	
1	*Reputation*	Reputasi/Kepercayaan	✓		
2	*Financial*	Keuangan	✓		
3	*Productivity*	Produktifitas	✓		
4	*Savety/Health*	Keamanan/Keselamatan	✓		

2. **Lembar Kerja Identifikasi Aset**

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERTANYAAN	PENGERTIAN	R	TR	
1	*What system do people in your organization need to perform their jobs?*	Sistem apa yang dibutuhkan oleh orang-orang dalam organisasi Anda untuk menjalankan tugas mereka?	✓		
2	*What information do people in your organization need to perform their jobs?*	Informasi apa yang dibutuhkan oleh orang-orang di organisasi Anda untuk melakukan pekerjaan mereka?	✓		

3	*What application dan services do people in your organization need to perform their jobs?*	Aplikasi dan layanan apa yang dibutuhkan oleh orang-orang di organisasi Anda untuk melaksanakan pekerjaan mereka?	✓		
4	*What other assets are closely related to these assets?*	Aset-aset lain apa yang terkait erat dengan asset ini?	✓		
5	*Which people have a special skill or knowledge that is vital to your organization and would be difficult to replace?*	Siapa saja orang-orang yang memiliki keterampilan atau pengetahuan khusus yang sangat penting bagi organisasi Anda dan sulit untuk digantikan?	✓		
6	*What are their special skills or knowledge?*	Apa keahlian atau pengetahuan khusus yang mereka miliki?	✓		
7	*Which system do these people use?*	Sistem apa yang digunakan oleh orang-orang ini?	✓		
8	*Which other assets do these people use? (i.e., information, services, and applications).*	Aset apa saja lainnya yang digunakan oleh orang-orang ini? (misalnya, informasi, layanan, dan aplikasi).	✓		

3. Lembar Kerja Praktik Keamanan

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
1	*Saff members understand their security roles and responsinilities. This is documented and verified.*	Anggota staf memahami peran dan tanggung jawab keamanan mereka. Hal ini didokumentasikan dan diverifikasi.	✓		
2	*There is adequate in-house expertise for all supported service, mechanism, and technologies (e.g., logging, monitoring, or encryption), including their secure operation. This is documented and verified.*	Terdapat keahlian internal yang memadai untuk semua layanan, dan teknologi yang didukung (misalnya, pencatatan, pemantauan, atau enkripsi), termasuk operasi yang aman. Hal ini didokumentasikan dan diverifikasi.	✓		
3	*Security awareness, training, and periodic reminders are provided for all personnel. Staff understanding is documented and conformance is periodically verified.*	Kesadaran akan keamanan, pelatihan, dan pengingat berkala disediakan untuk semua personel. Pemahaman staf didokumentasikan dan kesesuaiannya diverifikasi secara berkala.	✓		

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
4	*Staff members follow good security practice, such as:* *a. Securing information for which they are responsible* *b. Not divulging sensitive information to others (resistance to social engineering)* *c. Having adequate ability to use information technology hardware and software* *d. Using good password practice* *e. Understanding and following security policies and regulations*	Anggota staf mengikuti praktik keamanan yang baik, seperti: a. Mengamankan informasi yang menjadi tanggung jawab mereka b. Tidak membocorkan informasi sensitif kepada orang lain (resistensi terhadap rekayasa sosial) c. Memiliki kemampuan yang memadai untuk menggunakan perangkat keras dan perangkat lunak teknologi informasi d. Menggunakan praktik kata sandi yang baik e. Memahami dan mengikuti kebijakan dan peraturan keamanan	✓		

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
	f. Recognizing and reporting incidents	f. Mengenali dan melaporkan insiden			
5	*The organization's business strategy routinely incorporate security considerations.*	Strategi bisnis organisasi secara rutin memasukkan pertimbangan keamanan.	✓		
6	*Security strategies and policies take into consideration the organization's business strategies and goals.*	Strategi dan kebijakan keamanan mempertimbangkan strategi dan tujuan bisnis organisasi.	✓		
7	*Security strategies, goals, and objectives are documented and are routinely reviewed, updated, and communicated to the organization.*	Strategi, tujuan, dan sasaran keamanan didokumentasikan dan secara rutin ditinjau, diperbarui dan dikomunikasikan kepada organisasi.	✓		
8	*Management allocates sufficient funds and resources to information security activities.*	Manajemen mengalokasikan dana dan sumber daya yang cukup untuk kegiatan keamanan informasi.	✓		

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
9	*Security roles and responsibilities are defined for all staff in the organization.*	Peran dan tanggung jawab keamanan ditetapkan untuk semua staf dalam organisasi.	✓		
10	*All staff at all levels of responsibility implement their assigned roles and responsibility for information security.*	Semua staf di semua tingkat tanggung jawab melaksanakan peran dan tanggung jawab mereka untuk keamanan informasi.	✓		
11	*There are documented procedures for authorizing and overseeing all staff (including personnel from third party organizations) who work with sensitive information or who work in locations where the information resides.*	Terdapat prosedur terdokumentasi untuk mengesahkan dan mengawasi semua staf (termasuk personil dari organisasi pihak ketiga) yang bekerja dengan infrmasi sensitif atau bekerja di lokasi tempat informasi tersebut berada).			
12	*The organization's hiring and termination practices for staff*	Praktik perekrutan dan pemberhentian staf mempertimbangkan masalah keamanan informasi	✓		

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
	take information security issues into account.				
13	*The organization manages information security risks, Including* *a. Assessing risks to information security* *b. Taking steps to mitigate information security risks*	Organisasi mengelola risiko keamanan informasi, termasuk; a. Menilai risiko terhadap keamanan informasi b. Mengambil langkah-langkah untuk mengurangi risiko keamanan informasi	✓		
14	*Management receives and acts upon routine reports summarizing security-related information (e.g., audits, logs, risk and vulnerability assessments).*	Manajemen menerima dan menindaklanjuti laporan rutin yang merangkum informasi terkait keamanan (misalnya, audit, log,penilaian risiko dan kerentanan).	✓		
15	*The organization has a comprehensive set of*	Organisasi memiliki seperangkat kebijakan terdokumentasi yang	✓		

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
	documented, current policies that are periodically reviewed and updated.	komprehensif dan terkini yang ditinjau dan diperbarui secara berkala.			
16	*There us a documented process for management of security policies, including* *a. Creation* *b. Administration (including periodic reviews and updates)* *c. Communication*	Terdapat proses yang terdokumentasi untuk pengelolaan kebijakan keamanan termasuk a. Penciptaan b. Administrasi (termasuk tinjauan dan pembaruan berkala) c. Komunikasi	✓		
17	*The organization has a documented process for evaluating and ensuring compliance with information security policies, applicable laws and regulations, and insurance requirements.*	Organisasi memiliki proses yang terdokumentasi untuk mengevaluasi dan memastikan kepatuhan terhadap kebijakan keamanan informasi, hukum dan peraturan yang berlaku, dan persyaratan asuransi.	✓		

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
18	*The organization uniformly enforce its security policies.*	Organisasi secara kompak menerapkan kebijakan keamanannya.	✓		
19	*The organization has policies and procedures for protecting information when working with external organizations ((e.g., third parties, collaborators, subcontractors, or partners), including* *a. Protecting information belonging to other organizations* *b. Understanding the security policies and procedures of external organizations* *c. Ending access to information by*	Organisasi memiliki kebijakan dan prosedur untuk melindungi informasi ketika bekerja dengan organisasi eksternal (misalnya, pihak ketiga, kolaborator, subskontraktor, atau mitra), termasuk; a. Melindungi informasi milik organisasi lain b. Memahami kebijakan dan prosedur keamanan organisasi eksternal c. Mengakhiri akses ke informasi oleh personel eksternal yang diberhentikan	✓		

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
	terminated external personel				
20	*The organization documents information protection requirements and explicitly communicates them to all appropriate third parties.*	Organisasi mendokumentasikan persyaratan perlindungan informasi dan secara eksplisit mengkomunikasikannya kepada semua pihak ketiga yang sesuai.	✓		
21	*The organization has formal mechanisms for verifying that all third-party organizations, outsourced security services, mechanisms, and technologies meet its needs and requirements.*	Organisasi memiliki mekanisme formal untuk memverifikasi bahwa semua organisasi pihak ketiga, layanan keamanan yang dialihdayakan, mekanisme, dan teknologi memenuhi kebutuhan dan persyaratannya.	✓		
22	*The organization has policies and procedures for collaborating with all third-party organizations that*	Organisasi memiliki kebijakan dan prosedur untuk berkolaborasi dengan semua organisasi pihak ketiga a. Menyediakan layanan pelatihan dan kesadaran keamanan	✓		

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
	a. *Provide security awareness and training services* b. *develop security policies for the organization* c. *develop contingency plans for the organization*	b. Mengembangkah kebijakan keamanan untuk organisasi c. Mengembangkan rencana kontinjensi untuk organisasi	✓		
23	*An analysis of operations, applications, and data criticality has been performed.*	Analisis operasi, aplikasi, dan kekritisan data telah dilakukan.	✓		
24	*The organization has documented, reviewed, and tested* a. *Contingency plan(s) for responding to emergencies* b. *Disaster recovery plan(s)*	Organisasi telah mendokumentasikan, menunjau, dan menguji a. Rencana kontinjensi untuk menanggapi keadaan darurat b. Rencana pemulihan bencana c. Kelangsungan rencana operasi darurat	✓		

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
	c. *Business continuity or emergency operation plans.*				
25	*The contingency, disaster recovery, and business continuity plans consider physical and electronic access requirements and controls.*	Rencana kontinjensi, pemulihan bencana, dan kelangsungan operasi mempertimbangkan persyaratan dan control akses fisik dan elektronik.	✓		
26	*All staff are* a. *Aware of the contingency, disaster recovery, and business continuity plans* b. *understand and are able to carry out their responsibilities*	Semua staf adalah a. Mengetahui rencana kontinjensi, pemulihan bencana, dan kelangsungan operasional b. Memahami dan mampu melaksanakan tanggung jawab mereka.	✓		
27	*Facility security plans and procedures for safeguarding the*	Rencana dan prosedur keamanan fasilitas untuk melindungi tempat, bangunan, dan	✓		

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
	premises, buildings, and any restricted areas are documented and tested.	area terlarang didokumentasikan dan diuji.			
28	*There are documented policies and procedures for managing visitors.*	Terdapat kebijakan dan prosedur yang terdokumentasi untuk mengelola pengunjung.	✓		
29	*There are documented policies and procedures for controlling physical access to work areas and hardware (computers, communication devices, etc.) and software media.*	Terdapat kebijakan dan prosedur yang terdokumentasi untuk mengendalikan akses fisik ke area kerja dan perangkat keras (komputer, perangkat komunikasi, dll) dan media perangkat lunak.	✓		
30	*Workstations and other components that allow access to sensitive information are physically safeguarded to prevent unauthorized access.*	Lingkungan kerja dan komponen lain yang memungkinkan akses ke informasi sensitive dilindungi secara fisik untuk mencegah akses yang tidak sah.	✓		

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
31	*Maintenance records are kept to document the repairs and modifications of a facility's physical components.*	Catatan pemeliharaan disimpan untuk mendokumentasikan perbaikan dan modifikasi komponen fisik fasilitas.	✓		
32	*An individual's or group's actions, with respect to all physically controlled media, can be accounted for.*	Tindakan individu atau kelompok, sehubungan dengan semua media dikontrol secara fisik, dapat dipertanggungjawabkan.	✓		
33	*Audit and monitoring records are routinely examined for anomalies, and corrective action is taken as needed.*	Catatan audit dan pemantauan secara rutin diperiksa untuk mengetahui adanya animali, dan tindakan kolektif diambil sesuai kebutuhan.	✓		
34	*There are documented and tested security plan(s) for safeguarding the systems and networks.*	Ada rencana keamanan yang didokumentasi dan teruji untuk melindungi sistem dan jaringan.	✓		
35	*Sensitive information is protected by secure storage*	Informasi sensitif dilindungi oleh penyimpanan yang aman (missal,	✓		

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
	(e.g., backups stored off site, discard process for sensitive information).	cadangan disimpan diluar lokasi, proses pembuangan informasi sensitive).			
36	*The integrity of installed software is regularly verified.*	Integritas perangkat lunak yang terinstal diverifikasi secara teratur.	✓		
37	*All systems are up to date with respect to revisions, patches, and recommendations in security advisories.*	Semua sistem selalu diperbarui sehubunga dengan revisi, tambalan, dan rekomendasi dalam saran keamanan.	✓		
38	*There is a documented and tested data backup plan for backups of both software and data. All staff understand their responsibilities under the backup plans.*	Ada rencana pencadangan data yang terdokumentasi dan teruji untuk pencadangan perangkat lunak dan data. Semua staf memahami tanggung jawab mereka di bawah rencana pencadangan.	✓		
39	*Changes to IT hardware and software are planned, controlled, and documented.*	Perubahan pada perangkat keras dan perangkat lunakTI direncanakan, dikontrol, dan didokumentasikan.	✓		

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
40	*IT staff members follow procedures when issuing, changing, and terminating users' passwords, accounts, and privileges.* a. *Unique user identification is required for all information system users, including third party users* b. *Default accounts and default passwords have been removed from systems.*	Anggota staf TI mengikuti prosedur saat menerbitkan, mengubah, dan mengehentikan kata sandi, akun, dan hak istimewa pengguna. a. Identifikasi pengguna yang unik diperlukan untuk semua pengguna sistem informasi, termasuk pengguna pihak ketiga. b. Aku defaukt dan kata sandi default telah dihapus dari sistem.	✓		
41	*Only necessary services are running on systems – all unnecessary services have been removed.*	Hanya layanan yang diperlukan yang berjalan pada sistem-semua layanan yang tidak perlu dihapus.	✓		

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
42	*Tools and mechanisms for secure system and network administration are used, and are routinely reviewed and updated or replaced.*	Alat dan mekanisme untuk administrasi sistem dan jaringan yang aman digunakan, dan secara rutin ditinjau dan diperbarui atau diganti.	✓		
43	*System and network monitoring and auditing tools are routinely used by the organization. Unusual activity is dealt with according to the appropriate policy or procedure.*	Alat-alat pemantauan dan audit sistem dan jaringan secara rutin digunakan oleh organisasi. Aktivitas yang tidak biasa ditangani sesuai dengan kebijakan atau prosedur yang berlaku.	✓		
44	*Firewall and other security components are periodically audited for compliance with policy.*	Firewall dan komponen keamanan lainnya diaudit secara berkala untuk memastikan kepatuhan terhadap kebijakan.	✓		
45	*Appropriate access controls and user authentication (e.g., file permissions, network*	Kontrol akses yang tepat dan autentikasi pengguna (misalnya, izin file, konfigurasi jaringan) yang sesuai dengan kebijakan	✓		

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
	configuration) consistent with policy are used to restrict user access to information, sensitive systems, specific applications and services, and network connections.	digunakan untuk membatasi akses pengguna ke informasi, sistem yang sensitif, aplikasi dan layanan tertentu, dan koneksi jaringan.			
46	*There are documented policies and procedures to establish and terminate the right of access to information for both individuals and groups.*	Terdapat kebijakan dan prosedur yang terdokumentasi untuk menetapkan dan mengakhiri hak akses terhadap informasi baik untuk individu maupun kelompok.	✓		
47	*Methods or mechanisms are provided to ensure that sensitive information has not been accessed, altered, or destroyed in an unauthorized manner. Methods or mechanisms are*	Metode atau mekanisme disediakan untuk memastikan bahwa informasi sensitif tidak diakses, diubah, atau dihancurkan dengan cara yang tidak sah. Metode atau mekanisme ditinjau dan diverifikasi secara berkala.	✓		

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
	periodically reviewed and verified.				
48	*There is a documented set of procedures for managing vulnerabilities, including* a. *Selecting vulnerability evaluation tools, checklists, and scripts* b. *Keeping up to date with known vulnerability types and attack methods* c. *Reviewing sources of information on vulnerability announcements, security alerts, and notices*	Terdapat serangkaian prosedur terdokumentasi untuk mengelola kerentanan, termasuk a. Memilih alat evaluasi terentanan, data periksa, dan skrip. b. Selalu mengikuti perkembangan jenis kerentanan dan metode serangan yang diketahui. c. Meninjau sumber informasi tentang pengumuman kerentanan, peringatan keamanan, dan permberitahuan. d. Mengidentifikasi komponen infrastruktur yang akan dievaluasi e. Penjadwalan evaluasi kerentanan.	✓		

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
	d. *Identifying infrastructure components to be evaluated* e. *Scheduling of vulnerability evaluations* f. *Interpreting and responding to the evaluation results* g. *Maintaining secure storage and disposition of vulnerability data*	f. Menafsirkan dan menganggapi hasil evaluasi. g. Menjaga penyimpanan dan disposisi data kerentanan yang aman.	✓		
49	*Vulnerability management procedures are followed and are periodically reviewed and updated.*	Prosedur manajemen kerentanan diikuti dan ditinjau serta diperbarui secara berkala.	✓		
50	*Technology vulnerability assessments are performed on a periodic basis, and*	Penilaian kerentanan teknologi dilakukan secara berkala, dan kerentanan diatasi ketika teridentifikasi.	✓		

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
	vulnerabilities are addressed when they are identified.				
51	*Appropriate security controls are used to protect sensitive information while in storage and during transmission (e.g., data encryption, public key infrastructure, virtual private network technology).*	Kontrol keamanan yang tepat digunakan untuk melindungi informasi sensitif saat berada dalam penyimpanan dan selama transmisi (misalnya, enkripsi data, infrastruktur kunci public, teknologi jaringan pribadi virtual).	✓		
52	*Encrypted protocols are used when remotely managing systems, routers, and firewalls.*	Protokol terenkripsi digunakan ketika mengelola sistem, router, dan firewall dari jarak jauh.	✓		
53	*System architecture and design for new and revised systems include considerations for* a. *Security strategies, policies, and procedures*	Arsitektur dan desain sistem untuk sistem baru dan sistem yang direvisi mencakup pertimbangan untuk: a. Strategi, kebijakan, dan prosedur keamanan b. Riwayat kompromi keamanan	✓		

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
	b. *History of security compromises* c. *Results of security risk assessments*	c. Hasil penilaian risiko keamanan	✓		
54	*The organization has up-to-date diagrams that show the enterprise-wide security architecture and network topology.*	Organisasi memiliki diagram terkini yang menunjukkan arsitektur keamanan di seluruh perusahaan topologi jaringan.	✓		
55	*Documented procedures exist for identifying, reporting, and responding to suspected security incidents and violations.*	Terdapat prosedur yang terdokumentasi untuk mengidentifikasi, melaporkan, dan menanggapi dugaan insiden dan pelanggaran keamanan.	✓		
56	*Incident management procedures are periodically tested, verified, and updated.*	Prosedur manajemen insiden diuji, diverifikasi, dan diperbarui secara berkala.	✓		

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
57	*There are documented policies and procedures for working with law enforcement agencies.*	Terdapat kebijakan dan prosedur yang terdokumentasi untuk bekerja dama dengan lembaga penegak hukum.	✓		

4. Lembar Kerja Pemilihan Aset Kritis

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERTANYAAN	PENGERTIAN	R	TR	
1	*Which assets would have a large adverse impact on the organization if* *a. They are disclosed to unauthorized people?* *b. They are modified without authorization?* *c. They are lost destroyed?*	Aset mana yang akan memiliki dampak buruk yang besar pada organisasi jika a. Informasi tersebut dibocorkan kepada pihak yang tidak berwenang? b. Informasi tersebut diubah tanpa otorsasi?	✓		

	d. Access to them is interrupted?	c. Informasi tersebut hilang atau hancur? d. Akses terhadap informasi tersebut terputus?			

5. Lembar Kerja Informasi Aset Kritis Untuk Informasi, Sistem, Aplikasi, dan Orang

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERTANYAAN	PENGERTIAN	R	TR	
1	*What is the critical Information, system, application, and people?*	Apa informasi, sistem, aplikasi, dan orang yang kritis?	✓		
2	*Why is this information, system, application, and people critical to the organization?*	Mengapa informasi, sistem, aplikasi, dan orang penting bagi organisasi?	✓		
3	*Which assets are related to this information, syetem, application, and people?* *a. Information* *b. System* *c. Application*	Aset apa saja yang terkait dengan informasi, sistem, aplikasi, dan orang? a. Informasi b. Sistem c. Aplikasi d. Orang	✓		

	d. Other	e. Lainnya			
4	*What are the security requirements for this information? (Hint: Focus on what the security requirements should be for this information,system, application, and people, not what they currently are).* *a. Confidentiality (Only authorized personnel can view...)* *b. Integrity (Only authorized personnel can modify ...)* *c. Availability (... must be available for personnel to perform their jobs. Unavailability cannot exceed ... hour(s) per every ... hours.* *d. Other*	Apa kebutuhan untuk informasi ini? (Petunjuk: Fokus pada persyaratan keamanan yang seharusnya untuk informasi, sistem, aplikasi, dan orang ini, bukan yang ada pada persyaratan keamanan saat ini). a. Kerahasiaan (hanya personel yang berwenang yang dapat melihat ...) b. Integritas (hanya personel yang berwenang yang dapat memodifikasi ...) c. Ketersediaan (... harus tersedia bagi personel untuk melakukan pekerjaannya. Ketidaktersediaan tidak boleh melebihi ... jam per setiap ... jam. d. Lainnya	✓		

5	*Which security requirement is most important for this information, system, application, and people?* *a. Confidentiality* *b. Integrity* *c. Avalilability* *d. Other*	Persyaratan keamanan manakah yang paling penting untuk informasi, sistem, aplikasi, dan orang ini? a. Kerahasiaan b. Integritas c. Ketersediaan d. Lainnya	✓		

Keterangan:

1. R: Relevan
2. TR: Tidak Relevan

Lampiran 6. Hasil Uji Kebahasaan Penguji Ahli 2

HASIL UJI KEBAHASAAN OLEH AHLI
DALAM RANGKA PENELITIAN ANALISIS MANAJEMEN RISIKO KEAMANAN INFORMASI MENGGUNAKAN OCTAVE-S DAN ISO 27001:2022 PADA UNIT PENUNJANG AKADEMIK TEKNOLOGI INFORMASI DAN KOMUNIKASI (UPA TIK) UNIVERSITAS PENDIDIKAN GANESHA.

Penguji Ahli

Nama	:	Ni Luh Dewi Sintiari, S.Pd., M.Sc., Ph.D.
Instansi	:	Universitas Pendidikan Ganesha
Jabatan	:	Tenaga Pengajar – Program Studi Ilmu Komputer
NIP	:	199205082024062002

Hasil Uji:

1.

Singaraja, 29 Agustus 2024

Penguji Ahli,

Ni Luh Dewi Sintiari, S.Pd., M.Sc., Ph.D.
NIP. 199205082024062002

Peneliti,

Hardiyanti Rohmania
NIM. 2015091018

1. Lembar Kerja Kriteria Evaluasi Dampak

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	NILAI DAMPAK	PENGERTIAN	R	TR	
1	*Reputation*	Reputasi/Kepercayaan	✓		
2	*Financial*	Keuangan	✓		
3	*Productivity*	Produktifitas	✓		
4	*Savety/Health*	Keamanan/~~Keselamatan~~ kesehatan		✓	

2. Lembar Kerja Identifikasi Aset

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERTANYAAN	PENGERTIAN	R	TR	
1	*What system do people in your organization need to perform their jobs?*	Sistem apa yang dibutuhkan oleh orang-orang dalam organisasi Anda untuk menjalankan tugas mereka?	✓		
2	*What information do people in your organization need to perform their jobs?*	Informasi apa yang dibutuhkan oleh orang-orang ~~di~~ dalam organisasi Anda untuk melakukan pekerjaan mereka?	✓		

3	***What application dan services do people in your organization need to perform their jobs?***	Aplikasi dan layanan apa yang dibutuhkan oleh orang-orang ~~di~~ dalam organisasi Anda untuk melaksanakan pekerjaan mereka?	✓		
4	***What other assets are closely related to these assets?***	Aset-aset lain apa yang terkait erat dengan asset ini?	✓		
5	***Which people have a special skill or knowledge that is vital to your organization and would be difficult to replace?***	Siapa saja orang-orang yang memiliki keterampilan atau pengetahuan khusus yang sangat penting bagi organisasi Anda dan sulit untuk digantikan?	✓		
6	***What are their special skills or knowledge?***	Apa keahlian atau pengetahuan khusus yang mereka miliki?	✓		
7	***Which system do these people use?***	Sistem apa yang digunakan oleh orang-orang ini?	✓		
8	***Which other assets do these people use? (i.e., information, services, and applications).***	Aset ~~apa saja lainnya~~ lain apa saja yang digunakan oleh orang-orang ini? (misalnya, informasi, layanan, dan aplikasi).	✓		

3. Lembar Kerja Praktik Keamanan

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
1	*Saff members understand their security roles and responsinilities. This is documented and verified.*	Anggota staf memahami peran dan tanggung jawab keamanan mereka. Hal ini didokumentasikan dan diverifikasi.	✓		
2	*There is adequate in-house expertise for all supported service, mechanism, and technologies (e.g., logging, monitoring, or encryption), including their secure operation. This is documented and verified.*	Terdapat keahlian internal yang memadai untuk semua layanan, dan teknologi yang didukung (misalnya, pencatatan, pemantauan, atau enkripsi), termasuk operasi yang aman. Hal ini didokumentasikan dan diverifikasi.	✓		
3	*Security awareness, training, and periodic reminders are provided for all personnel. Staff understanding is documented and conformance is periodically verified.*	Kesadaran akan keamanan, pelatihan, dan pengingat berkala disediakan untuk semua personel. Pemahaman staf didokumentasikan dan kesesuaiannya diverifikasi secara berkala.	✓		

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
4	*Staff members follow good security practice, such as:* *a. Securing information for which they are responsible* *b. Not divulging sensitive information to others (resistance to social engineering)* *c. Having adequate ability to use information technology hardware and software* *d. Using good password practice* *e. Understanding and following security policies and regulations*	Anggota staf mengikuti praktik keamanan yang baik, seperti: a. Mengamankan informasi yang menjadi tanggung jawab mereka b. Tidak membocorkan informasi sensitif kepada orang lain (resistensi terhadap rekayasa sosial) c. Memiliki kemampuan yang memadai untuk menggunakan perangkat keras dan perangkat lunak teknologi informasi d. Menggunakan ~~praktik~~ kata sandi yang baik e. Memahami dan mengikuti kebijakan dan peraturan keamanan	✓		

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
	f. Recognizing and reporting incidents	f. Mengenali dan melaporkan insiden			
5	***The organization's business strategy routinely incorporate security considerations.***	Strategi bisnis organisasi secara rutin memasukkan pertimbangan keamanan.	✓		
6	***Security strategies and policies take into consideration the organization's business strategies and goals.***	Strategi dan kebijakan keamanan mempertimbangkan strategi dan tujuan bisnis organisasi.	✓		
7	***Security strategies, goals, and objectives are documented and are routinely reviewed, updated, and communicated to the organization.***	Strategi, tujuan, dan sasaran keamanan didokumentasikan dan secara rutin ditinjau, diperbarui dan dikomunikasikan kepada organisasi.	✓		
8	***Management allocates sufficient funds and resources to information security activities.***	Manajemen mengalokasikan dana dan sumber daya yang cukup untuk kegiatan keamanan informasi.	✓		

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
9	*Security roles and responsibilities are defined for all staff in the organization.*	Peran dan tanggung jawab keamanan ditetapkan untuk semua staf dalam organisasi.	✓		
10	*All staff at all levels of responsibility implement their assigned roles and responsibility for information security.*	Semua staf di semua tingkat tanggung jawab melaksanakan peran dan tanggung jawab mereka untuk keamanan informasi.	✓		
11	*There are documented procedures for authorizing and overseeing all staff (including personnel from third party organizations) who work with sensitive information or who work in locations where the information resides.*	Terdapat prosedur terdokumentasi untuk mengesahkan dan mengawasi semua staf (termasuk personil dari organisasi pihak ketiga) yang bekerja dengan ~~infrmasi~~ informasi sensitif atau bekerja di lokasi tempat informasi tersebut berada).		✓	
12	*The organization's hiring and termination practices for staff*	Praktik perekrutan dan pemberhentian staf mempertimbangkan masalah keamanan informasi	✓		

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
	take information security issues into account.				
13	*The organization manages information security risks, Including* *a. Assessing risks to information security* *b. Taking steps to mitigate information security risks*	Organisasi mengelola risiko keamanan informasi, termasuk: a. Menilai risiko terhadap keamanan informasi b. Mengambil langkah-langkah untuk mengurangi risiko keamanan informasi	✓		
14	*Management receives and acts upon routine reports summarizing security-related information (e.g., audits, logs, risk and vulnerability assessments).*	Manajemen menerima dan menindaklanjuti laporan rutin yang merangkum informasi terkait keamanan (misalnya, audit, log, penilaian risiko dan kerentanan). Tambah ISMS	✓		
15	*The organization has a comprehensive set of*	Organisasi memiliki seperangkat kebijakan terdokumentasi yang	✓		

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
	documented, current policies that are periodically reviewed and updated.	komprehensif dan terkini yang ditinjau dan diperbarui secara berkala.			
16	*There us a documented process for management of security policies, including* *a. Creation* *b. Administration (including periodic reviews and updates)* *c. Communication*	Terdapat proses yang terdokumentasi untuk pengelolaan kebijakan keamanan termasuk a. Penciptaan b. Administrasi (termasuk tinjauan dan pembaruan berkala) c. Komunikasi	✓		
17	*The organization has a documented process for evaluating and ensuring compliance with information security policies, applicable laws and regulations, and insurance requirements.*	Organisasi memiliki proses yang terdokumentasi untuk mengevaluasi dan memastikan kepatuhan terhadap kebijakan keamanan informasi, hukum dan peraturan yang berlaku, dan persyaratan asuransi.	✓		

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
18	*The organization uniformly enforce its security policies.*	Organisasi secara kompak menerapkan kebijakan keamanannya.		✓	
19	*The organization has policies and procedures for protecting information when working with external organizations ((e.g., third parties, collaborators, subcontractors, or partners), including* *a. Protecting information belonging to other organizations* *b. Understanding the security policies and procedures of external organizations* *c. Ending access to information by*	Organisasi memiliki kebijakan dan prosedur untuk melindungi informasi ketika bekerja dengan organisasi eksternal (misalnya, pihak ketiga, kolaborator, subskontraktor, atau mitra), termasuk: a. Melindungi informasi milik organisasi lain b. Memahami kebijakan dan prosedur keamanan organisasi eksternal c. Mengakhiri akses ke informasi oleh personel eksternal yang diberhentikan		✓	Bagian (c) perlu ditambah.

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
	terminated external personel				
20	*The organization documents information protection requirements and explicitly communicates them to all appropriate third parties.*	Organisasi mendokumentasikan persyaratan perlindungan informasi dan secara eksplisit mengkomunikasikannya kepada semua pihak ketiga yang sesuai.	✓		
21	*The organization has formal mechanisms for verifying that all third-party organizations, outsourced security services, mechanisms, and technologies meet its needs and requirements.*	Organisasi memiliki mekanisme formal untuk memverifikasi bahwa semua organisasi pihak ketiga, layanan keamanan yang dialihdayakan, mekanisme, dan teknologi memenuhi kebutuhan dan persyaratannya.	✓		
22	*The organization has policies and procedures for collaborating with all third-party organizations that*	Organisasi memiliki kebijakan dan prosedur untuk berkolaborasi dengan semua organisasi pihak ketiga a. Menyediakan layanan pelatihan dan kesadaran keamanan	✓		

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
	a. *Provide security awareness and training services* b. *develop security policies for the organization* c. *develop contingency plans for the organization*	b. Mengembangkan kebijakan keamanan untuk organisasi c. Mengembangkan rencana kontinjensi untuk organisasi			
23	*An analysis of operations, applications, and data criticality has been performed.*	Analisis operasi, aplikasi, dan kekritisan data telah dilakukan.	✓		
24	*The organization has documented, reviewed, and tested* a. *Contingency plan(s) for responding to emergencies* b. *Disaster recovery plan(s)*	Organisasi telah mendokumentasikan, menunjau, dan menguji a. Rencana kontinjensi untuk menanggapi keadaan darurat b. Rencana pemulihan bencana c. Kelangsungan rencana operasi darurat	✓		

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
	c. *Business continuity or emergency operation plans.*				
25	*The contingency, disaster recovery, and business continuity plans consider physical and electronic access requirements and controls.*	Rencana kontinjensi, pemulihan bencana, dan kelangsungan operasi mempertimbangkan persyaratan dan control akses fisik dan elektronik.	✓		
26	*All staff are* *a. Aware of the contingency, disaster recovery, and business continuity plans* *b. understand and are able to carry out their responsibilities*	Semua staf ~~adalah~~ (semuanya) a. Mengetahui rencana kontinjensi, pemulihan bencana, dan kelangsungan operasional b. Memahami dan mampu melaksanakan tanggung jawab mereka.	✓		Sesuaikan revisi yg maksud pernyataan.
27	*Facility security plans and procedures for safeguarding the*	Rencana dan prosedur keamanan fasilitas untuk melindungi tempat, bangunan, dan			

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
	premises, buildings, and any restricted areas are documented and tested.	area terlarang didokumentasikan dan diuji.			
28	*There are documented policies and procedures for managing visitors.*	Terdapat kebijakan dan prosedur yang terdokumentasi untuk mengelola pengunjung.	✓		
29	*There are documented policies and procedures for controlling physical access to work areas and hardware (computers, communication devices, etc.) and software media.*	Terdapat kebijakan dan prosedur yang terdokumentasi untuk mengendalikan akses fisik ke area kerja dan perangkat keras (komputer, perangkat komunikasi, dll) dan media perangkat lunak.	✓		
30	*Workstations and other components that allow access to sensitive information are physically safeguarded to prevent unauthorized access.*	Lingkungan kerja dan komponen lain yang memungkinkan akses ke informasi sensitive dilindungi secara fisik untuk mencegah akses yang tidak sah.	✓		

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
31	*Maintenance records are kept to document the repairs and modifications of a facility's physical components.*	Catatan pemeliharaan disimpan untuk mendokumentasikan perbaikan dan modifikasi komponen fisik fasilitas.	✓		
32	*An individual's or group's actions, with respect to all physically controlled media, can be accounted for.*	Tindakan individu atau kelompok, sehubungan dengan semua media dikontrol secara fisik, dapat dipertanggungjawabkan.	✓		
33	*Audit and monitoring records are routinely examined for anomalies, and corrective action is taken as needed.*	Catatan audit dan pemantauan secara rutin diperiksa untuk mengetahui adanya ~~animalj~~ anomali, dan tindakan kolektif diambil sesuai kebutuhan.	✓		
34	*There are documented and tested security plan(s) for safeguarding the systems and networks.*	Ada rencana keamanan yang ~~did~~ terdokumentasi dan teruji untuk melindungi sistem dan jaringan.	✓		
35	*Sensitive information is protected by secure storage*	Informasi sensitif dilindungi oleh penyimpanan yang aman (~~misal~~ misalnya,	✓		

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
	(e.g., backups stored off site, discard process for sensitive information).	cadangan disimpan di luar lokasi, proses pembuangan informasi sensitif).			
36	*The integrity of installed software is regularly verified.*	Integritas perangkat lunak yang terinstal diverifikasi secara teratur.	✓		
37	*All systems are up to date with respect to revisions, patches, and recommendations in security advisories.*	Semua sistem selalu diperbarui sehubungan dengan revisi, pembaruan, dan rekomendasi dalam saran keamanan.	✓		
38	*There is a documented and tested data backup plan for backups of both software and data. All staff understand their responsibilities under the backup plans.*	Ada rencana pencadangan data yang terdokumentasi dan teruji untuk pencadangan perangkat lunak dan data. Semua staf memahami tanggung jawab mereka di bawah rencana pencadangan.	✓		
39	*Changes to IT hardware and software are planned, controlled, and documented.*	Perubahan pada perangkat keras dan perangkat lunak TI direncanakan, dikontrol, dan didokumentasikan.	✓		

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
40	*IT staff members follow procedures when issuing, changing, and terminating users' passwords, accounts, and privileges.* a. *Unique user identification is required for all information system users, including third party users* b. *Default accounts and default passwords have been removed from systems.*	Anggota staf TI mengikuti prosedur saat menerbitkan, mengubah, dan menghentikan kata sandi, akun, dan hak istimewa pengguna. a. Identifikasi pengguna yang unik diperlukan untuk semua pengguna sistem informasi, termasuk pengguna pihak ketiga. b. ~~Aku defau~~kt dan kata sandi ~~default~~ telah dihapus dari sistem. Akun bawaan dan kata sandi bawaan	✓		
41	*Only necessary services are running on systems – all unnecessary services have been removed.*	Hanya layanan yang diperlukan yang ~~berjalan~~ dijalankan pada sistem-semua layanan yang tidak perlu dihapus. Saja	✓		

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
42	*Tools and mechanisms for secure system and network administration are used, and are routinely reviewed and updated or replaced.*	Alat dan mekanisme untuk administrasi sistem dan jaringan yang aman digunakan, dan secara rutin ditinjau dan diperbarui atau diganti.	✓		
43	*System and network monitoring and auditing tools are routinely used by the organization. Unusual activity is dealt with according to the appropriate policy or procedure.*	Alat-alat pemantauan dan audit sistem dan jaringan secara rutin digunakan oleh organisasi. Aktivitas yang tidak biasa ditangani sesuai dengan kebijakan atau prosedur yang berlaku. Cek mining	✓		
44	*Firewall and other security components are periodically audited for compliance with policy.*	Firewall dan komponen keamanan lainnya diaudit secara berkala untuk memastikan kepatuhan terhadap kebijakan.	✓		
45	*Appropriate access controls and user authentication (e.g., file permissions, network*	Kontrol akses yang tepat dan autentikasi pengguna (misalnya, izin file, konfigurasi jaringan) yang sesuai dengan kebijakan	✓		

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
	configuration) consistent with policy are used to restrict user access to information, sensitive systems, specific applications and services, and network connections.	digunakan untuk membatasi akses pengguna ke informasi, sistem yang sensitif, aplikasi dan layanan tertentu, dan koneksi jaringan.			
46	*There are documented policies and procedures to establish and terminate the right of access to information for both individuals and groups.*	Terdapat kebijakan dan prosedur yang terdokumentasi untuk menetapkan dan mengakhiri hak akses terhadap informasi, ~~baik untuk~~ Individu maupun kelompok.	✓		
47	*Methods or mechanisms are provided to ensure that sensitive information has not been accessed, altered, or destroyed in an unauthorized manner. Methods or mechanisms are*	Metode atau mekanisme disediakan untuk memastikan bahwa informasi sensitif tidak diakses, diubah, atau dihancurkan dengan cara yang tidak sah. Metode atau mekanisme ditinjau dan diverifikasi secara berkala.	✓		

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
	periodically reviewed and verified.				
48	*There is a documented set of procedures for managing vulnerabilities, including* a. *Selecting vulnerability evaluation tools, checklists, and scripts* b. *Keeping up to date with known vulnerability types and attack methods* c. *Reviewing sources of information on vulnerability announcements, security alerts, and notices*	Terdapat serangkaian prosedur terdokumentasi untuk mengelola kerentanan, termasuk a. Memilih alat evaluasi terentanan, data periksa, dan skrip. b. Selalu mengikuti perkembangan jenis kerentanan dan metode serangan yang diketahui. c. Meninjau sumber informasi tentang pengumuman kerentanan, peringatan keamanan, dan permberitahuan. d. Mengidentifikasi komponen infrastruktur yang akan dievaluasi. e. Penjadwalan evaluasi kerentanan.	✓		185 titik semua atau hapus semua

untuk

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
	d. *Identifying infrastructure components to be evaluated* e. *Scheduling of vulnerability evaluations* f. *Interpreting and responding to the evaluation results* g. *Maintaining secure storage and disposition of vulnerability data*	f. Menafsirkan dan menganggapi hasil evaluasi. g. Menjaga penyimpanan dan disposisi data kerentanan yang aman.			
49	*Vulnerability management procedures are followed and are periodically reviewed and updated.*	Prosedur manajemen kerentanan diikuti dan ditinjau serta diperbarui secara berkala.	✓		
50	*Technology vulnerability assessments are performed on a periodic basis, and*	Penilaian kerentanan teknologi dilakukan secara berkala, dan kerentanan diatasi ketika teridentifikasi.	✓		

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
	vulnerabilities are addressed when they are identified.				
51	*Appropriate security controls are used to protect sensitive information while in storage and during transmission (e.g., data encryption, public key infrastructure, virtual private network technology).*	Kontrol keamanan yang tepat digunakan untuk melindungi informasi sensitif saat berada dalam penyimpanan dan selama transmisi (misalnya, enkripsi data, infrastruktur kunci publik, teknologi jaringan pribadi virtual).	✓		
52	*Encrypted protocols are used when remotely managing systems, routers, and firewalls.*	Protokol terenkripsi digunakan ketika mengelola sistem, router, dan firewall dari jarak jauh. miring	✓		
53	*System architecture and design for new and revised systems include considerations for* a. *Security strategies, policies, and procedures*	Arsitektur dan desain sistem untuk sistem baru dan sistem yang direvisi mencakup pertimbangan untuk: a. Strategi, kebijakan, dan prosedur keamanan b. Riwayat kompromi keamanan	✓		

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
	b. *History of security compromises* c. *Results of security risk assessments*	c. Hasil penilaian risiko keamanan			
54	*The organization has up-to-date diagrams that show the enterprise-wide security architecture and network topology.*	Organisasi memiliki diagram terkini yang menunjukkan arsitektur keamanan di seluruh perusahaan topologi jaringan.	✓		
55	*Documented procedures exist for identifying, reporting, and responding to suspected security incidents and violations.*	Terdapat prosedur yang terdokumentasi untuk mengidentifikasi, melaporkan, dan menanggapi dugaan insiden dan pelanggaran keamanan.	✓		
56	*Incident management procedures are periodically tested, verified, and updated.*	Prosedur manajemen insiden diuji, diverifikasi, dan diperbarui secara berkala.	✓		

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERNYATAAN	PENGERTIAN	R	TR	
57	*There are documented policies and procedures for working with law enforcement agencies.*	Terdapat kebijakan dan prosedur yang terdokumentasi untuk bekerja dama dengan lembaga penegak hukum.	✓		

4. Lembar Kerja Pemilihan Aset Kritis

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERTANYAAN	PENGERTIAN	R	TR	
1	*Which assets would have a large adverse impact on the organization if* *a. They are disclosed to unauthorized people?* *b. They are modified without authorization?* *c. They are lost destroyed?*	Aset mana yang akan memiliki dampak buruk yang besar pada organisasi jika a. Informasi tersebut dibocorkan kepada pihak yang tidak berwenang? b. Informasi tersebut diubah tanpa ~~otersasi~~? Otorisasi	✓		

	d. Access to them is interrupted?	c. Informasi tersebut hilang atau hancur? d. Akses terhadap informasi tersebut terputus?			

5. Lembar Kerja Informasi Aset Kritis Untuk Informasi, Sistem, Aplikasi, dan Orang

NO	ASPEK YANG DIUJI		BUTIR PENILAIAN		SARAN
	PERTANYAAN	PENGERTIAN	R	TR	
1	*What is the critical Information, system, application, and people?*	Apa informasi, sistem, aplikasi, dan orang yang kritis?		✓	Apakah arti dari informasi kritis, sistem, aplikasi, dan orang?
2	*Why is this information, system, application, and people critical to the organization?*	Mengapa informasi, sistem, aplikasi, dan orang penting bagi organisasi?	✓		
3	*Which assets are related to this information, syetem, application, and people?* *a. Information* *b. System* *c. Application*	Aset apa saja yang terkait dengan informasi, sistem, aplikasi, dan orang? a. Informasi b. Sistem c. Aplikasi d. Orang	✓		

R human / people

	d. Other	e. Lainnya			
4	***What are the security requirements for this information? (Hint: Focus on what the security requirements should be for this information,system, application, and people, not what they currently are).*** ***a. Confidentiality (Only authorized personnel can view...)*** ***b. Integrity (Only authorized personnel can modify ...)*** ***c. Availability (...must be available for personnel to perform their jobs. Unavailability cannot exceed ... hour(s) per every ... hours.*** ***d. Other***	Apa kebutuhan untuk informasi ini? (Petunjuk: Fokus pada persyaratan keamanan yang seharusnya untuk informasi, sistem, aplikasi, dan orang ini, bukan yang ada pada persyaratan keamanan saat ini). a. Kerahasiaan (hanya personil yang berwenang yang dapat melihat ...) b. Integritas (hanya personil yang berwenang yang dapat memodifikasi ...) c. Ketersediaan (... harus tersedia bagi personil untuk melakukan pekerjaannya. Ketidaktersediaan tidak boleh melebihi ... jam per setiap ... jam. d. Lainnya	✓		Apa saya kebutuhan keamanan untuk informasi ini.

5	***Which security requirement is most important for this information, system, application, and people?*** ***a. Confidentiality*** ***b. Integrity*** ***c. Avalilability*** ***d. Other***	Persyaratan keamanan manakah yang paling penting untuk informasi, sistem, aplikasi, dan orang ini? a. Kerahasiaan b. Integritas c. Ketersediaan d. Lainnya	✓		

Keterangan:

1. **R: Relevan**
2. **TR: Tidak Relevan**

Lampiran 7. Rancangan Pertanyaan Kuesioner Tahap Ke-1

1. Lembar Kerja Kriteria Evaluasi Dampak

No	Kriteria	Pertanyaan	Plihan Jawaban			Narasumber
			Dampak Rendah	Dampak Sedang	Dampak Tinggi	
1.	Reputasi	Jika terjadi insiden pada aset kritis yang dimiliki UPA TIK, apakah hal itu bisa memengaruhi reputasi UPA TIK?	Tidak terlalu berpengaruh.	Ada sedikit dampaknya, tapi masih bisa diperbaiki.	Pengaruhnya besar dan sulit memulihkan reputasi organisasi.	Sekretaris UPA TIK Undiksha.
	Kehilangan Aset	Jika aset kritis hilang atau tidak tersedia, apa dampaknya pada pekerjaan?	Pekerjaan tetap bisa berjalan seperti biasa.	Ada sedikit gangguan, tapi masih bisa disiasati.	Pekerjaan akan sangat terganggu dan sulit dilanjutkan.	
2.	Keuangan	Jika terjadi insiden pada aset kritis, bagaimana dampaknya pada biaya operasional perusahaan?	Tidak ada peningkatan biaya, semuanya tetap normal.	Ada sedikit peningkatan biaya, tapi masih bisa ditangani.	Biaya naik cukup banyak, UPA TIK Undiksha harus melakukan penyesuaian besar.	
3.	Produktivitas	Jika terjadi insiden pasa aset kritis, apakah memengaruhi pekerjaan sehari-hari?	Pekerjaan tetap berjalan seperti biasa.	Ada beberapa gangguan, tapi pekerjaan masih bisa diselesaikan.	Pekerjaan sangat terganggu dan banyak yang tidak bisa dilakukan.	
4.	Kesehatan/ Keselamatan Pegawai	Jika terjadi suatu masalah peralatan atau sistem jaringan yang Anda tangani, bagaimana dampaknya terhadap kesehatan atau keselamatan?	Tidak ada risiko kesehatan atau keselamatan.	Ada beberapa risiko, tapi bisa diatasi dengan penanganan medis sederhana.	Risiko serius yang dapat mengancam kesehatan atau keselamatan pegawai.	

2. Lembar Kerja Identifikasi Aset

No	Kategori	Pertanyaan	Jawaban	Narasumber
Tabel 1				
1.	Sistem	Sistem apa yang dibutuhkan oleh staf UPA TIK Undiksha dalam menjalankan tugasnya? (pringkat keras, perangkat lunak, jaringan dan komunikasi)		Sekretaris UPA TIK.
2.	Informasi	Informasi apa yang dibutuhkan orang –orang di UPA TIK untuk melakukan tugas mereka? (data)		
3.	Aplikasi	Aplikasi apa yang digunakan oleh UPA TIK untuk mendukung aset penting di UPA TIK?		
4.	Aset Lainnya	Aset lain apa yang berhubungan dengan aset penting?		
Tabel 2				
5.	Sumber Daya Manusia	Siapa staf/divisi kunci yang berperan penting dalam menjaga aset tersebut?		
6.	Keterampilan	Apa keahlian atau pengetahuan khusus yang dimiliki staf ini?		
7.	Sistem Terkait	Sistem apa yang digunakan oleh staf/divisi ini untuk bekerja?		

8.	Aset Terkait	Aset apa saja yang digunakan oleh staf/divisi ini dalam pekerjaannya?		

3. Lembar Kerja Evaluasi Praktik Keamanan

No	Praktik Keamanan	Pertanyaan	Pilihan Jawaban				Narasumber
			Sangat Banyak	Agak	Tidak Sama Sekali	Tidak Tahu	
1.	**Kesadaran dan Pelatihan Keamanan**	**Tabel 1**					
		Seberapa baik staf di UPA TIK memahami peran dan tanggung jawab mereka terkait keamanan? Hal ini didokumentasikan dan diverifikasi.	Sangat Baik	Cukup Baik	Tidak Baik	Tidak Tahu	Divisi Infrastruktur, Jaringan, & Keamanan.
		Seberapa baik layanan, mekanisme, dan teknologi yang digunakan di UPA TIK didokumentasikan dan diperiksa untuk keamanan? Hal ini di dokumentasikan dan diverifikasi.	Sangat Baik	Cukup Baik	Tidak Baik	Tidak Tahu	

		Seberapa sering keamanan, pelatihan, dan pengingat/pemberitahuan rutin diberikan kepada staf untuk membantu mereka tetap ingat dan patuh terhadap prosedur keamanan yang telah ditetapkan? Pemahaman staf didokumentasikan dan kesesuaiannya diverifikasi.	Sangat Sering	Cukup Sering	Jarang	Tidak Tahu	
		Seberapa baik staf mengikuti aturan keamanan seperti; a. Mengamankan informasi yang menjadi tanggung jawab mereka b. Tidak membocorkan informasi sensitif kepada orang lain c. Memiliki kemampuan yang memadai untuk menggunakan perangkat keras dan perangkat lunak teknologi informasi d. Menggunakan praktik kata sandi yang baik	Sangat Baik	Cukup Baik	Tidak Baik	Tidak Tahu	

		e. Memahami dan mengikuti kebijakan dan peraturan keamanan f. Mengenali dan melaporkan insiden					
		Tabel 2	**Jawaban**				
		Apa yang saat ini sudah dilakukan dengan baik oleh UPA TIK terkait bidang keamanan dan Pelatihan? Tuliskan semua praktik yang telah dilakukan terkait keamanan dan pelatihan, misalnya pelatihan berkala, penyusunan SOP, atau penerapan kebijakan keamanan.					
		Apa yang saat ini tidak dilakukan dengan baik pada bidang ini? Jelaskan praktik-praktik yang seharusnya dilakukan namun belum diterapkan atau belum dilakukan dengan baik, misalnya kurangnya pelatihan atau kebijakan yang belum disosialisasikan dengan baik.					
			Pilihan Jawaban				

		Seberapa efektif UPA TIK menerapkan praktik keamanan dan pelatihan?	**Merah**	**Kuning**	**Hijau**	**Tidak Berlaku**	
			Sangat tidak efektif, banyak masalah yang perlu diperbaiki.	Cukup efektif, namun masih ada ruang untuk perbaikan.	Sangat efektif, semua berjalan sesuai harapan.	Praktik ini tidak relevan atau tidak diterapkan.	
2.	**Strategi Keamanan**	**Tabel 1**	**Pilihan Jawaban**				Sekretaris UPA TIK.
			Sangat Banyak	**Agak**	**Tidak Sama Sekali**	**Tidak Tahu**	
		Seberapa sering keamanan dipertimbangkan dalam perencanaan strategi bisnis di UPA TIK?	Sangat Sering	Cukup Sering	Tidak Pernah	Tidak Tahu	
		Seberapa baik strategi dan kebijakan keamanan di UPA TIK sudah mendukung tujuan UPA TIK?	Sangat Baik	Cukup Baik	Tidak Baik Sama Sekali	Tidak Tahu	
		Seberapa sering strategi, tujuan, dan kebijakan keamanan didokumentasikan, diperbarui dan disosialisasikan kepada staf di UPA TIK?	Sangat Sering	Cukup Serimg	Tidak Pernah	Tidak Tahu	
		Tabel 2	**Jawaban**				

		Apa yang saat ini sudah dilakukan dengan baik oleh UPA TIK terkait bidang Strategi Keamanan? Tulis apa saja yang sudah dilakukan terkait dengan strategi keamanan, misalnya “UPA TIK secara berkala memperbarui kebijakan keamanan dan menyelaraskannya dengan tujuan bisnis.”					
		Apa yang saat ini tidak dilakukan dengan baik pada bidang strategi keamanan? Tulis kekurangan yang ada, seperti “UPA TIK belum mengintegrasikan kebijakan keamanan ke dalam semua proyek bisnis.”					
		Seberapa efektif UPA TIK menerapkan strategi keamanan di UPA TIK?	**Pilihan Jawaban**				
			Merah	**Kuning**	**Hijau**	**Tidak Berlaku**	
			Sangat tidak efektif, banyak masalah	Cukup efektif, namun masih ada ruang	Sangat efektif, semua berjalan	Praktik ini tidak relevan atau tidak diterapkan.	

			yang perlu diperbaiki.	untuk perbaikan.	sesuai harapan.		
3.	**Manajemen Keamanan**	**Tabel 1**	**Pilihan Jawaban**				Sekretaris UPA TIK.
			Sangat Banyak	**Agak**	**Tidak Sama Sekali**	**Tidak Tahu**	
		Apakah UPA TIK selalu menyediakan dana yang cukup untuk kegiatan keamanan informasi?	Ya, dana selalu cukup dan tersedia.	Kadang-kadang dana tersedia, tapi belum cukup.	Dana tidak disediakan sama sekali.	Saya tidak tahu tentang alokasi ini.	
		Apakah peran dan tanggung jawab keamanan sudah ditetapkan untuk semua staf dalam organisasi?	Ya, peran dan tanggung jawab keamanan sudah ditetapkan untuk semua staf.	Peran dan yanggung jawab hanya ditetapkan untuk beberapa staf.	Peran dan tanggung jawab belum ditetapkan sama sekali.	Saya tidak tahu apakah peran dan tanggung jawab keamanan sudah ditetapkan.	
		Seberapa baik staf memahami peran mereka dalam menjaga keamanan informasi?	Semua staf sangat paham melaksanaka	Bebera astaf paham, tetapi	Hampir semua staf tidak memahami	Saya tidak tahu bagaimana pemahama	

			n tanggung jawab mereka.	masih ada yang belum paham.	peran mereka.	n staf soal ini.	
		Seberapa baik prosedur pengawasan untuk melindungi informasi sensitif diterapkan di UPA TIK?	Prosedur pengawasan diterapkan dengan sangat baik.	Prosedur pengawasan kadang-kadang diterapkan, tapi belum konsisten.	Prosedur pengawasan hampir tidak pernah diterapkan.	Saya tidak tahu tentang adanya prosedur ini.	
		Seberapa sering organisasi memperhatikan keamanann informasi saat mereka merekrut dan melatih staf?	Keamanan informasi selalu dipertimbangkan.	Kadang-kadang dipertimbangkan, tetapi tidak selalu.	Hampir tidak pernah dipertimbangkan.	Saya tidak tahu apakah keamanan informasi dipertimbangkan.	
		Seberapa sering UPA TIK melakukan penilaian dan pengelolaan risiko terkait keamanan informasi?	Organisasi secara rutin melakukan penilaian risiko.	Organisasi melakukan penilaian risiko sesekali saja.	Organisasi hampir tidak pernah melakukan penilaian risiko.	Saya tidak tahu tentang kegiatan penilaian risiko.	

		Apakah laporan insiden keamanan informasi selalu ditinjaklanjuti oleh manajemen? (misalnua, audit, log, penilaian risiko dan kerentanan).	Laporan selalu diterima dan segera ditinjaklanjuti.	Laporan kadang-kadang diterima, tapi tidak selalu ditindaklanjuti.	Laporan jarag ditinjaklanjuti atau bahkan tidak pernah diterima.	Saya tidak tahu bagaimana laporan insiden diproses.	
		Tabel 2	**Jawaban**				
		Apa yang saat ini sudah dilakukan oleh UPA TIK pada bidang manajemen keamanan ini? Berikan contoh apa yang sudah dilakukan dengan baik pada bidang ini.					
		Apa yang saat ini tidak dilakukan dengan baik pada bidang manajemen keamanan ini? Sebutkan hal-hal yang masih kurang atau perlu diperbaiki dalam manajemen keamanan ini (seperti belum tersedianya kebijakan atau prosedur)					
			Pilihan Jawaban				

		Seberapa efektif UPA TIK menerapkan praktik-praktik di bidang manajemen keamanan ini?	**Merah**	**Kuning**	**Hijau**	**Tidak Berlaku**	
			Sangat tidak efektif, banyak masalah yang perlu diperbaiki.	Cukup efektif, namun masih ada ruang untuk perbaikan.	Sangat efektif, semua berjalan sesuai harapan.	Praktik ini tidak relevan atau tidak diterapkan.	
4.	**Peraturan dan Kebijakan Keamanan**	**Tabel 1**	**Pilihan Jawaban**				Divisi Infrastruktur, Jaringan, & Keamanan.
			Sangat Banyak	**Agak**	**Tidak Sama Sekali**	**Tidak Tahu**	
		Apakah organisasi memiliki kebijakan keamanan yang selalu diperbarui dan terdokumentasi?	Ya, selalu diperbarui	Ya, tapi kadang-kadang	Tidak, belum ada	Tidak tahu	
		Apakah ada prosedur yang terdokumentasi dengan jelas untuk mengelola kebijakan keamanan, termasuk pembuatan dan pembaruan?	Ya, ada prosedur yang jelas	Ya, tapi tidak sepenuhnya jelas	Tidak, belum ada prosedur	Tidak tahu	

		Apakah ada proses yang terdokumentasi untuk memeriksa dan memastikan kepatuhan terhadap kebijakan keamanan dan hukum?	Ya, sudah lengkap	Ya, tapi belum sepenuhnya	Tidak, belum ada	Tidak tahu	
		Apakah kebijakan keamanan informasi diterapkan secara konsisten di seluruh divisi yang ada di UPA TIK?	Ya, diterapkan di seluruh divisi yang ada di UPA TIK Undiksha	Ya, tapi tidak merata	Tidak, belum diterapkan	Tidak tahu	
		Tabel 2	**Jawaban**				
		Apa yang saat ni sudah dilakukan dengan baik oleh UPA TIK dalam menerapkan kebijakan keamanan? Berikan jawaban yang konkret (misalnya, dokumentasi kebijakan keamanan ada dan sudah diperbarui sesuai dengan perkembangan terbaru)					
		Apa yang saat ini tidak dilakukan dengan baik oleh UPA TIK dalam menerapkan kebijakan keamanan?					

		Sebutkan apa yang mungkin perlu ditingkatkan dan ditambahkan (misalnya, dokuemntasi kebijakan keamanan belum sesuai dan belum diperbarui, kebijakan keamanan belum ada).					
		Seberapa efektif UPA TIK U ndiksha dalam menerapkan kebijakan keamanan?	**Pilihan Jawaban**				
			Merah	**Kuning**	**Hijau**	**Tidak Berlaku**	
			Sangat tidak efektif, banyak masalah yang perlu diperbaiki.	Cukup efektif, namun masih ada ruang untuk perbaikan.	Sangat efektif, semua berjalan sesuai harapan.	Praktik ini tidak relevan atau tidak diterapkan.	
5.	**Manajemen Keamanan Kolaboratif**	**Tabel 1**	**Pilihan Jawaban**				Sekretaris UPA TIK.
			Sangat Banyak	**Agak**	**Tidak Sama Sekali**	**Tidak Tahu**	
		Seberapa efektif kebijakan organisasi dalam melindungi informasi saat bekerja dengan pihak eksternal termasuk pemahaman kebijakannya dan memutus akses	Kebijakan sangat komprehensif dan efektif.	Kebijakan efektif hanya di beberapa area.	Kebijakan tidak ada.	Tidak tahu informasi mengenai hal itu atau tidak	

		informasi ke eksternal yang diberhentikan?				relevan dengan UPA TIK Undiksha.	
		Sejauh mana UPA TIK Unidksha mendokumentasikan persyaratan perlindungan informasi dan secara eksplisit mengkomunikasikannya kepada semua pihak ketiga yang sesuai?	Dokumentasi dan komunikasi dilakukan dengan sangat baik dan jelas.	Dokumentasi dan komunikasi masih kurang efektif dan perlu ditingkatkan.	Tidak ada dokumentasi dan komunikasi.	Tidak ada informasi mengenai dokumentasi dan komunikasi ini. Tidak relevan dengan kondisi UPA TIK Undiksha.	
		Seberapa baik UPA TIK dalam memverifikasi keamanan pihak eksternal, layanan, dan teknologi?	Verifikasi dilakukan secara menyeluruh dan detail.	Verifikasi tidak konsisten atau kurang mendalam	Tidak ada verifikasi keamanan.	Tidak relevan dengan kondisi UPA TIK Undiksha.	

		Bagaimana efektivitas kebijakan kolaborasi keamanan dengan pihak eksternal?	Kebijakan diterapkan dengan sangat baik.	Kebijakan ada, tapi tidak sepenuhnya diterapkan atau tidak konsisten.	Tidak ada kebijakan kolaborasi keamanan.	Tidak relevan dengan kondisi UPA TIK Undiksha.	
		Tabel 2	**Jawaban**				
		Apa yang saat ini sudah dilakukan dengan baik oleh UPA TIK dalam menerapkan Manajemen Keamanan Kolaboratif? Berikan contoh apa yang sudah dilakukan dengan baik pada bidang ini.					
		Apa yang saat ini tidak dilakukan dengan baik oleh UPA TIK dalam menerapkan manajemen keamanan kolaboratif? Sebutkan hal-hal yang masih kurang atau perlu diperbaiki dalam manajemen keamanan ini.					
			Pilihan Jawaban				

		Seberapa efektif penerapan praktik keamanan kolaboratif oleh UPA TIK?	**Merah**	**Kuning**	**Hijau**	**Tidak Berlaku**	
			Sangat tidak efektif, banyak masalah yang perlu diperbaiki.	Cukup efektif, namun masih ada ruang untuk perbaikan.	Sangat efektif, semua berjalan sesuai harapan.	Praktik ini tidak relevan atau tidak diterapkan.	
6.	**Perancanaan Contingency / Pemulihan Bencana**	**Tabel 1**	**Pilihan Jawaban**				Divisi Infrastruktur, Jaringan, & Keamanan.
			Sangat Banyak	**Agak**	**Tidak Sama Sekali**	**Tidak Tahu**	
		Sejauh mana organisasi telah melakukan analisis operasi, aplikasi, serta kekeritisan data, dan mendokumentasikan, meninjau, serta menguji rencana kontinjensi, pemulihan bencana, serta kelangsungan operasi darurat?	Telah dilakukan dan didokumentasikan dengan baik.	Hanya sebagian rencana yang telah diuji dan didokumentasikan.	Belum dilakukan sama sekali.	Saya tidak tahu dan tidak memiliki informasi mengenai hal ini.	
		Apakah rencana kontinjensi/pemulihan bencana, dan kelangsungan operasi mempertimbangkan kontrol akses fisik dan elektronik serta apakah staf	Ya, seluruh staf memahami dan rencana mempertimb	Rencana sudah mempertimbangkan kontrol	Belum ada rencana yang mempertimbangkan kontrol akses	Saya tidak tahu dan tidak memiliki informasi	

		mengetahui dan memahami tanggung jawab mereka dalam pelaksanaan rencana tersebut?	angkan kontrol akses.	akses, namun staf belum memahami sepenuhnya.	dan staf belum memahami tanggung jawabnya.	mengenai hal ini.	
		Apakah organisasi secara rutin mendokumentasikan, meninjau, dan menguji rencana-rencana tersebut, termasuk rencana pemulihan bencana dan kelangsungan operasi?	Sudah dilakukan dengan rutin dan menyeluruh.	Hanya beberapa aspek yang diuji dan didokumentasikan.	Tidak dilakukan sama sekali.	Saya tidak tahu dan tidak memiliki informasi mengenai hal ini	
		Seberapa jauh seluruh staf dalam organisasi memahami rencana kontinjensi, pemulihan bencana, serta kelangsungan operasi, dan seberapa baik mereka mampu melaksanakan tanggung jawab mereka?	Seluruh staf memahami dan mampu melaksanakan tanggung jawab mereka	Hanya sedikit staf yang memahami dan mampu melaksanakan.	Tidak ada staf yang memahami atau mampu melaksanakan tanggung jawab mereka.	Saya tidak tahu dan tidak memiliki informasi mengenai hal ini	
		Tabel 2	**Jawaban**				
		Apa yang saat ini sudah dilakukan dengan baik oleh UPA TIK dalam					

		menerapkan Perancanaan Contingency / Pemulihan Bencana?					
		Apa yang saat ini tidak dilakukan dengan baik oleh UPA TIK dalam menerapkan Perancanaan Contingency / Pemulihan Bencana?					
		Seberapa efektif UPA TIK menerapkan praktik-praktik perencanaan kontinjensi/pemulihan bencana dalam mendukung operasional?	**Pilihan Jawaban**				
			Merah	**Kuning**	**Hijau**	**Tidak Berlaku**	
			Sangat tidak efektif, banyak masalah yang perlu diperbaiki.	Cukup efektif, namun masih ada ruang untuk perbaikan.	Sangat efektif, semua berjalan sesuai harapan.	Praktik ini tidak relevan atau tidak diterapkan.	
7.	**Pengendalian Akses Fisik**	**Tabel 1**	**Pilihan Jawaban**				Divisi Infrastruktur, Jaringan, & Keamanan.
			Sangat Banyak	**Agak**	**Tidak Sama Sekali**	**Tidak Tahu**	
		Apakah rencana dan prosedur keamanan fasilitas untuk melindungi tempat, bangunan, dan area terlarang sudah didokumentasikan dan diuji di UPA TIK Undiksha?	Sudah didokumentasikan dan diuji dengan sangat baik.	Hanya sebagian yang didokumentasikan,	Tidak ada dokumentasi atau uji coba.	Tidak ada informasi tentang hal ini dan tidak	

				belum diuji.		relevan dengan UPA TIK Undiksha.	
		Apakah terdapat kebijakan dan prosedur yang terdokumentasi untuk mengelola pengunjung di UPA TIK Undiksha?	Kebijakan sudah lengkap dan diikuti dengan baik.	Ada kebijakan tetapi tidak terdokumentasi dan penerapannya tidak konsisten.	Tidak ada kebijakan tentang hal ini sama sekali.	Tidak ada informasi tentang hal ini dan tidak relevan dengan UPA TIK Undiksha.	
		Apakah terdapat kebijakan dan prosedur yang terdokumentasi untuk mengendalikan akses fisik ke area kerja dan perangkat keras seperti komputer, perangkat komunikasi, dan media perangkat lunak di UPA TIK Undiksha?	Akses fisik sudah dikelola dengan baik, kebijakan terdokumentasi lengkap.	Pengelolaan akses fisik dilakukan, tetapi kebijakan tidak terdokumentasi.	Tidak ada kebijakan atau prosedur terkait akses fisik.	Tidak ada informasi tentang hal ini dan tidak relevan dengan UPA TIK Undiksha.	
		Apakah lingkungan kerja dan komponen lain yang memungkinkan	Sudah dilindungi	Perlindungan ada,	Tidak ada perlindungan	Tidak ada informasi	

		akses ke informasi sensitif sudah dilindungi secara fisik untuk mencegah akses yang tidak sah?	sepenuhnya dengan kontrol fisik yang kuat.	tetapi kontrol fisik tidak konsisten.	atau kontrol fisik.	tentang hal ini dan tidak relevan dengan UPA TIK Undiksha.	
		Tabel 2	**Jawaban**				
		Apa yang saat ini dilakukan dengan baik oleh UPA TIK dalam pengendalian akses fisik? Tuliskan hal yang sudah dengan baik dilakukan dalam bidang ini (misalnya, penerapan kebijakan akses fisik sudah berjalan dengan baik. Staf menggunakan kartu akses elektronik untuk masuk ke area terbatas, dan akses ke ruangan server selalu diawasi).					
		Apa yang saat ini tidak dilakukan dengan baik oleh UPA TIK dalam pengendalian akses fisik? Tuliskan hal yang masih perlu diperbaiki atau ditambahkan dalam					

		bidang ini (misalnya, Beberapa pintu ke area sensitif seringkali dibiarkan terbuka tanpa pengawasan, terutama di luar jam kerja dan mengenai pencatatan pengunjung dll).					
		Seberapa efektif UPA TIK menerapkan praktik-praktik dalam pengendalian akses fisik?	**Pilihan Jawaban**				
			Merah	**Kuning**	**Hijau**	**Tidak Berlaku**	
			Sangat tidak efektif, banyak masalah yang perlu diperbaiki.	Cukup efektif, namun masih ada ruang untuk perbaikan.	Sangat efektif, semua berjalan sesuai harapan.	Praktik ini tidak relevan atau tidak diterapkan.	
8.	**Pemantauan dan Audit Keamanan Fisik**	**Tabel 1**	**Pilihan Jawaban**				Divisi Infrastruktur, Jaringan, & Keamanan.
			Sangat Banyak	**Agak**	**Tidak Sama Sekali**	**Tidak Tahu**	
		Seberapa baik organisasi Anda menyimpan dan mengelola catatan pemeliharaan terkait perbaikan dan modifikasi fasilitas fisik?	Semua catatan terdokumentasi dengan baik dan	Hanya sebagian kecil catatan yang	Tidak ada dokumentasi catatan atau saya tidak tahu.	Tidak ada informasi tentang hal ini dan tidak relevan	

			mudah diakses.	terdokumentasi.		dengan UPA TIK Undiksha.	
		Seberapa baik tindakan individu atau kelompok dalam organisasi dipantau terkait penggunaan media yang dikontrol secara fisik?	Selalu dipantau dengan jelas dan bisa dipertanggungjawabkan.	Jarang dipantau dan sulit dipertanggungjawabkan.	Tidak dipantau sama sekali.	Tidak ada informasi tentang hal ini dan tidak relevan dengan UPA TIK Undiksha.	
		Seberapa sering catatan audit dan pemantauan diperiksa untuk menemukan anomali, dan tindakan perbaikan diambil jika diperlukan?	Selalu diperiksa secara rutin dan tindakan korektif segera dilakukan.	Jarang diperiksa, tindakan korektif jarang diambil.	Tidak diperiksa sama sekali.	Tidak ada informasi tentang hal ini dan tidak relevan dengan UPA TIK Undiksha.	
		Tabel 2	**Jawaban**				
		Apa yang saat ini dilakukan oleh UPA TIK dengan baik dalam					

		pemantauan dan audit keamanan fisik? Berikan informasi tentang apa yang berjalan baik dalam bidang ini.					
		Apa yang saat ini tidak dilakukan dengan baik pada pemantauan dan audit keamanan fisik? Berikan informasi tentang apa yang kurang dalam bidang ini.					
		Seberapa efektif UPA TIK menerapkan praktik-praktik dalam pemantauan dan audit keamanan fisik?	**Pilihan Jawaban**				
			Merah	**Kuning**	**Hijau**	**Tidak Berlaku**	
			Sangat tidak efektif, banyak masalah yang perlu diperbaiki.	Cukup efektif, namun masih ada ruang untuk perbaikan.	Sangat efektif, semua berjalan sesuai harapan.	Praktik ini tidak relevan atau tidak diterapkan.	
9.	**Manajemen Jaringan dan Sistem**	**Tabel 1**	**Pilihan Jawaban**				Divisi Infrastruktur,
			Sangat Banyak	**Agak**	**Tidak Sama Sekali**	**Tidak Tahu**	

		Apakah ada rencana keamanan yang terdokumentasi dan teruji untuk melindungi sistem dan jaringan?	Sudah ada dan selalu diperbarui	Ada, tetapi belum diperbarui secara rutin.	Ada, tetapi belum pernah diuji.	Tidak ada rencana keamanan.	Jaringan, & Keamanan.
		Bagaimana informasi sensitif dilindungi oleh penyimpanan yang aman (misal, cadangan disimpan di luar lokasi, proses pembuangan informasi sensitif)?	Sudah terlindungi dengan baik.	Hanya sebagian yang dilindungi.	Tidak ada proteksi khusus.	Tidak tahu atau tidak ada informasi mengenai hal ini.	
		Seberapa sering integritas perangkat lunak yang terinstal diverifikasi secara teratur?	Secara rutin diverifikasi setiap kali ada pembaruan.	Jarang di verifikasi.	Tidak pernah diverifikasi.	Tidak tahu atau tidak ada informasi mengenai hal ini.	
		Apakah semua sistem selalu diperbarui sesuai revisi, tambalan, dan rekomendasi dalam saran keamanan?	Semua sistem diperbarui tepat waktu.	Hanya beberapa sistem yang diperbarui.	Tidak ada sistem yang diperbarui.	Tidak tahu atau tidak ada informasi mengenai hal ini.	

		Apakah ada rencana pencadangan data yang terdokumentasi dan teruji, serta apakah semua staf memahami tanggung jawab mereka terkait pencadangan?	Ada rencana pencadangan, dan staf memahami tanggung jawabnya.	Ada pencadangan, tetapi belum terdokumentasi dan diuji serta staf kurang memahami tanggung jawabnya.	Tidak ada rencana pencadangan dan staf tidak memahami tanggung jawabnya.	Tidak tahu atau tidak ada informasi mengenai hal ini.	
		Bagaimana perubahan pada perangkat keras dan perangkat lunak TI direncanakan, dikontrol, dan didokumentasikan?	Semua perubahan direncanakan, dikontrol, dan didokumentasikan.	Beberapa perubahan tidak direncanakan dan kurang didokumentasikan.	Tidak ada perencanaan dan dokumentasi yang jelas.	Tidak tahu atau tidak ada informasi mengenai hal ini.	
		Apakah prosedur diikuti saat menerbitkan, mengubah, dan menghentikan kata sandi, akun, serta hak istimewa pengguna, dan apakah identifikasi pengguna yang unik	Semua prosedur diikuti, identifikasi pengguna	Prosedur kadang-kadang diabaikan, identifikasi	Tidak ada prosedur yang jelas, identifikasi pengguna	Tidak tahu atau tidak ada informasi	

		diperlukan serta akun dan kata sandi bawaan sudah dihapus dari sistem?	unik diperlukan, dan akun/kata sandi bawaan sudah dihapus.	pengguna unik tidak selalu diperlukan, dan akun/kata sandi bawaan masih digunakan.	unik tidak diperlukan, dan akun/kata sandi bawaan belum dihapus.	mengenai hal ini.	
		Apakah hanya layanan yang diperlukan yang berjalan pada sistem, dan semua layanan yang tidak perlu dihapus?	Ya, semua layanan yang tidak diperlukan sudah dihapus.	Beberapa layanan tidak perlu masih berjalan.	Tidak ada tindakan untuk menghapus layanan yang tidak perlu.	Tidak tahu atau tidak ada informasi mengenai hal ini.	
		Apakah alat dan mekanisme untuk administrasi sistem dan jaringan yang aman digunakan, dan secara rutin ditinjau?	Digunakan dan ditinjau secara rutin.	Jarang digunakan dan jarang ditinjau.	Tidak pernah ditinjau sama sekali.	Tidak tahu atau tidak ada informasi mengenai hal ini.	
		Tabel 2	**Jawaban**				

		Apa yang saat ini dilakukan oleh UPA TIK dengan baik dalam manajemen sistem dan jaringan?					
		Apa yang saat ini tidak dilakukan dengan baik pada manajemen sistem dan jaringan?					
		Seberapa efektif UPA TIK menerapkan praktik-praktik dalam manajemen sistem dan jaringan?	**Pilihan Jawaban**				
			Merah	**Kuning**	**Hijau**	**Tidak Berlaku**	
			Sangat tidak efektif, banyak masalah yang perlu diperbaiki.	Cukup efektif, namun masih ada ruang untuk perbaikan.	Sangat efektif, semua berjalan sesuai harapan.	Praktik ini tidak relevan atau tidak diterapkan.	
10.	**Pemantauan dan Audit Keamanan TI**	**Tabel 1**	**Pilihan Jawaban**				Divisi Pusat Data & Informasi.
			Sangat Banyak	**Agak**	**Tidak Sama Sekali**	**Tidak Tahu**	
		Seberapa sering organisasi Anda menggunakan alat-alat pemantauan	Alat-alat pemantauan	Sebagian besar alat	Alat-alat tersebut	Saya tidak tahu	

		dan audit sistem serta jaringan secara rutin? Apakah aktivitas yang tidak biasa ditangani sesuai dengan kebijakan atau prosedur yang berlaku?	dan audit selalu diguakan dengan konsisten dan sesuai prosedur.	digunakan secara rutin, tetapi ada pengecualian.	jarang atau tidak pernah digunakan.	apakah alat-alat ini digunakan secara rutin atau tidak.	
		Seberapa sering firewall dan komponen keamanan lainnya diaudit untuk memastikan kepatuhan terhadap kebijakan?	Firewall dan komponen keamanan lainnya diaudit secara berkala.	Audit dilakukan, tetapi tidak selalu konsisten.	Audit jarang atau tidak pernah dilakukan.	Saya tidak tahu apakah audit tersebut dilakukan atau tidak.	
		Tabel 2	**Jawaban**				
		Apa saja yang dilakukan dengan baik oleh UPA TIK saat ini dalam pemantauan dan audit keamanan TI? Jawablah secara rinci tindakan atau praktik yang menurut Anda sudah baik dalam pelaksanaan pemantauan dan audit keamanan TI oleh UPA TIK Undiksha.					

		Apa yang tidak dilakukan dengan baik oleh UPA TIK dalam pemantauan dan audit keamanan TI? Jawablah secara rinci hal-hal atau area yang menurut Anda masih kurang atau belum optimal dalam pelaksanaan pemantauan dan audit keamanan TI oleh UPA TIK.					
		Seberapa efektif menurut Anda UPA TIK dalam menerapkan praktik-praktik manajemen sistem dan jaringan?	**Pilihan Jawaban**				
			Merah	**Kuning**	**Hijau**	**Tidak Berlaku**	
			Sangat tidak efektif, banyak masalah yang perlu diperbaiki.	Cukup efektif, namun masih ada ruang untuk perbaikan.	Sangat efektif, semua berjalan sesuai harapan.	Praktik ini tidak relevan atau tidak diterapkan.	
11.	**Otentikasi dan Otorisasi**	**Tabel 1**	**Pilihan Jawaban**				Divisi Infrastruktur, Jaringan, & Keamanan.
			Sangat Banyak	**Agak**	**Tidak Sama Sekali**	**Tidak Tahu**	
		Seberapa baik kontrol akses dan autentikasi pengguna (seperti izin file, konfigurasi jaringan) diterapkan	Kontrol akses dan autentikasi	Kontrol akses dan autentikasi	Kontrol akses dan autentikasi	Tidak yakin mengenai	

		sesuai kebijakan untuk membatasi akses ke informasi, sistem, aplikasi, dan jaringan sensitif?	diterapkan secara menyeluruh sesuai kebijakan.	diterapkan, tetapi ada beberapa kekurangan.	tidak diterapkan.	penerapan kontrol akses dan autentikasi.	
		Apakah ada kebijakan dan prosedur yang terdokumentasi untuk menetapkan dan mengakhiri hak akses terhadap informasi, baik untuk individu maupun kelompok?	Kebijakan dan prosedur terdokumentasi dengan baik.	Kebijakan dan prosedur ada, tetapi tidak sepenuhnya terdokumentasi.	Tidak ada kebijakan atau prosedur terdokumentasi.	Tidak tahu mengenai kebijakan dan prosedur tersebut.	
		Seberapa baik metode atau mekanisme disediakan untuk memastikan informasi sensitif tidak diakses, diubah, atau dihancurkan secara tidak sah, dan seberapa sering metode tersebut ditinjau dan diverifikasi?	Metode sangat baik dan ditinjau secara berkala.	Metode ada dan ditinjau, tetapi tidak secara konsisten.	Metode tidak ada atau tidak ditinjau.	Tidak tahu mengenai metode atau mekanisme tersebut.	
		Tabel 2	**Jawaban**				
		Apa yang saat ini dilakukan dengan baik oleh UPA TIK Undiksha dalam bidang otentikasi dan otorisasi?					

		Apa yang saat ini tidak dilakukan dengan baik dalam hal otentikasi dan otorisasi?					
		Seberapa efektif UPA TIK dalam menerapkan praktik otentikasi dan otorisasi?	**Pilihan Jawaban**				
			Merah	**Kuning**	**Hijau**	**Tidak Berlaku**	
			Sangat tidak efektif, banyak masalah yang perlu diperbaiki.	Cukup efektif, namun masih ada ruang untuk perbaikan.	Sangat efektif, semua berjalan sesuai harapan.	Praktik ini tidak relevan atau tidak diterapkan.	
12.	**Manajemen Kerentanan**	**Tabel 1**	**Pilihan Jawaban**				Divisi Infrastrukutr, Jaringan, & Keamanan.
			Sangat Banyak	**Agak**	**Tidak Sama Sekali**	**Tidak Tahu**	
		Seberapa lengkap prosedur terdokumentasi untuk mengelola keamanan di organisasi, termasuk:	Semua aspek dikelola	Beberapa aspek dikelola dengan	Tidak ada sama sekali aspek yang dikelola.	Tidak yakin mengenai	

		a. Memilih alat evaluasi kerentanan, daftar periksa, dan skrip. b. Mengikuti perkembangan jenis kerentanan dan metode serangan yang diketahui. c. Meninjau sumber informasi tentang pengumuman kerentanan, peringatan keamanan, dan pemberitahuan. d. Mengidentifikasi komponen infrastruktur yang akan dievaluasi. e. Penjadwalan evaluasi kerentanan. f. Menafsirkan dan menanggapi hasil evaluasi. g. Menjaga penyimpanan dan disposisi data kerentanan yang aman.	dengan sangat baik.	baik, tapi banyak area yang masih kurang.		kelengkapan prosedur.	
		Seberapa konsisten prosedur manajemen kerentanan diikuti, ditinjau, dan diperbarui?	Prosedur selalu diikuti,	Prosedur tidak selalu diikuti atau	Tidak sama sekali diikuti,	Tidak memiliki informasi	

			ditinjau, dan diperbarui secara rutin.	diperbarui dengan baik.	ditinjau, dan diperbarui.	mengenai konsistensi prosedur.	
		Seberapa sering penilaian kerentanan teknologi dilakukan dan kerentanan diatasi ketika teridentifikasi?	Penilaian dilakukan secara berkala dan semua kerentanan segera diatasi.	Penilaian dilakukan tidak teratur dan beberapa kerentanan mungkin tidak segera diatasi.	Tidak sama sekali dilakukan	Tidak mengetahui frekuensi atau efektivitas penilaian kerentanan.	
		Tabel 2	**Jawaban**				
		Apa yang saat ini dilakukan oleh UPA TIK dengan baik dalam manajemen kerentanan?					

		Apa yang saat ini tidak dilakukan dengan baik pada manajemen kerentanan?					
		Seberapa efektif UPA TIK menerapkan praktik-praktik dalam manajemen kerentanan?	**Pilihan Jawaban**				
			Merah	**Kuning**	**Hijau**	**Tidak Berlaku**	
			Sangat tidak efektif, banyak masalah yang perlu diperbaiki.	Cukup efektif, namun masih ada ruang untuk perbaikan.	Sangat efektif, semua berjalan sesuai harapan.	Praktik ini tidak relevan atau tidak diterapkan.	
13.	**Enkripsi**	**Tabel 1**	**Pilihan Jawaban**				Divisi Pusat Data & Informasi.
			Sangat Banyak	**Agak**	**Tidak Sama Sekali**	**Tidak Tahu**	
		Seberapa baik kontrol keamanan, seperti enkripsi data dan teknologi jaringan pribadi virtual, diterapkan untuk melindungi informasi sensitif saat disimpan dan selama transmisi?	Kontrol keamanan diterapkan secara menyeluruh.	Kontrol keamanan diterapkan, tetapi ada beberapa	Kontrol keamanan tidak diterapkan.	Tidak yakin mengenai penerapan	

				area yang belum sepenuhnya diterapkan.		kontrol keamanan.	
		Seberapa sering protokol terenkripsi digunakan saat mengelola sistem, router, dan firewall dari jarak jauh?	Protokol terenkripsi selalu digunakan.	Protokol terenkripsi sering digunakan, tetapi tidak selalu.	Protokol terenkripsi tidak pernah digunakan.	Tidak tahu tentang penggunaan protokol terenkripsi.	
		Tabel 2	**Jawaban**				
		Apa yang sudah dilakukan dengan baik oleh UPA TIK dalam praktik keamanan enkripsi? Berikan jawaban dalam bentuk paragraf singkat misalnya, UPA TIK Undiksha secara rutin menggunakan enkripsi end-to-end untuk semua data sensitif.					
		Apa yang tidak dilakukan dengan baikoleh UPA TIK Undiksha dalam praktik keamanan enkripsi?					

		Berikan jawaban dalam bentuk paragraf singkat misalnya, Proses enkripsi data tidak diterapkan secara konsisten di seluruh sistem.					
		Seberapa efektif penerapan praktik enkripsi oleh UPA TIK Undiksha?	**Pilihan Jawaban**				
			Merah	**Kuning**	**Hijau**	**Tidak Berlaku**	
			Sangat tidak efektif, banyak masalah yang perlu diperbaiki.	Cukup efektif, namun masih ada ruang untuk perbaikan.	Sangat efektif, semua berjalan sesuai harapan.	Praktik ini tidak relevan atau tidak diterapkan.	
14.	**Desain/perancangan dan arsitektur keamanan**	**Tabel 1**	**Pilihan Jawaban**				Divisi Infrastruktur, Jaringan, & Keamanan.
			Sangat Banyak	**Agak**	**Tidak Sama Sekali**	**Tidak Tahu**	
		Seberapa baik desain/perancangan dan arsitektur keamanan sistem baru dan sistem yang direvisi mencakup strategi, kebijakan, dan prosedur keamanan?	Seluruh aspek telah dipertimbangkan dan diimplement	Hanya beberapa bagian yang mencakup aspek-	Tidak ada sama sekali aspek yang dipertimbangkan.	Tidak memiliki informasi mengenai cakupan	

			asikan dengan baik.	aspek tersebut.		perancangan ini.	
		Seberapa baik desain/perancangan dan arsitektur keamanan mencakup riwayat kerjasama keamanan?	Sangat komprehensif dan mencakup semua aspek.	Cukup mencakup, tapi ada yang bisa diperbaiki.	Tidak mencakup sama sekali.	Tidak yakin.	
		Apakah UPA TIK Undiksha memiliki diagram terkini yang menunjukkan arsitektur keamanan di seluruh topologi jaringan?	Diagram sangat detail dan up-to-date.	Diagram ada, tetapi kurang lengkap	Tidak ada diagram sama sekali.	Tidak Tahu.	
		Tabel 2	**Jawaban**				
		Apa yang dilakukan dengan baik oleh UPA TIK dalam Desain/Perancangan dan Arsitektur Keamanan? Anda dapat menuliskan hal-hal yang sudah berjalan dengan baik, seperti pengembangan prosedur yang jelas					

		atau pengelolaan topologi jaringan yang efektif.					
		Apa yang tidak dilakukan dengan baik oleh UPA TIK Undiksha dalam Desain/Perancangan dan Arsitektur Keamanan? Anda dapat menuliskan saran perbaikan, misalnya pada dokumentasi keamanan yang kurang lengkap atau proses kerjasama yang belum optimal.					
		Seberapa efektif UPA TIK Undiksha dalam menerapkan praktik-praktik di Desain/Perancangan dan Arsitektur Keamanan?	**Pilihan Jawaban**				
			Merah	**Kuning**	**Hijau**	**Tidak Berlaku**	
			Sangat tidak efektif, banyak masalah yang perlu diperbaiki.	Cukup efektif, namun masih ada ruang untuk perbaikan.	Sangat efektif, semua berjalan sesuai harapan.	Praktik ini tidak relevan atau tidak diterapkan.	

15.	**Manajemen Insiden**	**Tabel 1**	**Pilihan Jawaban**				Divisi Infrastruktur, Jaringan, & Keamanan.
			Sangat Banyak	**Agak**	**Tidak Sama Sekali**	**Tidak Tahu**	
		Apakah terdapat prosedur yang terdokumentasi untuk mengidentifikasi, melaporkan, dan menanggapi dugaan insiden dan pelanggaran keamanan?	Prosedur terdokumentasi dengan baik dan diterapkan secara konsisten.	Prosedur ada, tapi implementasinya belum maksimal.	Prosedur tidak ada atau tidak terdokumentasi.	Tidak tahu tentang keberadaan prosedur ini.	
		Seberapa sering prosedur manajemen insiden diuji, diverifikasi, dan diperbarui secara berkala?	Uji dan pembaruan dilakukan secara teratur dan konsisten.	Uji dilakukan, tapi tidak secara rutin.	Uji dan pembaruan hampir tidak pernah dilakukan.	Tidak tahu mengenai frekuensi uji dan pembaruan.	
		Apakah terdapat kebijakan dan prosedur yang terdokumentasi untuk bekerja sama dengan lembaga penegak hukum dalam menangani insiden?	Prosedur kerjasama terdokumentasi dan dijalankan dengan baik.	Ada prosedur, tapi implementasi masih perlu diperbaiki.	Prosedur kerjasama tidak ada.	Tidak tahu mengenai kebijakan atau prosedur ini.	

		Tabel 2	**Jawaban**				
		Apa yang saat ini dilakukan dengan baik oleh UPA TIK dalam manajemen insiden?					
		Apa yang saat ini tidak dilakukan dengan baik oleh UPA TIK dalam manajemen insiden?					
		Seberapa efektif UPA TIK Undiksha menerapkan praktik-praktik dalam manajemen insiden?	**Pilihan Jawaban**				
			Merah	**Kuning**	**Hijau**	**Tidak Berlaku**	
			Sangat tidak efektif, banyak masalah yang perlu diperbaiki.	Cukup efektif, namun masih ada ruang untuk perbaikan.	Sangat efektif, semua berjalan sesuai harapan.	Praktik ini tidak relevan atau tidak diterapkan.	

Lampiran 8. Rancangan Pertanyaan Kuesioner Tahap Ke-2

1. Lembar Kerja Memilih Aset Kritis

No	Pertanyaan	Jawaban	Narasumber
1.	Diantara aset yang telah diidentifikasi, pilihlah aset-aset yang menurut anda paling penting, rentan, dan berisiko tinggi terhadap dampak merugikan jika skenario berikut terjadi: • Dibocorkan kepada pihak yang tidak berwenang • Diubah tanpa otorisasi • Hilang atau hancur • Akses terhadap aset kritis tersebut terputus Daftar aset yang telah diidentifikasi sebelumnya: • Server • SOP dan Instruksi Kerja		Sekretaris UPA TIK Undiksha.

	• SIAK • Perangkat Jaringan • Sekretaris UPA TIK Undiksha • Divisi Infrastruktur, Jaringan, & Keamanan Silakan pilih aset-aset yang menurut Anda paling penting, rentan dan beresiko tinggi ketika skenario tersebut terjadi. Anda bisa memilih lebih dari satu (1) dan bisa memilih beberapa jika aset tersebut dirasa tidak beresiko tinggi dan jika dirasa tidak relevan. Jawab dengan cara mengurutkan aset dengan skala prioritas paling rentan terlebih dahulu.		

2.	Divisi yang bertanggung jawab atas server?	Divisi Helpdesk & Dokumentasi	Divisi Manajemen Konten	Divisi Pusat Data & Informasi	Divisi Infrastruktur, Jaringan, & Keamanan	Divisi Sistem Informasi	
3.	Divisi yang bertanggung jawab atas izin pembuatan dan perubahan SOP dan Instruksi Kerja?	Divisi Helpdesk & Dokumentasi	Divisi Manajemen Konten	Divisi Pusat Data & Informasi	Divisi Infrastruktur, Jaringan, & Keamanan	Divisi Sistem Informasi	
4.	Divisi yang bertanggung jawab atas pengembangan SIAK?	Divisi Helpdesk & Dokumentasi	Divisi Manajemen Konten	Divisi Pusat Data & Informasi	Divisi Infrastruktur, Jaringan, & Keamanan	Divisi Sistem Informasi	
5.	Divisi yang bertanggung jawab atas Perangkat Jaringan?	Divisi Helpdesk & Dokumentasi	Divisi Manajemen Konten	Divisi Pusat Data & Informasi	Divisi Infrastruktur, Jaringan, & Keamanan	Divisi Sistem Informasi	

Server (catatan)			
1.	Apakah server pernah memiliki masalah pada perangkat keras (seperti komponen rusak) atau perangkat lunak (seperti konfigurasi salah atau celah keamanan/ Kelemahan yang dapat dimanfaatkan oleh peretas untuk mengakses data atau sistem tanpa izin)?		Divisi Pusat Data & Informasi
2.	Seberapa sering server mengalami downtime atau gangguan operasional dan apa dampaknya?		
SOP dan instruksi Kerja (catatan)			
1.	Apakah ada kemungkinan perubahan tidak sah pada SOP dan instruksi kerja dan apa dampaknya pada kegiatan operasionel sehari-hari?		Divisi Helpdesk & Dokumentasi

2.	Bagaimana cara UPA TIK Undiksha dalam menjaga agar dokumen SOP tetap aman dari akses tidak berwenang?		
SIAK (catatan)			Divisi Sistem Informasi
1.	Apakah ada risiko kegagalan sistem yang dapat mengakibatkan kehilangan data pada SIAK?		
2.	Apakah SIAK memiliki prosedur cadangan (backup) yang memadai?		
Perangkat Jaringan (catatan)			Divisi Infrastruktur, Jaringan, & Keamanan
1.	Apakah ada potensi penyalahgunaan akses ke perangkat jaringan dan seberapa besar potensinya?		

2.	Seberapa sering perangkat jaringan diperiksa untuk mendeteksi adanya kerentanan? Berikan skala dengan contoh: 1 kali/minggu.		
SDM – Sekretaris dan Divisi Infrastruktur, Jaringan, & Keamanan (catatan)			Divisi Infrastruktur, Jaringan, & Keamanan
1.	Apakah terdapat risiko dalam pengelolaan data sensitif dan informasi teknis oleh sekretaris dan divisi infrastruktur?		
2.	Seberapa sering dilakukan pemantauan dan evaluasi terhadap prosedur keamanan yang diterapkan oleh sekretaris dan divisi infrastruktur?		

2. Lembar Kerja Informasi Aset Kritis Untuk Server

No	Pertanyaan	Jawaban			Narasumber
1.	Berikan penjelasan mengapa server dianggap sangat penting bagi organisasi?				Divisi Pusat Data & Informasi
2.	Aset apa saja yang terkait dengan server?				
3.	Siapa saja yang menggunakan server?				
Persyaratan Keamanan					
1.	Apa persyaratan keamanan untuk server? (petunjuk: berfokus pada persyaratan apa yang seharusnya ada pada sebuah aset, bukan pada apa yang ada saat ini)	**Kerahasiaan**: hanya diakses oleh pihak tertentu	**Integritas**: server tidak boleh diakses oleh pihak yang berwenang	**Ketersediaan** : akses tersedia selama 24/7, *maintenance* …/minggu	
2	Persyaratan keamanan mana yang paling penting untuk aset server?	Kerahasiaan	Integritas	Ketersediaan	

3. Lembar Kerja Informasi Aset Kritis Untuk SOP dan Instruksi Kerja

No	Pertanyaan	Jawaban			Narasumber
1.	Berikan alasan mengapa SOP dan Instruksi Kerja penting bagi organisasi?				Divisi Helpdesk & Dokumentasi
2.	Aset apa saja yang terkait dengan SOP dan Instruksi Kerja?				
3.	Siapa saja yang menggunakan SOP dan Instruksi Kerja?				
Persyaratan Keamanan					
1.	Apa persyaratan keamanan untuk SOP dan Instruksi Kerja? (petunjuk: berfokus pada persyaratan apa yang seharusnya ada pada sebuah aset, bukan pada apa yang ada saat ini)	**Kerahasiaan**: dokumen hanya dibatasi aksesnya hanya kepada personil yang berwenang.	**Integritas**: dokumen harus dilindungi dari perubahan yang tidak sah dan harus dapat dilacak siapa yang membuat perubahan.	**Ketersediaan**: dokumen harus tersedia dan mudah diakses oleh staf UPA TIK Undiksha.	
2	Persyaratan keamanan mana yang paling penting untuk SOP dan Instruksi Kerja?	Kerahasiaan	Integritas	Ketersediaan	

4. Lembar Kerja Informasi Aset Kritis Untuk SIAK

No	Pertanyaan	Jawaban			Narasumber
1.	Berikan alasan mengapa SIAK penting bagi organisasi?				Divisi Sistem Informasi
2.	Aset apa saja yang terkait dengan SIAK?				
3.	Siapa saja yang menggunakan SIAK?				
Persyaratan Keamanan					
1.	Apa persyaratan keamanan untuk SIAK? (petunjuk: berfokus pada persyaratan apa yang seharusnya ada pada sebuah aset, bukan pada apa yang ada saat ini)	**Kerahasiaan**: data akademik dan informasi pribadi harus dilindungi agar hanya dapat diakses oleh pengguna yang sah.	**Integritas**: data dalam sistem harus tetap akurat dan tidak boleh diubah oleh pihak yang tidak berwenang.	**Ketersediaan**: sistem harus tersedia untuk pengguna yang berwenang selama jam operasional yang diperlukan, dengan waktu pemulihan yang cepat jika terjadi gangguan.	
2	Persyaratan keamanan mana yang paling penting untuk SIAK?	Kerahasiaan	Integritas	Ketersediaan	

5. Lembar Kerja Informasi Aset Kritis Untuk Perangkat Jaringan

No	Pertanyaan	Jawaban	Narasumber
1.	Berikan alasan mengapa perangkat jaringan penting bagi organisasi?		Divisi Infrastruktur, Jaringan & Keamanan
2.	Aset apa saja yang terkait dengan perangkat jaringan?		
3.	Siapa saja yang menggunakan perangkat jaringan?		

Persyaratan Keamanan					
1.	Apa persyaratan keamanan untuk perangkat jaringan? (petunjuk: berfokus pada persyaratan apa yang seharusnya ada pada sebuah aset, bukan pada apa yang ada saat ini)	**Kerahasiaan**: pengaturan dan data konfigurasi perangkat jaringan harus hanya diakses oleh personel jaringan yang berwenang.	**Integritas**: monitoring jaringan pada lingkup organisasi, termasuk menjaga perangkat agar tidak dimodifikasi secara tidak sah.	**Ketersediaan**: perangkat harus beroperasi secara optimal dan dapat diakses kapan saja untuk memastikan konektivitas jaringan yang konsisten.	
2	Persyaratan keamanan mana yang paling penting untuk perangkat jaringan?	Kerahasiaan	Integritas	Ketersediaan	

6. Lembar Kerja Informasi Aset Kritis Untuk SDM; Sekretaris UPA TIK Undiksha

No	Pertanyaan	Jawaban	Narasumber
1.	Mengapa Sekretaris UPA TIK dianggap penting bagi organisasi?		Sekretaris UPA TIK Undiksha
2.	Aset apa saja yang terkait dengan Sekretaris UPA TIK dalam pekerjaan sehari-hari?		
Persyaratan Keamanan			

1.	Apa persyaratan keamanan untuk Sekretaris UPA TIK? (petunjuk: berfokus pada persyaratan apa yang seharusnya ada pada sebuah aset, bukan pada apa yang ada saat ini)	**Kerahasiaan**: sekretaris harus menjaga bahwa informasi dan data sensitive yang dikelola tidak boleh diakses oleh pihak yang tidak berwenang.	**Integritas**: memastikan bahwa informasi yang diakses disimpan pada peralatan teknologi informasi serta server tetap utuh dan akurat.	**Ketersediaan**: akses ke system dann data harus selalu tersedia sesuai dengan kebutuhan operasional. Sekretaris dan staf pendukung harus siap memberikan dukungan teknis kapan saja untuk memastikan kelancaran operasional.	
2	Persyaratan keamanan mana yang paling penting untuk Sekretaris UPA TIK?	Kerahasiaan	Integritas	Ketersediaan	

7. Lembar Kerja Informasi Aset Kritis Untuk SDM; Divisi Infrastruktur, Jaringan & Keamanan

No	Pertanyaan	Jawaban	Narasumber
1.	Mengapa Divisi Infrastruktur, Jaringan, & Keamanan penting bagi organisasi?		Divisi Infrastruktur, Jaringan, & Keamanan
2.	Aset apa saja yang terkait dengan Divisi Infrastruktur, Jaringan & Keamanan?		
Persyaratan Keamanan			

1.	Apa persyaratan keamanan Divisi Infrastruktur, Jaringan & Keamanan? (petunjuk: berfokus pada persyaratan apa yang seharusnya ada pada sebuah aset, bukan pada apa yang ada saat ini)	**Kerahasiaan**: Divisi Infrastruktur, Jaringan & Keamanan harus memastikan bahwa semua akses ke system dan data terbatas hanya kepada pihak yang berwenang.	**Integritas**: Divisi Infrastruktur, Jaingan & Keamanan harus memastikan bahwa sumber daya, termasuk perangkat keras, perankat lunak, dan data yang digunakan dalam operasi tetap utug dan berjalan sebagaimana mestinya.	**Ketersediaan**: siap memberikan dukungan kapan saja dperlukan untuk memecahkan masalah terkait jaringan, server, atau aplikasi yang berjalan.	
2	Persyaratan keamanan mana yang paling penting untuk Divisi Infrastruktur, Jaringan & Keamanan?	Kerahasiaan	Integritas	Ketersediaan	

8. Lembar Kerja Profil Risiko untuk Server – Jalur Akses Jaringan

No	Pertanyaa	Jawaban	Responden
Cabang Aktor/Pelaku Ancaman			
1.	Siapa aktor yang memiliki potensi ancaman terbesar terhadap server melalui akses jaringan? Aktor dapat berasal dari pihak internal atau eksternal. Berikan deskripsi apakah aktor tersebut termasuk ke dalam pihak internal atau eksternal pada jawaban seperti contoh berikut: Staf UPA TIK Undiksha (pihak internal).		Divisi Pusat Data & Informasi

2.	Apakah akses fisik ke ruang server dikendalikan dengan baik dan bagaimana ruang server dikendalikan dari akses fisik?		
3.	Siapa yang bertanggung jawab dalam pengelolaan server dan memiliki akses administratif penuh?		
Cabang Motif Ancaman			
1.	Berdasarkan riwayat insiden dan kemungkinan dimasa depan, apa motif utama yang mungkin dimiliki pelaku dalam menyerang atau mengakses server secara illegal? Motif terdapat 2 kelompok yaitu sengaja dan tidak sengaja.		

	Berikan deskripsi apakah motif tersebut sengaja atau tidak sengaja pada jawaban seperti contoh berikut: Melakukan modifikasi atau sabotase terhadap server (sengaja).		
2.	Seberapa tinggi kemungkinan motif dari pihak internal untuk melakukan serangan terhadap server?		
3.	Seberapa tinggi kemungkinan server akan menjadi target serangan dari pihak eksternal (seperti hacker atau pencuri data)?		

Cabang Jenis Ancaman						
Jika aktor berasal dari pihak internal		**Pengungkapan**	**Modifikasi**	**Kehilangan, kerusakan**	**Gangguan**	
1.	Apa jenis ancaman yang paling mungkin terjadi pada server yang dilakukan oleh pihak internal? Anda bisa memilih lebih dari 1 pilihan jawaban yang disediakan.	Pengungkapan data sensitif oleh pihak internal UPA TIK Undiksha.	Modifikasi data oleh internal UPA TIK Undiksha yang tidak sah dan tidak adanya otorisasi.	Kehilangan data akibat human eror.	Serangan jaringan yang diakibatkan karena internal UPA TIK Undikhsa mengakses server dengan jaringan ilegal.	
Jika aktor berasal dari pihak eksternal						

1.	Apa jenis ancaman yang paling mungkin terjadi pada server yang dilakukan pihak eksternal? Anda bisa memilih lebih dari 1 pilihan jawaban yang disediakan.	Penyusupan oleh hacker atau pihak tidak dikenal	Modifikasi data oleh aktor yang tidak dikena/diketahui	Kehilangan data akibat serangan dari luar/pihak eksternal yang tidak diketahui.	Serangan yang dikirimkan oleh pihak luar yang mengakibatkan server down.	
2.	Berapa kali server mengalami gangguan di masa lalu? Sebutkan dan jelaskan seperti apa gangguannya.					
3.	Seberapa sering melakukan pemeliharaan server untuk mencegah ancaman keamanan? berikan skala seperti contohnya: 1kali perminggu					

9. Lembar Kerja Profil Risiko untuk Server – Jalur Akses Fisik

No	Pertanyaan	Jawaban	Responden
Cabang Aktor/Pelaku Ancaman			Divisi Pusat Data & Informasi
1.	Siapa aktor yang memiliki potensi ancaman terbesar terhadap server melalui akses fisik?		
2.	Apakah akses fisik ke ruang server terbatas pada personil yang berwenang?		
3.	Apakah ada catatan atau log akses fisik ke server?		
Cabang Motif Ancaman			

1.	Apa kemungkinan motif ancaman fisik terhadap server? Motif terdapat 2 kelompok yaitu sengaja dan tidak sengaja. Berikan deskripsi apakah motif tersebut sengaja atau tidak sengaja pada jawaban seperti contoh berikut: Melakukan modifikasi atau sabotase pada server (sengaja).		
2.	Seberapa tinggi kemungkinan motif dari pihak internal untuk melakukan serangan terhadap server?		
3.	Seberapa tinggi kemungkinan server akan menjadi target serangan dari pihak eksternal (seperti vendor atau tamu) yang mengakses ruang server secara fisik?		

Cabang Jenis Ancaman						
Jika aktor berasal dari pihak internal		**Pengungkapan**	**Modifikasi**	**Kehilangan, kerusakan**	**Gangguan**	
1.	Apa ancaman fisik utama yang mungkin terjadi pada server? Anda bisa memilih lebih dari 1 pilihan jawaban yang disediakan.	Publikasi data sensitive oleh internal UPA TIK Undiksha.	Kerusakan akibat sabotase.	Pencurian perangkat keras atau suku cadang.	Kesalahan pegawai dalam penanganan kerusakan server secara fisik	
Jika Aktor berasal dari pihak eksternal						
1.	Apa ancaman fisik utama yang mungkin terjadi pada server?	Publikasi data sensitive oleh eksternal UPA TIK Undiksha	Perubahan yang dilakukan secara tidak sah	Pencurian perangkat keras atau suku cadang.	Bencana alam	
2.	Apakah ruang server dilengkapi dengan sistem keamanan fisik seperti CCTV, kunci elektronik, atau penjaga?					

3.	Seberapa sering pemeliharaan fisik ruang server dilakukan untuk memastikan keamanan? berikan skala seperti contohnya: 1 kali perminggu		
4.	Apakah pernah ada insiden terkait ancaman fisik pada server sebelumnya? Berapa kali terjadi? Dan jelaskan insidennya.		
5.	Apakah pernah ada risiko fisik seperti bencana alam atau kebakaran yang dapat memengaruhi server?		

10. Lembar Kerja Profil Risiko untuk Server – Masalah Sistem

No	Pertanyaa	Jawaban	Responden
Cabang Kerusakan Perangkat lunak			
1.	Bagaimana pengaruh kerusakan perangkat lunak pada server dalam operasional sehari-hari? Jelaskan dampaknya. Jenis dampak: 1) Penyingkapan: Penyingkapan terjadi ketika informasi atau data yang seharusnya dirahasiakan terungkap atau diakses oleh pihak yang tidak berwenang. 2) Modifikasi: Modifikasi adalah perubahan data atau sistem oleh pihak yang tidak berwenang, baik disengaja maupun tidak. Ini dapat mengubah integritas data yang disimpan dalam sistem. 3) Kehilangan, kehancuran: Kehilangan terjadi ketika data atau aset tidak lagi tersedia, baik karena kerusakan fisik (kehancuran) atau kehilangan secara digital. Ini bisa berupa data yang hilang atau rusak tanpa dapat dipulihkan.		Divisi Pusat Data & Informasi

	4) Gangguan: Gangguan terjadi ketika operasional sistem terganggu atau terhenti, sehingga akses ke data atau layanan tidak bisa dilakukan. Ini sering disebabkan oleh masalah jaringan, kegagalan sistem, atau serangan siber.		
2.	Berapa kali dan dalam kurun waktu berapa lama server mengalami gangguan kerusakan perangkat lunak?		
3.	Catatan tambahan apa tentang ancaman kerusakan perangkat lunak pada server yang ingin Anda catat?		
4.	Berikan contoh bagaimana kerusakan perangkat lunak dapat mengancam server.		
Cabang Kegagalan system			

1.	Bagaimana pengaruh kegagalan sistem pada server dalam operasional sehari-hari? Jelaskan dampaknya. Jenis dampak: 1) Penyingkapan: Penyingkapan terjadi ketika informasi atau data yang seharusnya dirahasiakan terungkap atau diakses oleh pihak yang tidak berwenang. 2) Modifikasi: Modifikasi adalah perubahan data atau sistem oleh pihak yang tidak berwenang, baik disengaja maupun tidak. Ini dapat mengubah integritas data yang disimpan dalam sistem. 3) Kehilangan, kehancuran: Kehilangan terjadi ketika data atau aset tidak lagi tersedia, baik karena kerusakan fisik (kehancuran) atau kehilangan secara digital. Ini bisa berupa data yang hilang atau rusak tanpa dapat dipulihkan. 4) Gangguan: Gangguan terjadi ketika operasional sistem terganggu atau terhenti, sehingga akses ke data atau layanan tidak bisa dilakukan. Ini sering disebabkan oleh masalah jaringan, kegagalan sistem, atau serangan siber.		
2.	Berapa kali dan dalam kurun waktu berapa lama server mengalami gangguan kegagalan sistem?		

3.	Catatan tambahan apa tentang ancaman kegagalan sistem pada server yang ingin Anda catat?		
4.	Berikan contoh bagaimana kegagalan sistem dapat mengancam server.		
Cabang Kerusakan perangkat keras			
1.	Bagaimana pengaruh kerusakan perangkat keras pada server dalam operasional sehari-hari? Jelaskan dampaknya. Jenis dampak: 1) Penyingkapan: Penyingkapan terjadi ketika informasi atau data yang seharusnya dirahasiakan terungkap atau diakses oleh pihak yang tidak berwenang. 2) Modifikasi: Modifikasi adalah perubahan data atau sistem oleh pihak yang tidak berwenang, baik disengaja maupun tidak. Ini dapat mengubah integritas data yang disimpan dalam sistem. 3) Kehilangan, kehancuran: Kehilangan terjadi ketika data atau aset tidak lagi tersedia, baik karena kerusakan fisik (kehancuran) atau kehilangan secara digital. Ini bisa berupa data yang hilang atau rusak tanpa dapat dipulihkan.		

	4) Gangguan: Gangguan terjadi ketika operasional sistem terganggu atau terhenti, sehingga akses ke data atau layanan tidak bisa dilakukan. Ini sering disebabkan oleh masalah jaringan, kegagalan sistem, atau serangan siber.		
2.	Berapa kali dan dalam kurun waktu berapa lama server mengalami gangguan kerusakan perangkat keras?		
3.	Catatan tambahan apa tentang ancaman kerusakan perangkat keras pada server yang ingin Anda catat?		
4.	Berikan contoh bagaimana kerusakan perangkat keras dapat mengancam server.		
Cabang Kode berbahaya			
1.	Kode berbahaya seperti apa yang pernah menyerang server dan bagaimana pengaruh kode berbahaya (virus, worm, Trojan horse, back door) pada server dalam operasional sehari-hari? Jelaskan dampaknya. Jenis dampak: 1) Penyingkapan: Penyingkapan terjadi ketika informasi atau data yang seharusnya dirahasiakan terungkap atau diakses oleh pihak yang tidak berwenang.		

	2) Modifikasi: Modifikasi adalah perubahan data atau sistem oleh pihak yang tidak berwenang, baik disengaja maupun tidak. Ini dapat mengubah integritas data yang disimpan dalam sistem. 3) Kehilangan, kehancuran: Kehilangan terjadi ketika data atau aset tidak lagi tersedia, baik karena kerusakan fisik (kehancuran) atau kehilangan secara digital. Ini bisa berupa data yang hilang atau rusak tanpa dapat dipulihkan. 4) Gangguan: Gangguan terjadi ketika operasional sistem terganggu atau terhenti, sehingga akses ke data atau layanan tidak bisa dilakukan. Ini sering disebabkan oleh masalah jaringan, kegagalan sistem, atau serangan siber.		
2.	Berapa kali dan dalam kurun waktu berapa lama server mengalami gangguan serangan kode berbahaya (virus, worm, Trojan horse, back door dll)?		
3.	Catatan tambahan apa tentang ancaman kode berbahaya pada server yang ingin Anda catat?		
4.	Berikan contoh bagaimana kode berbahaya dapat mengancam server.		

11. Lembar Kerja Profil Risiko untuk SOP dan Instruksi Kerja – Jalur Akses Jaringan

No	Pertanyaa	Jawaban	Responden
Cabang Aktor/Pelaku Ancaman			
1.	Siapa yang memiliki akses ke SOP dan Instruksi Kerja melalui akses jaringan? Aktor dapat berasal dari pihak internal atau eksternal. Berikan deskripsi apakah aktor tersebut termasuk ke dalam pihak internal atau eksternal pada jawaban seperti contoh berikut: Staf UPA TIK Undiksha (pihak internal).		Divisi Helpdesk & Dokumentasi

2.	Apakah akses jaringan ke SOP dan Instruksi Kerja dibatasi hanya untuk personil yang berwenang?	Terbatas hanya pada sebagian personil.	Akses terbuka bagi semua pegawai.	Akses tersedia bagi pihak eksternal juga.	
3.	Apakah ada sistem log untuk mencatat akses jaringan ke SOP dan Instruksi Kerja?				
Cabang Motif Ancaman					
1.	Apa kemungkinan motif ancaman melalui akses jaringan terhadap SOP dan Instruksi Kerja? Motif terdapat 2 kelompok yaitu sengaja dan tidak sengaja. Berikan deskripsi apakah motif tersebut sengaja atau tidak sengaja pada jawaban seperti contoh berikut: Melakukan pencurian data untuk kepentingan pihak ketiga (sengaja).				

2.	Seberapa tinggi kemungkinan risiko perubahan atau modifikasi tidak sah pada SOP dan Instruksi Kerja melalui jaringan?					
3.	Seberapa tinggi kemungkinan pihak eksternal (seperti vendor atau tamu) dapat mengakses SOP dan Instruksi Kerja melalui jaringan?					
Cabang Jenis Ancaman						
Jika aktor berasal dari pihak internal		**Pengungkapan**	**Modifikasi**	**Kehilangan, kerusakan**	**Gangguan**	
1.	Apa ancaman jaringan utama yang mungkin terjadi pada SOP dan Instruksi Kerja yang dilakukan oleh pihak internal? Anda bisa memilih lebih dari 1 pilihan jawaban yang disediakan.	Pembocoran SOP dan Instruksi Kerja ke publik oleh pegawai internal secara tidak sah.	Perubahan tidak sah oleh pegawai internal.	Penghapusan data akibat kelalaian.	Kesalahan dalam pemeliharaan sistem.	

Jika aktor berasal dari pihak eksternal.		**Pengungkapan**	**modifikasi**	**Kehilangan, kerusakan**	**Gangguan**	
2.	Apa ancaman jaringan utama yang mungkin terjadi pasa SOP dan Instruksi Kerja yang dilakukan oleh pihak eksternal?	Pengungkapan ke publik oleh pihak eksternal.	Perubahan tanpa otorisasi oleh pihak yang tidak diketahui.	Pencurian data oleh pihak eksternal.	Percobaan mengakses data tersebut.	
2.	Apakah SOP dan Instruksi Kerja dilindungi oleh enkripsi atau kontrol akses jaringan?					
3.	Seberapa sering jaringan yang mengakses SOP dan Instruksi Kerja dipantau untuk mendeteksi ancaman?					
4.	Apakah pernah ada insiden terkait ancaman jaringan terhadap SOP dan Instruksi Kerja sebelumnya? Sebutkan dan jelaskan insiden tersebut.					

12. Lembar Kerja Profil Risiko untuk SOP dan Instruksi Kerja – Jalur Akses Fisik

No	Pertanyaan	Jawaban	Responden
Cabang Aktor/Pelaku Ancaman			**Divisi Helpdesk & Dokumentasi**
1.	Siapa yang memiliki akses fisik ke dokumen SOP dan Instruksi Kerja (misalnya, versi cetak atau file yang disimpan secara lokal)? (penyimpanan dokumen SOP dan Instruksi Kerja di perangkat fisik atau media penyimpanan yang tidak terhubung ke jaringan eksternal atau cloud)		
2.	Apakah akses fisik ke dokumen SOP dan Instruksi Kerja dibatasi hanya untuk personel yang berwenang atau terbuka bagi semua		

	pegawai UPA TIK atau tersedia bagi pihak eksternal juga?		
3.	Apakah ada sistem pencatatan atau log untuk mencatat akses fisik ke dokumen SOP dan Instruksi Kerja?		
Cabang Motif Ancaman			
1.	Apa kemungkinan motif ancaman fisik terhadap dokumen SOP dan Instruksi Kerja? Motif terdapat 2 kelompok yaitu sengaja dan tidak sengaja. Berikan deskripsi apakah motif tersebut sengaja atau tidak sengaja pada jawaban seperti contoh berikut:		

	Melakukan modifikasi atau perubahan dokumen tidak sah (sengaja).					
2.	Seberapa besar risiko perubahan tidak sah pada SOP dan Instruksi Kerja akibat akses fisik?					
3.	Seberapa besar kemungkinan pihak eksternal (seperti vendor atau tamu) dapat mengakses dokumen SOP dan Instruksi Kerja secara fisik?					
Cabang Jenis Ancaman						
Jika aktor berasal dari pihak internal		**Pengungkapan**	**Modifikasi**	**Kehilangan, kerusakan**	**Gangguan**	
1.	Apa ancaman fisik utama yang mungkin terjadi pada dokumen SOP dan Instruksi Kerja?	Mempublikasi dokumen secara tidak sah dan	Perubahan tidak sah oleh pegawai.	Kehilangan atau kerusakan dokumen	Penghapusan yang disengaja.	

	Anda bisa memilih lebih dari 1 pilihan jawaban yang disediakan.	tanpa adanya izin.		akibat kelalaian.		
2.	Apakah dokumen SOP dan Instruksi Kerja disimpan dalam lemari yang terkunci atau di lokasi yang aman secara fisik?					
3.	Seberapa sering pengecekan atau audit fisik dilakukan untuk memastikan keamanan dokumen SOP dan Instruksi Kerja? berikan skala seperti contohnya: 1 kali perminggu					
4.	Apakah pernah ada insiden terkait ancaman fisik terhadap dokumen SOP dan Instruksi Kerja sebelumnya? Berapa kali terjadi? Dan jelaskan insidennya.					

13. Lembar Kerja Profil Risiko untuk SIAK – Jalur Akses Jaringan

No	Pertanyaa	Jawaban	Responden
Cabang Aktor/Pelaku Ancaman			
1.	Siapa aktor yang paling mungkin menimbulkan ancaman terhadap SIAK melalui akses jaringan? Aktor dapat berasal dari pihak internal atau eksternal. Berikan deskripsi apakah aktor tersebut termasuk ke dalam pihak internal atau eksternal pada jawaban seperti contoh berikut: Mahasiswa (pihak eksternal).		Divisi Pusat Data & Informasi
2.	Apakah akses jaringan ke SIAK dikendalikan dengan baik?		

3.	Siapa yang bertanggung jawab dalam mengelola keamanan akses jaringan pada SIAK?		
Cabang Motif Ancaman			
1.	Apa motif utama yang mungkin dimiliki pelaku dalam menyerang atau mengakses SIAK secara illegal melalui jaringan? Motif terdapat 2 kelompok yaitu sengaja dan tidak sengaja. Berikan deskripsi apakah motif tersebut sengaja atau tidak sengaja pada jawaban seperti contoh berikut: Mencuri atau memodifikasi data mahasiswa (sengaja).		

2.	Seberapa tinggi kemungkinan motif dari pihak internal untuk melakukan serangan terhadap SIAK?					
3.	Seberapa tinggi kemungkinan SIAK akan menjadi target serangan dari pihak eksternal (seperti hacker atau pencuri data)?					
Cabang Jenis Ancaman						
Jika aktor berasal dari pihak internal		**Pengungkapan**	**Modifikasi**	**Kehilangan, kerusakan**	**Gangguan**	

1.	Apa jenis ancaman yang paling mungkin terjadi pada SIAK yang dilakukan oleh pihak internal melalui jaringan? Anda bisa memilih lebih dari 1 pilihan jawaban yang disediakan. Berikan penejelasan ancaman seperti: “pengungkapan: pengungkapan/kebocoran data sensitif seperti data mahasiswa oleh pihak internal.”	Pengungkapan / kebocoran data sensitif oleh staf UPA TIK Undiksha.	Modifikasi data oleh staf UPA TIK yang tidak sah dan tidak adanya otorisasi.	Kehilangan data akibat human eror.	Serangan malware atau peretasan.	
Jika aktor berasal dari pihak eksternal						

1.	Apa jenis ancaman yang paling mungkin terjadi pada SIAK yang dilakukan pihak eksternal? Anda bisa memilih lebih dari 1 pilihan jawaban yang disediakan. Berikan penejelasan ancaman seperti: “gangguan: serangan malware atau peretasan.”	Penyusupan oleh hacker atau pihak tidak dikenal	Modifikasi data oleh aktor yang tidak dikena/diketahui	Kehilangan data akibat serangan dari luar/pihak eksternal yang tidak diketahui.	Serangan malware atau peretasan.	
2.	Berapa kali SIAK mengalami gangguan jaringan atau serangan jaringan? Sebutkan dan jelaskan gangguannya.					
3.	Seberapa sering dilakukan pemeliharaan pada SIAK untuk mencegah ancaman keamanan? berikan skala seperti contohnya: 1kali perminggu					

14. Lembar Kerja Profil Risiko untuk SIAK – Jalur Akses Fisik

No	Pertanyaa	Jawaban	Responden
Cabang Aktor/Pelaku Ancaman			
1.	Siapa aktor yang memiliki akses fisik perangkat yang menjadi host SIAK di Universitas Pendidikan Ganesha dan apakah actor tersebut memiliki peluang menjadi ancaman? Aktor dapat berasal dari pihak internal atau eksternal. Berikan deskripsi apakah aktor tersebut termasuk ke dalam pihak internal atau eksternal pada jawaban seperti contoh berikut: Divisi Sistem Informasi (pihak internal).		Divisi Pusat Data & Informasi
2.	Apakah akses jaringan ke SIAK dikendalikan dengan baik?		

3.	Siapa yang bertanggung jawab atas keamanan fisik perangkat yang digunakan divisi sistem informasi (SIAK)?		
Cabang Motif Ancaman			
1.	Apa motif utama yang mungkin ingin mengakses perangkat fisik yang menjalankan SIAK? Motif terdapat 2 kelompok yaitu sengaja dan tidak sengaja. Berikan deskripsi apakah motif tersebut sengaja atau tidak sengaja pada jawaban seperti contoh berikut: Mencuri data (sengaja).		
2.	Seberapa besar kemungkinan adanya ancaman dari aktor internal yang ingin mengakses perangkat yang dimiliki divisi sistem informasi secara fisik?		

3.	Seberapa tinggi kemungkinan SIAK akan menjadi target serangan dari pihak eksternal secara fisik (seperti vendor atau tamu)?					
Cabang Jenis Ancaman						
Jika aktor berasal dari pihak internal		**Pengungkapan**	**Modifikasi**	**Kehilangan, kerusakan**	**Gangguan**	
1.	Apa ancaman yang mungkin terjadi jika ada akses fisik tidak sah dari pihak internal pada perangkat yang dimiliki divisi Sistem Informasi utuk melakukan pekerjaannya? Anda bisa memilih lebih dari 1 pilihan jawaban yang disediakan. Berikan penejelasan ancaman seperti: "kehilangan: pencurian perangkat keras seperti laptop/komputer."	Pengungkapan / kebocoran data sensitif oleh staf UPA TIK Undiksha.	Modifikasi data oleh staf UPA TIK yang tidak sah dan tidak adanya otorisasi.	Kehilangan data akibat human eror.	Serangan malware atau peretasan.	

Jika aktor berasal dari pihak eksternal						
2.	Apa ancaman yang mungkin terjadi jika ada akses fisik tidak sah dari pihak eksternal (seperti vendor atau tamu) atau perangkat yang dimiliki divisi Sistem Informasi? Anda bisa memilih lebih dari 1 pilihan jawaban yang disediakan. Berikan penejelasan ancaman seperti: “gangguan: bencana alam (kebakaran, banjir, gempa)."	Penyusupan oleh hacker atau pihak tidak dikenal	Modifikasi data oleh aktor yang tidak dikena/diketahui	Pencurian perangkat keras atau suku cadang	Bencana alam	
3.	Berapa kali perangkat yang dimiliki divisi dalam mengembangkan sistem mengalami ancaman fisik? Sebutkan dan jelaskan gangguannya.					
4.	Langkah apa yang telah diterapkan untuk mengamankan akses fisik ke perangkat?					

15. Lembar Kerja Profil Risiko untuk SIAK – Masalah Sistem

No	Pertanyaa	Jawaban	Responden
Cabang Kerusakan Perangkat lunak			
1.	Bagaimana pengaruh kerusakan perangkat lunak pada SIAK dalam operasional sehari-hari? Jelaskan dampaknya. Jenis dampak: 1) Penyingkapan: Penyingkapan terjadi ketika informasi atau data yang seharusnya dirahasiakan terungkap atau diakses oleh pihak yang tidak berwenang. 2) Modifikasi: Modifikasi adalah perubahan data atau sistem oleh pihak yang tidak berwenang, baik disengaja maupun tidak. Ini dapat		Divisi Infrastruktur, Jaringan, & Keamanan

	mengubah integritas data yang disimpan dalam sistem. 3) Kehilangan, kehancuran: Kehilangan terjadi ketika data atau aset tidak lagi tersedia, baik karena kerusakan fisik (kehancuran) atau kehilangan secara digital. Ini bisa berupa data yang hilang atau rusak tanpa dapat dipulihkan. 4) Gangguan: Gangguan terjadi ketika operasional sistem terganggu atau terhenti, sehingga akses ke data atau layanan tidak bisa dilakukan. Ini sering disebabkan oleh masalah jaringan, kegagalan sistem, atau serangan siber.		

2.	Berapa kali dan dalam kurun waktu berapa lama SIAK mengalami gangguan kerusakan perangkat lunak?		
3.	Catatan tambahan apa tentang ancaman kerusakan perangkat lunak pada SIAK yang ingin Anda catat?		
4.	Berikan contoh bagaimana kerusakan perangkat lunak dapat mengancam SIAK.		
Cabang Kegagalan sistem			
1.	Bagaimana pengaruh kegagalan sistem pada SIAK dalam operasional sehari-hari? Jelaskan dampaknya. Jenis dampak: 1) Penyingkapan: Penyingkapan terjadi ketika informasi atau data		

	yang seharusnya dirahasiakan terungkap atau diakses oleh pihak yang tidak berwenang. 2) Modifikasi: Modifikasi adalah perubahan data atau sistem oleh pihak yang tidak berwenang, baik disengaja maupun tidak. Ini dapat mengubah integritas data yang disimpan dalam sistem. 3) Kehilangan, kehancuran: Kehilangan terjadi ketika data atau aset tidak lagi tersedia, baik karena kerusakan fisik (kehancuran) atau kehilangan secara digital. Ini bisa berupa data yang hilang atau rusak tanpa dapat dipulihkan. 4) Gangguan: Gangguan terjadi ketika operasional sistem terganggu atau terhenti, sehingga		

	akses ke data atau layanan tidak bisa dilakukan. Ini sering disebabkan oleh masalah jaringan, kegagalan sistem, atau serangan siber.		
2.	Berapa kali dan dalam kurun waktu berapa lama SIAK mengalami gangguan kegagalan sistem?		
3.	Catatan tambahan apa tentang ancaman kegagalan sistem pada SIAK yang ingin Anda catat?		
4.	Berikan contoh bagaimana kegagalan sistem dapat mengancam SIAK.		
Cabang Kerusakan perangkat keras			
1.	Bagaimana pengaruh kerusakan perangkat keras pada SIAK dalam operasional sehari-hari? Jelaskan dampaknya.		

	Jenis dampak: 1) Penyingkapan: Penyingkapan terjadi ketika informasi atau data yang seharusnya dirahasiakan terungkap atau diakses oleh pihak yang tidak berwenang. 2) Modifikasi: Modifikasi adalah perubahan data atau sistem oleh pihak yang tidak berwenang, baik disengaja maupun tidak. Ini dapat mengubah integritas data yang disimpan dalam sistem. 3) Kehilangan, kehancuran: Kehilangan terjadi ketika data atau aset tidak lagi tersedia, baik karena kerusakan fisik (kehancuran) atau kehilangan secara digital. Ini bisa berupa data yang hilang atau rusak tanpa dapat dipulihkan.		

	4) Gangguan: Gangguan terjadi ketika operasional sistem terganggu atau terhenti, sehingga akses ke data atau layanan tidak bisa dilakukan. Ini sering disebabkan oleh masalah jaringan, kegagalan sistem, atau serangan siber.		
2.	Berapa kali dan dalam kurun waktu berapa lama SIAK mengalami gangguan kerusakan perangkat keras?		
3.	Catatan tambahan apa tentang ancaman kerusakan perangkat keras pada SIAK yang ingin Anda catat?		
4.	Berikan contoh bagaimana kerusakan perangkat keras dapat mengancam SIAK.		

Cabang Kode berbahaya			
1.	Kode berbahaya seperti apa yang pernah menyerang atau mengancam SIAK dan bagaimana pengaruh kode berbahaya (virus, worm, Trojan horse, back door) pada SIAK dalam operasional sehari-hari? Jelaskan dampaknya. Jenis dampak: 1) Penyingkapan: Penyingkapan terjadi ketika informasi atau data yang seharusnya dirahasiakan terungkap atau diakses oleh pihak yang tidak berwenang. 2) Modifikasi: Modifikasi adalah perubahan data atau sistem oleh pihak yang tidak berwenang, baik disengaja maupun tidak. Ini dapat		

	mengubah integritas data yang disimpan dalam sistem. 3) Kehilangan, kehancuran: Kehilangan terjadi ketika data atau aset tidak lagi tersedia, baik karena kerusakan fisik (kehancuran) atau kehilangan secara digital. Ini bisa berupa data yang hilang atau rusak tanpa dapat dipulihkan. 4) Gangguan: Gangguan terjadi ketika operasional sistem terganggu atau terhenti, sehingga akses ke data atau layanan tidak bisa dilakukan. Ini sering disebabkan oleh masalah jaringan, kegagalan sistem, atau serangan siber.		

2.	Berapa kali dan dalam kurun waktu berapa lama SIAK mengalami gangguan serangan kode berbahaya (virus, worm, Trojan horse, back door dll)?		
3.	Catatan tambahan apa tentang ancaman kode berbahaya pada SIAK yang ingin Anda catat?		
4.	Berikan contoh bagaimana kode berbahaya dapat mengancam SIAK.		

16. Lembar Kerja Profil Risiko untuk Perangkat Jaringan – Jalur Akses Jaringan

No	Pertanyaa	Jawaban	Responden
Cabang Aktor/Pelaku Ancaman			
1.	Siapa aktor yang paling mungkin menimbulkan ancaman terhadap perangkat jaringan melalui akses jaringan? Aktor dapat berasal dari pihak internal atau eksternal. Berikan deskripsi apakah aktor tersebut termasuk ke dalam pihak internal atau eksternal pada jawaban seperti contoh berikut: Mahasiswa (pihak eksternal).		Divisi Infrastruktur, Jaringan, & Keamanan
2.	Apakah akses ke perangkat jaringan dikendalikan dengan baik?		

3.	Siapa yang bertanggung jawab dalam mengelola dan memelihara keamanan perangkat jaringan?		
Cabang Motif Ancaman			
1.	Apa motif utama yang mungkin dimiliki pelaku dalam menyerang atau mengakses perangkat jaringan secara illegal melalui jaringan? Motif terdapat 2 kelompok yaitu sengaja dan tidak sengaja. Berikan deskripsi apakah motif tersebut sengaja atau tidak sengaja pada jawaban seperti contoh berikut: Melakukan modifikasi pada konfigurasi perangkat (sengaja).		
2.	Seberapa tinggi kemungkinan motif dari pihak internal untuk melakukan serangan terhadap perangkat jaringan?		

3.	Seberapa tinggi kemungkinan perangkat jaringan akan menjadi target serangan dari pihak eksternal (seperti hacker atau pencuri data)?					
Cabang Jenis Ancaman						
Jika aktor berasal dari pihak internal		**Pengungkapan**	**Modifikasi**	**Kehilangan, kerusakan**	**Gangguan**	
1.	Apa jenis ancaman yang paling mungkin terjadi pada perangkat jaringan yang dilakukan oleh pihak internal melalui akses jaringan? Anda bisa memilih lebih dari 1 pilihan jawaban yang disediakan. Berikan penejelasan ancaman seperti: "gangguan: kehilangan konektivitas akibat human error."	Pengungkapan / kebocoran data sensitif oleh staf UPA TIK Undiksha.	Modifikasi data oleh staf UPA TIK yang tidak sah dan tidak adanya otorisasi.	Kehilangan data akibat human eror.	Serangan malware atau peretasan.	
Jika aktor berasal dari pihak eksternal						

2.	Apa jenis ancaman yang paling mungkin terjadi pada perangkat jaringan yang dilakukan pihak eksternal? Anda bisa memilih lebih dari 1 pilihan jawaban yang disediakan. Berikan penejelasan ancaman seperti: "gangguan: penyusupan oleh phak yang tidak dikenal"	Penyusupan oleh hacker atau pihak tidak dikenal untuk mempublikasi data sensitif	Modifikasi data oleh aktor yang tidak dikena/diketahui	Kehilangan data akibat serangan dari luar/pihak eksternal yang tidak diketahui.	Serangan malware atau peretasan.	
3.	Berapa kali perangkat jaringan mengalami gangguan jaringan atau serangan jaringan? Sebutkan dan jelaskan gangguannya.					
4.	Seberapa sering dilakukan pemeliharaan pada peragkat jaringan untuk mencegah ancaman keamanan? berikan skala seperti contohnya: 1kali perminggu					

17. Lembar Kerja Profil Risiko untuk Perangkat Jaringan – Jalur Akses Fisik

No	Pertanyaa	Jawaban	Responden
Cabang Aktor/Pelaku Ancaman			
1.	Siapa aktor yang paling mungkin menimbulkan ancaman terhadap perangkat jaringan melalui akses fisik? Aktor dapat berasal dari pihak internal atau eksternal. Berikan deskripsi apakah aktor tersebut termasuk ke dalam pihak internal atau eksternal pada jawaban seperti contoh berikut: Mahasiswa (pihak eksternal).		Divisi Infrastruktur, Jaringan, & Keamanan

2.	Apakah akses ke ruang server dan perangkat jaringan dikendalikan dengan baik?		
3.	Siapa yang bertanggung jawab dalam mengelola akses fisik ke perangkat jaringan?		
Cabang Motif Ancaman			
1.	Apa motif utama yang mungkin dimiliki pelaku dalam mengakses jalur fisik perangkat jaringan secara ilegal? Motif terdapat 2 kelompok yaitu sengaja dan tidak sengaja. Berikan deskripsi apakah motif tersebut sengaja atau tidak sengaja pada jawaban seperti contoh berikut: Mencuri perangkat keras jaringan (sengaja).		

2.	Seberapa tinggi kemungkinan motif dari pihak internal untuk melakukan serangan terhadap perangkat jaringan melalui akses fisik?					
3.	Seberapa tinggi kemungkinan perangkat jaringan akan menjadi target serangan dari pihak eksternal melalui akses fisik (seperti mencuri perangkat keras jaringan)					
Cabang Jenis Ancaman						
Jika aktor berasal dari pihak internal		**Pengungkapan**	**Modifikasi**	**Kehilangan, kerusakan**	**Gangguan**	
1.	Apa jenis ancaman yang paling mungkin terjadi pada perangkat jaringan yang dilakukan oleh pihak internal melalui akses fisik?	Pengungkapan / kebocoran data sensitif oleh staf UPA TIK Undiksha.	Modifikasi data oleh staf UPA TIK yang tidak sah dan tidak	Kehilangan data akibat human eror.	Serangan malware atau peretasan.	

	Anda bisa memilih lebih dari 1 pilihan jawaban yang disediakan. Berikan penejelasan ancaman seperti: "gangguan: pencurian perangkat keras."		adanya otorisasi.			
Jika aktor berasal dari pihak eksternal						
1.	Apa jenis ancaman yang paling mungkin terjadi pada perangkat jaringan yang dilakukan pihak eksternal melalui akses fisik? Anda bisa memilih lebih dari 1 pilihan jawaban yang disediakan. Berikan penejelasan ancaman seperti: "gangguan: kerusakan akibat bencana alam"	Penyusupan oleh hacker atau pihak tidak dikenal	Modifikasi data oleh aktor yang tidak dikena/diketahui	Pencurian perangkat keras atau suku cadang	Bencana Alam	

18. Lembar Kerja Profil Risiko untuk Perangkat Jaringan – Masalah Sistem

No	Pertanyaa	Jawaban	Responden
Cabang Kerusakan Perangkat lunak			
1.	Bagaimana pengaruh kerusakan perangkat lunak pada perangkat jaringan dalam operasional sehari-hari? Jelaskan dampaknya. Jenis dampak: 1) Penyingkapan: Penyingkapan terjadi ketika informasi atau data yang seharusnya dirahasiakan terungkap atau diakses oleh pihak yang tidak berwenang. 2) Modifikasi: Modifikasi adalah perubahan data atau sistem oleh pihak yang tidak berwenang, baik disengaja maupun tidak. Ini dapat		Divisi Infrastruktur, Jaringan, & Keamanan

	mengubah integritas data yang disimpan dalam sistem. 3) Kehilangan, kehancuran: Kehilangan terjadi ketika data atau aset tidak lagi tersedia, baik karena kerusakan fisik (kehancuran) atau kehilangan secara digital. Ini bisa berupa data yang hilang atau rusak tanpa dapat dipulihkan. 4) Gangguan: Gangguan terjadi ketika operasional sistem terganggu atau terhenti, sehingga akses ke data atau layanan tidak bisa dilakukan. Ini sering disebabkan oleh masalah jaringan, kegagalan sistem, atau serangan siber.		

2.	Berapa kali dan dalam kurun waktu berapa lama perangkat jaringan mengalami gangguan kerusakan perangkat lunak?		
3.	Catatan tambahan apa tentang ancaman kerusakan perangkat lunak pada perangkat jaringan yang ingin Anda catat?		
4.	Berikan contoh bagaimana kerusakan perangkat lunak dapat mengancam perangkat jaringan.		
Cabang Kegagalan sistem			
1.	Bagaimana pengaruh kegagalan sistem pada perangkat jaringan dalam operasional sehari-hari? Jelaskan dampaknya. Jenis dampak:		

	1) Penyingkapan: Penyingkapan terjadi ketika informasi atau data yang seharusnya dirahasiakan terungkap atau diakses oleh pihak yang tidak berwenang. 2) Modifikasi: Modifikasi adalah perubahan data atau sistem oleh pihak yang tidak berwenang, baik disengaja maupun tidak. Ini dapat mengubah integritas data yang disimpan dalam sistem. 3) Kehilangan, kehancuran: Kehilangan terjadi ketika data atau aset tidak lagi tersedia, baik karena kerusakan fisik (kehancuran) atau kehilangan secara digital. Ini bisa berupa data yang hilang atau rusak tanpa dapat dipulihkan.		

	4) Gangguan: Gangguan terjadi ketika operasional sistem terganggu atau terhenti, sehingga akses ke data atau layanan tidak bisa dilakukan. Ini sering disebabkan oleh masalah jaringan, kegagalan sistem, atau serangan siber.		
2.	Berapa kali dan dalam kurun waktu berapa lama perangkat jaringan mengalami gangguan kegagalan sistem?		
3.	Catatan tambahan apa tentang ancaman kegagalan sistem pada perangkat jaringan yang ingin Anda catat?		
4.	Berikan contoh bagaimana kegagalan sistem dapat mengancam perangkat jaringan.		

Cabang Kerusakan perangkat keras			
1.	Bagaimana pengaruh kerusakan perangkat keras pada perangkat jaringan dalam operasional sehari-hari? Jelaskan dampaknya. Jenis dampak: 1) Penyingkapan: Penyingkapan terjadi ketika informasi atau data yang seharusnya dirahasiakan terungkap atau diakses oleh pihak yang tidak berwenang. 2) Modifikasi: Modifikasi adalah perubahan data atau sistem oleh pihak yang tidak berwenang, baik disengaja maupun tidak. Ini dapat mengubah integritas data yang disimpan dalam sistem.		

	3) Kehilangan, kehancuran: Kehilangan terjadi ketika data atau aset tidak lagi tersedia, baik karena kerusakan fisik (kehancuran) atau kehilangan secara digital. Ini bisa berupa data yang hilang atau rusak tanpa dapat dipulihkan. 4) Gangguan: Gangguan terjadi ketika operasional sistem terganggu atau terhenti, sehingga akses ke data atau layanan tidak bisa dilakukan. Ini sering disebabkan oleh masalah jaringan, kegagalan sistem, atau serangan siber.		
2.	Berapa kali dan dalam kurun waktu berapa lama perangkat jaringan mengalami gangguan kerusakan perangkat keras?		

3.	Catatan tambahan apa tentang ancaman kerusakan perangkat keras pada perangkat jaringan yang ingin Anda catat?		
4.	Berikan contoh bagaimana kerusakan perangkat keras dapat mengancam perangkat jaringan.		
Cabang Kode berbahaya			
1.	Kode berbahaya seperti apa yang pernah menyerang atau mengancam perangkat jaringan dan bagaimana pengaruh kode berbahaya (virus, worm, Trojan horse, back door) pada perangkat jaringan dalam operasional sehari-hari? Jelaskan dampaknya. Jenis dampak: 1) Penyingkapan: Penyingkapan terjadi ketika informasi atau data		

	yang seharusnya dirahasiakan terungkap atau diakses oleh pihak yang tidak berwenang. 2) Modifikasi: Modifikasi adalah perubahan data atau sistem oleh pihak yang tidak berwenang, baik disengaja maupun tidak. Ini dapat mengubah integritas data yang disimpan dalam sistem. 3) Kehilangan, kehancuran: Kehilangan terjadi ketika data atau aset tidak lagi tersedia, baik karena kerusakan fisik (kehancuran) atau kehilangan secara digital. Ini bisa berupa data yang hilang atau rusak tanpa dapat dipulihkan. 4) Gangguan: Gangguan terjadi ketika operasional sistem terganggu atau terhenti, sehingga		

	akses ke data atau layanan tidak bisa dilakukan. Ini sering disebabkan oleh masalah jaringan, kegagalan sistem, atau serangan siber.		
2.	Berapa kali dan dalam kurun waktu berapa lama perangkat jaringan mengalami gangguan serangan kode berbahaya (virus, worm, Trojan horse, back door dll)?		
3.	Catatan tambahan apa tentang ancaman kode berbahaya pada perangkat jaringan yang ingin Anda catat?		
4.	Berikan contoh bagaimana kode berbahaya dapat mengancam perangkat jaringan.		

19. Lembar Kerja Profil Risiko untuk SDM – Sekretaris UPA TIK

No	Pertanyaa	Jawaban	Responden
Cabang Pengambilan Cuti Sementara (misalnya karena sakit/ada kegiatan penting diluar organisasi) oleh Sekretaris			
1.	Bagaimana pengaruh pengambilan cuti sementara (misalnya sakit atau kegiatan penting diluar organisasi) oleh sekretaris UPA TIK terhadap kelancaran operasional harian? Jelaskan dampaknya. Jenis dampak: 1) Penyingkapan: Penyingkapan terjadi ketika informasi atau data yang seharusnya dirahasiakan terungkap atau diakses oleh pihak yang tidak berwenang. 2) Modifikasi: Modifikasi adalah perubahan data atau sistem oleh		Divisi Infrastruktur, Jaringan, & Keamanan

	pihak yang tidak berwenang, baik disengaja maupun tidak. Ini dapat mengubah integritas data yang disimpan dalam sistem. 3) Kehilangan, kehancuran: Kehilangan terjadi ketika data atau aset tidak lagi tersedia, baik karena kerusakan fisik (kehancuran) atau kehilangan secara digital. Ini bisa berupa data yang hilang atau rusak tanpa dapat dipulihkan. 4) Gangguan: Gangguan terjadi ketika operasional sistem terganggu atau terhenti, sehingga akses ke data atau layanan tidak bisa dilakukan. Ini sering disebabkan oleh masalah jaringan, kegagalan sistem, atau serangan siber.		

	Berikan jawaban jenis dampak yang terjadi dan jelaskan seperti apa dampaknya.		
2.	Seberapa sering sekretaris UPA TIK mengambil cuti sementara, dan bagaimana hal ini bisa mempengaruhi tugas administrasinya?		
Cabang Meninggalkan Organisasi Secara Permanen (misalnya pensiun atau pindah kerja) oleh Sekretaris			
1.	Apa dampak jika sekretaris UPA TIK meninggalkan organisasi secara permanen (misalnya pensiun atau pindah kerja)? Jelaskan dampaknya pada operasional dan kelancaran administrasi. Jenis dampak: 1) Penyingkapan: Penyingkapan terjadi ketika informasi atau data yang seharusnya dirahasiakan		

	terungkap atau diakses oleh pihak yang tidak berwenang. 2) Modifikasi: Modifikasi adalah perubahan data atau sistem oleh pihak yang tidak berwenang, baik disengaja maupun tidak. Ini dapat mengubah integritas data yang disimpan dalam sistem. 3) Kehilangan, kehancuran: Kehilangan terjadi ketika data atau aset tidak lagi tersedia, baik karena kerusakan fisik (kehancuran) atau kehilangan secara digital. Ini bisa berupa data yang hilang atau rusak tanpa dapat dipulihkan. 4) Gangguan: Gangguan terjadi ketika operasional sistem terganggu atau terhenti, sehingga akses ke data atau layanan tidak		

	bisa dilakukan. Ini sering disebabkan oleh masalah jaringan, kegagalan sistem, atau serangan siber. Berikan jawaban jenis dampak yang terjadi dan jelaskan seperti apa dampaknya.		
2.	Seberapa sering terjadi pergantian sekretaris UPA TIK, dan bagaimana organisasi menangani kehilangan personel tersebut?		
Cabang Ancaman yang Mempengaruhi pihak ketiga atau penyedia layanan.			

1.	Bagaimana ancaman terhadap pihak ketiga berdampak pada kinerja sekretaris? Jelaskan. Jenis dampak: 1) Penyingkapan: Penyingkapan terjadi ketika informasi atau data yang seharusnya dirahasiakan terungkap atau diakses oleh pihak yang tidak berwenang. 2) Modifikasi: Modifikasi adalah perubahan data atau sistem oleh pihak yang tidak berwenang, baik disengaja maupun tidak. Ini dapat mengubah integritas data yang disimpan dalam sistem. 3) Kehilangan, kehancuran: Kehilangan terjadi ketika data atau aset tidak lagi tersedia, baik karena kerusakan fisik (kehancuran) atau		

	kehilangan secara digital. Ini bisa berupa data yang hilang atau rusak tanpa dapat dipulihkan. 4) Gangguan: Gangguan terjadi ketika operasional sistem terganggu atau terhenti, sehingga akses ke data atau layanan tidak bisa dilakukan. Ini sering disebabkan oleh masalah jaringan, kegagalan sistem, atau serangan siber. Berikan jawaban jenis dampak yang terjadi dan jelaskan seperti apa dampaknya.		
2.	Seberapa sering ancaman terhadap pihak ketiga terjadi, dan bagaimana dampaknya pada tugas sekretaris?		

20. Lembar Kerja Profil Risiko untuk SDM – Divisi Infrastruktur, Jaringan & Keamanan

No	Pertanyaa	Jawaban	Responden
Cabang Pengambilan Cuti Sementara (misalnya karena sakit/ada kegiatan penting dilar organisasi) oleh Staf Divisi Infrastruktur, Jaringan, & Keamanan			
1.	Bagaimana pengaruh pengambilan cuti sementara oleh staf Divisi Infrastruktur, Jaringan, & Keamanan terhadap kelancaran operasional harian? Jelaskan dampaknya. Jenis dampak: 1) Penyingkapan: Penyingkapan terjadi ketika informasi atau data yang seharusnya dirahasiakan terungkap atau diakses oleh pihak yang tidak berwenang. 2) Modifikasi: Modifikasi adalah perubahan data atau sistem oleh pihak yang tidak berwenang, baik		Divisi Infrastruktur, Jaringan, & Keamanan

	disengaja maupun tidak. Ini dapat mengubah integritas data yang disimpan dalam sistem. 3) Kehilangan, kehancuran: Kehilangan terjadi ketika data atau aset tidak lagi tersedia, baik karena kerusakan fisik (kehancuran) atau kehilangan secara digital. Ini bisa berupa data yang hilang atau rusak tanpa dapat dipulihkan. 4) Gangguan: Gangguan terjadi ketika operasional sistem terganggu atau terhenti, sehingga akses ke data atau layanan tidak bisa dilakukan. Ini sering disebabkan oleh masalah jaringan, kegagalan sistem, atau serangan siber.		

	Berikan jawaban jenis dampak yang terjadi dan jelaskan seperti apa dampaknya.		
2.	Seberapa sering staf Divisi Infrastruktur, Jaringan, & Keamanan mengambil cuti sementara, dan bagaimana hal ini bisa mempengaruhi tugas administrasinya?		
Cabang Meninggalkan Organisasi Secara Permanen (misalnya pensiun atau pindah kerja) oleh Staf Divisi Infrastruktur, Jaringan, & Keamanan			
1.	Apa dampak jika staf Divisi Infrastruktur, Jaringan, & Keamanan meninggalkan organisasi secara permanen? Jelaskan dampaknya pada operasional dan kelancaran administrasi. Jenis dampak:		

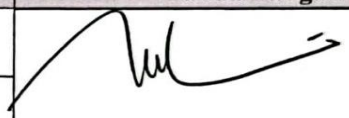
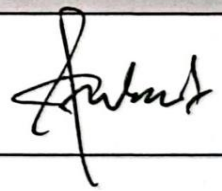
	1) Penyingkapan: Penyingkapan terjadi ketika informasi atau data yang seharusnya dirahasiakan terungkap atau diakses oleh pihak yang tidak berwenang. 2) Modifikasi: Modifikasi adalah perubahan data atau sistem oleh pihak yang tidak berwenang, baik disengaja maupun tidak. Ini dapat mengubah integritas data yang disimpan dalam sistem. 3) Kehilangan, kehancuran: Kehilangan terjadi ketika data atau aset tidak lagi tersedia, baik karena kerusakan fisik (kehancuran) atau kehilangan secara digital. Ini bisa berupa data yang hilang atau rusak tanpa dapat dipulihkan.		

	4) Gangguan: Gangguan terjadi ketika operasional sistem terganggu atau terhenti, sehingga akses ke data atau layanan tidak bisa dilakukan. Ini sering disebabkan oleh masalah jaringan, kegagalan sistem, atau serangan siber. Berikan jawaban jenis dampak yang terjadi dan jelaskan seperti apa dampaknya.		
2.	Seberapa sering terjadi pergantian staf divisi ini, dan bagaimana dampaknya pada operasional?		
Cabang Ancaman yang Mempengaruhi pihak ketiga atau penyedia layanan.			
1.	Bagaimana ancaman terhadap pihak ketiga (misalnya vendor) berdampak		

	pada layanan yang diberikan kepada divisi ini? Jelaskan. Jenis dampak: 1) Penyingkapan: Penyingkapan terjadi ketika informasi atau data yang seharusnya dirahasiakan terungkap atau diakses oleh pihak yang tidak berwenang. 2) Modifikasi: Modifikasi adalah perubahan data atau sistem oleh pihak yang tidak berwenang, baik disengaja maupun tidak. Ini dapat mengubah integritas data yang disimpan dalam sistem. 3) Kehilangan, kehancuran: Kehilangan terjadi ketika data atau aset tidak lagi tersedia, baik karena kerusakan fisik (kehancuran) atau kehilangan secara digital. Ini bisa		

	berupa data yang hilang atau rusak tanpa dapat dipulihkan. 4) Gangguan: Gangguan terjadi ketika operasional sistem terganggu atau terhenti, sehingga akses ke data atau layanan tidak bisa dilakukan. Ini sering disebabkan oleh masalah jaringan, kegagalan sistem, atau serangan siber. Berikan jawaban jenis dampak yang terjadi dan jelaskan seperti apa dampaknya.		
2.	Seberapa sering ancaman terhadap pihak ketiga terjadi, dan bagaimana dampaknya terhadap operasional divisi?		

Lampiran 9. Hasil Kuesioner Lembar Kerja OCTAVE-S Tahap Ke-1

INFORMASI PELAKSANAAN PENGISIAN KUESIONER TAHAP KE-1 LEMBAR KERJA OCTAVE-S PENELITIAN PADA UPA TIK UNDIKSHA			
Peneliti	:	Hardiyanti Rohmania	
Hari, Tanggal	:	Rabu, 11 September 2024.	
Lokasi	:	UPA TIK Undiksha	
INFORMASI RESPONDEN 1			**Tanda Tangan**
Nama:	:	Ida Komang Widiarsana	
Jabatan	:	Sekretaris UPA TIK Undiksha.	
INFORMASI RESPONDEN 2			
Nama:	:	Kadek Surya Mahedy	
Jabatan	:	~~Kepala Divisi~~/Anggota Divisi Pusat Data & Informasi UPA TIK Undiksha.	
INFORMASI RESPONDEN 3			
Nama:	:	I Ketut Parwata	
Jabatan	:	~~Kepala Divisi~~/Anggota Divisi Infrastruktur, Jaringan, & Keamanan UPA TIK Undiksha.	

**Pada bagian jabatan, coret bagian yang tidak diperlukan*

Responses cannot be edited

Kuesioner OCTAVE-S Tahap ke-1

Salam Harmoni,

Tujuan dari kuesioner ini adalah untuk mengumpulkan informasi. Informasi yang Anda berikan akan membantu saya dalam mengevaluasi efektivitas serta menentukan area yang perlu perbaikan lebih lanjut. Saya mengharapkan kejujuran dan keterbukaan Anda dalam menjawab setiap pertanyaan. Semua jawaban akan dijaga kerahasiaannya dan hanya digunakan untuk keperluan penelitian saya yang berjudul "**ANALISIS MANAJEMEN RISIKO KEAMANAN INFORMASI MENGGUNAKAN *FRAMEWORK* OCTAVE-S DAN ISO 27001:2022.**"

* Indicates required question

Nama *

Ida Komang Widhiarjaya

NIP *

198108032006041002

Instansi *

UPA TIK Undiksha.

Jabatan *

Sekretaris UPA TIK Undiksha.

Evaluasi Kriteria Dampak

Reputasi *

Jika terjadi insiden pada aset kritis yang dimiliki UPA TIK, apakah hal itu bisa memengaruhi reputasi UPA TIK?

- ○ Tidak terlalu berpengaruh
- ◉ Ada sedikit dampaknya, tapi masih bisa diperbaiki.
- ○ Pengaruhnya besar dan sulit memulihkan reputasi organisasi.

Kehilangan Aset *

Jika aset kritis hilang atau tidak tersedia, apa dampaknya pada pekerjaan?

- ○ Pekerjaan tetap bisa berjalan seperti biasa.
- ○ Ada sedikit gangguan, tapi masih bisa disiasati.
- ◉ Pekerjaan akan sangat terganggu dan sulit dilanjutkan.

Keuangan *

Jika terjadi insiden pada aset kritis, bagaimana dampaknya pada biaya operasional perusahaan?

- ○ Tidak ada peningkatan biaya, semuanya tetap normal.
- ○ Ada sedikit peningkatan biaya, tapi masih bisa ditangani.
- ◉ Biaya naik cukup banyak, UPA TIK Undiksha harus melakukan penyesuaian besar.

Produktivitas *

Jika terjadi insiden pasa aset kritis, apakah memengaruhi pekerjaan sehari-hari?

- ○ Pekerjaan tetap berjalan seperti biasa.
- ○ Ada beberapa gangguan, tapi pekerjaan masih bisa diselesaikan.
- ◉ Pekerjaan sangat terganggu dan banyak yang tidak bisa dilakukan.

Kesehatan/Keselamatan Pegawai *

Jika terjadi suatu masalah peralatan atau sistem jaringan yang Anda tangani, bagaimana dampaknya terhadap kesehatan atau keselamatan?

- ○ Tidak ada risiko kesehatan atau keselamatan.
- ◉ Ada beberapa risiko, tapi bisa diatasi dengan penanganan medis sederhana.
- ○ Risiko serius yang dapat mengancam kesehatan atau keselamatan pegawai.

Identifikasi Aset

Sistem *

Sistem apa yang memiliki status kritis pada UPA TIK Undiksha?

Server

Informasi *

Informasi apa yang dibutuhkan orang-orang di UPA TIK untuk melakukan tugas mereka? (misalnya, SOP, Kebijakan, dll)

SOP, Instruksi Kerja

Aplikasi/Layanan *

Aplikasi apa yang digunakan oleh UPA TIK untuk mendukung aset penting di UPA TIK?

siaka

Aset Lainnya *

Aset lain apa yang berhubungan dengan aset penting?

Perangkat Jaringan

Smber Daya Manusia *

Siapa staf/divisi kunci yang berperan penting dalam menjaga aset tersebut?

Sekretaris, Divisi jaringan dan infrastruktur

Keterampilan *

Apa keahlian atau pengetahuan khusus yang dimiliki staf/divisini ini?

Jaringan, Pemrograman

Sistem Terkait *

Sistem apa yang gunakan oleh staf/divisi ini untuk bekerja?

OS Windows, Linux, Tool Pemrograman

Aset Terkait *

Aset apa saja yang digunakan oleh staf/divisi ini dalam pekerjaannya?

Komputer, Laptop

Praktik Keamanan

Strategi Keamanan.

Seberapa sering keamanan dipertimbangkan dalam perencanaan strategi bisnis di UPA TIK? *

- (●) Sangat Sering
- ( ) Cukup Sering
- ( ) Tidak Pernah
- ( ) Tidak Tahu

Seberapa baik strateg dan kebijakan keamanan di UPA TIK sudah mendukung tujuan UPA TIK? *

- ( ) Sangat Baik
- (●) Cukup Baik
- ( ) Tidak Baik Sama Sekali
- ( ) Tidak Tahu

Seberapa sering strategi, tujuan, dan kebijakan keamanan didokumentasikan, diperbarui dan disosialisasikan kepada staf di UPA TIK? *

- (●) Sangat Sering
- ( ) Cukup Sering
- ( ) Tidak Pernah
- ( ) Tidak Tahu

Apa yang saat ini sudah dilakukan dengan baik oleh UPA TIK terkait bidang Strategi Keamanan? *

Tulis apa saja yang sudah dilakukan terkait dengan strategi keamanan, misalnya "UPA TIK secara berkala memperbarui kebijakan keamanan dan menyelaraskannya dengan tujuan bisnis."

Update versi teknologi, pemantauan setiap hari

Apa yang saat ini tidak dilakukan dengan baik pada bidang strategi keamanan? *

Tulis kekurangan yang ada, seperti "UPA TIK belum mengintegrasikan kebijakan keamanan ke dalam semua proyek bisnis."

kekurangan SDM, dan teknologi

Seberapa Efektif UPA TIK menerapkan strategi keamanan di UPA TIK? *

- ( ) Sangat tidak efektif, banyak masalah yang perlu diperbaiki.
- (●) Cukup efektif, namun masih ada ruang untuk perbaikan.
- ( ) Sangat efektif, semua berjalan sesuai harapan.
- ( ) Praktik ini tidak relevan atau tidak diterapkan

Praktik Keamanan

Manajemen Keamanan

Apakah UPA TIK selalu menyediakan dana yang cukup untuk kegiatan keamanan informasi? *

- ○ Ya, dana selalu cukup dan tersedia.
- ◉ Kadang-kadang dana tersedia, tapi belum cukup.
- ○ Dana tidak disediakan sama sekali.
- ○ Saya tidak tahu tentang alokasi ini.

Apakah peran dan tanggung jawab keamanan sudah ditetapkan untuk semua staf dalam organisasi? *

- ○ Ya, peran dan tanggung jawab keamanan sudah ditetapkan untuk semua staf.
- ◉ Peran dan yanggung jawab hanya ditetapkan untuk beberapa staf.
- ○ Peran dan tanggung jawab belum ditetapkan sama sekali.
- ○ Saya tidak tahu apakah peran dan tanggung jawab keamanan sudah ditetapkan.

Seberapa baik staf memahami peran mereka dalam menjaga keamanan informasi? *

- ◉ Semua staf sangat paham melaksanakan tanggung jawab mereka.
- ○ Bebera astaf paham, tetapi masih ada yang belum paham.
- ○ Hampir semua staf tidak memahami peran mereka.
- ○ Saya tidak tahu bagaimana pemahaman staf soal ini.

Seberapa baik prosedur pengawasan untuk melindungi informasi sensitif diterapkan di UPA TIK? *

- ◉ Prosedur pengawasan diterapkan dengan sangat baik.
- ○ Prosedur pengawasan kadang-kadang diterapkan, tapi belum konsisten.
- ○ Prosedur pengawasan hampir tidak pernah diterapkan.
- ○ Saya tidak tahu tentang adanya prosedur ini.

Seberapa sering organisasi memperhatikan keamanann informasi saat mereka merekrut dan melatih staf? *

- (●) Keamanan informasi selalu dipertimbangkan.
- ( ) Kadang-kadang dipertimbangkan, tetapi tidak selalu.
- ( ) Hampir tidak pernah dipertimbangkan.
- ( ) Saya tidak tahu apakah keamanan informasi dipertimbangkan.

Seberapa sering UPA TIK melakukan penilaian dan pengelolaan risiko terkait keamanan informasi? *

- (●) Organisasi secara rutin melakukan penilaian risiko.
- ( ) Organisasi melakukan penilaian risiko sesekali saja.
- ( ) Organisasi hampir tidak pernah melakukan penilaian risiko.
- ( ) Saya tidak tahu tentang kegiatan penilaian risiko.

Apakah laporan insiden keamanan informasi selalu ditinjaklanjuti oleh manajemen? (misalnua, audit, log, penilaian risiko dan kerentanan). *

- (●) Laporan selalu diterima dan segera ditinjaklanjuti.
- ( ) Laporan kadang-kadang diterima, tapi tidak selalu ditindaklanjuti.
- ( ) Laporan jarag ditinjaklanjuti atau bahkan tidak pernah diterima.
- ( ) Saya tidak tahu bagaimana laporan insiden diproses.

Apa yang saat ini sudah dilakukan oleh UPA TIK pada bidang manajemen keamanan ini? *

Berikan contoh apa yang sudah dilakukan dengan baik pada bidang ini.

pelatihan keamanan SI/TI, manajemen resiko secara rutin dilakukan

Apa yang saat ini tidak dilakukan dengan baik pada bidang manajemen keamanan ini? *

Sebutkan hal-hal yang masih kurang atau perlu diperbaiki dalam manajemen keamanan ini (seperti belum tersedianya kebijakan atau prosedur).

pengadaan insfrastruktur terbatas

Seberapa efektif UPA TIK menerapkan praktik-praktik di bidang manajemen keamanan ini? *

- ○ Sangat tidak efektif, banyak masalah yang perlu diperbaiki.
- ◉ Cukup efektif, namun masih ada ruang untuk perbaikan.
- ○ Sangat efektif, semua berjalan sesuai harapan.
- ○ Praktik ini tidak relevan atau tidak diterapkan.

Praktik Keamanan

Manajemen Keamanan Kolaboratif

Seberapa efektif kebijakan organisasi dalam melindungi informasi saat bekerja dengan pihak eksternal termasuk pemahaman kebijakannya dan memutus akses informasi ke eksternal yang diberhentikan? *

- ○ Kebijakan sangat komprehensif dan efektif.
- ◉ Kebijakan efektif hanya di beberapa area.
- ○ Kebijakan tidak ada.
- ○ Tidak tahu informasi mengenai hal itu atau tidak relevan dengan UPA TIK Undiksha.

Sejauh mana UPA TIK Unidksha mendokumentasikan persyaratan perlindungan informasi dan secara eksplisit mengkomunikasikannya kepada semua pihak ketiga yang sesuai? *

- ○ Dokumentasi dan komunikasi dilakukan dengan sangat baik dan jelas.
- ◉ Dokumentasi dan komunikasi masih kurang efektif dan perlu ditingkatkan
- ○ Tidak ada dokumentasi dan komunikasi.
- ○ Tidak ada informasi mengenai dokumentasi dan komunikasi ini. Tidak relevan dengan kondisi UPA TIK Undiksha.

Seberapa baik UPA TIK dalam memverifikasi keamanan pihak eksternal, layanan, dan teknologi? *

- ○ Verifikasi dilakukan secara menyeluruh dan detail.
- ◉ Verifikasi tidak konsisten atau kurang mendalam.
- ○ Tidak ada verifikasi keamanan.
- ○ Tidak relevan dengan kondisi UPA TIK Undiksha.

Bagaimana efektivitas kebijakan kolaborasi keamanan dengan pihak eksternal? *

- ○ Kebijakan diterapkan dengan sangat baik.
- ◉ Kebijakan ada, tapi tidak sepenuhnya diterapkan atau tidak konsisten.
- ○ Tidak ada kebijakan kolaborasi keamanan.
- ○ Tidak relevan dengan kondisi UPA TIK Undiksha.

*

Apa yang saat ini sudah dilakukan dengan baik oleh UPA TIK dalam menerapkan Manajemen Keamanan Kolaboratif?

Berikan contoh apa yang sudah dilakukan dengan baik pada bidang ini.

kerjasama dengan BSSN

*

Apa yang saat ini tidak dilakukan dengan baik oleh UPA TIK dalam menerapkan manajemen keamanan kolaboratif?

Sebutkan hal-hal yang masih kurang atau perlu diperbaiki dalam manajemen keamanan ini.

perlu dilakukan audit keamanan secara rutin

Seberapa efektif penerapan praktik keamanan kolaboratif oleh UPA TIK? *

- ○ Sangat tidak efektif, banyak masalah yang perlu diperbaiki.
- ◉ Cukup efektif, namun masih ada ruang untuk perbaikan.
- ○ Sangat efektif, semua berjalan sesuai harapan.
- ○ Praktik ini tidak relevan atau tidak diterapkan.

Responses cannot be edited

Kuesioner OCTAVE-S Tahap ke-1

Salam Harmoni,
Tujuan dari kuesioner ini adalah untuk mengumpulkan informasi. Informasi yang Anda berikan akan membantu saya dalam mengevaluasi efektivitas serta menentukan area yang perlu perbaikan lebih lanjut. Saya mengharapkan kejujuran dan keterbukaan Anda dalam menjawab setiap pertanyaan. Semua jawaban akan dijaga kerahasiaannya dan hanya digunakan untuk keperluan penelitian saya yang berjudul "**ANALISIS MANAJEMEN RISIKO KEAMANAN INFORMASI MENGGUNAKAN *FRAMEWORK* OCTAVE-S DAN ISO 27001:2022.**"

* Indicates required question

Nama *

Kadek Surya Mahedy

NIP *

198301132005011001

Instansi *

UPA TIK Undiksha.

Jabatan *

Anggota Divisi Pusat Data & Informasi.

Praktik Keamanan

Pemantauan dan Audit Keamanan TI

Seberapa sering organisasi Anda menggunakan alat-alat pemantauan dan audit sistem serta jaringan secara rutin? Apakah aktivitas yang tidak biasa ditangani sesuai dengan kebijakan atau prosedur yang berlaku? *

- ○ Alat-alat pemantauan dan audit selalu diguakan dengan konsisten dan sesuai prosedur.
- ◉ Sebagian besar alat digunakan secara rutin, tetapi ada pengecualian.
- ○ Alat-alat tersebut jarang atau tidak pernah digunakan.
- ○ Saya tidak tahu apakah alat-alat ini digunakan secara rutin atau tidak.

Seberapa sering firewall dan komponen keamanan lainnya diaudit untuk memastikan kepatuhan terhadap kebijakan? *

- ○ Firewall dan komponen keamanan lainnya diaudit secara berkala.
- ◉ Audit dilakukan, tetapi tidak selalu konsisten.
- ○ Audit jarang atau tidak pernah dilakukan.
- ○ Saya tidak tahu apakah audit tersebut dilakukan atau tidak.

Apa saja yang dilakukan dengan baik oleh UPA TIK saat ini dalam pemantauan dan audit keamanan TI? *

Jawablah secara rinci tindakan atau praktik yang menurut Anda sudah baik dalam pelaksanaan pemantauan dan audit keamanan TI oleh UPA TIK Undiksha.

Audit kemanan sistem informasi dilakukan mulai dari scaning sistem secara berkala untuk memastikan sistem dapat berjalan dengan baik dan bebas dari kerentaan. hasil scan akan dilakukan tindakan pencegahan jangka pendek dan pencegahan jangka panjang. pencegahan jangka pendek biasanya dilakukan pembersihan file-file yang rentan terhadap serangan cyber. pencegahan jangka panjang dilakukan dengan menambah kemanan sistem baik dari sisi hardware ataupun dari sisi perangkat lunak.

Apa yang tidak dilakukan dengan baik oleh UPA TIK dalam pemantauan dan audit keamanan TI? *

Jawablah secara rinci hal-hal atau area yang menurut Anda masih kurang atau belum optimal dalam pelaksanaan pemantauan dan audit keamanan TI oleh UPA TIK.

audit atau pemantauan sistem dilakukan saat terjadi serangan atau pada saat terjadi kerentanan sistem, audit keamanan sistem tidak dimulai dari penerapan manajemen resiko. sehingga penanganan kerentanan sering diantisipasi dengan pencegahan jangka pendek.

Seberapa efektif menurut Anda UPA TIK dalam menerapkan praktik-praktik manajemen sistem dan jaringan? *

- ○ Sangat tidak efektif, banyak masalah yang perlu diperbaiki.
- ◉ Cukup efektif, namun masih ada ruang untuk perbaikan.
- ○ Sangat efektif, semua berjalan sesuai harapan.
- ○ Praktik ini tidak relevan atau tidak diterapkan.

Praktik Keamanan

Enkripsi

Seberapa baik kontrol keamanan, seperti enkripsi data dan teknologi jaringan pribadi virtual, diterapkan untuk melindungi informasi sensitif saat disimpan dan selama transmisi? *

- ◉ Kontrol keamanan diterapkan secara menyeluruh.
- ○ Kontrol keamanan diterapkan, tetapi ada beberapa area yang belum sepenuhnya diterapkan.
- ○ Kontrol keamanan tidak diterapkan.
- ○ Tidak yakin mengenai penerapan kontrol keamanan.

Seberapa sering protokol terenkripsi digunakan saat mengelola sistem, router, dan firewall dari jarak jauh? *

- (●) Protokol terenkripsi selalu digunakan.
- ( ) Protokol terenkripsi sering digunakan, tetapi tidak selalu.
- ( ) Protokol terenkripsi tidak pernah digunakan.
- ( ) Tidak tahu tentang penggunaan protokol terenkripsi.

*

Apa yang sudah dilakukan dengan baik oleh UPA TIK dalam praktik keamanan enkripsi?

Berikan jawaban dalam bentuk paragraf singkat misalnya, UPA TIK Undiksha secara rutin menggunakan enkripsi end-to-end untuk semua data sensitif.

UPA TIK secara rutin sudah menerapkan pengaman user dan password secara end to end, termasuk juga akses ke API sudah menggunakan token dan setiap aplikasi sudah disedikan fitur log pengguna.

*

Apa yang tidak dilakukan dengan baikoleh UPA TIK Undiksha dalam praktik keamanan enkripsi?

Berikan jawaban dalam bentuk paragraf singkat misalnya, Proses enkripsi data tidak diterapkan secara konsisten di seluruh sistem.

Perlu menerapkan OTP (One time password) untuk beberapa aplikasi seperti penginputan nilai oleh dosen pengajar matakuliah, atau sistem-sistem yang dianggap perlu menerapkan OTP

Seberapa efektif penerapan praktik enkripsi oleh UPA TIK Undiksha? *

- ( ) Sangat tidak efektif, banyak masalah yang perlu diperbaiki.
- ( ) Cukup efektif, namun masih ada ruang untuk perbaikan.
- (●) Sangat efektif, semua berjalan sesuai harapan.
- ( ) Praktik ini tidak relevan atau tidak diterapkan.

Submitted 9/11/24, 9:30 AM

Responses cannot be edited

Kuesioner OCTAVE-S Tahap ke-1

Salam Harmoni,
Tujuan dari kuesioner ini adalah untuk mengumpulkan informasi. Informasi yang Anda berikan akan membantu saya dalam mengevaluasi efektivitas serta menentukan area yang perlu perbaikan lebih lanjut. Saya mengharapkan kejujuran dan keterbukaan Anda dalam menjawab setiap pertanyaan. Semua jawaban akan dijaga kerahasiaannya dan hanya digunakan untuk keperluan penelitian saya yang berjudul "**ANALISIS MANAJEMEN RISIKO KEAMANAN INFORMASI MENGGUNAKAN *FRAMEWORK* OCTAVE-S DAN ISO 27001:2022.**"

* Indicates required question

Nama *

I Ketut Parwata

NIP *

198106122002121003

Instansi. *

UPA TIK Undiksha.

Jabatan *

Anggota Divisi Infrastruktur, Jaringan, & Keamanan.

Praktik Keamanan

Kesadaran dan Pelatihan Keamanan

Seberapa baik staf di UPA TIK memahami peran dan tanggung jawab mereka terkait keamanan? *

Hal ini didokumentasikan dan diverifikasi.

- (●) Sangat Baik
- ( ) Cukup Baik
- ( ) Tidak Baik
- ( ) Tidak Tahu

Seberapa baik layanan, mekanisme, dan teknologi yang digunakan di UPA TIK didokumentasikan dan diperiksa untuk keamanan? *

Hal ini di dokumentasikan dan diverifikasi.

- (●) Sangat Baik
- ( ) Cukup Baik
- ( ) Tidak Baik
- ( ) Tidak Tahu

Seberapa sering keamanan, pelatihan, dan pengingat/pemberitahuan rutin diberikan kepada staf untuk membantu mereka tetap ingat dan patuh terhadap prosedur keamanan yang telah ditetapkan? *

Pemahaman staf didokumentasikan dan kesesuaiannya diverifikasi.

- (●) Sangat Sering
- ( ) Cukup Sering
- ( ) Jarang
- ( ) Tidak Tahu

Seberapa baik staf mengikuti aturan keamanan seperti;

a. Mengamankan informasi yang menjadi tanggung jawab mereka

b. Tidak membocorkan informasi sensitif kepada orang lain

c. Memiliki kemampuan yang memadai untuk menggunakan perangkat keras dan perangkat lunak teknologi informasi

d. Menggunakan praktik kata sandi yang baik

e. Memahami dan mengikuti kebijakan dan peraturan keamanan

f. Mengenali dan melaporkan insiden

- (●) Sangat Baik
- ( ) Cukup Baik
- ( ) Tidak Baik
- ( ) Tidak Tahu

Apa yang saat ini sudah dilakukan dengan baik oleh UPA TIK terkait bidang keamanan dan Pelatihan?

Tuliskan semua praktik yang telah dilakukan terkait keamanan dan pelatihan, misalnya pelatihan berkala, penyusunan SOP, atau penerapan kebijakan keamanan.

Dilakukan beberapa pelatihan berkaitan tentang keamanan sistem seperti pelatihan network penetration testing untuk mengetahui celah kerentanan dari jaringan server yang kita miliki

Apa yang saat ini tidak dilakukan dengan baik pada bidang ini?

Jelaskan praktik-praktik yang seharusnya dilakukan namun belum diterapkan atau belum dilakukan dengan baik, misalnya kurangnya pelatihan atau kebijakan yang belum disosialisasikan dengan baik.

semuanya sudah dilakukan dengan baik, seperti pemantauan resource pengunaan server secara rutin dan jika terjadi kejadian-kejadian yang janggal akan ditelusuri untuk mencari penyebabnya, untuk antisipasi serangan mallware dan ddos akan segera dipasangkan pengaman berupa firewall untuk menjaga kemanan sistem dan server kita

Seberapa efektif UPA TIK menerapkan praktik keamanan dan pelatihan? *

- ○ Sangat tidak efektif, banyak masalah yang perlu diperbaiki.
- ◉ Cukup efektif, namun masih ada ruang untuk perbaikan.
- ○ Sangat efektif, semua berjalan sesuai harapan.
- ○ Praktik ini tidak relevan atau tidak diterapkan.

Praktik Keamanan

Peraturan dan Kebijakan Keamanan

Apakah organisasi memiliki kebijakan keamanan yang selalu diperbarui dan terdokumentasi? *

- ○ Ya, selalu diperbarui
- ◉ Ya, tapi kadang-kadang
- ○ Tidak, belum pernah
- ○ Tidak tahu

Apakah ada prosedur yang terdokumentasi dengan jelas untuk mengelola kebijakan keamanan, termasuk pembuatan dan pembaruan? *

- ◉ Ya, ada prosedur yang jelas
- ○ Ya, tapi tidak sepenuhnya jelas
- ○ Tdak, belum ada prosedur
- ○ Tidak tahu

Apakah ada proses yang terdokumentasi untuk memeriksa dan memastikan kepatuhan terhadap kebijakan keamanan dan hukum? *

- ○ Ya, sudah lengkap
- ◉ Ya, tapi belum sepenuhnya
- ○ Tidak, belum ada
- ○ Tidak tahu

Apakah kebijakan keamanan informasi diterapkan secara konsisten di seluruh divisi yang ada di UPA TIK? *

- ◉ Ya, diterapkan di seluruh divisi yang ada di UPA TIK Undiksha.
- ○ Ya, tapi tidak merata
- ○ Tidak, belum diterapkan
- ○ Tidak tahu

*

Apa yang saat ni sudah dilakukan dengan baik oleh UPA TIK dalam menerapkan kebijakan keamanan?

Berikan jawaban yang konkret (misalnya, dokumentasi kebijakan keamanan ada dan sudah diperbarui sesuai dengan perkembangan terbaru)

untuk di divisi infra, dilakuakan pemantuan terhadap versi os dari server untuk dilakukan update/di rekomendasikan ke os versi terbaru

*

Apa yang saat ini tidak dilakukan dengan baik oleh UPA TIK dalam menerapkan kebijakan keamanan?

Sebutkan apa yang mungkin perlu ditingkatkan dan ditambahkan (misalnya, dokuemntasi kebijakan keamanan belum sesuai dan belum diperbarui, kebijakan keamanan belum ada).

melakukan koordinasi dengan inten terhadap pengembang system untuk tindakan update versi os agar pengembang dapat menyesuaikan versi aplikasi yang dikembangkan

Seberapa efektif UPA TIK U ndiksha dalam menerapkan kebijakan keamanan? *

- ○ Sangat tidak efektif, banyak masalah yang perlu diperbaiki.
- ◉ Cukup efektif, namun masih ada ruang untuk perbaikan.
- ○ Sangat efektif, semua berjalan sesuai harapan.
- ○ Praktik ini tidak relevan atau tidak diterapkan.

Praktik Keamanan

Pemulihan Bencana

Sejauh mana organisasi telah melakukan analisis operasi, aplikasi, serta kekeritisan data, dan mendokumentasikan, meninjau, serta menguji rencana kontinjensi, pemulihan bencana, serta kelangsungan operasi darurat? *

- ○ Telah dilakukan dan didokumentasikan dengan baik.
- ◉ Hanya sebagian rencana yang telah diuji dan didokumentasikan.
- ○ Belum dilakukan sama sekali.
- ○ Saya tidak tahu dan tidak memiliki informasi mengenai hal ini.

Apakah rencana kontinjensi/pemulihan bencana, dan kelangsungan operasi mempertimbangkan kontrol akses fisik dan elektronik serta apakah staf mengetahui dan memahami tanggung jawab mereka dalam pelaksanaan rencana tersebut? *

- ◉ Ya, seluruh staf memahami dan rencana mempertimbangkan kontrol akses.
- ○ Rencana sudah mempertimbangkan kontrol akses, namun staf belum memahami sepenuhnya.
- ○ Belum ada rencana yang mempertimbangkan kontrol akses dan staf belum memahami tanggung jawabnya.
- ○ Saya tidak tahu dan tidak memiliki informasi mengenai hal ini.

Apakah organisasi secara rutin mendokumentasikan, meninjau, dan menguji rencana-rencana tersebut, termasuk rencana pemulihan bencana dan kelangsungan operasi? *

- ○ Sudah dilakukan dengan rutin dan menyeluruh.
- ◉ Hanya beberapa aspek yang diuji dan didokumentasikan.
- ○ Tidak dilakukan sama sekali.
- ○ Saya tidak tahu dan tidak memiliki informasi mengenai hal ini.

Seberapa jauh seluruh staf dalam organisasi memahami rencana kontinjensi, pemulihan bencana, serta kelangsungan operasi, dan seberapa baik mereka mampu melaksanakan tanggung jawab mereka? *

- ○ Seluruh staf memahami dan mampu melaksanakan tanggung jawab mereka
- ◉ Hanya sedikit staf yang memahami dan mampu melaksanakan.
- ○ Tidak ada staf yang memahami atau mampu melaksanakan tanggung jawab mereka.
- ○ Saya tidak tahu dan tidak memiliki informasi mengenai hal ini

Apa yang saat ini sudah dilakukan dengan baik oleh UPA TIK dalam menerapkan Perancanaan Contingency / Pemulihan Bencana? *

sudah dilakukan

Apa yang saat ini tidak dilakukan dengan baik oleh UPA TIK dalam menerapkan Perancanaan Contingency / Pemulihan Bencana? *

melakukan backup data secara berkala

Seberapa efektif UPA TIK menerapkan praktik-praktik perencanaan kontinjensi/pemulihan bencana dalam mendukung operasional? *

- ○ Sangat tidak efektif, banyak masalah yang perlu diperbaiki.
- ◉ Cukup efektif, namun masih ada ruang untuk perbaikan.
- ○ Sangat efektif, semua berjalan sesuai harapan.
- ○ Praktik ini tidak relevan atau tidak diterapkan.

Praktik Keamanan

Pengendalian Akses Fisik

Apakah rencana dan prosedur keamanan fasilitas untuk melindungi tempat, bangunan, dan area terlarang sudah didokumentasikan dan diuji di UPA TIK Undiksha? *

- ◉ Sudah didokumentasikan dan diuji dengan sangat baik.
- ○ Hanya sebagian yang didokumentasikan, belum diuji.
- ○ Tidak ada dokumentasi atau uji coba.
- ○ Tidak ada informasi tentang hal ini dan tidak relevan dengan UPA TIK Undiksha.

Apakah terdapat kebijakan dan prosedur yang terdokumentasi untuk mengelola pengunjung di UPA TIK Undiksha? *

- ◉ Kebijakan sudah lengkap dan diikuti dengan baik.
- ○ Ada kebijakan tetapi tidak terdokumentasi dan penerapannya tidak konsisten.
- ○ Tidak ada kebijakan tentang hal ini sama sekali.
- ○ Tidak ada informasi tentang hal ini dan tidak relevan dengan UPA TIK Undiksha.

Apakah terdapat kebijakan dan prosedur yang terdokumentasi untuk mengendalikan akses fisik ke area kerja dan perangkat keras seperti komputer, perangkat komunikasi, dan media perangkat lunak di UPA TIK Undiksha? *

- (●) Kebijakan sudah lengkap dan diikuti dengan baik.
- ( ) Ada kebijakan tetapi tidak terdokumentasi dan penerapannya tidak konsisten.
- ( ) Tidak ada kebijakan tentang hal ini sama sekali.
- ( ) Tidak ada informasi tentang hal ini dan tidak relevan dengan UPA TIK Undiksha.

Apakah terdapat kebijakan dan prosedur yang terdokumentasi untuk mengendalikan akses fisik ke area kerja dan perangkat keras seperti komputer, perangkat komunikasi, dan media perangkat lunak di UPA TIK Undiksha? *

- (●) Akses fisik sudah dikelola dengan baik, kebijakan terdokumentasi lengkap.
- ( ) Pengelolaan akses fisik dilakukan, tetapi kebijakan tidak terdokumentasi.
- ( ) Tidak ada kebijakan atau prosedur terkait akses fisik.
- ( ) Tidak ada informasi tentang hal ini dan tidak relevan dengan UPA TIK Undiksha.

Apakah lingkungan kerja dan komponen lain yang memungkinkan akses ke informasi sensitif sudah dilindungi secara fisik untuk mencegah akses yang tidak sah? *

- (●) Sudah dilindungi sepenuhnya dengan kontrol fisik yang kuat.
- ( ) Perlindungan ada, tetapi kontrol fisik tidak konsisten.
- ( ) Tidak ada perlindungan atau kontrol fisik.
- ( ) Tidak ada informasi tentang hal ini dan tidak relevan dengan UPA TIK Undiksha.

Apa yang saat ini dilakukan dengan baik oleh UPA TIK dalam pengendalian akses fisik? *

Tuliskan hal yang sudah dengan baik dilakukan dalam bidang ini (misalnya, penerapan kebijakan akses fisik sudah berjalan dengan baik. Staf menggunakan kartu akses elektronik untuk masuk ke area terbatas, dan akses ke ruangan server selalu diawasi).

pemakaian accers door lock untuk masuk gedung dan ruangan, jadi hanya staf tertentu saja yang punya akses ke ruangan

Apa yang saat ini tidak dilakukan dengan baik oleh UPA TIK dalam pengendalian akses fisik? *

Tuliskan hal yang masih perlu diperbaiki atau ditambahkan dalam bidang ini (misalnya, Beberapa pintu ke area sensitif seringkali dibiarkan terbuka tanpa pengawasan, terutama di luar jam kerja dan mengenai pencatatan pengunjung dll).

untuk akes masuk ke lab komputer masih mengunakan kunci manual

Seberapa efektif UPA TIK menerapkan praktik-praktik dalam pengendalian akses fisik? *

- ○ Sangat tidak efektif, banyak masalah yang perlu diperbaiki.
- ◉ Cukup efektif, namun masih ada ruang untuk perbaikan.
- ○ Sangat efektif, semua berjalan sesuai harapan.
- ○ Praktik ini tidak relevan atau tidak diterapkan.

Praktik Keamanan

Pemantauan dan Audit Keamanan Fisik

Seberapa baik organisasi Anda menyimpan dan mengelola catatan pemeliharaan terkait perbaikan dan modifikasi fasilitas fisik? *

- (●) Semua catatan terdokumentasi dengan baik dan mudah diakses.
- ( ) Hanya sebagian kecil catatan yang terdokumentasi.
- ( ) Tidak ada dokumentasi catatan atau saya tidak tahu.
- ( ) Tidak ada informasi tentang hal ini dan tidak relevan dengan UPA TIK Undiksha.

Seberapa baik tindakan individu atau kelompok dalam organisasi dipantau terkait penggunaan media yang dikontrol secara fisik? *

- (●) Selalu dipantau dengan jelas dan bisa dipertanggungjawabkan.
- ( ) Jarang dipantau dan sulit dipertanggungjawabkan.
- ( ) Tidak dipantau sama sekali.
- ( ) Tidak ada informasi tentang hal ini dan tidak relevan dengan UPA TIK Undiksha.

Seberapa sering catatan audit dan pemantauan diperiksa untuk menemukan anomali, dan tindakan perbaikan diambil jika diperlukan? *

- (●) Selalu diperiksa secara rutin dan tindakan korektif segera dilakukan.
- ( ) Jarang diperiksa, tindakan korektif jarang diambil.
- ( ) Tidak diperiksa sama sekali.
- ( ) Tidak ada informasi tentang hal ini dan tidak relevan dengan UPA TIK Undiksha.

Apa yang saat ini dilakukan oleh UPA TIK dengan baik dalam pemantauan dan audit keamanan fisik? *

Berikan informasi tentang apa yang berjalan baik dalam bidang ini.

perawatan piranti smart lock door, pengantian battry

Apa yang saat ini tidak dilakukan dengan baik pada pemantauan dan audit keamanan fisik? *

Berikan informasi tentang apa yang kurang dalam bidang ini.

sudah baik

Seberapa efektif UPA TIK menerapkan praktik-praktik dalam pemantauan dan audit keamanan fisik? *

- ○ Sangat tidak efektif, banyak masalah yang perlu diperbaiki.
- ○ Cukup efektif, namun masih ada ruang untuk perbaikan.
- ◉ Sangat efektif, semua berjalan sesuai harapan.
- ○ Praktik ini tidak relevan atau tidak diterapkan.

Praktik Keamanan

Manajemen Jaringan dan Sistem

Apakah ada rencana keamanan yang terdokumentasi dan teruji untuk melindungi sistem dan jaringan? *

- ○ Sudah ada dan selalu diperbarui.
- ◉ Ada, tetapi belum diperbarui secara rutin.
- ○ Ada, tetapi belum pernah diuji.
- ○ Tidak ada rencana keamanan.

Bagaimana informasi sensitif dilindungi oleh penyimpanan yang aman (misal, cadangan disimpan di luar lokasi, proses pembuangan informasi sensitif)? *

- (●) Sudah terlindungi dengan baik.
- ( ) Hanya sebagian yang dilindungi.
- ( ) Tidak ada proteksi khusus.
- ( ) Tidak tahu atau tidak ada informasi mengenai hal ini.

Seberapa sering integritas perangkat lunak yang terinstal diverifikasi secara teratur? *

- (●) Secara rutin diverifikasi setiap kali ada pembaruan.
- ( ) Jarang di verifikasi.
- ( ) Tidak pernah diverifikasi.
- ( ) Tidak tahu atau tidak ada informasi mengenai hal ini.

Apakah semua sistem selalu diperbarui sesuai revisi, tambalan, dan rekomendasi dalam saran keamanan? *

- ( ) Semua sistem diperbarui tepat waktu.
- (●) Hanya beberapa sistem yang diperbarui.
- ( ) Tidak ada sistem yang diperbarui.
- ( ) Tidak tahu atau tidak ada informasi mengenai hal ini.

Apakah ada rencana pencadangan data yang terdokumentasi dan teruji, serta apakah semua staf memahami tanggung jawab mereka terkait pencadangan? *

- (●) Ada rencana pencadangan, dan staf memahami tanggung jawabnya.
- ( ) Ada pencadangan, tetapi belum terdokumentasi dan diuji serta staf kurang memahami tanggung jawabnya.
- ( ) Tidak ada rencana pencadangan dan staf tidak memahami.
- ( ) Tidak tahu atau tidak ada informasi mengenai hal ini.

Bagaimana perubahan pada perangkat keras dan perangkat lunak TI direncanakan, dikontrol, dan didokumentasikan? *

- (●) Semua perubahan direncanakan, dikontrol, dan didokumentasikan.
- ( ) Beberapa perubahan tidak direncanakan dan kurang didokumentasikan.
- ( ) Tidak ada perencanaan dan dokumentasi yang jelas.
- ( ) Tidak tahu atau tidak ada informasi mengenai hal ini.

Apakah prosedur diikuti saat menerbitkan, mengubah, dan menghentikan kata sandi, akun, serta hak istimewa pengguna, dan apakah identifikasi pengguna yang unik diperlukan serta akun dan kata sandi bawaan sudah dihapus dari sistem? *

- (●) Semua prosedur diikuti, identifikasi pengguna unik diperlukan, dan akun/kata sandi bawaan sudah dihapus.
- ( ) Prosedur kadang-kadang diabaikan, identifikasi pengguna unik tidak selalu diperlukan, dan akun/kata sandi bawaan masih digunakan.
- ( ) Tidak ada prosedur yang jelas, identifikasi pengguna unik tidak diperlukan, dan akun/kata sandi bawaan belum dihapus.
- ( ) Tidak tahu atau tidak ada informasi mengenai hal ini.

Apakah hanya layanan yang diperlukan yang berjalan pada sistem, dan semua layanan yang tidak perlu dihapus? *

- ○ Ya, semua layanan yang tidak diperlukan sudah dihapus.
- ◉ Beberapa layanan tidak perlu masih berjalan.
- ○ Tidak ada tindakan untuk menghapus layanan yang tidak perlu.
- ○ Tidak tahu atau tidak ada informasi mengenai hal ini.

Apakah alat dan mekanisme untuk administrasi sistem dan jaringan yang aman digunakan, dan secara rutin ditinjau? *

- ◉ Digunakan dan ditinjau secara rutin.
- ○ Jarang digunakan dan jarang ditinjau.
- ○ Tidak pernah ditinjau sama sekali.
- ○ Tidak tahu atau tidak ada informasi mengenai hal ini.

Apa yang saat ini dilakukan oleh UPA TIK dengan baik dalam manajemen sistem dan jaringan? *

mengunakan tool monitoring jaringan

Apa yang saat ini tidak dilakukan dengan baik pada manajemen sistem dan jaringan? *

sudah dilakukan

Seberapa efektif UPA TIK menerapkan praktik-praktik dalam manajemen sistem dan jaringan? *

- ○ Sangat tidak efektif, banyak masalah yang perlu diperbaiki.
- ◉ Cukup efektif, namun masih ada ruang untuk perbaikan.
- ○ Sangat efektif, semua berjalan sesuai harapan.
- ○ Praktik ini tidak relevan atau tidak diterapkan.

Praktik Keamanan

Otentikasi dan Otorisasi

Seberapa baik kontrol akses dan autentikasi pengguna (seperti izin file, konfigurasi jaringan) diterapkan sesuai kebijakan untuk membatasi akses ke informasi, sistem, aplikasi, dan jaringan sensitif? *

- ◉ Kontrol akses dan autentikasi diterapkan secara menyeluruh sesuai kebijakan.
- ○ Kontrol akses dan autentikasi diterapkan, tetapi ada beberapa kekurangan.
- ○ Kontrol akses dan autentikasi tidak diterapkan.
- ○ Tidak yakin mengenai penerapan kontrol akses dan autentikasi.

Apakah ada kebijakan dan prosedur yang terdokumentasi untuk menetapkan dan mengakhiri hak akses terhadap informasi, baik untuk individu maupun kelompok? *

- ◉ Kebijakan dan prosedur terdokumentasi dengan baik.
- ○ Kebijakan dan prosedur ada, tetapi tidak sepenuhnya terdokumentasi.
- ○ Tidak ada kebijakan atau prosedur terdokumentasi.
- ○ Tidak tahu mengenai kebijakan dan prosedur tersebut.

Seberapa baik metode atau mekanisme disediakan untuk memastikan informasi sensitif tidak diakses, diubah, atau dihancurkan secara tidak sah, dan seberapa sering metode tersebut ditinjau dan diverifikasi? *

- (●) Metode sangat baik dan ditinjau secara berkala.
- ( ) Metode ada dan ditinjau, tetapi tidak secara konsisten.
- ( ) Metode tidak ada atau tidak ditinjau.
- ( ) Tidak tahu mengenai metode atau mekanisme tersebut.

Apa yang saat ini dilakukan dengan baik oleh UPA TIK Undiksha dalam bidang otentikasi dan otorisasi? *

sudah ada kasifikasi user akses

Apa yang saat ini tidak dilakukan dengan baik dalam hal otentikasi dan otorisasi? *

sudah dilakukan

Seberapa efektif UPA TIK dalam menerapkan praktik otentikasi dan otorisasi? *

- ( ) Sangat tidak efektif, banyak masalah yang perlu diperbaiki.
- ( ) Cukup efektif, namun masih ada ruang untuk perbaikan.
- (●) Sangat efektif, semua berjalan sesuai harapan.
- ( ) Praktik ini tidak relevan atau tidak diterapkan.

Praktik Keamanan

Manajmeen Kerentanan

Seberapa lengkap prosedur terdokumentasi untuk mengelola keamanan di organisasi, termasuk: *

a. Memilih alat evaluasi kerentanan, daftar periksa, dan skrip.

b. Mengikuti perkembangan jenis kerentanan dan metode serangan yang diketahui.

c. Meninjau sumber informasi tentang pengumuman kerentanan, peringatan keamanan, dan pemberitahuan.

d. Mengidentifikasi komponen infrastruktur yang akan dievaluasi.

e. Penjadwalan evaluasi kerentanan.

f. Menafsirkan dan menanggapi hasil evaluasi.

g. Menjaga penyimpanan dan disposisi data kerentanan yang aman.

- ○ Semua aspek dikelola dengan sangat baik.
- ◉ Beberapa aspek dikelola dengan baik, tapi banyak area yang masih kurang.
- ○ Tidak ada sama sekali aspek yang dikelola.
- ○ Tidak yakin mengenai kelengkapan prosedur.

Seberapa konsisten prosedur manajemen kerentanan diikuti, ditinjau, dan diperbarui? *

- ◉ Prosedur selalu diikuti, ditinjau, dan diperbarui secara rutin.
- ○ Prosedur tidak selalu diikuti atau diperbarui dengan baik.
- ○ Tidak sama sekali diikuti, ditinjau, dan diperbarui.
- ○ Tidak memiliki informasi mengenai konsistensi prosedur.

Seberapa sering penilaian kerentanan teknologi dilakukan dan kerentanan diatasi ketika teridentifikasi? *

- (●) Penilaian dilakukan secara berkala dan semua kerentanan segera diatasi.
- ( ) Penilaian dilakukan tidak teratur dan beberapa kerentanan mungkin tidak segera diatasi.
- ( ) Tidak sama sekali dilakukan.
- ( ) Tidak mengetahui frekuensi atau efektivitas penilaian kerentanan.

Apa yang saat ini dilakukan oleh UPA TIK dengan baik dalam manajemen kerentanan? *

melakukan uji kerentanan pada kepada sistem atau server yang memiliki aktifitas tinggi

Apa yang saat ini tidak dilakukan dengan baik pada manajemen kerentanan? *

belum semua server atau system dilakukan uji kerentanan

Seberapa efektif UPA TIK menerapkan praktik-praktik dalam manajemen kerentanan? *

- ( ) Sangat tidak efektif, banyak masalah yang perlu diperbaiki.
- (●) Cukup efektif, namun masih ada ruang untuk perbaikan.
- ( ) Sangat efektif, semua berjalan sesuai harapan.
- ( ) Praktik ini tidak relevan atau tidak diterapkan.

Praktik Keamanan

Perancangan dan arsitektur keamanan

Seberapa baik desain/perancangan dan arsitektur keamanan sistem baru dan sistem yang direvisi mencakup strategi, kebijakan, dan prosedur keamanan? *

- (●) Seluruh aspek telah dipertimbangkan dan diimplementasikan dengan baik.
- ( ) Hanya beberapa bagian yang mencakup aspek-aspek tersebut.
- ( ) Tidak ada sama sekali aspek yang dipertimbangkan.
- ( ) Tidak memiliki informasi mengenai cakupan perancangan ini.

Seberapa baik desain/perancangan dan arsitektur keamanan mencakup riwayat kerjasama keamanan? *

- (●) Sangat komprehensif dan mencakup semua aspek.
- ( ) Cukup mencakup, tapi ada yang bisa diperbaiki.
- ( ) Tidak mencakup sama sekali.
- ( ) Tidak yakin.

Apakah UPA TIK Undiksha memiliki diagram terkini yang menunjukkan arsitektur keamanan di seluruh topologi jaringan? *

- (●) Diagram sangat detail dan up-to-date.
- ( ) Diagram ada, tetapi kurang lengkap.
- ( ) Tidak ada diagram sama sekali.
- ( ) Tidak Tahu.

Apa yang dilakukan dengan baik oleh UPA TIK dalam Desain/Perancangan dan Arsitektur Keamanan? *

Anda dapat menuliskan hal-hal yang sudah berjalan dengan baik, seperti pengembangan prosedur yang jelas atau pengelolaan topologi jaringan yang efektif.

dalam topologi sudah dimasukkan forti sebagai pelindung/firewall jaringan dalam undiksha

Apa yang tidak dilakukan dengan baik oleh UPA TIK Undiksha dalam Desain/Perancangan dan Arsitektur Keamanan? *

Anda dapat menuliskan saran perbaikan, misalnya pada dokumentasi keamanan yang kurang lengkap atau proses kerjasama yang belum optimal.

sudah dilakuakan dengan optimal

Seberapa efektif UPA TIK Undiksha dalam menerapkan praktik-praktik di Desain/Perancangan dan Arsitektur Keamanan? *

- ○ Sangat tidak efektif, banyak masalah yang perlu diperbaiki.
- ◉ Cukup efektif, namun masih ada ruang untuk perbaikan.
- ○ Sangat efektif, semua berjalan sesuai harapan.
- ○ Praktik ini tidak relevan atau tidak diterapkan.

Praktik Keamanan

Manajemen Insiden

Apakah terdapat prosedur yang terdokumentasi untuk mengidentifikasi, melaporkan, dan menanggapi dugaan insiden dan pelanggaran keamanan? *

- ○ Prosedur terdokumentasi dengan baik dan diterapkan secara konsisten.
- ◉ Prosedur ada, tapi implementasinya belum maksimal.
- ○ Prosedur tidak ada atau tidak terdokumentasi.
- ○ Tidak tahu tentang keberadaan prosedur ini.

Seberapa sering prosedur manajemen insiden diuji, diverifikasi, dan diperbarui secara berkala? *

- ○ Uji dan pembaruan dilakukan secara teratur dan konsisten.
- ◉ Uji dilakukan, tapi tidak secara rutin.
- ○ Uji dan pembaruan hampir tidak pernah dilakukan.
- ○ Tidak tahu mengenai frekuensi uji dan pembaruan.

Apakah terdapat kebijakan dan prosedur yang terdokumentasi untuk bekerja sama dengan lembaga penegak hukum dalam menangani insiden? *

- ○ Prosedur kerjasama terdokumentasi dan dijalankan dengan baik.
- ○ Ada prosedur, tapi implementasi masih perlu diperbaiki.
- ◉ Prosedur kerjasama tidak ada.
- ○ Tidak tahu mengenai kebijakan atau prosedur ini.

Apa yang saat ini dilakukan dengan baik oleh UPA TIK dalam manajemen insiden? *

melakukan tindakan prefentiv dalam menangani insiden seperti melakukan backup dan monitoring resoucre pengunaan server

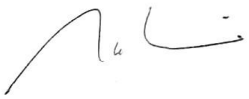
Apa yang saat ini tidak dilakukan dengan baik oleh UPA TIK dalam manajemen insiden? *

belum melakukan prosedur kerjasama

Seberapa efektif UPA TIK Undiksha menerapkan praktik-praktik dalam manajemen insiden? *

- ○ Sangat tidak efektif, banyak masalah yang perlu diperbaiki.
- ◉ Cukup efektif, namun masih ada ruang untuk perbaikan.
- ○ Sangat efektif, semua berjalan sesuai harapan.
- ○ Praktik ini tidak relevan atau tidak diterapkan.

Lampiran 10. Hasil Kuesioner Lembar Kerja OCTAVE-S Tahap ke-

INFORMASI PELAKSANAAN PENGISIAN KUESIONER TAHAP KE-2 LEMBAR KERJA OCTAVE-S PENELITIAN PADA UPA TIK UNDIKSHA			
Peneliti	:	Hardiyanti Rohmania	
Hari, Tanggal	:	23 September 2024 .	
Lokasi	:	UPA TIK Undiksha	
INFORMASI RESPONDEN 1			**Tanda Tangan**
Nama	:	Ida Komang Widhiarjaya, S.T., M.Pd.	
Jabatan	:	Sekretaris UPA TIK Undiksha	
INFORMASI RESPONDEN 2			**Tanda Tangan**
Nama	:	Putu Wendy Aryani, S.Pd. M.Kom.	
Jabatan	:	~~Kepala~~/Anggota Divisi Helpdesk & Dokumentasi	
INFORMASI RESPONDEN 3			**Tanda Tangan**
Nama	:	Kadek Surya Mahedy, S.T., M.Pd.	
Jabatan	:	~~Kepala~~/Anggota Divisi Pusat Data & Informasi	

INFORMASI RESPONDEN 4			Tanda Tangan
Nama	:	I Nyoman Yoga Setyawan, S.ST., M.Kom	
Jabatan	:	~~Kepala~~/Anggota Divisi Sistem Informasi	
INFORMASI RESPONDEN 5			**Tanda Tangan**
Nama	:	Gede Arna Jude Saskara	
Jabatan	:	Kepala/~~Anggota~~ Divisi Infrastruktur, Jaringan & Keamanan	

**Pada bagian jabatan, coret bagian yang tidak diperlukan*

Responses cannot be edited

Kuesioner OCTAVE-S Tahap ke-2

Salam Harmoni,
Tujuan dari kuesioner ini adalah untuk mengumpulkan informasi. Informasi yang Anda berikan akan membantu saya dalam mengevaluasi ancaman aset kritis melalui jalur akses.
Saya mengharapkan kejujuran dan keterbukaan Anda dalam menjawab setiap pertanyaan. Semua jawaban akan dijaga kerahasiaannya dan hanya digunakan untuk keperluan penelitian saya yang berjudul "**ANALISIS MANAJEMEN RISIKO KEAMANAN INFORMASI MENGGUNAKAN *FRAMEWORK* OCTAVE-S DAN ISO 27001:2022.**"

* Indicates required question

Nama *

Ida Komang Widhiarjaya

NIP *

198108032006041002

Instansi *

UPA TIK Undiksha

Jabatan *

Sekretaris UPA TIK Undiksha

Memilih Aset Kritis

Diantara aset yang telah diidentifikasi pada kuesioner tahap ke-1, pilihlah aset-aset yang menurut Anda paling penting, rentan, dan berisiko tinggi terhadap dampak merugikan jika skenario berikut terjadi: *
- dibocorkan kepada pihak yang tidak berwenang
- diubah tanpa otorisasi
- hilang atau hancur
- akses terhadap ast kritis tersebut terputus

Daftar aset yang telah diidentifikasi sebelumnya sebagai berikut:
- Server
- SOP dan Instruksi Kerja
- SIAK
- Perangkat Jaringan
- Sekretaris UPA TIK dan Divisi Infrastruktur, Jaringan, & Keamanan

Silakan pilihh aset-aset yang menurut Anda paling penting, rentan, dan berisiko tinggi ketika skenario tersebut terjadi. Anda bisa memilih lebih dari satu (1) dan bisa memilih beberapa jika aset tersebut tidak dirasa berisiko tinggi dan jika dirasa tidak relevan.

*catatan: jawab dengan cara mengurutkan aset dengan skala prioritas paling rentan terlebih dahulu.

Server, Perangkat Jaringan, Sekretaris UPA TIK dan Divisi Infrastruktur, Jaringan, & Keamanan, SIAK, SOP dan Instruksi Kerja

Divisi apa yang bertanggung jawab atas Server? *

- ○ Divisi Helpdesk & Dokumentasi
- ○ Divisi Manajemen Konten
- ◉ Divisi Pusat Data & Informasi
- ○ Divisi Infrastruktur, Jaringan, & Keamanan
- ○ Divisi Sistem Informasi

Divisi apa yang bertanggung jawab atas pembuatan dan perubahan SOP dan Instruksi Kerja? *

- (●) Divisi Helpdesk & Dokumentasi
- ( ) Divisi Manajemen Konten
- ( ) Divisi Pusat Data & Informasi
- ( ) Divisi Infrastruktur, Jaringan, & Keamanan
- ( ) Divisi Sistem Informasi

Divisi apa yang bertanggung jawab atas pengembangan SIAK? *

- ( ) Divisi Helpdesk & Dokumentasi
- ( ) Divisi Manajemen Konten
- ( ) Divisi Pusat Data & Informasi
- ( ) Divisi Infrastruktur, Jaringan, & Keamanan
- (●) Divisi Sistem Informasi

Divisi apa yang bertanggung jawab atas perangkat jaringan? *

- ( ) Divisi Helpdesk & Dokumentasi
- ( ) Divisi Manajemen Konten
- ( ) Divisi Pusat Data & Informasi
- (●) Divisi Infrastruktur, Jaringan, & Keamanan
- ( ) Divisi Sistem Informasi

Submitted 9/23/24, 11:26 AM

Informasi Aset Kritis

Mengapa Sekretaris UPA TIK Undiksha dianggap penting bagi organisasi?

1 response

membantu kerja kepala untuk manajemen anggaran, sdm, vendor

Aset apa saja yang terkait dengan Sekretaris UPA TIK Undiksha dalam pekerjaan sehari-hari?

1 response

laptop, printer

Persyaratan Keamanan

Apa persyaratan keamanan untuk Sekretaris UPA TIK?
(petunjuk: berfokus pada persyaratam apa yang seharusnya ada pada aset, bukan pada apa yang ada saat ini).
Berikut adalah syarat keamanannya:
1. **Kerahasiaan**: Sekretaris harus menjaga bahwa informasi dan data sensitif yang dikelola tidak boleh diakses oleh pihak yang tidak berwenang.
2. **Integritas**: Sekretaris harus memastikan bahwa informasi yang diakses dan disimpan pada peralatan teknologi informasi serta server tetap utuh dan akurat.
3. **Ketersediaan**: Akses ke sistem dan data harus selalu tersedia sesuai dengan kebutuhan operasional. Sekretaris dan staf pendukung harus siap memberikan dukungan teknis kapan saja untuk memastikan kelancaran operasional.

1 response

1, 2, 3

Persyaratan keamanan mana yang paling penting untuk Sekretaris UPA TIK Undiksha?

Copy chart

1 response

Pengambilan Cuti Sementara

Bagaimana pengaruh pengambilan cuti sementara (misalnya sakit atau kegiatan penting diluar organisasi) oleh sekretaris UPA TIK terhadap kelancaran operasional harian? Jelaskan dampaknya.

Jenis dampaknya:

1. **Pengungkapan/penyingkapan**: Terbukanya akses informasi atau dokumen penting yang seharusnya dirahasiakan kepada pihak yang tidak berwenang.
2. **Modifikasi**: Perubahan yang tidak sah atau tidak sesuai terhadap data, dokumen, atau informasi penting.
3. **Kehilangan, Kerusakan/kehancuran**: Hilangnya akses atau rusaknya informasi, dokumen, atau aset lain yang dikelola oleh sekretaris.
4. **Gangguan**: Terhambatnya proses atau aktivitas operasional akibat ketidakhadiran sekretaris yang berfungsi sebagai pusat administrasi.

1 response

tidak pengaruh

Seberapa sering Sekretaris UPA TIK mengambil cuti sementara dan bagaimana hal ini bisa mempengaruhi tugas administrasinya?

1 response

tidak pengaruh, karena bisa dikerjakan online, dan waktu juga tidak terbatas

Meninggalkan Organisasi Secara Permanen

Apa dampak jika sekretaris UPA TIK meninggalkan organisasi secara permanen (misalnya pensiun atau pindah kerja)? Jelaskan dampaknya pada operasional dan kelancaran administrasi.

Jenis dampaknya:

1. **Pengungkapan/penyingkapan**: Pengungkapan data rahasia kepada pihak eksternal atau pihak yang tidak berkepentingan dapat mengancam keamanan informasi organisasi.
2. **Modifikasi**: Perubahan data tanpa pengawasan bisa mengakibatkan prosedur operasional yang tidak konsisten atau informasi yang salah, memengaruhi pengambilan keputusan yang tepat di masa depan.
3. **Kehilangan, Kerusakan/kehancuran**: Kerusakan fisik pada arsip kertas atau file digital yang tidak di-backup dapat menyebabkan hilangnya informasi penting, mengganggu proses kerja administratif.
4. **Gangguan**: Gangguan merujuk pada hambatan yang terjadi dalam proses administrasi dan operasional akibat kekosongan peran atau transisi yang tidak lancar setelah sekretaris meninggalkan organisasi.

1 response

tidak ada pengaruh

Seberapa sering terjadi pergantian sekretaris UPA TIK, dan bagaimana organisasi menangani kehilangan personel tersebut?

1 response

tidak ada pengaruh, karena semua ada dokumentasi terarsipd dengan baik, proses peralihan juga sudah disiapkan

Pengaruh Pihak Ketiga Atau Penyedia Layanan

Bagaimana ancaman terhadap pihak ketiga berdampak pada kinerja sekretaris? Jelaskan.

Jenis dampaknya:

1. **Pengungkapan/penyingkapan**: bocornya informasi atau data sensitif kepada pihak yang tidak berwenang, yang seharusnya dirahasiakan.
2. **Modifikasi**: perubahan yang tidak sah atau tanpa otorisasi terhadap data, dokumen, atau informasi yang dikelola.
3. **Kehilangan, Kerusakan/kehancuran**: hilangnya akses ke data atau dokumen penting, atau rusaknya informasi yang tidak dapat dipulihkan.
4. **Gangguan**: penghentian sementara atau permanen akses ke sistem, data, atau dokumen yang dibutuhkan untuk operasional harian.

1 response

tidak ada dampak

Seberapa sering ancaman terhadap pihak ketiga terjadi, dan bagaimana dampaknya pada tugas sekretaris?

1 response

tidak pernah ada

Informasi Aset Kritis

Apakah server pernah memiliki masalah pada perangkat keras (seperti komponen rusak) atau perangkat lunak (seperti konfigurasi salah atau celah keamanan/ Kelemahan yang dapat dimanfaatkan oleh peretas untuk mengakses data atau sistem tanpa izin)?

1 response

masalah tersebut sering terjadi, seperti kehabisan memory dan kapasistas HD, masalah ini bisa kita atasi dengan upgrade hardware atau migrasi sistem ke server sementara/cadangan. untuk celah keamanan kita sudah atasi dengan pemasangan filewall dan di monitor setiap saat

Seberapa sering server mengalami downtime atau gangguan operasional dan apa dampaknya?

1 response

untuk saat ini down time server biasanya terjadi karena migrasi sistem atau upgrade hardware, ini akan berdampak sistem informasi tidak dapat diakses selama proses upgrade atau migrasi sistem. rata 1 bulan sekali dengan downtime dibawah 30 menit

Persyaratan Keamanan

Berikan penjelasan mengapa server dianggap sangat penting bagi organisasi?

1 response

server adalah pusat dari data dan sistem informasi sebagai jantungnya sebuah organisasi, server down hampir semua aktifitas tidak dapat berjalan dengan baik. karena hampir semua kegiatan organisasi menggunakan sistem informasi

Aset apa saja yang terkait dengan server?

1 response

data civitas akademika dan semua sistem informasi yang dikembangkan oleh organisaasi (UNDIKSHA)

Siapa saja yang menggunakan server?

1 response

pengguna server adalah admin database dan sistem informasi termasuk juga programmer dan admin jaringan dengan privileges sesuai kebutuhan masing-masing

Apa persyaratan keamanan untuk server? (petunjuk: berfokus pada persyaratan apa yang seharusnya ada pada sebuah aset, bukan pada apa yang ada saat ini)

Berikut adalah persyaratan keamannya:

1) **Kerahasiaan**: hanya diakses oleh pihak tertentu

2) **Integritas**: server tidak boleh diakses oleh pihak yang berwenang

3) **Ketersediaan**: akses tersedia selama 24/7, *maintenance* .../minggu

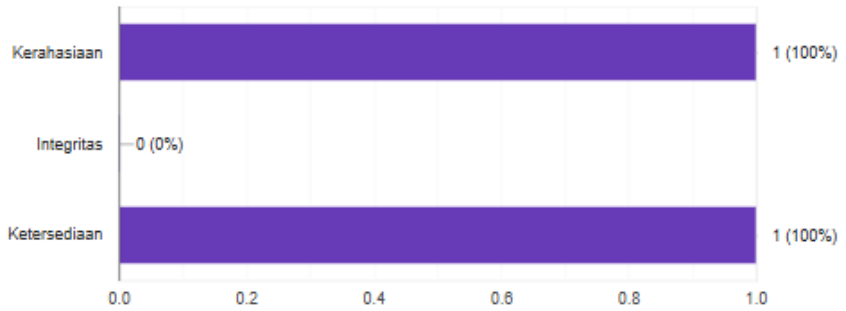
1 response

kerahasisan dan ketersedian akses selama 24 jam. server hanya dapat diakses oleh orang2 tertentu saja dengan role yang sudah disesuaikan dengan kebutuhan dengan semua akses harus melewati server tunnel.

Persyaratan keamanan mana yang paling penting untuk aset server?

Copy chart

1 response



Identifikasi Ancaman Pada Server Melalui Jalur Akses Jaringan

Siapa aktor yang memiliki potensi ancaman terbesar terhadap server melalui akses jaringan?

1 response

Pihak UPA TIK (Internal) masyarakat umum (Pihak Eksternal)

Apakah akses fisik ke ruang server dikendalikan dengan baik dan bagaimana ruang server dikendalikan dari akses fisik?

1 response

akses fisik ke ruang server menggunakan sidik jari dan hanya orang2 tertentu saja yang memeliki akses

Siapa yang bertanggung jawab dalam pengelolaan server dan memiliki akses administratif penuh?

1 response

akses server database di pegang oleh divisi Data center dan akses sever web di pegang oleh tim infra

Berdasarkan riwayat insiden dan kemungkinan dimasa depan, apa motif utama yang mungkin dimiliki pelaku dalam menyerang atau mengakses server secara illegal?

1 response

mendownkan sever dan pencurian data (secara sengaja)

Seberapa tinggi kemungkinan motif dari pihak internal untuk melakukan serangan terhadap server?

1 response

5%

Seberapa tinggi kemungkinan server akan menjadi target serangan dari pihak eksternal (seperti hacker atau pencuri data)?

1 response

10%

Jawab pertanyaan ini jika aktor berasal dari pihak internal silakan jawab pertanyaan ini, jika aktor berasal dari pihak eksternal silakan jawab pertanyaan selanjutnya.

1 response

Kehilangan, kerusakan: Kehilangan data akibat human error/kerusakan HD

Jawab pertanyaan ini jika aktor berasal dari pihak eksternal silakan jawab pertanyaan ini, jika aktor berasal dari pihak internal silakan jawab pertanyaan sebelumnya.

1 response

Gangguan: Serangan yang dikirimkan oleh pihak luar yang mengakibatkan server down

Berapa kali server mengalami gangguan di masa lalu?

1 response

1 bulan sekali, sernagan DDos dll

Seberapa sering melakukan pemeliharaan server untuk mencegah ancaman keamanan?

1 response

pengecekan dilakukan setiap hari untuk mendeteksi kemungkinan terjadi serangan, jika ditemukan kerentanan akan segera di antisipasi

Identifikasi Ancaman Pada Server Melalui Jalur Akses Fisik

Siapa aktor yang memiliki potensi ancaman terbesar terhadap server melalui akses fisik?

1 response

tim infra

Apakah akses fisik ke ruang server terbatas pada personil yang berwenang atau kepada semua staf dan pihak eksternal?

1 response

hanya pihak personil yang berwenang

Apakah ada catatan atau log akses fisik ke server?

1 response

ada

Apa kemungkinan motif ancaman fisik terhadap server?

1 response

tidak

Seberapa tinggi kemungkinan motif dari pihak internal untuk melakukan serangan terhadap server?

1 response

0%

Seberapa tinggi kemungkinan server akan menjadi target serangan dari pihak eksternal (seperti vendor atau tamu) yang mengakses ruang server secara fisik?

1 response

5%

Jawab pertanyaan ini jika aktor berasal dari pihak internal silakan jawab pertanyaan ini, jika aktor berasal dari pihak eksternal silakan jawab pertanyaan selanjutnya.

1 response

Gangguan: Kesalahan pegawai dalam penanganan kerusakan server secara fisik

Jawab pertanyaan ini jika aktor berasal dari pihak eksternal silakan jawab pertanyaan ini, jika aktor berasal dari pihak internal silakan jawab pertanyaan sebelumnya.

1 response

Gangguan: Bencana alam

Apakah ruang server dilengkapi dengan sistem keamanan fisik seperti CCTV, kunci elektronik, atau penjaga?

1 response

iya dengan CCTV dan kunci elektronik (sidik jari)

Seberapa sering pemeliharaan fisik ruang server dilakukan untuk memastikan keamanan?

1 response

1 kali perminggu

Apakah pernah ada insiden terkait ancaman fisik pada server sebelumnya? Berapa kali terjadi? Dan jelaskan insidennya.

1 response

tidak

Apakah pernah ada risiko fisik seperti bencana alam atau kebakaran yang dapat memengaruhi server?

1 response

tidak

Kerusakan Perangkat Lunak

Bagaimana pengaruh kerusakan perangkat lunak pada server dalam operasional sehari-hari? Jelaskan dampaknya.

1 response

Gangguan: Gangguan terjadi ketika operasional sistem terganggu atau terhenti, sehingga akses ke data atau layanan tidak bisa dilakukan. Ini sering disebabkan oleh masalah jaringan, kegagalan sistem, atau serangan siber.

Berapa kali dan dalam kurun waktu berapa lama server mengalami gangguan kerusakan perangkat lunak?

1 response

2 kali dalam kurun waktu 5 tahun

Catatan tambahan apa tentang ancaman kerusakan perangkat lunak pada server yang ingin Anda catat?

1 response

terjadi masalah dalam sistem operasi yang menyebabkan tidak bisa menyimpan data di Hardisk

Berikan contoh bagaimana kerusakan perangkat lunak dapat mengancam server.

1 response

kerusakan sistem yang menyebabkan gagal login ke sistem operasi

Kegagalan Sistem

Bagaimana pengaruh kegagalan sistem pada server dalam operasional sehari-hari? Jelaskan dampaknya.

1 response

Gangguan: Gangguan terjadi ketika operasional sistem terganggu atau terhenti, sehingga akses ke data atau layanan tidak bisa dilakukan. Ini sering disebabkan oleh masalah jaringan, kegagalan sistem, atau serangan siber.

Berapa kali dan dalam kurun waktu berapa lama server mengalami gangguan kegagalan sistem?

1 response

1 kali dalam kurum waktu 5 tahun

Catatan tambahan apa tentang ancaman kegagalan sistem pada server yang ingin Anda catat?

1 response

-

Berikan contoh bagaimana kegagalan sistem dapat mengancam server.

1 response

-

Kerusakan Perangkat Keras

Bagaimana pengaruh kerusakan perangkat keras pada server dalam operasional sehari-hari? Jelaskan dampaknya.

1 response

Gangguan: Gangguan terjadi ketika operasional sistem terganggu atau terhenti, sehingga akses ke data atau layanan tidak bisa dilakukan. Ini sering disebabkan oleh masalah jaringan, kegagalan sistem, atau serangan siber.

Catatan tambahan apa tentang ancaman kerusakan perangkat keras pada server yang ingin Anda catat?

1 response

kerusakan hardisk dan processor

Berikan contoh bagaimana kerusakan perangkat keras dapat mengancam server.

1 response

hardisk dan processor tidak berfungsi dengan baik

Kode Berbahaya

Kode berbahaya seperti apa yang pernah menyerang server dan bagaimana pengaruh kode berbahaya (virus, worm, Trojan horse, back door) pada server dalam operasional sehari-hari? Jelaskan dampaknya.

1 response

Gangguan: Gangguan terjadi ketika operasional sistem terganggu atau terhenti, sehingga akses ke data atau layanan tidak bisa dilakukan. Ini sering disebabkan oleh masalah jaringan, kegagalan sistem, atau serangan siber.

Berapa kali dan dalam kurun waktu berapa lama server mengalami gangguan kerusakan perangkat keras?

1 response

3 kali dalam kurum waktu 5 tahun

Catatan tambahan apa tentang ancaman kode berbahaya pada server yang ingin Anda catat?

1 response

serangan DDOS dan judi online

Berikan contoh bagaimana kode berbahaya dapat mengancam server.

1 response

kode tidak legal masuk ke server

Informasi Aset Kritis

Apakah ada potensi penyalahgunaan akses ke perangkat jaringan dan seberapa besar potensinya?

1 response

Ada

Seberapa sering perangkat jaringan diperiksa untuk mendeteksi adanya kerentanan?

Berikan skala dengan contoh:

1 kali/minggu.

1 response

1 Bulan Sekali

Apakah terdapat risiko dalam pengelolaan data sensitif dan informasi teknis oleh sekretaris dan divisi infrastruktur?

1 response

Terdapat

Seberapa sering dilakukan pemantauan dan evaluasi terhadap prosedur keamanan yang diterapkan oleh sekretaris dan divisi infrastruktur?

1 response

1 bulan sekali

Persyaratan Keamanan

Berikan alasan mengapa perangkat jaringan penting bagi organisasi?

1 response

Menjadi layanan inti dari lembaga kepada dosen, pegawai dan mahasiswa

Aset apa saja yang terkait dengan perangkat jaringan?

1 response

Aset data

Siapa saja yang menggunakan perangkat jaringan?

1 response

Tim Upa TIk

Apa persyaratan keamanan untuk perangkat jaringan? (petunjuk: berfokus pada persyaratan apa yang seharusnya ada pada sebuah aset, bukan pada apa yang ada saat ini)

Berikut adalah persyaratan keamanannya:

1) **Kerahasiaan**: Pengaturan dan data konfigurasi jaringan harus hanya diakses oleh personel jaringan yang berwenang.

2) **Integritas**: Monitoring jaringan pada lingkup organisasi, termasuk menjaga perangkat agar tidak dimodifikasi secara tidak sah.

3) **Ketersediaan**: Perangkat harus beroperasi secara optimal dan dapat diakses kapan saja untuk memastikan konektivitas jaringan yang konsisten.

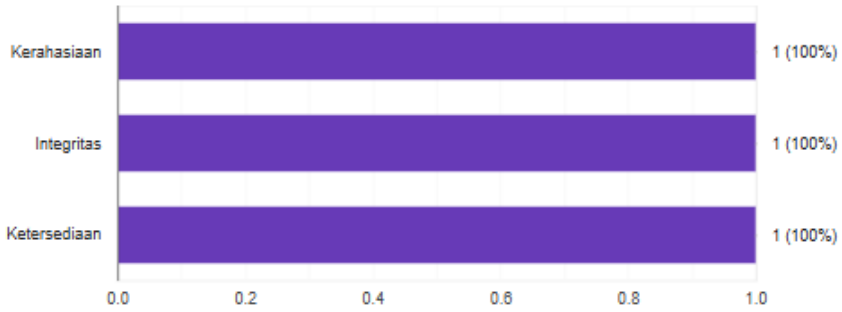
1 response

1) Kerahasiaan: Pengaturan dan data konfigurasi jaringan harus hanya diakses oleh personel jaringan yang berwenang.
2) Integritas: Monitoring jaringan pada lingkup organisasi, termasuk menjaga perangkat agar tidak dimodifikasi secara tidak sah.
3) Ketersediaan: Perangkat harus beroperasi secara optimal dan dapat diakses kapan saja untuk memastikan konektivitas jaringan yang konsisten.

Persyaratan Keamanan mana yang paling penting untuk perangkat jaringan?

Copy chart

1 response



Identifikasi Ancaman Pada Perangkat Jaringan Melalui Jalur Akses Jaringan

Siapa aktor yang paling mungkin menimbulkan ancaman terhadap perangkat jaringan melalui akses jaringan?

1 response

Internal UPA TIK dan Pihak Eksternal

Apakah akses ke perangkat jaringan dikendalikan dengan baik?

1 response

Ya

Siapa yang bertanggung jawab dalam mengelola dan memelihara keamanan perangkat jaringan?

1 response

tim Infra

Apa motif utama yang mungkin dimiliki pelaku dalam menyerang atau mengakses perangkat jaringan secara illegal melalui jaringan?

1 response

Sengaja untuk mencuri data dan untuk mengambil alih jaringan

Seberapa tinggi kemungkinan motif dari pihak internal untuk melakukan serangan terhadap perangkat jaringan?

1 response

Kecil

Seberapa tinggi kemungkinan perangkat jaringan akan menjadi target serangan dari pihak eksternal (seperti hacker atau pencuri data)?

1 response

Tinggi

Jawab pertanyaan ini jika aktor berasal dari pihak internal silakan jawab pertanyaan ini, jika aktor berasal dari pihak eksternal silakan jawab pertanyaan selanjutnya.

1 response

Serangan malware pada perangkat pc internal

Jawab pertanyaan ini jika aktor berasal dari pihak eksternal silakan jawab pertanyaan ini, jika aktor berasal dari pihak internal silakan jawab pertanyaan sebelumnya.

1 response

Penyusupan oleh hacker atau pihak tidak sah untuk mempublikasi data sensitif,
2) Modifikasi: Modifikasi data oleh aktor yang tidak dikenal/diketahui
3) Kehilangan, Kehancuran: Kehilangan data akibat serangan dari pihak luar/pihak eksternal yang tidak diketahui
4) Gangguan: Serangan malware atau peretasan

Berapa kali perangkat jaringan mengalami gangguan jaringan atau serangan jaringan?

1 response

Sering, serangan judi online dan ddos

Seberapa sering dilakukan pemeliharaan pada peragkat jaringan untuk mencegah ancaman keamanan?

1 response

1 bulan sekali

Identifikasi Ancaman Pada Perangkat Jaringan Melalui Jalur Akses Fisik

Siapa aktor yang paling mungkin menimbulkan ancaman terhadap perangkat jaringan melalui akses fisik?

1 response

Internal dan External

Apakah akses ke ruang server dan perangkat jaringan dikendalikan dengan baik?

1 response

Dikendalikan dengan baik

Siapa yang bertanggung jawab dalam mengelola akses fisik ke perangkat jaringan?

1 response

Tim Infra

Seberapa tinggi kemungkinan motif dari pihak internal untuk melakukan serangan terhadap perangkat jaringan melalui akses fisik?

1 response

Kecil

Apa motif utama yang mungkin dimiliki pelaku dalam mengakses jalur fisik perangkat jaringan secara ilegal?

1 response

Sengaja, untuk mencuri data

Seberapa tinggi kemungkinan perangkat jaringan akan menjadi target serangan dari pihak eksternal melalui akses fisik (seperti mencuri perangkat keras jaringan)

1 response

Sedang

Jawab pertanyaan ini jika aktor berasal dari pihak internal silakan jawab pertanyaan ini, jika aktor berasal dari pihak eksternal silakan jawab pertanyaan selanjutnya.

1 response

Gangguan: Serangan malware atau peretasan

Jawab pertanyaan ini jika aktor berasal dari pihak eksternal silakan jawab pertanyaan ini, jika aktor berasal dari pihak internal silakan jawab pertanyaan sebelumnya.

1 response

1) Pengungkapan: Penyusupan oleh hacker atau pihak tidak dikenal
2) Modifikasi: Modifikasi data oleh aktor yang tidak dikena/diketahui
3) Kehilangan, kerusakan: Pencurian perangkat keras atau suku cadang
4) Gangguan: Bencana alam

Informasi Aset Kritis

Meapa Divisi Infrastruktur, Jaringan, & Keamanan dianggap penting bagi organisasi?

1 response

Karena menjadi tim inti dalam organisasi, jika jaringan internet terputus maka layanan akan tidak tersedia, selain itu juga menjaga keamanan dari layanan

Aset apa saja yang terkait dengan Divisi Infrastruktur, Jaringan, & Keamanan dalam kegiatan operasionalnya sehari-hari?

1 response

Aset infrastruktur seperti switch, router

Persyaratan Keamanan

Apa persyaratan keamanan Divisi Infrastruktur, Jaringan & Keamanan?

(petunjuk: berfokus pada persyaratan apa yang seharusnya ada pada sebuah aset, bukan pada apa yang ada saat ini)

Berikut adalah syarat keamanannya:
1. **Kerahasiaan**: Divisi Infrastruktur, Jaringan, dan Keamanan harus memastikan bahwa semua akses ke sistem dan data terbatas hanya kepada pihak yang berwenang.
2. **Integritas**: Divisi harus memastikan bahwa sumber daya, termasuk perangkat keras, perangkat lunak, dan data yang digunakan dalam operasi tetap utuh dan berjalan sebagaimana mestinya.
3. **Ketersediaan**: siap memberikan dukungan kapan saja diperlukan untuk memecahkan masalah terkait jaringan, server, atau aplikasi yang berjalan.

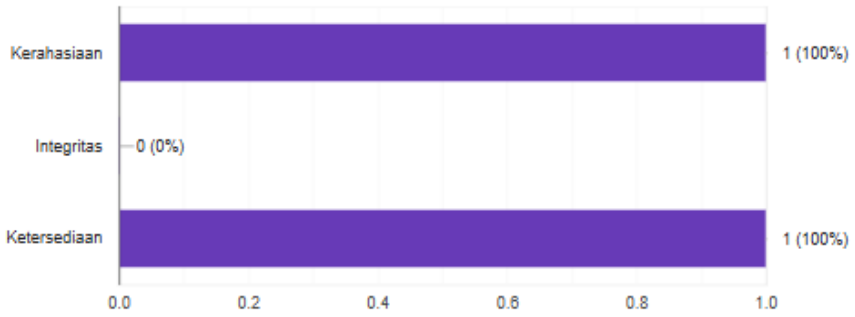
1 response

Divisi Infrastruktur memastikan kerahasiaan data, dan juga datanya tersedia

Persyaratankeamanan mana yang palig penting untuk Divisi Infrastruktur, Jaringan & Keamanan?

Copy chart

1 response



Identifikasi Ancaman Pada SDM - Divisi Infrastruktur, Jaringan & Keamanan

Bagaimana dampak pengambilan cuti sementara (misalnya karena sakit, keperluan diluar organisasi) oleh staf Divisi Infrastruktur, Jaringan & Keamanan?
Jenis Dampaknya:
1) **Pengungkapan/penyingkapan:** informasi sensitif atau data rahasia secara tidak sengaja atau sengaja diketahui oleh pihak yang tidak berwenang selama staf yang berwenang tidak berada di tempat. Pengungkapan ini bisa disebabkan oleh kelalaian dalam penanganan data atau pengelolaan akses yang tidak tepat.
contohnya: Saat staf Divisi Infrastruktur sedang cuti, dokumen akses jaringan yang mengandung informasi sensitif mengenai konfigurasi jaringan diakses oleh pegawai yang tidak memiliki otoritas.

2) **Modifikasi:** data atau sistem diubah secara tidak sah atau tanpa sepengetahuan staf yang bertanggung jawab selama cuti, baik disengaja oleh pihak internal atau akibat kesalahan teknis.
contohnya: SOP atau instruksi kerja untuk pemeliharaan perangkat jaringan diubah tanpa persetujuan oleh pihak yang tidak berwenang, yang dapat menyebabkan pelanggaran protokol keamanan.

3) **Kehilangan, Kerusakan:** data penting, konfigurasi jaringan, atau perangkat keras mengalami kehilangan atau kerusakan selama staf yang bertanggung jawab sedang tidak berada di tempat untuk mencegah atau memulihkan insiden tersebut.
contohnya: perangkat jaringan mengalami kerusakan fisik atau perangkat lunak dan karena staf Divisi Infrastruktur sedang cuti, perbaikan atau pemulihan tidak bisa segera dilakukan sehingga data penting hilang atau rusak.

4) **Gangguan:** operasional normal terganggu, menyebabkan keterlambatan atau penghentian layanan karena staf yang bertanggung jawab sedang cuti dan tidak ada pengganti yang memadai untuk menangani masalah teknis.
contohnya: Ketika ada gangguan jaringan yang mengakibatkan pengguna tidak dapat mengakses sistem internal organisasi, dan karena staf Divisi Infrastruktur yang memiliki pengetahuan khusus sedang cuti, masalah ini tidak dapat segera diatasi, menyebabkan downtime yang berkepanjangan.

1 response

ketika pegawai cuti, sudah aman pekerjaan yang seharusnya akan dilimpahkan ke pegawai yang tidak cuti

Seberapa seing staf Divisi Infrastruktur, Jaringan & Kean mengambil cuti sementara dan jelaskan bagaimana hal ini bisa mempengaruhi tugasnya?

1 response

jarang, 1 bulan terkadang 1 kali

Bagaimana dampaknya jika staf Divisi Infrastruktur, Jaringan & Keamanan meninggalkan oeganisasi secara permanen (misalnya karena pensiun atau pindah kerja)?
Jenis Dampaknya:
1) **Pengungkapan/penyingkapan:** Pengungkapan atau penyingkapan terjadi ketika informasi sensitif atau rahasia yang dimiliki oleh staf yang meninggalkan organisasi terungkap kepada pihak yang tidak berwenang.
contohnya: Mantan staf bisa tidak sengaja atau sengaja membocorkan rincian protokol keamanan jaringan kepada orang lain, termasuk pihak yang tidak berwenang.

2) **Modifikasi:** ada perubahan pada sistem atau data yang dilakukan tanpa otorisasi yang tepat, yang bisa disebabkan oleh ketidakhadiran staf kunci yang mengelola infrastruktur.
contohnya: Setelah staf yang bertanggung jawab meninggalkan organisasi, tidak ada orang lain yang memiliki pemahaman yang cukup mendalam tentang konfigurasi jaringan. Akibatnya, ada perubahan konfigurasi yang salah oleh staf baru yang tidak terlatih dengan baik, yang menyebabkan kerusakan pada sistem keamanan atau kinerja jaringan.

3) **Kehilangan, Kerusakan:** Kehilangan atau kerusakan terjadi ketika data, aset, atau perangkat penting tidak bisa ditemukan atau mengalami kerusakan akibat kurangnya pengelolaan setelah staf meninggalkan organisasi.
contohnya: file konfigurasi jaringan yang tidak terdokumentasi dengan baik, sehingga staf pengganti kesulitan untuk memulihkan atau mengelola jaringan dengan benar.

4) **Gangguan:** proses atau operasi normal terganggu karena ketidakhadiran staf yang berpengalaman dalam menangani infrastruktur jaringan dan keamanan.
contohnya: Penanganan insiden keamanan mungkin menjadi lambat atau tidak efektif, karena staf baru atau yang tersisa tidak memiliki pengetahuan teknis yang mendalam tentang sistem keamanan dan jaringan organisasi.

1 response

ketika ada pegawai yang pindah organisasi secara permanen, kami akan meminta aksesnya meminta dokumentasi yang selama ini dipegang. kamudian menonaktifkan semua akses yg dimiliki

Seberapa sering terjadi pergantian staf divisi ini dan bagaimana dampaknya pada operasional?

1 response

tidak pernah ada pergantian staff

Bagaimana ancaman terhadap pihak ketiga (misalnya pihak ketiga atau penyedia layanan) berdampak pada layanan yang diberikan kepada Divisi Infrastrutur, Jaringan & Keamanan?
Jenis Dampaknya:
1) **Pengungkapan/penyingkapan:** Pengungkapan adalah situasi di mana informasi sensitif atau rahasia dari pihak ketiga (misalnya penyedia layanan) dibocorkan atau diakses oleh pihak yang tidak berwenang.
contohnya: Jika penyedia layanan cloud mengalami kebocoran data, informasi rahasia tentang konfigurasi jaringan Divisi Infrastruktur bisa terungkap kepada publik atau hacker, sehingga menimbulkan risiko lebih lanjut bagi keamanan organisasi.

2) **Modifikasi:** Modifikasi terjadi ketika data atau sistem pihak ketiga diubah secara tidak sah, baik disengaja maupun tidak disengaja, yang bisa memengaruhi layanan yang diberikan kepada organisasi.
contohnya: Jika pihak ketiga yang mengelola perangkat jaringan mengalami modifikasi perangkat lunak tanpa otorisasi, perubahan tersebut bisa menyebabkan gangguan pada konfigurasi jaringan yang digunakan oleh Divisi Infrastruktur. Ini bisa menurunkan kinerja jaringan atau membuat jaringan rentan terhadap serangan.

3) **Kehilangan, Kerusakan:** Kehilangan atau kerusakan terjadi ketika data atau aset pihak ketiga hilang atau rusak, mengakibatkan gangguan pada layanan yang diberikan kepada organisasi.
contohnya: Jika penyedia layanan penyimpanan data mengalami kegagalan perangkat keras yang menyebabkan hilangnya data, Divisi Infrastruktur tidak bisa mengakses informasi penting yang disimpan di server eksternal, seperti backup data konfigurasi jaringan.

4) **Gangguan:** Gangguan adalah interupsi atau pemutusan layanan yang diberikan oleh pihak ketiga, yang dapat mengganggu operasional dan kinerja Divisi Infrastruktur dan Jaringan.
contohnya: Jika penyedia layanan internet mengalami gangguan besar (seperti serangan DDoS), Divisi Infrastruktur mungkin tidak dapat mengakses internet atau layanan jaringan eksternal yang diperlukan untuk menjalankan tugas harian mereka, menyebabkan penurunan produktivitas.

1 response

pihak ketiga, tidak memiliki akses server. Kendala yang munkin disebabkan oleh pihak ketiga adalah ketidak ketersediaan layanan. seperti internet yang mati atau ketika listrik mati.

Seberapa sering ancaman terjadi pada pihak ketiga, dan bagaimana itu memengaruhi kerja sehari-hari di divisi Infrastruktur, Jaringan & Keamanan?

1 response

ketidak ketersediaan layanan. seperti internet yang mati atau ketika listrik mati.

Kerusakan Perangkat Lunak

Bagaimana pengaruh kerusakan perangkat lunak pada perangkat jaringan dalam operasional sehari-hari? Jelaskan dampaknya.

1 response

kerusakan perangkat lunak tentu saja bisa menyebabkan data atau infomasi yang dapat diakses. atau terjadi penyingkapan informasi atau data. Kehilangan akses sistem, dan gangguan ketika mengakses layanan.

Berapa kali dan dalam kurun waktu berapa lama perangkat jaringan mengalami gangguan kerusakan perangkat lunak?

1 response

Sebulan bisa sampai 2 atau 3 kali dan perlu ditangani selama 1 jam

Catatan tambahan apa tentang ancaman kerusakan perangkat lunak pada perangkat jaringan yang ingin Anda catat?

1 response

selalu meminta anggota dalam melakukan update perangkat lunak

Berikan contoh bagaimana kerusakan perangkat lunak dapat mengancam perangkat jaringan.

1 response

perangkat lunak yang tidak pernah di update

Kegagalan Sistem

Bagaimana pengaruh kegagalan sistem pada perangkat jaringan dalam operasional sehari-hari? Jelaskan dampaknya.

1 response

gangguang terhadap layanan, sehingga pengguna tidak dapat mengakses layanan

Berapa kali dan dalam kurun waktu berapa lama perangkat jaringan mengalami gangguan kegagalan sistem?

1 response

jarang, 1 Tahun sekali dalam kurun waktu 1 jam

Catatan tambahan apa tentang ancaman kegagalan sistem pada perangkat jaringan yang ingin Anda catat?

1 response

melakukan perawatan terhadap perangkat jaringan

Berikan contoh bagaimana kegagalan sistem dapat mengancam perangkat jaringan.

1 response

switcth atau router tidak dapat dipakai

Kerusakan Perangkat Keras

Bagaimana pengaruh kerusakan perangkat keras pada perangkat jaringan dalam operasional sehari-hari? Jelaskan dampaknya.

1 response

Gangguan terjadi ketika operasional sistem terganggu atau terhenti, sehingga akses ke data atau layanan tidak bisa dilakukan. Ini sering disebabkan oleh masalah jaringan, kegagalan sistem, atau serangan siber.

Berapa kali dan dalam kurun waktu berapa lama perangkat jaringan mengalami gangguan kerusakan perangkat keras?

1 response

jarang, 1 tahun terkadang 1 kali selama 1 jam

Catatan tambahan apa tentang ancaman kerusakan perangkat keras pada perangkat jaringan yang ingin Anda catat?

1 response

melakukan pengecekan terhadap perangkat jaringan

Berikan contoh bagaimana kerusakan perangkat keras dapat mengancam perangkat jaringan.

1 response

Switch atau router mati

Kode Berbahaya

Kode berbahaya seperti apa yang pernah menyerang atau mengancam perangkat jaringan dan bagaimana pengaruh kode berbahaya (virus, worm, Trojan horse, back door) pada perangkat jaringan dalam operasional sehari-hari? Jelaskan dampaknya.

1 response

DDOS, menyebabkan gangguan, Gangguan terjadi ketika operasional sistem terganggu atau terhenti, sehingga akses ke data atau layanan tidak bisa dilakukan. Ini sering disebabkan oleh masalah jaringan, kegagalan sistem, atau serangan siber.

Berapa kali dan dalam kurun waktu berapa lama perangkat jaringan mengalami gangguan serangan kode berbahaya (virus, worm, Trojan horse, back door dll)?

1 response

1 bulan bisa 1 kali

Catatan tambahan apa tentang ancaman kode berbahaya pada perangkat jaringan yang ingin Anda catat?

1 response

mengidentidikasi sumber awal terjadi serangan

Berikan contoh bagaimana kode berbahaya dapat mengancam perangkat jaringan.

1 response

menyebabkan bandwith penuh dan layanan tidak dapat diakses, kode bahayanya terjadi peningkatan Bandwidth yang cukup tinggi

Siapa aktor yang paling mungkin menimbulkan ancaman terhadap perangkat jaringan melalui akses fisik?

1 response

External

Apakah akses ke ruang server dan perangkat jaringan dikendalikan dengan baik?

1 response

Dikendalikan dengan Baik

Siapa yang bertanggung jawab dalam mengelola akses fisik ke perangkat jaringan?

1 response

Tim Infra

Apa motif utama yang mungkin dimiliki pelaku dalam mengakses jalur fisik perangkat jaringan secara ilegal?

1 response

Faktor disengaja yang bertujuan untuk mencuri data

Seberapa tinggi kemungkinan motif dari pihak internal untuk melakukan serangan terhadap perangkat jaringan melalui akses fisik?

1 response

Kecil

Seberapa tinggi kemungkinan perangkat jaringan akan menjadi target serangan dari pihak eksternal melalui akses fisik (seperti mencuri perangkat keras jaringan)

1 response

Jawab pertanyaan ini jika aktor berasal dari pihak internal silakan jawab pertanyaan ini, jika aktor berasal dari pihak eksternal silakan jawab pertanyaan selanjutnya.

Apa jenis ancaman yang paling mungkin terjadi pada perangkat jaringan yang dilakukan oleh pihak internal melalui akses fisik?

1) **Pengungkapan**: Pengungkapan / kebocoran data sensitif oleh staf UPA TIK Undiksha

2) **Modifikasi**: Modifikasi data oleh staf UPA TIK yang tidak sah dan tidak adanya otorisasi

3) **Kehilangan, Kerusakan**: Kehilangan data akibat human eror

4) **Gangguan**: Serangan malware atau peretasan

**tuliskan deskripsi jawaban dalam bentuk seperti poin, isinya tidak harus sama bisa disesuaikan dengan kebutuhan atau kondisi organisasi*
**Anda bisa memilih lebih dari 1 pilihan jawaban yang disediakan.*

1 response

Serangan Malware

Jawab pertanyaan ini jika aktor berasal dari pihak eksternal silakan jawab pertanyaan ini, jika aktor berasal dari pihak internal silakan jawab pertanyaan sebelumnya.
*

Apa jenis ancaman yang paling mungkin terjadi pada perangkat jaringan yang dilakukan pihak eksternal melalui akses fisik?

1) **Pengungkapan**: Penyusupan oleh hacker atau pihak tidak dikenal

2) **Modifikasi**: Modifikasi data oleh aktor yang tidak dikena/diketahui

3) **Kehilangan, kerusakan**: Pencurian perangkat keras atau suku cadang

4) **Gangguan**: Bencana alam

**tuliskan deskripsi jawaban dalam bentuk seperti poin, isinya tidak harus sama bisa disesuaikan dengan kebutuhan atau kondisi organisasi*
**Anda bisa memilih lebih dari 1 pilihan jawaban yang disediakan.*

1 response

Pengungkapan: Penyusupan oleh hacker atau pihak tidak dikenal, Modifikasi: Modifikasi data oleh aktor yang tidak dikena/diketahui, dan Kehilangan, kerusakan: Pencurian perangkat keras atau suku cadang

Berapa kali perangkat jaringan mengalami gangguan fisik atau serangan fisik?

1 response

sangat jarang, gangguang fisik disebabkan ketidak tahuan pihak internal dengan asal memasang kabel jaringan ke perangkat jaringan sehingga menyebabkan loop dan jaringan menjadi error.

Responses cannot be edited

Kuesioner OCTAVE-S Tahap ke-2

Salam Harmoni,
Tujuan dari kuesioner ini adalah untuk mengumpulkan informasi. Informasi yang Anda berikan akan membantu saya dalam mengevaluasi ancaman aset kritis melalui jalur akses.
Saya mengharapkan kejujuran dan keterbukaan Anda dalam menjawab setiap pertanyaan. Semua jawaban akan dijaga kerahasiaannya dan hanya digunakan untuk keperluan penelitian saya yang berjudul "**ANALISIS MANAJEMEN RISIKO KEAMANAN INFORMASI MENGGUNAKAN *FRAMEWORK* OCTAVE-S DAN ISO 27001:2022.**"

* Indicates required question

Nama *

I Nyoman Yoga Setyawan

NIP *

199010162016080126l

Instansi *

UPA TIK Undiksha

Jabatan *

Anggota Divisi Sistem Informasi

Informasi Aset Kritis

Apakah ada risiko kegagalan sistem yang dapat mengakibatkan kehilangan data pada SIAK? *

ada

Apakah SIAK memiliki prosedur cadangan (backup) yang memadai? *

saat ini siak masih dilakukan backup manual, karena siak lama masih menggunakan teknologi federeted

Persyaratan Keamanan

Berikan alasan mengapa SIAK penting bagi organisasi? *

- core universitas adalah akademik. semua data penunjang akademik, proses pembelajaran digunakan untuk mempermudah pengadministrasian pencatatan riwayat pembelajaran, dan diperlukan untuk dilaporkan ke pangkalan data pendidikan tinggi. mulai dari mata kuliah, penawaran, kartu rencana studi, nilai matakuliah, perangkat pembelajaran (RPS,SPP,silabus), aktivitas kuliah mahasiswa, dan penunjang lainnya yang berhubungan dengan akademik.

Aset apa saja yang terkait dengan SIAK? *

Data riwayat pembelajaran meliputi, data mata kuliah, data krs, data nilai mahasiswa, data Perangkat Pembelajaran, dan aset untuk mengetahui data mining, untuk memutuskan sesuatu yang berhubungan dengan akademik.

Siapa saja yang menggunakan SIAK? *

Mahasiswa, Dosen, dan Pegawai

Apa persyaratan keamanan untuk perangkat jaringan? (petunjuk: berfokus pada persyaratan apa yang seharusnya ada pada sebuah aset, bukan pada apa yang ada saat ini) *

Berikut adalah persyaratan keamanannya:

1) **Kerahasiaan**: data akademik dan informasi pribadi harus dilindungi agar hanya dapat diakses oleh pengguna yang sah.

2) **Integritas**: data dalam sistem harus tetap akurat dan tidak boleh diubah oleh pihak yang tidak berwenang.

3) **Ketersediaan**: sistem harus tersedia untuk pengguna yang berwenang selama jam operasional yang diperlukan, dengan waktu pemulihan yang cepat jika terjadi gangguan.

tuliskan deskripsi jawaban dalam bentuk seperti poin, isinya tidak harus sama bisa disesuaikan dengan kebutuhan atau kondisi organisasi
**** bisa memilih lebih dari 1 persyaratan keamanan***

- Otentikasi (Authentication):
Setiap pengguna SIAK yang mencoba mengakses sistem harus diverifikasi identitasnya. Ini bisa dilakukan melalui kata sandi yang kuat, biometrik, otentikasi multi-faktor, atau sertifikat digital.

-Otorisasi (Authorization):
Pengguna yang telah terotentikasi hanya diberikan akses sesuai dengan hak mereka. Ini membatasi apa yang dapat dilakukan pengguna di dalam sistem SIAK.

Persyaratan keamanan mana yang paling penting untuk SIAK? *

- ○ Kerahasiaan
- ◉ Integritas
- ○ Ketersediaan

Identifikasi Ancaman Pada SIAK Melalui Jalur Akses Jaringan

Siapa aktor yang paling mungkin menimbulkan ancaman terhadap SIAK melalui akses jaringan? *

Aktor dapat berasal dari pihak internal atau eksternal.

Berikan deskripsi apakah aktor tersebut termasuk ke dalam pihak internal atau eksternal pada jawaban seperti contoh berikut: Mahasiswa (pihak eksternal).

1. Mahasiswa (pihak eksternal):
Mahasiswa dapat menjadi ancaman jika mencoba mendapatkan akses ke data akademik untuk mengubah nilai, melihat data pribadi mahasiswa lain, atau mencari informasi sensitif. Mereka umumnya adalah pengguna eksternal sistem yang dapat mencoba meretas atau memanipulasi data.
2. Dosen (pihak internal):
Sebagai pengguna internal, dosen memiliki akses langsung ke SIAK untuk mengelola nilai dan informasi akademik. Jika ada kesalahan atau niat jahat, mereka bisa memanipulasi data secara langsung atau membocorkan informasi sensitif.
3. Pegawai operator (pihak internal):
Pegawai yang terlibat dalam proses administrasi akademik memiliki akses ke berbagai data sensitif di SIAK. Meskipun sebagian besar mungkin tidak bermaksud jahat, mereka bisa menjadi ancaman baik melalui kecerobohan (seperti penggunaan kata sandi lemah) atau penyalahgunaan akses.
4. Peretas (pihak eksternal):
Peretas dari luar organisasi yang mencoba masuk ke dalam sistem SIAK untuk tujuan keuangan, sabotase, atau hanya mencari tantangan. Mereka bisa memanfaatkan kelemahan dalam keamanan jaringan atau perangkat lunak untuk mencuri atau merusak data.
5. Mantan Pegawai (pihak internal/eksternal):
Mantan pegawai atau staf yang tidak lagi bekerja di institusi tetapi masih memiliki akses ke sistem. Mereka bisa menggunakan akses lama mereka untuk merusak sistem, mencuri data, atau melakukan tindakan pembalasan.

Apakah akses jaringan ke SIAK dikendalikan dengan baik? *

Ya

Siapa yang bertanggung jawab dalam mengelola keamanan akses jaringan pada SIAK? *

Divisi Infrastruktur, Jaringan, dan Keamanan

*

Apa motif utama yang mungkin dimiliki pelaku dalam menyerang atau mengakses SIAK secara illegal melalui jaringan?

Motif terdapat 2 kelompok yaitu sengaja dan tidak sengaja.

Berikan deskripsi apakah motif tersebut sengaja atau tidak sengaja pada jawaban seperti contoh berikut: Melakukan modifikasi pada konfigurasi perangkat (sengaja).

Melakukan perubahan nilai, yang dilakukan oleh mahasiswa menggunakan akun dosen (sengaja)

Seberapa tinggi kemungkinan motif dari pihak internal untuk melakukan serangan terhadap SIAK?

Sedang

Seberapa tinggi kemungkinan SIAK akan menjadi target serangan dari pihak eksternal (seperti hacker atau pencuri data)? *

Tinggi

Jawab pertanyaan ini jika aktor berasal dari pihak eksternal silakan jawab pertanyaan ini, jika aktor berasal dari pihak internal silakan jawab pertanyaan sebelumnya.

Apa jenis ancaman yang paling mungkin terjadi pada SIAK yang dilakukan pihak eksternal?

Apa jenis ancaman yang paling mungkin terjadi pada perangkat jaringan yang dilakukan pihak eksternal?

1) **Pengungkapan**: Penyusupan oleh hacker atau pihak tidak sah untuk mempublikasi data sensitif

2) **Modifikasi**: Modifikasi data oleh aktor yang tidak dikenal/diketahui

3) **Kehilangan, Kehancuran**: Kehilangan data akibat serangan dari pihak luar/pihak eksternal yang tidak diketahui

4) **Gangguan**: Serangan malware atau peretasan

**tuliskan deskripsi jawaban dalam bentuk seperti poin, isinya tidak harus sama bisa disesuaikan dengan kebutuhan atau kondisi organisasi*

**Anda bisa memilih lebih dari 1 pilihan jawaban yang disediakan.*

2. Modifikasi, Perubahan nilai yang dilakukan oleh mahasiswa sendiri dikarenakan dosen memberikan akun masuk sistem.

Jawab pertanyaan ini jika aktor berasal dari pihak internal silakan jawab pertanyaan ini, jika aktor berasal dari pihak eksternal silakan jawab pertanyaan selanjutnya.

Apa jenis ancaman yang paling mungkin terjadi pada SIAK yang dilakukan oleh pihak internal melalui jaringan?

1) **Pengungkapan**: Pengungkapan / kebocoran data sensitif oleh staf UPA TIK Undiksha.

2) **Modifikasi**: Modifikasi data oleh Staf UPA TIK yang tidak sah dan tidak adanya otorisasi

3) **Kehilangan, Kerusakan**: Kehilangan data akibat human error

4) **Gangguan**: Serangan malware atau peretasan

**tuliskan deskripsi jawaban dalam bentuk seperti poin, isinya tidak harus sama bisa disesuaikan dengan kebutuhan atau kondisi organisasi*

**Anda bisa memilih lebih dari 1 pilihan jawaban yang disediakan.*

2. Modifikasi data oleh staf UPA TIK. Ini dikarenakan pada SIAK lama, terdapat kebijakan, seharusnya tidak bisa dilakukan namun terdapat persetujuan pimpinan. sehingga dilakukan secara paksa.

Berapa kali SIAK mengalami gangguan jaringan atau serangan jaringan? *

Sebutkan dan jelaskan gangguannya

Karena down banyak akses secara bersamaan

Seberapa sering dilakukan pemeliharaan pada SIAK untuk mencegah ancaman keamanan? *

berikan skala seperti contohnya: 1kali perminggu

1 kali per 6 bulan (akan padatnya akses)

Identifikasi Ancaman Pada Perangkat Jaringan Melalui Jalur Akses Fisik

Siapa aktor yang memiliki akses fisik perangkat yang menjadi host SIAK di Universitas Pendidikan Ganesha dan apakah actor tersebut memiliki peluang menjadi ancaman? *

Aktor dapat berasal dari pihak internal atau eksternal.

Berikan deskripsi apakah aktor tersebut termasuk ke dalam pihak internal atau eksternal pada jawaban seperti contoh berikut: Divisi Sistem Informasi (pihak internal).

Peluang Menjadi Ancaman: Karena memiliki kontrol penuh, staf dari divisi SI berpotensi menjadi ancaman jika ada kesalahan konfigurasi atau jika ada individu dengan niat jahat yang dapat menyalahgunakan akses mereka.

Apakah akses jaringan ke SIAK dikendalikan dengan baik? *

Iya

Siapa yang bertanggung jawab atas keamanan fisik perangkat yang digunakan divisi sistem informasi (SIAK)? *

Divisi Infrastruktur, Jaringan, dan Keamanan

Apa motif utama yang mungkin ingin mengakses perangkat fisik yang menjalankan SIAK? *

**Motif terdapat 2 kelompok yaitu sengaja dan tidak sengaja.*

**Berikan deskripsi apakah motif tersebut sengaja atau tidak sengaja pada jawaban seperti contoh berikut: Mencuri data (sengaja).*

Motif serangan supaya layanan tidak bisa d akses (sengaja)

Seberapa besar kemungkinan adanya ancaman dari aktor internal yang ingin mengakses perangkat yang dimiliki divisi sistem informasi secara fisik? *

Tinggi: Jika ada motivasi seperti kepentingan pribadi, ketidakpuasan kerja, atau balas dendam, aktor internal dengan akses fisik bisa mencoba mengeksploitasi sistem. Contohnya, seorang pegawai yang merasa tidak puas atau terancam dengan perubahan kebijakan dapat termotivasi untuk menyalahgunakan aksesnya.

Seberapa tinggi kemungkinan SIAK akan menjadi target serangan dari pihak eksternal secara fisik (seperti vendor atau tamu)? *

Jika SIAK menyimpan data akademik sensitif (seperti nilai mahasiswa, data pribadi, atau dokumen penting lainnya), ini bisa menjadi target menarik bagi pihak eksternal yang ingin mencuri informasi atau merusak reputasi institusi.
Vendor atau pihak tamu yang memiliki akses fisik ke perangkat SIAK mungkin dimotivasi oleh keuntungan finansial, pencurian data untuk dijual, atau bahkan sabotase untuk tujuan tertentu.

Jawab pertanyaan ini jika aktor berasal dari pihak internal silakan jawab pertanyaan ini, jika aktor berasal dari pihak eksternal silakan jawab pertanyaan selanjutnya.

Apa ancaman yang mungkin terjadi jika ada akses fisik tidak sah dari pihak internal pada perangkat yang dimiliki divisi Sistem Informasi utuk melakukan pekerjaannya?

1) **Pengungkapan**: Pengungkapan / kebocoran data sensitif oleh staf UPA TIK Undiksha

2) **Modifikasi**: Modifikasi data oleh staf UPA TIK yang tidak sah dan tidak adanya otorisasi

3) **Kehilangan, Kerusakan**: Kehilangan data/perangkat akibat human eror

4) **Gangguan**: Serangan malware atau peretasan.

**tuliskan deskripsi jawaban dalam bentuk seperti poin, isinya tidak harus sama bisa disesuaikan dengan kebutuhan atau kondisi organisasi*
**Anda bisa memilih lebih dari 1 pilihan jawaban yang disediakan.*

3)Kehilangan, Kehilangan diakbiatkan human error, terjadi kesalahan query.
Kehilangan data dapat mengakibatkan kerugian operasional yang signifikan, termasuk downtime sistem, kehilangan informasi penting, dan gangguan dalam layanan akademik. Jika perangkat rusak secara fisik, waktu dan biaya pemulihan bisa tinggi.

*

Berapa kali perangkat yang dimiliki divisi dalam mengembangkan sistem mengalami ancaman fisik?

**Sebutkan dan jelaskan gangguannya.*

Beberapa kali:
1. Pernah mengalami serangan ddos, ini sengaja dilakukan agar sistem sulit untuk di akses dari pihak luar (saingan)
2. Pernah mengalami down database karena akses membludak

Langkah apa yang telah diterapkan untuk mengamankan akses fisik ke perangkat? *

1. Pemindahan ke server docker dari server cluster
2. Pemasangan Porti Git
3. Update Dependency pada sistem

Submitted 9/27/24, 2:43 PM

Kerusakan Perangkat Lunak

*

Bagaimana pengaruh kerusakan perangkat lunak pada SIAK dalam operasional sehari-hari? Jelaskan dampaknya.

Jenis Dampak

1) Penyingkapan: Penyingkapan terjadi ketika informasi atau data yang seharusnya dirahasiakan terungkap atau diakses oleh pihak yang tidak berwenang.

2) Modifikasi: Modifikasi adalah perubahan data atau sistem oleh pihak yang tidak berwenang, baik disengaja maupun tidak. Ini dapat mengubah integritas data yang disimpan dalam sistem.

3) Kehilangan, kehancuran: Kehilangan terjadi ketika data atau aset tidak lagi tersedia, baik karena kerusakan fisik (kehancuran) atau kehilangan secara digital. Ini bisa berupa data yang hilang atau rusak tanpa dapat dipulihkan.

4) Gangguan: Gangguan terjadi ketika operasional sistem terganggu atau terhenti, sehingga akses ke data atau layanan tidak bisa dilakukan. Ini sering disebabkan oleh masalah jaringan, kegagalan sistem, atau serangan siber.

Kerusakan perangkat lunak pada Sistem Informasi Akademik (SIAK) bisa berdampak sangat signifikan pada operasional harian di lingkungan pendidikan, terutama karena SIAK merupakan sistem inti yang mengelola data akademik dan administrasi.

Berapa kali dan dalam kurun waktu berapa lama SIAK mengalami gangguan kerusakan perangkat lunak? *

Setahun 2 kali, biasanya saat padat akses (musim krsan, dan aktivitas lain terjadi berbarengan)

Catatan tambahan apa tentang ancaman kerusakan perangkat lunak pada SIAK yang ingin Anda catat? *

Kegagalan Sistem atau Downtime: Pemeliharaan perangkat keras atau perangkat lunak yang tidak terjadwal dapat mengakibatkan kegagalan sistem. Ketika SIAK tidak dapat diakses, kegiatan akademik seperti pengisian KRS dan pengambilan nilai dapat terganggu.

Berikan contoh bagaimana kerusakan perangkat lunak dapat mengancam SIAK. *

Contoh : jadwal aktivitas dilakukan secara berbarengan, semisal KRSan, Pendaftaran Wisuda, Cetak Nominatif, cetak ijazah, dan transkrip nilai

Kegagalan Sistem

Bagaimana pengaruh kegagalan sistem pada SIAK dalam operasional sehari-hari? Jelaskan dampaknya. *

Jenis Dampak

1) Penyingkapan: Penyingkapan terjadi ketika informasi atau data yang seharusnya dirahasiakan terungkap atau diakses oleh pihak yang tidak berwenang.

2) Modifikasi: Modifikasi adalah perubahan data atau sistem oleh pihak yang tidak berwenang, baik disengaja maupun tidak. Ini dapat mengubah integritas data yang disimpan dalam sistem.

3) Kehilangan, kehancuran: Kehilangan terjadi ketika data atau aset tidak lagi tersedia, baik karena kerusakan fisik (kehancuran) atau kehilangan secara digital. Ini bisa berupa data yang hilang atau rusak tanpa dapat dipulihkan.

4) Gangguan: Gangguan terjadi ketika operasional sistem terganggu atau terhenti, sehingga akses ke data atau layanan tidak bisa dilakukan. Ini sering disebabkan oleh masalah jaringan, kegagalan sistem, atau serangan siber.

Kegagalan sistem pada Sistem Informasi Akademik (SIAK) dapat memberikan dampak yang serius pada operasional sehari-hari di institusi pendidikan, karena sistem ini berperan penting dalam pengelolaan data akademik, administrasi, dan layanan kepada mahasiswa, dosen, serta staf.

Secara keseluruhan, kegagalan sistem pada SIAK berdampak negatif pada efisiensi, keamanan data, serta kepuasan pengguna, sehingga penting bagi institusi untuk memastikan ketahanan sistem, keamanan data, dan prosedur pemulihan yang cepat untuk meminimalkan risiko dan dampak dari kegagalan sistem.

Berapa kali dan dalam kurun waktu berapa lama SIAK mengalami gangguan kegagalan sistem? *

Biasanya setiap Semester 1 tahun 2 kali

Catatan tambahan apa tentang ancaman kegagalan sistem pada SIAK yang ingin Anda catat? *

Skalabilitas dan Ketahanan Sistem: SIAK perlu dibangun agar mampu menangani lonjakan beban, khususnya saat periode pendaftaran atau pengumuman nilai. Kegagalan skalabilitas dapat menyebabkan sistem tidak merespons di waktu-waktu kritis.

Berikan contoh bagaimana kegagalan sistem dapat mengancam SIAK. *

Contoh secara bersamaan terjadi aktivitas yang berbeda, seperti saat krs dilakukan berbarengan dengan pendaftaran wisuda, unduh nominatif wisuda, unduh ijazah, unduh transkrip nilai

Kerusakan Perangkat Keras

Bagaimana pengaruh kerusakan perangkat keras pada SIAK dalam operasional sehari-hari? Jelaskan dampaknya. *

Jenis Dampak

1) Penyingkapan: Penyingkapan terjadi ketika informasi atau data yang seharusnya dirahasiakan terungkap atau diakses oleh pihak yang tidak berwenang.

2) Modifikasi: Modifikasi adalah perubahan data atau sistem oleh pihak yang tidak berwenang, baik disengaja maupun tidak. Ini dapat mengubah integritas data yang disimpan dalam sistem.

3) Kehilangan, kehancuran: Kehilangan terjadi ketika data atau aset tidak lagi tersedia, baik karena kerusakan fisik (kehancuran) atau kehilangan secara digital. Ini bisa berupa data yang hilang atau rusak tanpa dapat dipulihkan.

4) Gangguan: Gangguan terjadi ketika operasional sistem terganggu atau terhenti, sehingga akses ke data atau layanan tidak bisa dilakukan. Ini sering disebabkan oleh masalah jaringan, kegagalan sistem, atau serangan siber.

Kegagalan sistem pada Sistem Informasi Akademik (SIAK) dapat memberikan dampak yang serius pada operasional sehari-hari di institusi pendidikan, karena sistem ini berperan penting dalam pengelolaan data akademik, administrasi, dan layanan kepada mahasiswa, dosen, serta staf.

Secara keseluruhan, kegagalan sistem pada SIAK berdampak negatif pada efisiensi, keamanan data, serta kepuasan pengguna, sehingga penting bagi institusi untuk memastikan ketahanan sistem, keamanan data, dan prosedur pemulihan yang cepat untuk meminimalkan risiko dan dampak dari kegagalan sistem.

Berapa kali dan dalam kurun waktu berapa lama SIAK mengalami gangguan kerusakan perangkat keras? *

Setiap tahun 2 kali

Catatan tambahan apa tentang ancaman kerusakan perangkat keras pada SIAK yang ingin Anda catat? *

Skalabilitas dan Ketahanan Sistem: SIAK perlu dibangun agar mampu menangani lonjakan beban, khususnya saat periode pendaftaran atau pengumuman nilai. Kegagalan skalabilitas dapat menyebabkan sistem tidak merespons di waktu-waktu kritis.

Berikan contoh bagaimana kerusakan perangkat keras dapat mengancam SIAK. *

Terdapat aktivitas banyak dilakukan secara berbarengan, seperti saat KRS dilakukan juga pendaftaran wisuda, cetak nominatif, cetak ijazah, cetak transkrip nilai

Kode Berbahaya

Kode berbahaya seperti apa yang pernah menyerang atau mengancam SIAK dan bagaimana pengaruh kode berbahaya (virus, worm, Trojan horse, back door) pada SIAK dalam operasional sehari-hari? Jelaskan dampaknya. *

Jenis Dampak

1) Penyingkapan: Penyingkapan terjadi ketika informasi atau data yang seharusnya dirahasiakan terungkap atau diakses oleh pihak yang tidak berwenang.

2) Modifikasi: Modifikasi adalah perubahan data atau sistem oleh pihak yang tidak berwenang, baik disengaja maupun tidak. Ini dapat mengubah integritas data yang disimpan dalam sistem.

3) Kehilangan, kehancuran: Kehilangan terjadi ketika data atau aset tidak lagi tersedia, baik karena kerusakan fisik (kehancuran) atau kehilangan secara digital. Ini bisa berupa data yang hilang atau rusak tanpa dapat dipulihkan.

4) Gangguan: Gangguan terjadi ketika operasional sistem terganggu atau terhenti, sehingga akses ke data atau layanan tidak bisa dilakukan. Ini sering disebabkan oleh masalah jaringan, kegagalan sistem, atau serangan siber.

Kode berbahaya, seperti virus, worm, Trojan horse, dan backdoor, dapat memberikan dampak serius pada Sistem Informasi Akademik (SIAK) yang digunakan dalam lingkungan pendidikan. Jenis-jenis kode berbahaya ini sering kali menyusup ke dalam sistem melalui jaringan yang terhubung ke internet, email, atau perangkat eksternal, yang pada akhirnya dapat mengganggu operasional harian SIAK.

Kode berbahaya dapat memengaruhi SIAK dalam berbagai cara, mulai dari penyingkapan data, modifikasi yang tidak sah, kehilangan data yang tidak dapat dipulihkan, hingga gangguan operasional yang menghambat akses ke layanan penting. Untuk meminimalkan risiko, institusi perlu menerapkan langkah-langkah keamanan seperti firewall, antivirus, backup data secara berkala, dan pemantauan sistem untuk mendeteksi dan mengatasi ancaman sebelum terjadi kerusakan lebih lanjut.

Berapa kali dan dalam kurun waktu berapa lama SIAK mengalami gangguan serangan kode berbahaya (virus, worm, Trojan horse, back door dll)? *

5 tahun sekali

Catatan tambahan apa tentang ancaman kode berbahaya pada SIAK yang ingin Anda catat? *

Pembaruan Sistem dan Keamanan Berkala: Kode berbahaya seperti virus dan Trojan sering mengeksploitasi celah keamanan pada perangkat lunak yang belum diperbarui. Melakukan pembaruan secara rutin dapat menutup celah tersebut dan mengurangi risiko infeksi.

Berikan contoh bagaimana kode berbahaya dapat mengancam SIAK. *

Backdoor yang Memungkinkan Akses Tidak Sah
Seorang penyerang dapat memasukkan backdoor ke dalam SIAK untuk mendapatkan akses tidak sah ke sistem. Setelah berhasil, penyerang dapat mengubah data penting, seperti nilai akademik atau jadwal kuliah. Misalnya, penyerang dapat memodifikasi catatan akademik, yang mengganggu integritas data dan menciptakan masalah serius bagi administrasi institusi. Selain itu, backdoor ini juga memungkinkan serangan berkelanjutan, karena penyerang dapat masuk kapan saja tanpa terdeteksi.

Submitted 11/4/24, 9:55AM

Responses cannot be edited

Kuesioner OCTAVE-S Tahap ke-2

Salam Harmoni,
Tujuan dari kuesioner ini adalah untuk mengumpulkan informasi. Informasi yang Anda berikan akan membantu saya dalam mengevaluasi ancaman aset kritis melalui jalur akses.
Saya mengharapkan kejujuran dan keterbukaan Anda dalam menjawab setiap pertanyaan. Semua jawaban akan dijaga kerahasiaannya dan hanya digunakan untuk keperluan penelitian saya yang berjudul "**ANALISIS MANAJEMEN RISIKO KEAMANAN INFORMASI MENGGUNAKAN *FRAMEWORK* OCTAVE-S DAN ISO 27001:2022.**"

* Indicates required question

Nama *

Putu Wendy Ariyani

NIP *

199611272002030201

Instansi *

UPA TIK Undiksha

Jabatan *

Anggota Helpdesk dan Dokumentasi

Persyaratan Keamanan

Berikan alasan mengapa SOP dan Instruksi Kerja penting bagi organisasi? *

memulai pekerjaan bisa berdasarkan SOP dan IK yang sudah ditetapkan

Aset apa saja yang terkait dengan SOP dan Instruksi Kerja? *

dokumen sop dan IK, template SOP dan IK, Log perubahan SOP dan IK

Siapa saja yang menggunakan SOP dan Instruksi Kerja? *

SOP digunakan oleh civitas akademikan, IK digunakan oleh masing-masing divisi terkait

Informasi Aset Kritis

Apakah ada kemungkinan perubahan tidak sah pada SOP dan instruksi kerja dan apa dampaknya pada kegiatan operasionel sehari-hari? *

Tidak ada, perubahan SOP dan instruksi kerja selalu melalui diskusi namun tidak pernah tercatat atau pembaharuan di daftar dokumen SOP

Bagaimana cara UPA TIK Undiksha dalam menjaga agar dokumen SOP tetap aman dari akses tidak berwenang? *

Menyimpan pada gdrive dan tidak memberikan akses ke semua orang, akses diberikan sesuai dengan divisi masing-masing.

Apa persyaratan keamanan untuk SOP dan Instruksi Kerja? *

Berikut adalah persyaratan keamanannya:

1) **Kerahasiaan**: dokumen hanya dibatasi aksesnya hanya kepada personil yang berwenang.

2) **Integritas**: dokumen harus dilindungi dari perubahan yang tidak sah dan harus dapat dilacak siapa yang membuat perubahan.

3) **Ketersediaan**: dokumen harus tersedia dan mudah diakses oleh staf UPA TIK Undiksha.

tuliskan deskripsi jawaban dalam bentuk seperti poin, isinya tidak harus sama bisa disesuaikan dengan kebutuhan atau kondisi organisasi
**** bisa memilih lebih dari 1 persyaratan keamanan***

1,3 kerahasiaan dokumen harus dijaga, namun ada beberapa SOP yang harus dipublish di ketahui civitas akademik seperti SOP permintaan layanan SI/TI. Ketersediaan harus bisa diakses dengan mudah juga oleh staff UPA TIK

Persyaratan keamanan mana yang paling penting untuk SOP dan Instruksi Kerja? *
**bisa memilih lebih dari 1 persyaratan keamanan*

- [x] Kerahasiaan
- [ ] Integritas
- [x] Ketersediaan

Identifikasi Ancaman Pada SOP dan Instruksi Kerja Melalui Jalur Akses Jaringan

Jalur akses jaringan mengacu pada cara dan proses yang digunakan untuk mengakses informasi sensitif secara online melalui jaringan internal atau eksternal.

Siapa yang memiliki akses ke SOP dan Instruksi Kerja melalui akses jaringan? *

****Aktor dapat berasal dari pihak internal atau eksternal.***

****Berikan deskripsi apakah aktor tersebut termasuk ke dalam pihak internal atau eksternal pada jawaban seperti contoh berikut: Staf UPA TIK Undiksha (pihak internal).***

Staf UPA TIK Undiksha (pihak internal)

Apakah akses jaringan ke SOP dan Instruksi Kerja dibatasi hanya untuk personil yang berwenang? *

- ○ Terbatas hanya pada sebagian personil
- ◉ Akses terbuka bagi semua pegawai
- ○ Akses tersedia bagi pihak eksternal juga

Apa kemungkinan motif ancaman melalui akses jaringan terhadap SOP dan Instruksi Kerja? *

Motif terdapat 2 kelompok yaitu sengaja dan tidak sengaja.

Berikan deskripsi apakah motif tersebut sengaja atau tidak sengaja pada jawaban seperti contoh berikut: Melakukan pencurian data untuk kepentingan pihak ketiga (sengaja).

Melakukan pencurian data untuk kepentingan pihak ketiga (sengaja).

Seberapa tinggi kemungkinan risiko perubahan atau modifikasi tidak sah pada SOP dan Instruksi Kerja melalui jaringan? *

Sangat tinggi

Seberapa tinggi kemungkinan pihak eksternal (seperti vendor atau tamu) dapat mengakses SOP dan Instruksi Kerja melalui jaringan? *

Terkait ini kurang tau

Jawab pertanyaan ini jika aktor berasal dari pihak internal silakan jawab pertanyaan ini, jika aktor berasal dari pihak eksternal silakan jawab pertanyaan selanjutnya.

Apa ancaman jaringan utama yang mungkin terjadi pada SOP dan Instruksi Kerja yang dilakukan oleh pihak internal?

1) **Pengungkapan**: Pembocoran SOP dan Instruksi Kerja ke publik oleh pegawai internal secara tidak sah.

2) **Modifikasi**: Perubahan tidak sah oleh pegawai internal.

3) **Kehilangan, Kerusakan**: Penghapusan data akibat kelalaian.

4) **Gangguan**: Kesalahan dalam pemeliharaan sistem.

**tuliskan deskripsi jawaban dalam bentuk seperti poin, isinya tidak harus sama bisa disesuaikan dengan kebutuhan atau kondisi organisasi*

**Anda bisa memilih lebih dari 1 pilihan jawaban yang disediakan.*

Gangguan Pemeliharaan Sistem: Kesalahan dalam pemeliharaan atau pembaruan sistem yang menyimpan SOP dan Instruksi Kerja dapat mengakibatkan ketidakmampuan karyawan untuk mengakses dokumen tersebut secara efisien. Hal ini bisa menghambat pelaksanaan SOP di lapangan.

Jawab pertanyaan ini jika aktor berasal dari pihak eksternal silakan jawab pertanyaan ini, jika aktor berasal dari pihak internal silakan jawab pertanyaan sebelumnya.

Apa ancaman jaringan utama yang mungkin terjadi pasa SOP dan Instruksi Kerja yang dilakukan oleh pihak eksternal?

1) **Pengungkapan**: Pengungkapan ke publik oleh pihak eksternal

2) **Modifikasi**: Perubahan tanpa otorisasi oleh pihak yang tidak diketahui.

3) **Kehilangan, Kehancuran**: Pencurian data oleh pihak eksternal.

4) **Gangguan**: Percobaan mengakses data tersebut.

**tuliskan deskripsi jawaban dalam bentuk seperti poin, isinya tidak harus sama bisa disesuaikan dengan kebutuhan atau kondisi organisasi*

**Anda bisa memilih lebih dari 1 pilihan jawaban yang disediakan.*

Kehilangan atau Kerusakan Data, SOP dan Instruksi Kerja dapat hilang atau rusak karena kelalaian, seperti penghapusan data yang tidak disengaja

Seberapa sering jaringan yang mengakses SOP dan Instruksi Kerja dipantau untuk mendeteksi ancaman? *

Terkait ini kurang mengetahui

Apakah pernah ada insiden terkait ancaman jaringan terhadap SOP dan Instruksi Kerja sebelumnya? *

Sebutkan dan jelaskan insiden tersebut.

belum pernah

Identifikasi Ancaman Pada SOP dan Instruksi Kerja Melalui Jalur Akses Jaringan

Penyimpanan dokumen SOP dan Instruksi Kerja di perangkat fisik atau media penyimpanan yang tidak terhubung ke jaringan eksternal atau cloud

Siapa yang memiliki akses fisik ke dokumen SOP dan Instruksi Kerja (misalnya, versi cetak atau file yang disimpan secara lokal)? *

Aktor dapat berasal dari pihak internal atau eksternal.

Berikan deskripsi apakah aktor tersebut termasuk ke dalam pihak internal atau eksternal pada jawaban seperti contoh berikut: Mahasiswa (pihak eksternal).

Div Helpdesk

Apakah akses fisik ke dokumen SOP dan Instruksi Kerja dibatasi hanya untuk personel yang berwenang atau terbuka bagi semua pegawai UPA TIK atau tersedia bagi pihak eksternal juga? *

Semua Pegawai UPA TIK

Apakah ada sistem pencatatan atau log untuk mencatat akses fisik ke dokumen SOP dan Instruksi Kerja? *

Ada daftar dokumen

Apa kemungkinan motif ancaman fisik terhadap dokumen SOP dan Instruksi Kerja? *

**Motif terdapat 2 kelompok yaitu sengaja dan tidak sengaja.*

**Berikan deskripsi apakah motif tersebut sengaja atau tidak sengaja pada jawaban seperti contoh berikut: Melakukan modifikasi atau perubahan dokumen tidak sah (sengaja).*

tidak sengaja kemungkinan hilang atau lupa menyimpan dimana

Seberapa besar risiko perubahan tidak sah pada SOP dan Instruksi Kerja akibat akses fisik? *

rendah

Apa ancaman fisik utama yang mungkin terjadi pada dokumen SOP dan Instruksi Kerja? *

1) **Pengungkapan**: Mempublikasi dokumen secara tidak sah dan tanpa adanya izin.

2) **Modifikasi**: Perubahan tidak sah oleh pegawai.

3) **Kehilangan, Kerusakan**: Kehilangan atau kerusakan dokumen akibat kelalaian.

4) **Gangguan**: Penghapusan yang disengaja.

**tuliskan deskripsi jawaban dalam bentuk seperti poin, isinya tidak harus sama bisa disesuaikan dengan kebutuhan atau kondisi organisasi*
**Anda bisa memilih lebih dari 1 pilihan jawaban yang disediakan.*

Kehilangan, Kerusakan: Kehilangan atau kerusakan dokumen akibat kelalaian.

Apakah dokumen SOP dan Instruksi Kerja disimpan dalam lemari yang terkunci atau di lokasi yang aman secara fisik? *

dilemari yang terkunci

Seberapa sering pengecekan atau audit fisik dilakukan untuk memastikan keamanan dokumen SOP dan Instruksi Kerja? *

Berikan skala seperti contohnya: 1 kali perminggu

1 bulan 1 kali

Apakah pernah ada insiden terkait ancaman fisik terhadap dokumen SOP dan Instruksi Kerja sebelumnya? Berapa kali terjadi? Dan jelaskan insidennya. *

belum pernah

Submitted 11/6/24, 11:10 AM

Lampiran 11. Lembar Kerja Evaluasi Kriteria Dampak

1. Lembar Kerja Evaluasi Kriteria Dampak – Reputasi dan Kehilangan Aset

Reputasi dan Kehilangan Aset			
Jenis Dampak	**Dampak Rendah**	**Dampak Sedang**	**Dampak Tinggi**
Reputasi		✓	
Kehilangan Aset			✓

2. Lembar Kerja Evaluasi Kriteria Dampak – Keuangan

Keuangan			
Jenis Dampak	**Dampak Rendah**	**Dampak Sedang**	**Dampak Tinggi**
Biaya Operasional			✓

3. Lembar Kerja Evaluasi Kriteria Dampak – Produktivitas

Produktivitas			
Jenis Dampak	**Dampak Rendah**	**Dampak Sedang**	**Dampak Tinggi**
Jam Kerja			✓

4. Lembar Kerja Kriteria Evaluasi Dampak – Kesehatan/Keselamatan

Kesehatan/Keselamatan			
Jenis Dampak	**Dampak Rendah**	**Dampak Sedang**	**Dampak Tinggi**
Kesehatan/Keselamatan Pegawai		✓	

Lampiran 12. Lembar Kerja Identifikasi Aset Organisasi

1. Identifikasi Aset Organisasi – Informasi, Sistem, dan Aplikasi

Informasi, Sistem, dan Aplikasi			
Sistem	**Informasi**	**Aplikasi dan Layanan**	**Aset Lainnya**
Server	SOP dan Instruksi Kerja	SIAK	Perangkat Jaringan

2. Identifikasi Aset Organisasi – Informasi, Sistem, dan Aplikasi

Sumber Daya Manusia			
Sumber Daya Manusia	**Keterampilan dan Pengetahuan**	**Sistem terkait**	**Aset Terkait**
Sekretaris UPA TIK Undiksha dan Divisi Infrastruktur, Jaringan & keamanan.	Jaringan dan Pemrograman	OS, Windows, Linux, Tool Pemrograman	Komputer dan Laptop

Lampiran 13. Lembar Kerja Evaluasi Praktik Keamanan

1. Evaluasi Praktik Keamanan – Kesadaran dan Pelatihan Keamanan

1. Kesadaran dan Pelatihan Keamanan				
Pernyataan	**Sejauh mana pernyataan ini tercermin dalam organisasi**			
	Sangat Banyak	Agak	Tidak sama sekali	Tidak Tahu
Anggota staf memahami peran dan tanggung jawab keamanan mereka. Hal ini didokumentasikan dan diverifikasi.	✓			
Terdapat keahlian internal yang memadai untuk semua layanan, mekanisme, dan teknologi yang didukung (misalnya, pencatatan, pemantauan, atau enkripsi), termasuk operasi yang aman. Hal ini didokumentasikan dan diverifikasi.	✓			

Kesadaran akan keamanan, pelatihan, dan pengingat berkala disediakan untuk semua personel. Pemahaman staf didokumentasikan dan kesesuaiannya diverifikasi secara berkala.	✓			
Anggota staf mengikuti praktik keamanan yang baik, seperti; a. Mengamankan informasi yang menjadi tanggung jawab mereka b. Tidak membocorkan informasi sensitif kepada orang lain (resistensi terhadap rekayasa sosial) c. Memiliki kemampuan yang memadai untuk menggunakan perangkat keras dan perangkat lunak teknologi informas d. Menggunakan praktik kata sandi yang baik e. Memahami dan mengikuti kebijakan dan peraturan keamanan f. Mengenali dan melaporkan insiden	✓			

Apa yang saat ini dilakukan oleh UPA TIK dengan baik pada bidang ini?	Apa yang saat ini tidak dilakukan dengan baik pada bidang ini?	Seberapa efektif UPA TIK menerapkan praktik-praktik di bidang ini?	
Dilakukan beberapa pelatihan berkaitan tentang keamanan sistem seperti pelatihan network penetration testing untuk mengetahui celah kerentanan dari jaringan server yang kita miliki	Semuanya sudah dilakukan dengan baik, seperti pemantauan resource pengunaan server secara rutin dan jika terjadi kejadian-kejadian yang janggal akan ditelusuri untuk mencari penyebabnya, untuk antisipasi serangan mallware dan ddos akan segera dipasangkan pengaman berupa firewall untuk menjaga kemanan sistem dan server kita		Merah
		✓	Kuning
			Hijau
			Tidak Berlaku

2. Evaluasi Praktik Keamanan – Strategi Keamanan

2. Strategi Keamanan				
Pernyataan	**Sejauh mana pernyataan ini tercermin dalam organisasi**			
	Sangat Banyak	Agak	Tidak sama sekali	Tidak Tahu
Strategi bisnis organisasi secara rutin memasukkan pertimbangan keamanan	✓			
Strategi dan kebijakan keamanan mempertimbangkan strategi dan tujuan bisnis organisasi.		✓		

Strategi, tujuan, dan sasaran keamanan didokumentasikan dan secara rutin ditinjau, diperbarui dan dikomunikasikan kepada orgaisasi.	✓			

Apa yang saat ini dilakukan oleh UPA TIK dengan baik pada bidang ini?	Apa yang saat ini tidak dilakukan dengan baik pada bidang ini?	Seberapa efektif UPA TIK menerapkan praktik-praktik di bidang ini?	
Update versi teknologi, pemantauan setiap hari.	kekurangan SDM, dan teknologi		Merah
		✓	Kuning
			Hijau
			Tidak Berlaku

3. Evaluasi Praktik Keamanan – Manajemen Keamanan

3. Manajemen Keamanan				
Pernyataan	**Sejauh mana pernyataan ini tercermin dalam organisasi**			
	Sangat Banyak	Agak	Tidak sama sekali	Tidak Tahu
Manajemen mengalokasikan dana dan sumber daya yang cukup untuk kegiatan keamanan informasi.		✓		
Peran dan tanggung jawab keamanan ditetapkan untuk semua staf dalam organisasi.		✓		
Semua staf di semua tingkat tanggung jawab melaksanakan peran dan tanggung jawab mereka untuk keamanan informasi.	✓			

Terdapat prosedur terdokumentasi untuk mengesahkan dan mengawasi semua staf (termasuk personil dari organisasi pihak ketiga) yang bekerja dengan infrmasi sensitif atau bekerja di lokasi tempat informasi tersebut berada).	✓			
Praktik perekrutan dan pemberhentian staf UPA TIK Undiksha mempertimbangkan masalah keamanan informasi	✓			
Organisasi mengelola risiko keamanan informasi, termasuk; a. Menilai risiko terhadap keamanan informasi b. Mengambil langkah-langkah untuk mengurangi risiko keamanan informasi	✓			
Manajemen menerima dan menindaklanjuti laporan rutin yang merangkum informasi terkait keamanan (misalnya, audit, log, penilaian risiko dan kerentanan).	✓			

Apa yang saat ini dilakukan oleh UPA TIK dengan baik pada bidang ini?	Apa yang saat ini tidak dilakukan dengan baik pada bidang ini?	Seberapa efektif UPA TIK menerapkan praktik-praktik di bidang ini?	
pelatihan keamanan SI/TI, manajemen resiko secara rutin dilakukan.	pengadaan insfrastruktur terbatas.		Merah
		✓	Kuning
			Hijau
			Tidak Berlaku

4. Evaluasi Praktik Keamanan – Peraturan dan Kebijakan Keamanan

4. Peraturan dan Kebijakan Keamanan				
Pernyataan	**Sejauh mana pernyataan ini tercermin dalam organisasi**			
	Sangat Banyak	Agak	Tidak sama sekali	Tidak Tahu
Organisasi memiliki seperangkat kebijakan terdokumentasi yang komprehensif dan terkini yang ditinjau dan diperbarui secara berkala		✓		
Terdapat proses yang terdokumentasi untuk pengelolaan kebijakan keamanan termasuk a. Penciptaan b. Administrasi (termasuk tinjauan dan pembaruan berkala) c. Komunikasi	✓			

Organisasi memiliki proses yang terdokumentasi untuk mengevaluasi dan memastikan kepatuhan terhadap kebijakan keamanan informasi, hukum dan peraturan yang berlaku, dan persyaratan asuransi.		✓		
Organisasi secara kompak menerapkan kebijakan keamanannya.	✓			

Apa yang saat ini dilakukan oleh UPA TIK dengan baik pada bidang ini?	Apa yang saat ini tidak dilakukan dengan baik pada bidang ini?	Seberapa efektif UPA TIK menerapkan praktik-praktik di bidang ini?	
untuk di divisi infra, dilakuakan pemantuan terhadap versi os dari server untuk dilakukan update/di rekomendasikan ke os versi terbaru	melakukan koordinasi dengan inten terhadap pengembang system untuk tindakan update versi os agar pengembang dapat menyesuaikan versi aplikasi yang dikembangkan		Merah
		✓	Kuning
			Hijau
			Tidak Berlaku

5. Evaluasi Praktik Keamanan – Manajemen Keamanan Kolaboratif

5. Manajemen Keamanan Kolaboratif				
Pernyataan	**Sejauh mana pernyataan ini tercermin dalam organisasi**			
	Sangat Banyak	Agak	Tidak sama sekali	Tidak tahu
Organisasi memiliki kebijakan dan prosedur untuk melindungi informasi ketika bekerja dengan organisasi eksternal (misalnya, pihak ketiga, kolaborator, subkontraktor, atau mitra), termasuk; a. Melindungi informasi milik organisasi lain b. Memahami kebijakan dan prosedur keamanan organisasi eksternal c. Mengakhiri akses ke informasi oleh personil eksternal yang diberhentikan		✓		
Organisasi mendokumentasikan persyaratan perlindungan informasi dan secara eksplisit mengkomunikasikannya kepada semua pihak ketiga yang sesuai.		✓		

Organisasi memiliki mekanisme formal untuk memverifikasi bahwa semua organisasi pihak ketiga, layanan keamanan yang dialihdayakan, mekanisme, dan teknologi memenuhi kebutuhan dan persyaratannya.		✓		
Organisasi memiliki kebijakan dan prosedur untuk berkolaborasi dengan semua organisasi pihak ketiga a. Menyediakan layanan pelatihan dan kesadaran keamanan b. Mengembangkan kebijakan untuk organisasi c. Mengambangkan rencana kontinjensi untuk organisasi		✓		

Apa yang saat ini dilakukan oleh UPA TIK dengan baik pada bidang ini?	Apa yang saat ini tidak dilakukan dengan baik pada bidang ini?	Seberapa efektif UPA TIK menerapkan praktik-praktik di bidang ini?	
kerjasama dengan BSSN	perlu dilakukan audit keamanan secara rutin		
		✓	

6. Evaluasi Praktik Keamanan – Perencanaan Contingency/Pemulihan Bencana

6. Perencanaan Contingency/Pemulihan Bencana				
Pernyataan	**Sejauh mana pernyataan ini tercermin dalam organisasi**			
	Sangat Banyak	Agak	Tidak sama sekali	Tidak tahu
Analisis operasi, aplikasi, dan kekritisan data telah dilakukan.		✓		
Organisasi telah mendokumentasikan, meninjau, dan menguji; a. Rencana kontinjensi untuk menanggapi keadaan darurat b. Rencana pemulihan bencana c. Kelangsungan rencana operasi darurat	✓			
Rencana kontinjensi, pemulihan bencana, dan kelangsungan operasi mempertimbangkan persyaratan dan kontrol akses fisik dan elektronik		✓		

Semua staf semestinya; a. Mengetahui rencana kontinjensi, pemulihan bencana, dan kelangsungan operasional b. Memahami dan mampu melaksanakan tanggung jawab mereka		✓		

Apa yang saat ini dilakukan oleh UPA TIK dengan baik pada bidang ini?	Apa yang saat ini tidak dilakukan dengan baik pada bidang ini?	Seberapa efektif UPA TIK menerapkan praktik-praktik di bidang ini?	
sudah dilakukan	melakukan backup data secara berkala		Merah
		✓	Kuning
			Hijau
			Tidak Berlaku

7. Evaluasi Praktik Keamanan – Pengendalian Akses Fisik

7. Pengendalian Akses Fisik				
Pernyataan	**Sejauh mana pernyataan ini tercermin dalam organisasi**			
	Sangat Banyak	Agak	Tidak sama sekali	Tidak tahu
Rencana dan prosedur keamanan fasilitas untuk melindungi tempat, bangunan, dan area terlarang didokumentasikan dan diuji	✓			
Terdapat kebijakan dan prosedur yang terdokumentasi untuk mengelola pengunjung.	✓			
Terdapat kebijakan dan prosedur yang terdokumentasi untuk mengendalikan akses fisik ke area kerja dan perangkat keras (komputer, perangkat komunikasi, dll) dan media perangkat lunak.	✓			

Lingkungan kerja dan komponen lain yang memungkinkan akses ke informasi sensitif dilindungi secara fisik untuk mencegah akses yang tidak sah.	✓			

Apa yang saat ini dilakukan oleh UPA TIK dengan baik pada bidang ini?	Apa yang saat ini tidak dilakukan dengan baik pada bidang ini?	Seberapa efektif UPA TIK menerapkan praktik-praktik di bidang ini?	
pemakaian accers door lock untuk masuk gedung dan ruangan, jadi hanya staf tertentu saja yang punya akses ke ruangan	untuk akes masuk ke lab komputer masih mengunakan kunci manual		Merah
		✓	Kuning
			Hijau
			Tidak Berlaku

8. Evaluasi Praktik Keamanan – Pemantauan dan Audit Keamanan Fisik

8. Pemantauan dan Audt Keamanan Fisik				
Pernyataan	**Sejauh mana pernyataan ini tercermin dalam organisasi**			
	Sangat Banyak	Agak	Tidak sama sekali	Tidak Tahu
Catatan pemeliharaan disimpan untuk mendokumentasikan perbaikan dan modifikasi komponen fisik fasilitas.	✓			
Tindakan individu atau kelompok, sehubungan dengan semua media yang dikontrol secara fisik, dapat dipertanggungjawabkan.	✓			
Catatan audit dan pemantauan secara rutin diperiksa untuk mengetahui adanya anomali, dan tindakan korektif diambil sesuai kebutuhan.	✓			

Apa yang saat ini dilakukan oleh UPA TIK dengan baik pada bidang ini?	Apa yang saat ini tidak dilakukan dengan baik pada bidang ini?	Seberapa efektif UPA TIK menerapkan praktik-praktik di bidang ini?	
perawatan piranti smart lock door, pengantian battry	sudah baik		Merah
			Kunging
		✓	Hijau
			Tidak Berlaku

9. Evaluasi Praktik Keamanan – Manajemen Jaringan dan Sistem

9. Manajemen Jaringan dan Sistem				
Pernyataan	**Sejauh mana pernyataan ini tercermin dalam organisasi**			
	Sangat Banyak	Agak	Tidak sama sekali	Tidak Tahu
Ada rencana keamanan yang terdokumentasikan dan teruji untuk melindungi sistem dan jaringan.		✓		
Informasi sensitif dilindungi oleh penyimpanan yang aman (misalnya, cadangan disimpann di luar lokasi, proses pembuangan informasi sensitif).	✓			
Integritas perangkat lunak yang terinsral diverifikasi secara teratur.	✓			
Semua sistem selalu diperbarui sehubungan dengan revisi, pembaruan, dan rekomendasi dalam saran keamanan.		✓		

Ada rencana pencadangan data yang terdokumentasi dan teruji untuk pencadangan perangkat lunak dan data. Semua staf memahami tanggung jawab mereka di bawah rencana pencadangan.	✓			
Perubahan pada perangkat keras dan perangkat lunak TI direncanakan, dikontrol, dan didokumentasikan.	✓			
Anggota staf TI mengikuti prosedur saat menerbitkan, mengubah, dan menghentikan kata sandi, akun, dan hak istimewa pengguna. a. Identifikasi pengguna yang unik diperlukan untuk semua pengguna sistem informasi, termasuk pengguna pihak ketiga b. Akun bawaan dan kata sandi bawaan telah dihapus dari sistem	✓			
Hanya layanan yang diperlukan yang dijalankan pada sistem - semua layanan yang tidak perlu telah dihapus.		✓		
Alat dan mekanisme untuk administrasi sistem dan jaringan yang aman digunakan, dan secara rutin ditinjau dan diperbarui atau diganti.	✓			

Apa yang saat ini dilakukan oleh UPA TIK dengan baik pada bidang ini?	Apa yang saat ini tidak dilakukan dengan baik pada bidang ini?	Seberapa efektif UPA TIK menerapkan praktik-praktik di bidang ini?	
mengunakan tool monitoring jaringan	sudah dilakukan		Merah
		✓	Kuning
			Hijau
			Tidak Berlaku

10. Evaluasi Praktik Keamanan – Pemantauan dan Audit Keamanan TI

10. Pemantauan dan Audit Keamanan TI				
Pernyataan	**Sejauh mana pernyataan ini tercermin dalam organisasi**			
	Sangat Banyak	Agak	Tidak sama sekali	Tidak Tahu
Alat-alat pemantauan dan audit sistem dan jaringan secara rutin digunakan oleh organisasi. Aktivitas yang tidak biasa ditangani sesuai dengan kebijakan atau prosedur yang berlaku.		✓		
Firewall dan komponen keamanan lainnya diaudit secara berkala untuk memastikan kepatuhan terhadapp kebijakan.		✓		

Apa yang saat ini dilakukan oleh UPA TIK dengan baik pada bidang ini?	Apa yang saat ini tidak dilakukan dengan baik pada bidang ini?	Seberapa efektif UPA TIK menerapkan praktik-praktik di bidang ini?	
Audit kemanan sistem informasi dilakukan mulai dari scaning sistem secara berkala untuk memastikan sistem dapat berjalan dengan baik dan bebas dari kerentaan. hasil scan akan dilakukan tindakan pencegahan jangka pendek dan pencegahan jangka panjang. pencegahan jangka pendek biasanya dilakukan pembersihan file-file yang rentan terhadap serangan cyber. pencegahan jangka panjang dilakukan dengan menambah kemanan sistem baik dari sisi hardware ataupun dari sisi perangkat lunak.	audit atau pemantauan sistem dilakukan saat terjadi serangan atau pada saat terjadi kerentanan sistem, audit keamanan sistem tidak dimulai dari penerapan manajemen resiko. sehingga penanganan kerentanan sering diantisipasi dengan pencegahan jangka pendek.		Merah
		✓	Kuning
			Hijau
			Tidak Berlaku

11. Evaluasi Praktik Keamanan – Otentikasi dan Otorisasi

11. Otentikasi dan Otorisasi				
Pernyataan	**Sejauh mana pernyataan ini tercermin dalam organisasi**			
	Sangat Banyak	Agak	Tidak sama sekali	Tidak Tahu
Kontrol akses yang tepat dan autentikasi pengguna (misalnya izin file, konfigurasi jaringan) yang sesuai dengan kebijakan digunakan untuk membatasi akses pengguna ke informasi, sistem yang sensitif, aplikasi dan layanan tertentu, dan koneksi jaringan.	✓			
Terdapat kebijakan dan prosedur yang terdokumentasi untuk menetapkan dan mengakhiri hak akses terhadap informasi bagi individu maupun kelompok.	✓			

Metode atau mekanisme disediakan untuk memastikan bahwa informasi sensitif tidak diakses, diubah, atau dihancurkan dengan cara yang tidak sah. Metode atau mekanisme ditinjau dan diverifikasi secara berkala.	✓			

Apa yang saat ini dilakukan oleh UPA TIK dengan baik pada bidang ini?	Apa yang saat ini tidak dilakukan dengan baik pada bidang ini?	Seberapa efektif UPA TIK menerapkan praktik-praktik di bidang ini?	
sudah ada kasifikasi user akses	sudah dilakukan		Marah
			Kuning
		✓	Hijau
			Tidak Beraku

12. Evaluasi Praktik Keamanan – Manajemen Kerentanan

12. Manajemen Kerentanan				
Pernyataan	**Sejauh mana pernyataan ini tercermin dalam organisasi**			
	Sangat Banyak	Agak	Tidak sama sekali	Tidak Tahu
Terdapat serangkaian prosedur terdokumentasi untuk mengelola kerentanan, termasuk: a. Memilih alat evaluasi kerentanan, daftar periksa, dan skrip b. Selalu mengikuti perkembangan jenis kerentanan dan metode serangan yang diketahui c. Meninjau sumber informasi tentang pengumuman kerentanan, peringatan keamanan, dan permberitahuan d. Mengidentifikasi komponen infrastruktur yang akan dievaluasi e. Penjadwalan untuk evaluasi kerentanan f. Menafsirkan dan menanggapi hasil evaluasi Menjaga penyimpanan dan disposisi data kerentanan yang aman		✓		

Prosedur manajemen kerentanan diikuti dan ditinjau serta diperbarui secara berkala.	✓			
Penilaian kerentanan teknologi dilakukan secara berkala, dan kerentanan diatasi ketika teridentifikasi.	✓			

Apa yang saat ini dilakukan oleh UPA TIK dengan baik pada bidang ini?	Apa yang saat ini tidak dilakukan dengan baik pada bidang ini?	Seberapa efektif UPA TIK menerapkan praktik-praktik di bidang ini?	
melakukan uji kerentanan pada kepada sistem atau server yang memiliki aktifitas tinggi	belum semua server atau system dilakukan uji kerentanan		Merah
		✓	Kuning
			Hijau
			Tidak Berlaku

13. Evaluasi Praktik Keamanan – Enkripsi

13. Enkripsi				
Pernyataan	**Sejauh mana pernyataan ini tercermin dalam organisasi**			
	Sangat Banyak	Agak	Tidak sama sekali	Tidak Tahu
Kontrol keamanan yang tepat digunakan untuk melindungi informasi sensitif saat berada dalam penyimpanan dan selama transmisi (misalnya, enkripsi data, infrastruktur kunci publik, teknologi jaringan pribadi virtual).	✓			
Protokol terenkripsi digunakan ketika mengelola sistem, *router*, dan *firewall* dari jarak jauh.	✓			

Apa yang saat ini dilakukan oleh UPA TIK dengan baik pada bidang ini?	Apa yang saat ini tidak dilakukan dengan baik pada bidang ini?	Seberapa efektif UPA TIK menerapkan praktik-praktik di bidang ini?	
UPA TIK secara rutin sudah menerapkan pengaman user dan password secara end to end, termasuk juga akses ke API sudah menggunakan token dan setiap aplikasi sudah disedikan fitur log pengguna.	Perlu menerapkan OTP (One time password) untuk beberapa aplikasi seperti penginputan nilai oleh dosen pengajar matakuliah, atau sistem-sistem yang dianggap perlu menerapkan OTP		Merah
			Kuning
		✓	Hijau
			Tidak Berlaku

14. Evaluasi Praktik Keamanan – Perancangan dan Arsitektur Keamanan

14. Desain/Perancangan dan Arsitektur Keamanan				
Pernyataan	**Sejauh mana pernyataan ini tercermin dalam organisasi**			
	Sangat Banyak	Agak	Tidak sama sekali	Tidak Tahu
Arsitektur dan desain/perancangan sistem untuk sistem baru dan sistem yang direvisi mencakup pertimbangan untuk; a. Strategi, kebijakan, dan prosedur keamanan b. Riwayat kompromi keamanan c. Hasil penilaian risiko keamanan	✓			
Organisasi memiliki diagram terkini yang menunjukkan arsitektur keamanan di seluruh perusahaan topologi jaringan.	✓			

Apa yang saat ini dilakukan oleh UPA TIK dengan baik pada bidang ini?	Apa yang saat ini tidak dilakukan dengan baik pada bidang ini?	Seberapa efektif UPA TIK menerapkan praktik-praktik di bidang ini?	
dalam topologi sudah dimasukkan forti sebagai pelindung/firewall jaringan dalam undiksha	sudah dilakuakan dengan optimal		Merah
		✓	Kuning
			Hijau
			Tidak Berlaku

15. Evaluasi Praktik Keamanan – Manajemen Insiden

15. Manajemen Insiden				
Pernyataan	**Sejauh mana pernyataan ini tercermin dalam organisasi**			
	Sangat Banyak	Agak	Tidak sama sekali	Tidak Tahu
Terdapat prosedur yang terdokumentasi untuk mengidentifikasi, melaporkan, dan menanggapi dugaan insiden dan pelanggaran keamanan.		✓		
Prosedur manajemen insiden diuji, diverifikasi, dan diperbarui secara berkala.		✓		

Terdapat kebijakan dan prosedur yang terdokumentasi untuk bekerja sama dengan lembaga penegak hukum.			✓	

Apa yang saat ini dilakukan oleh UPA TIK dengan baik pada bidang ini?	Apa yang saat ini tidak dilakukan dengan baik pada bidang ini?	Seberapa efektif UPA TIK menerapkan praktik-praktik di bidang ini?	
melakukan tindakan prefentiv dalam menangani insiden seperti melakukan backup dan monitoring resoucre pengunaan server	belum melakukan prosedur kerjasama		Merah
		✓	Kuning
			Hijau
			Tidak Berlaku

Lampiran 14. Lembar Kerja Memilih Aset Kritis

1. Aset Kritis UPA TIK Undiksha

ASET KRITIS	CATATAN/DASAR PEMILIHAN	ASET TERKAIT
Server	Karena server adalah pusat dari data dan sistem informasi sebagai jantungnya sebuah organisasi, server down hampir semua aktifitas tidak dapat berjalan dengan baik. Karena hampir semua kegiatan organisasi menggunakan sistem informasi.	Data civitas akademika dan semua sistem informasi yang dikembangkan oleh organisaasi (UNDIKSHA).
Perangkat Jaringan	Menjadi layanan inti dari lembaga kepada dosen, pegawai, dan mahasiswa.	Aset informasi berupa data.
Sekretaris UPA TIK Undiksha	Membantu kerja kepala untuk manajemen anggaran, sdm, vendor	Laptop, printer
Divisi Infrastruktur, Jaringan, & Keamanan	Tim inti dalam organisasi, jika jaringan internet terputus maka layanan tidak akan tersedia. Divisi ini menjaga keamanan layanan.	Switch dan router.
SIAK	SIAK dipilih sebagai aset kritis karena data akademik yang dikelola, seperti mata kuliah, nilai, perangkat pembelajaran, dan	Asset yang terkait dengan SIAK adalah asset informasi yang berupa Data riwayat pembelajaran meliputi,

	aktivitas mahasiswa, merupakan inti dari administrasi pendidikan.	data mata kuliah, data krs, data nilai mahasiswa, data Perangkat Pembelajaran, dan aset untuk mengetahui data mining, untuk memutuskan sesuatu yang berhubungan dengan akademik.
SOP dan Instruksi Kerja	Karena pekerjaan bias dimulai berdasarkan SOP dan Instruksi Kerja yang sudah ditetapkan dimana SOP digunakan oleh civitas akademikan dan IK digunakan oleh masing-masing divisi pada UPA TIK Unsiksha.	Dokumen SOP dan IK, template SOP dan IK, dan Log perubahan SOP dan IK.

Lampiran 15. Identifikasi Persyaratan Keamanan Aset Kritis

1. Persyaratan Keamanan Aset Kritis - Server

Persyaratan Keamanan		**Persyaratan keamanan yang paling penting**	
✓	Kerahasiaan	✓	Kerahasiaan
	Integritas		Integritas
✓	Ketersediaan	✓	Ketersediaan
	Lainnya		Lainnya

2. Persyaratan Keamanan Aset Kritis – Perangkat Jaringan

Persyaratan Keamanan		**Persyaratan keamanan yang paling penting**	
✓	Kerahasiaan	✓	Kerahasiaan
✓	Integritas	✓	Integritas
✓	Ketersediaan	✓	Ketersediaan
	Lainnya		Lainnya

3. Persyaratan Keamanan Aset Kritis – SDM; Sekretaris UPA TIK Undiksha

Persyaratan Keamanan		**Persyaratan keamanan yang paling penting**	
✓	Kerahasiaan	✓	Kerahasiaan
✓	Integritas	✓	Integritas
✓	Ketersediaan	✓	Ketersediaan
	Lainnya		Lainnya

4. Persyaratan Keamanan Aset Kritis – SDM; Divisi Infrastruktur, Jaringan & Keamanan

Persyaratan Keamanan		**Persyaratan keamanan yang paling penting**	
✓	Kerahasiaan	✓	Kerahasiaan
	Integritas		Integritas
✓	Ketersediaan	✓	Ketersediaan
	Lainnya		Lainnya

5. Persyaratan Keamanan Aset Kritis – SIAK

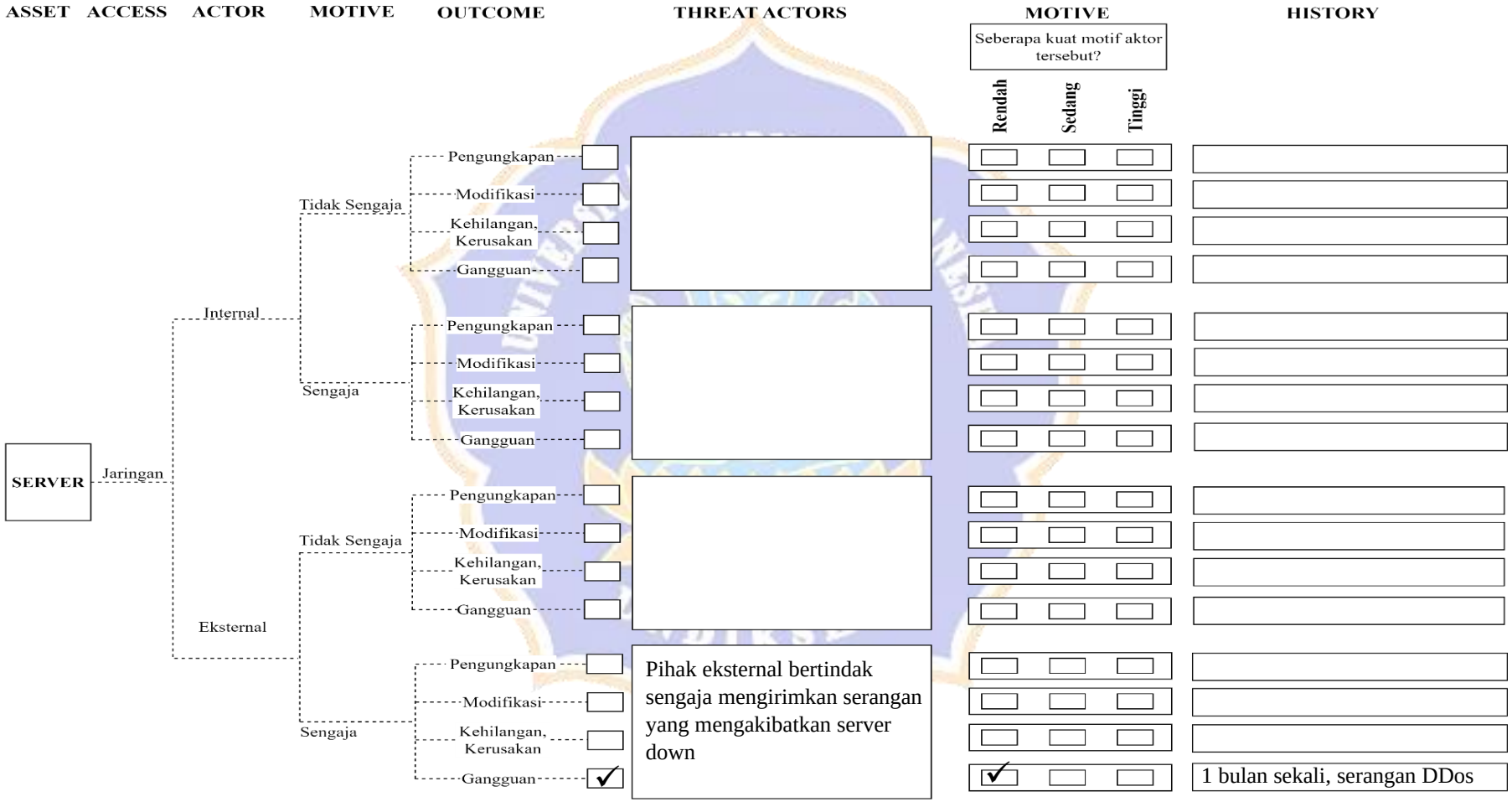
Persyaratan Keamanan		Persyaratan keamanan yang paling penting	
	Kerahasiaan		Kerahasiaan
	Integritas	✓	Integritas
	Ketersediaan		Ketersediaan
✓	Otentikasi		Otentikasi
✓	Otorisasi		Otorisasi

6. Persyaratan Keamanan Aset Kritis – SOP dan Instruksi Kerja

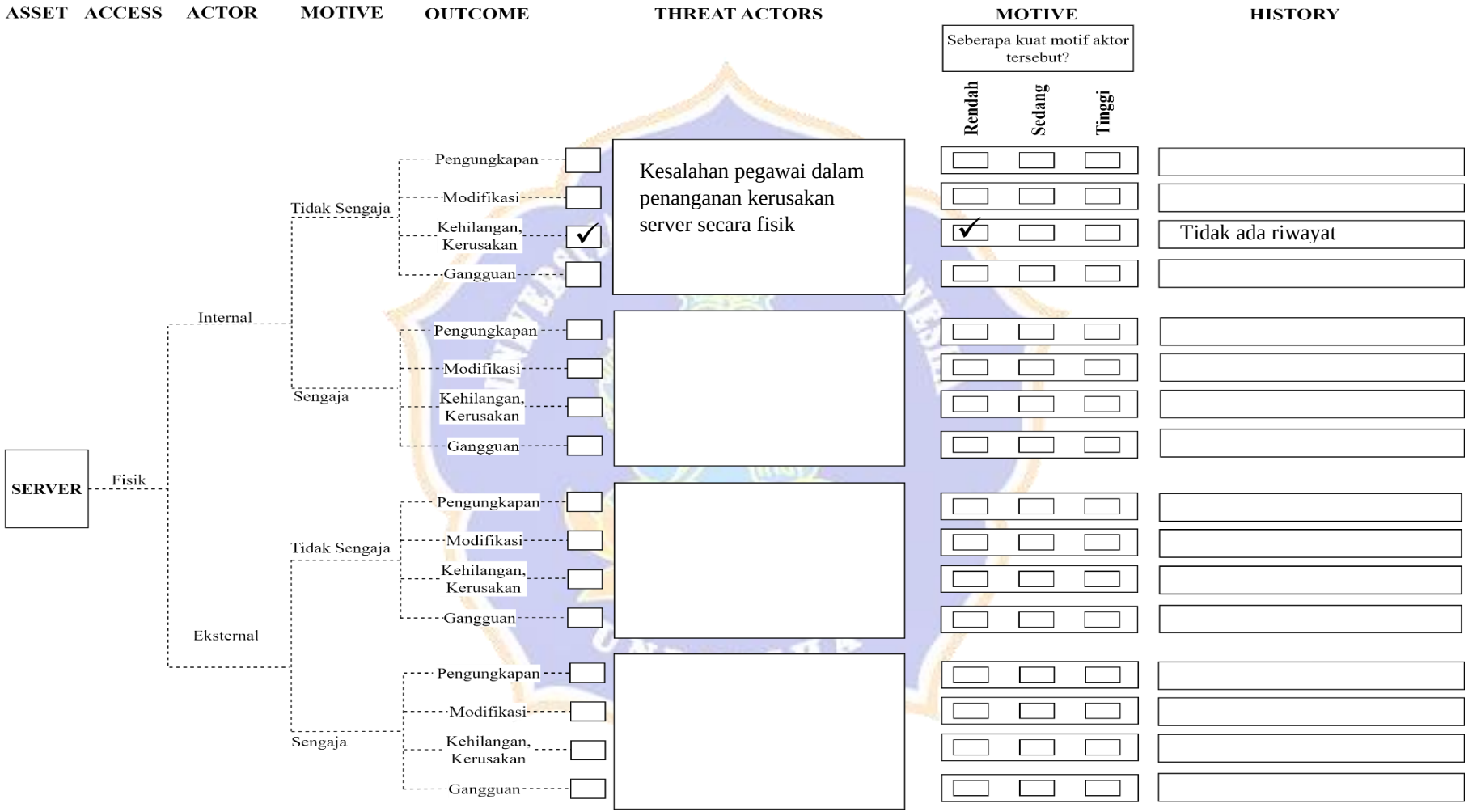
Persyaratan Keamanan		Persyaratan keamanan yang paling penting	
✓	Kerahasiaan	✓	Kerahasiaan
	Integritas		Integritas
✓	Ketersediaan	✓	Ketersediaan
	Lainnya		Lainnya

Lampiran 16. Identifikasi Ancaman Terhadap Aset Kritis

1. Identifikasi ancaman terhadap server melalui jalur akses jaringan

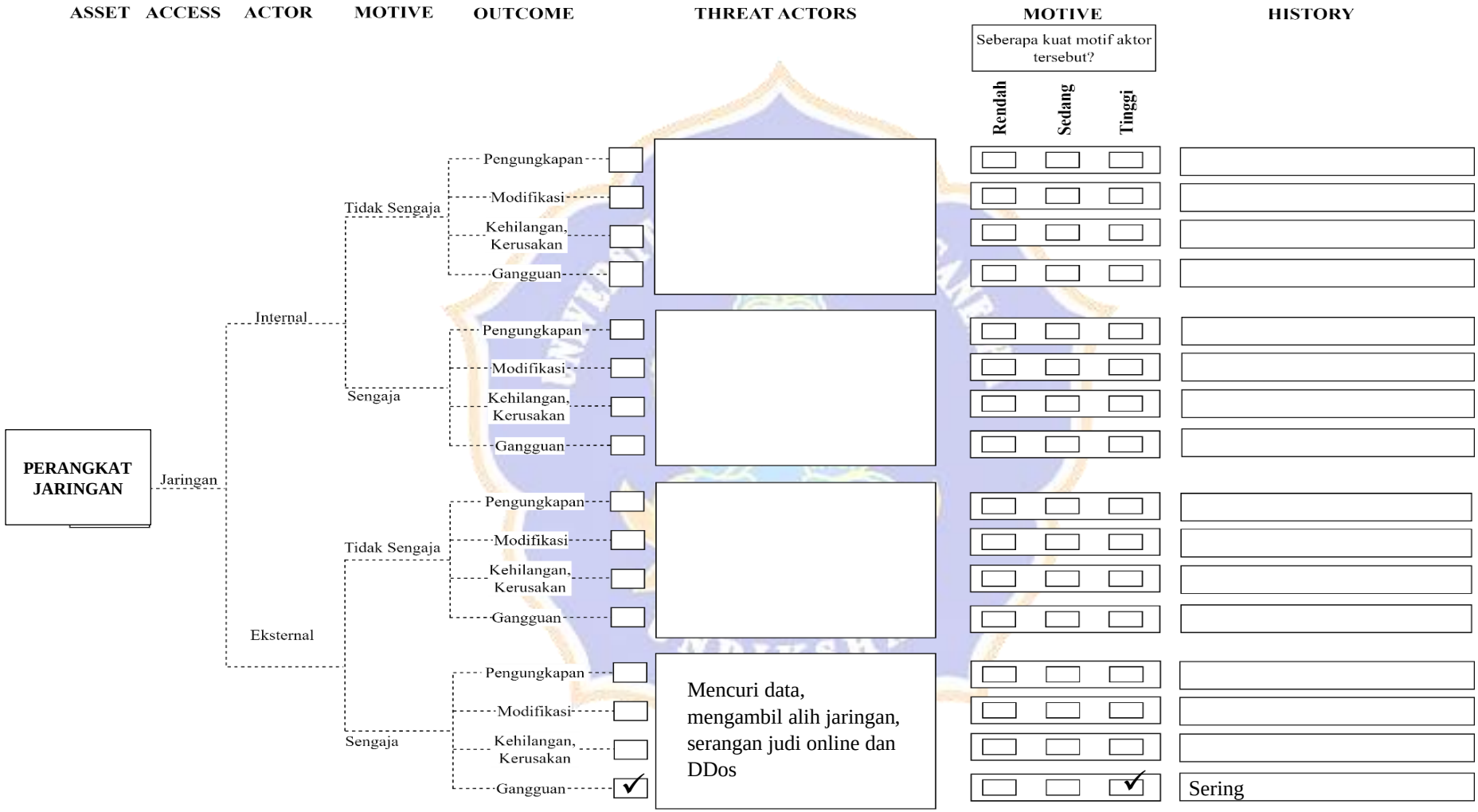


2. Identifikasi ancaman terhadap server melalui jalur akses fisik

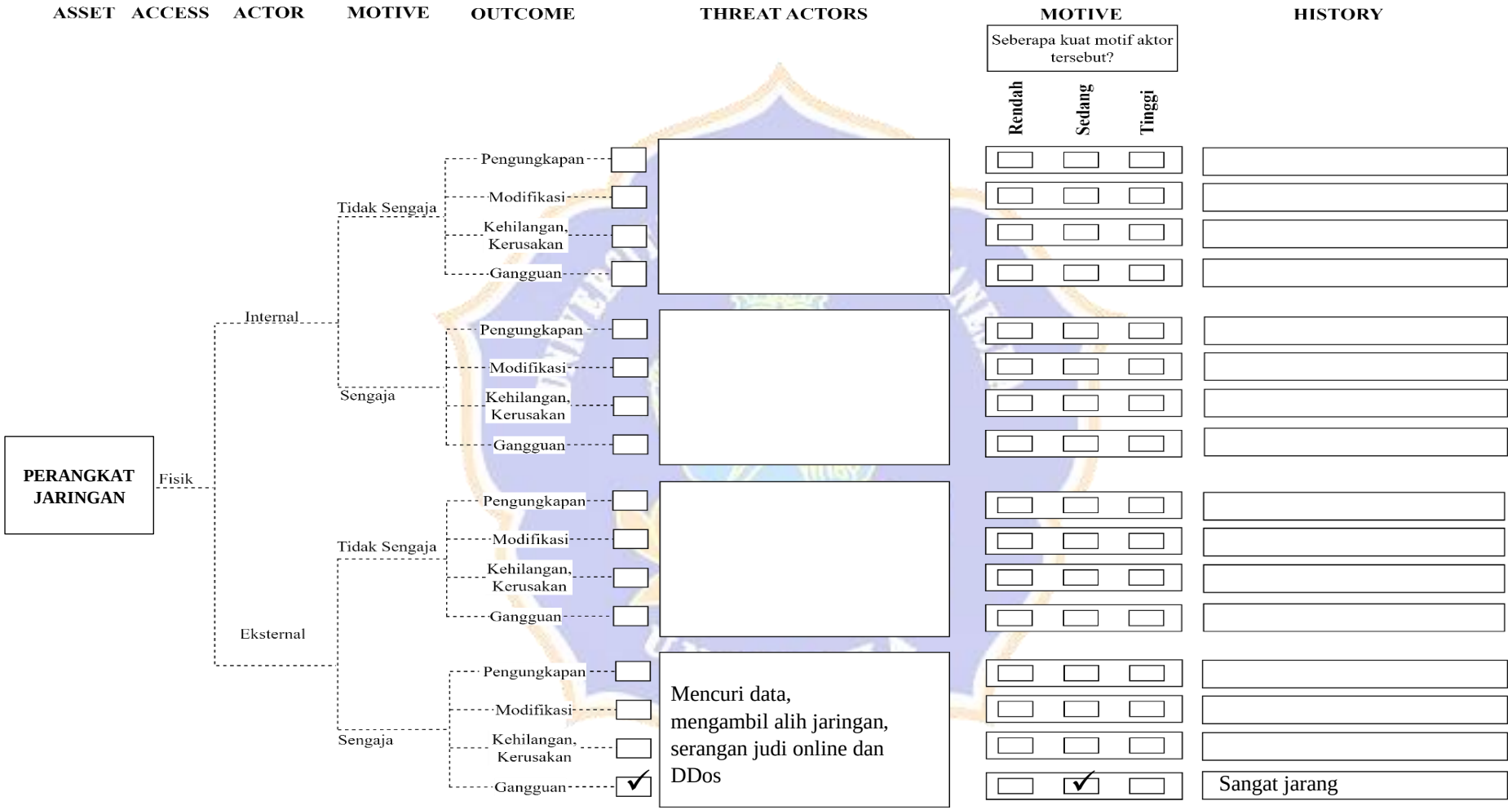


3. Identifikasi ancaman terhadap server melalui jalur masalah sistem

4. Identifikasi ancaman terhadap perangkat jaringan melalui jalur akses jaringan



5. Identifikasi ancaman terhadap perangkat jaringan melalui jalur akses fisik

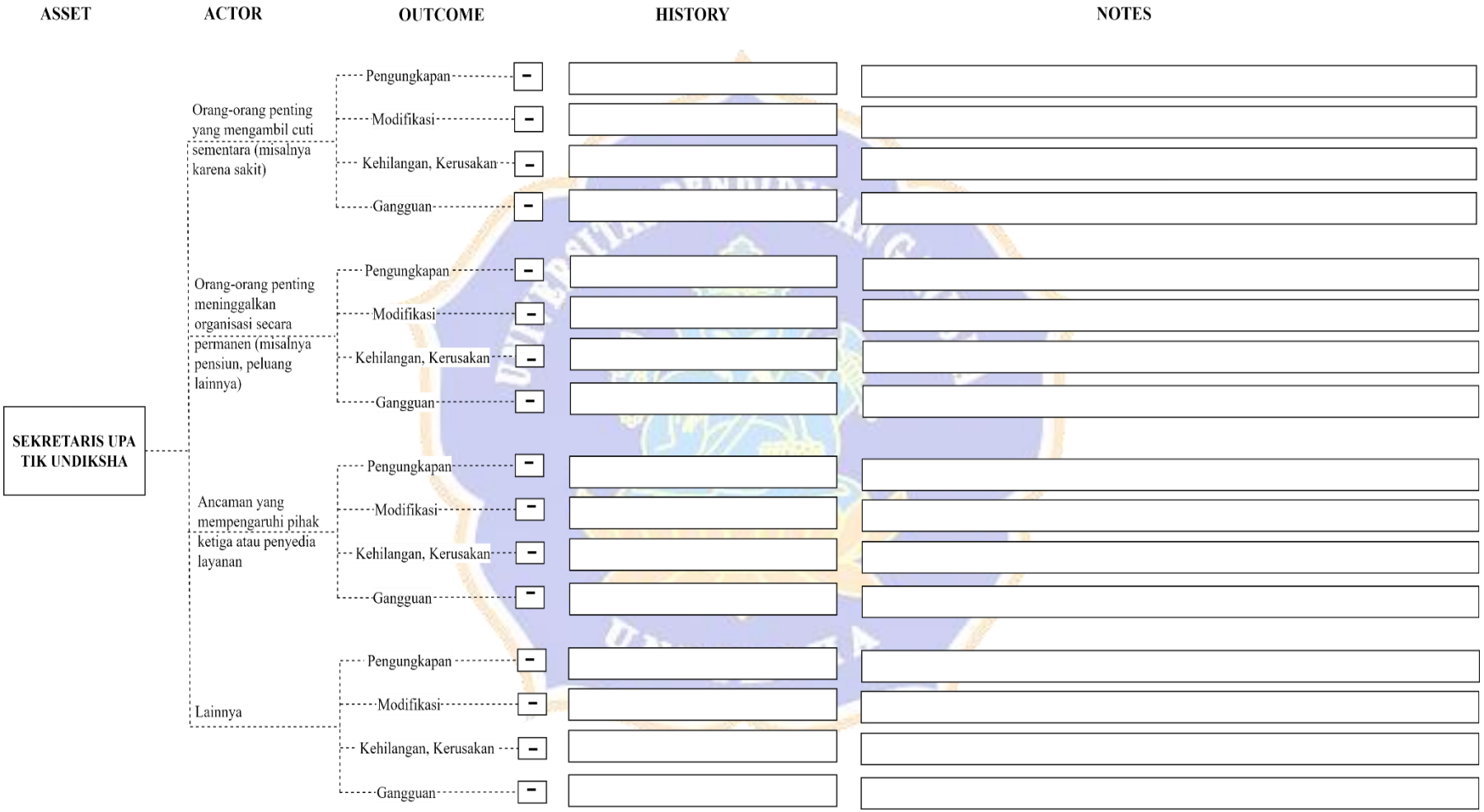


6. Identifikasi acaman terhadap perangkat jaringan melalui jalur akses masalah sistem

ASSET	ACTOR	OUTCOME		HISTORY	NOTES
PERANGKAT JARINGAN	Kerusakan Perangkat Lunak	Pengungkapan	✓	2-3 kali dalam 1 bulan	Selalu meminta anggota dalam melakukan update perangkat lunak
		Modifikasi			
		Kehilangan, Kerusakan	✓	2-3 kali dalam 1 bulan	Selalu meminta anggota dalam melakukan update perangkat lunak
		Gangguan	✓	2-3 kali dalam 1 bulan	Selalu meminta anggota dalam melakukan update perangkat lunak
	Kegagalan Sistem	Pengungkapan			
		Modifikasi			
		Kehilangan, Kerusakan			
		Gangguan	✓	1 tahun sekali	Melakukan perawatan terhadap perangkat jaringan
	Kerusakan Perangkat Keras	Pengungkapan			
		Modifikasi			
		Kehilangan, Kerusakan			
		Gangguan	✓	1 tahun terkadang 1 kali selama 1 jam	Melakukan pengecekan terhadap perangkat jaringan
	Kode berbahaya (virus, worm, trojan horse, back door)	Pengungkapan			
		Modifikasi			
		Kehilangan, Kerusakan			
		Gangguan	✓	1 bulan bisa 1 kali	Mengidentifikasi sumber awal terjadi serangan

7.

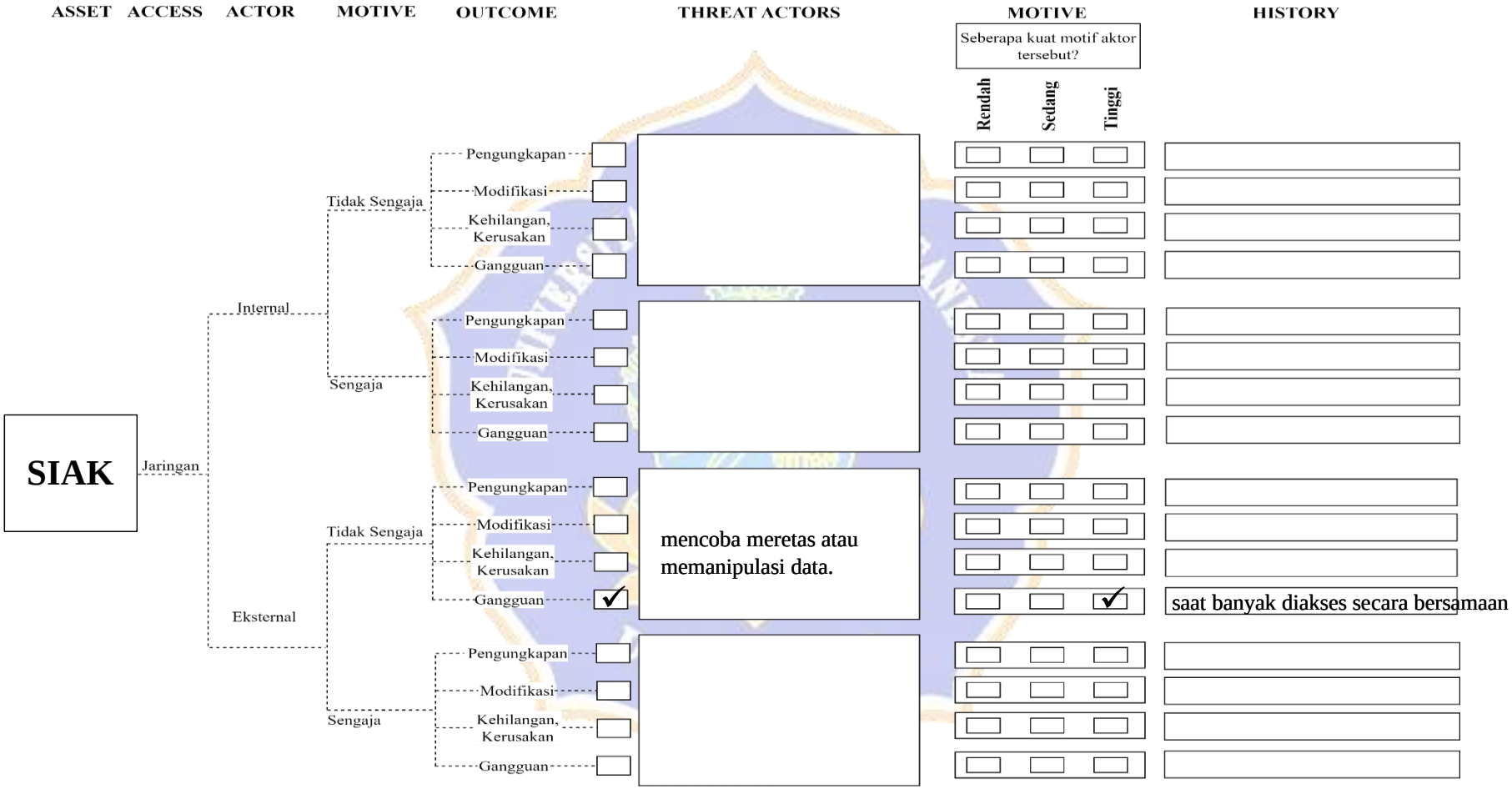
8. Identifikasi ancaman terhadap SDM; Sekretaris UPA TIK



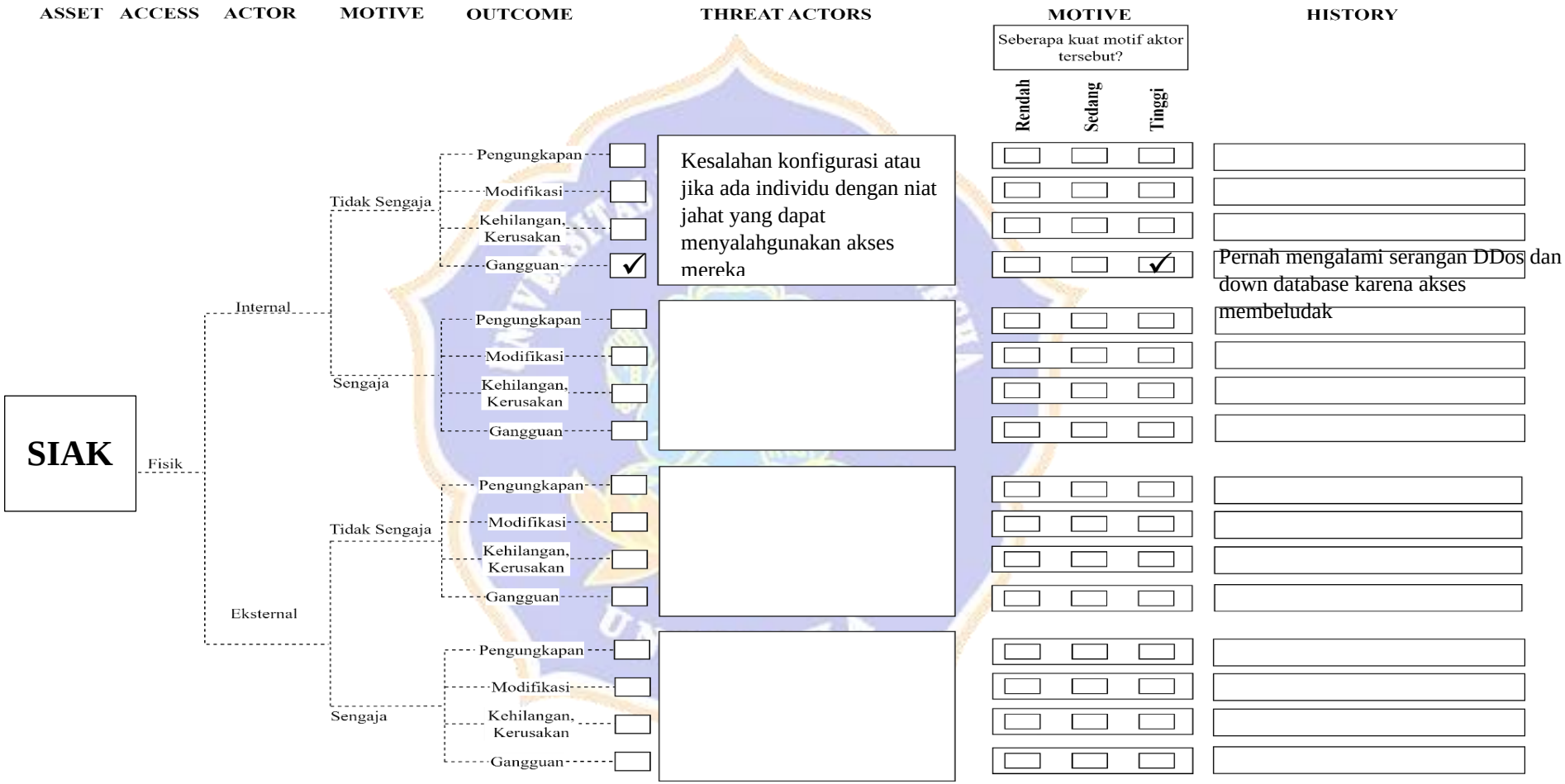
9. Identifikasi ancaman terhadap Divisi Infrastruktur, Jaringan & Keamanan

ASSET	ACTOR	OUTCOME	HISTORY	NOTES
DIVISI INFRASTRUKTUR, JARINGAN, & KEAMANAN	Orang-orang penting yang mengambil cuti sementara (misalnya karena sakit)	Pengungkapan	Tidak ada pengaruh, jarang terjadi1 bulan terkadang 1 kali	Sudah dikendalikan dengan baik karena tugas-tugas yang bersangkutan telah dialihkan kepada staf lain yang tidak sedang cuti.
		Modifikasi		
		Kehilangan, Kerusakan		
		Gangguan		
	Orang-orang penting meninggalkan organisasi secara permanen (misalnya pensiun, peluang lainnya)	Pengungkapan	Tidak pernah ada pergantian staf	Ketika ada pegawai yang pindah organisasi secara permanen, kami akan meminta aksesnya, meminta dokumentasi yang selama ini dipegang. Kemudian menonaktifkan semua akses yg dimiliki
		Modifikasi		
		Kehilangan, Kerusakan		
		Gangguan		
	Ancaman yang mempengaruhi pihak ketiga atau penyedia layanan	Pengungkapan		
		Modifikasi		
		Kehilangan, Kerusakan		
		Gangguan ✓	–	ketidak ketersediaan layanan. seperti internet yang mati atau ketika listrik mati.
	Lainnya	Pengungkapan		
		Modifikasi		
		Kehilangan, Kerusakan		
		Gangguan		

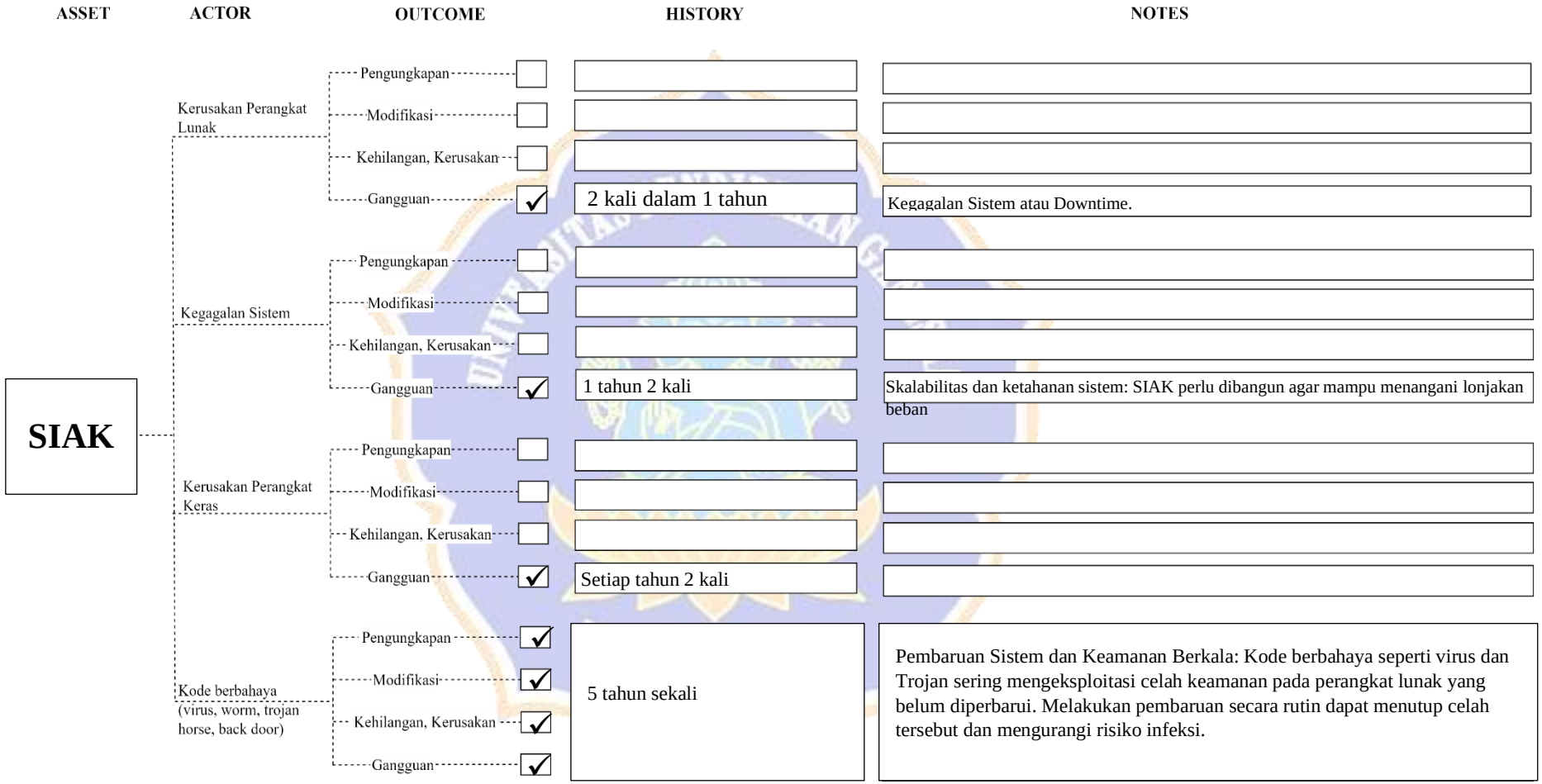
10. Identifikasi ancaman terhadap SIAK melalui jalur akses jaringan



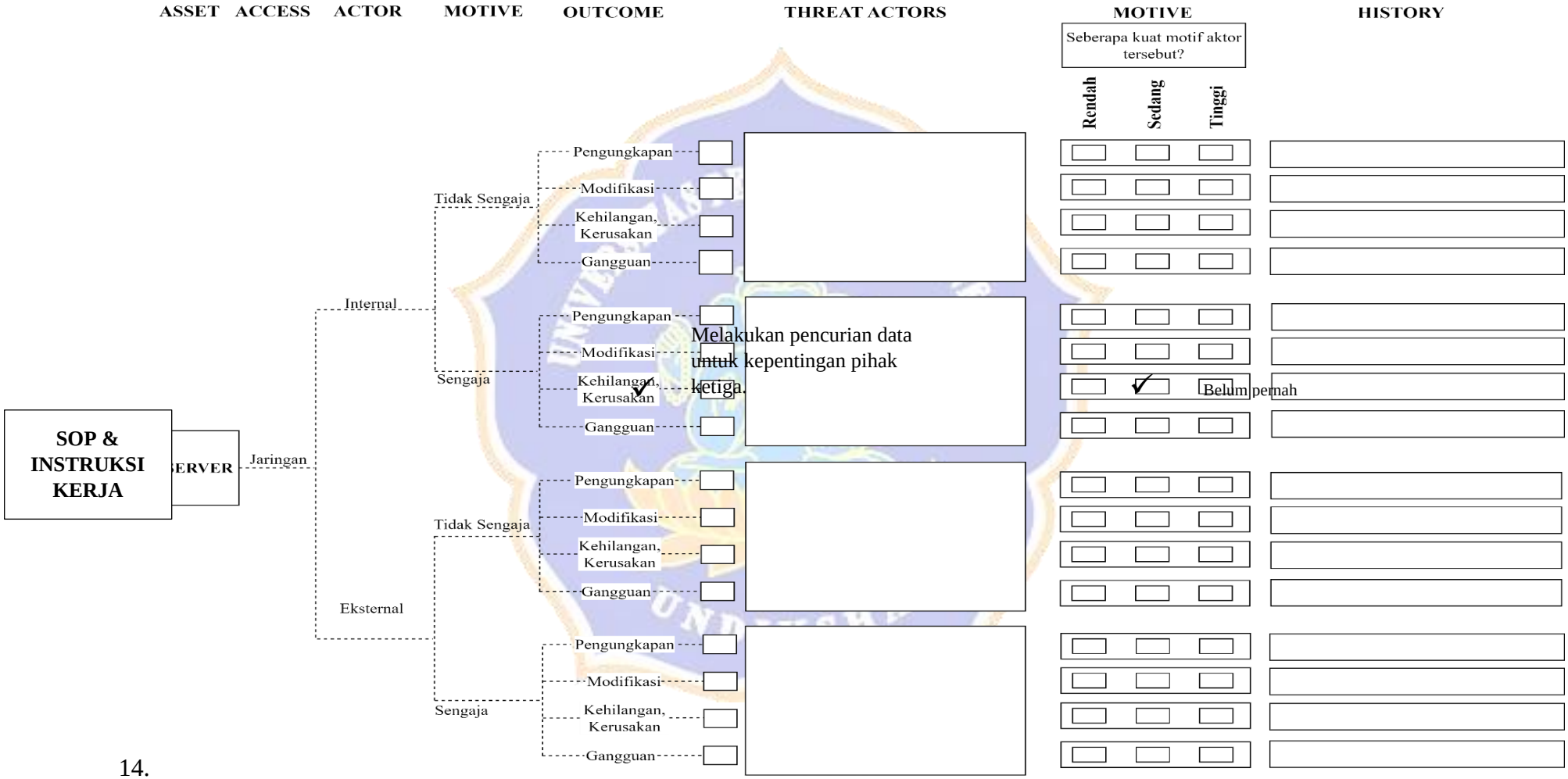
11. Identifikasi ancaman terhadap SIAK melalui jalur akses fisik



12. Identifikasi ancaman terhadap SIAK melalui jalur akses masalah system

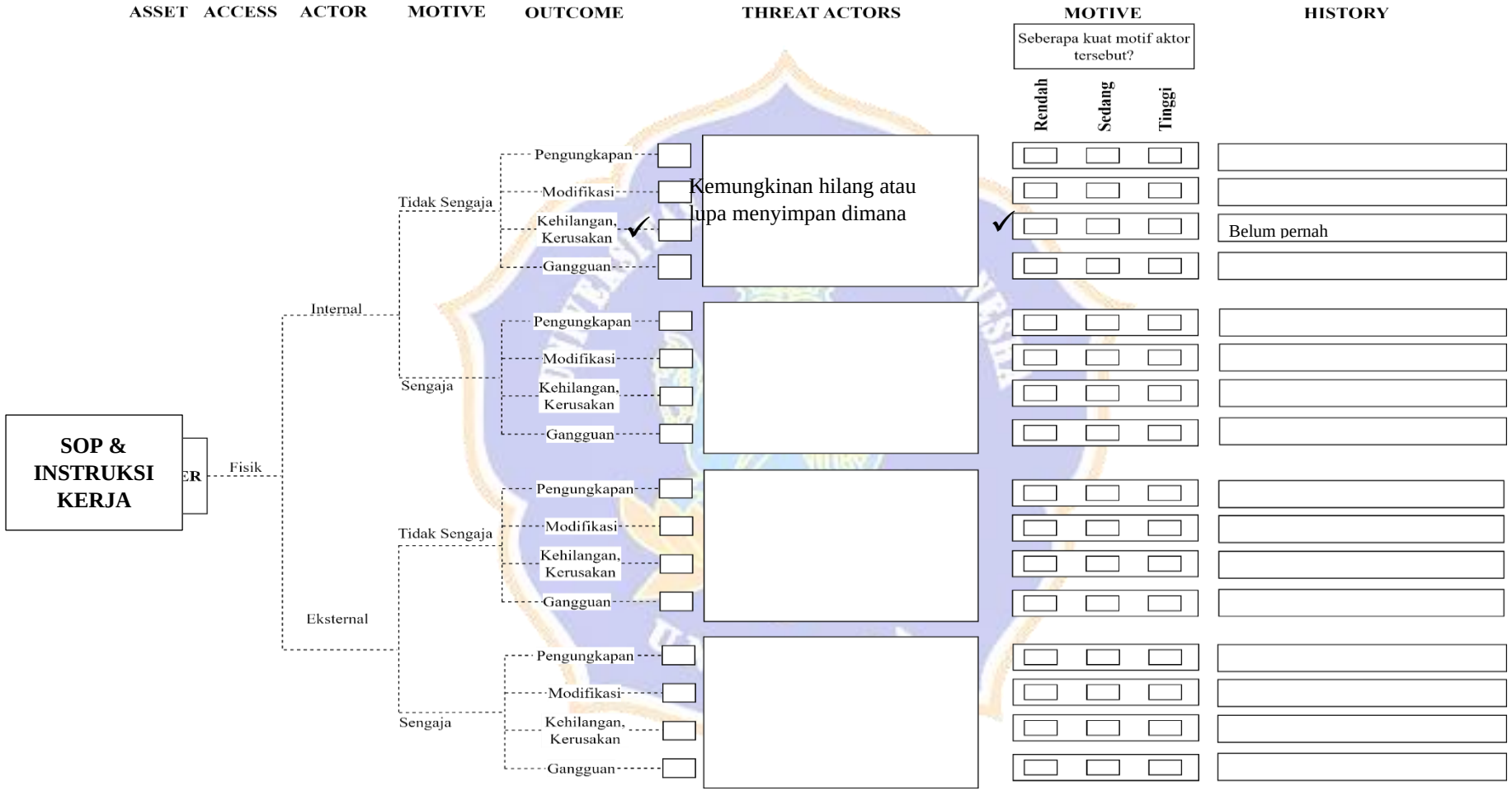


13. Identifikasi ancaman terhadap SOP dan Instruksi Kerja melalui jalur akses jaringan

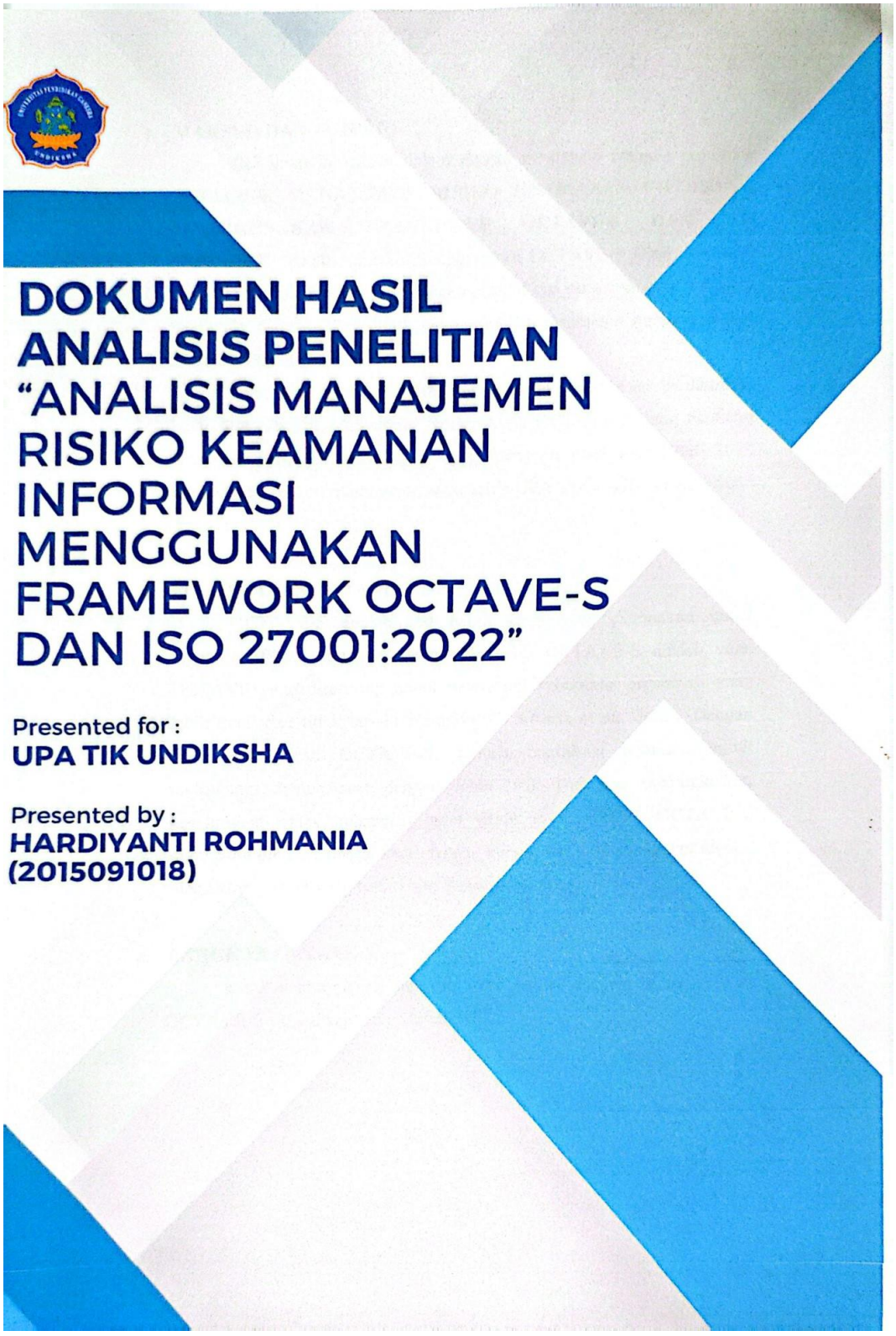


14.

15. Identifikasi ancaman terhadap SOP dan Instruksi Kerja melalui jalur akses fisik



Lampiran 17. Konfirmasi Temuan



1. MAKSUD DAN TUJUAN

Dokumen ini dibuat dalam rangka memenuhi tahapan penelitian **"ANALISIS MANAJEMEN RISIKO KEAMANAN INFORMASI MENGGUNAKAN *FRAMEWORK* OCTAVE-S DAN ISO 27001:2022"**. Analisis risiko menggunakan OCTAVE-S telah dilakukan dengan melakukan pengisian kuesioner oleh divisi yang terlibat. Pembuatan kuesioner dimaksudkan untuk mempermudah responden mengisi lembar kerja OCTAVE-S.

Data yang tertuang dalam dokumen ini benar-benar berdasarkan hasil dari pengisian kuesioner lembar kerja OCTAVE-S yang nantinya diberikan rekomendasi mitigasi yang mengacu pada ISO 27001:2022 berdasarkan risiko terhadap asset-aset kritis UPA TIK Undiksha yang telah dianalisis.

2. PENGENALAN OCTAVE-S

OCTAVE-S adalah alat bantu kerja yang digunakan untuk mengidentifikasi ancaman risiko terkait TI. OCTAVE-S adalah versi OCTAVE yang dirancang untuk memenuhi kebutuhan organisasi yang lebih kecil dan tidak terlalu hierarkis (C. Alberts et al., 2005). Dengan menerapkan hasil OCTAVE-S, sebuah organisasi berusaha untuk melindungi semua aset dengan lebih baik lagi dan meningkatkan keseluruhan aspek keamanan asset (Rido et al., 2023). OCTAVE-S digunakan oleh organisasi kecil dengan kurang dari 100 orang dan dicoba oleh kelompok TI yang terdiri dari 3 hingga 5 orang.

3. LANGKAH OCTAVE-S

Berikut merupakan langkah atau proses analisis menggunakan OCTAVE-S yang disajikan pada tabel 1.

Tabel 1 Langkah OCTAVE-S

No	Fase	Deskripsi
1.	Membangun Profil Ancaman Berbasis Aset	Mengidentifikasi area informasi penting di organisasi yang menyimpan informasi sensitif, serta aset utama yang penting untuk kelangsungan bisnis. Termasuk di dalamnya adalah identifikasi aset yang berisiko tinggi berdasarkan kerentanan dan dampak
2.	Mengidentifikasi Kerentanan Infrastruktur	Mengidentifikasi ancaman terhadap aset utama organisasi, baik ancaman internal maupun eksternal. Pada fase ini, juga diidentifikasi kerentanan yang bisa dieksploitasi oleh ancaman tersebut untuk meningkatkan risiko terhadap aset.
3.	Mengembangkan Strategi dan Rencana Keamanan	Berdasarkan hasil analisis dan identifikasi, dikembangkan strategi mitigasi risiko, serta hasil analisis diintegrasikan ke dalam keputusan strategis dan operasional organisasi.

4. HASIL ANALISIS

1) Evaluasi Kriteria Dampak

Proses ini menentukan serangkaian ukuran kualitatif (tinggi, sedang, rendah) yang digunakan untuk mengevaluasi pengaruh risiko terhadap misi dan tujuan organisasi. Lembar kerja yang diperlukan pada aktivitas ini adalah Lembar Kerja Kriteria Evaluasi Dampak. Dari hasil evaluasi kriteria dampak yang dilakukan dengan cara mengisi kuesioner lembar kerja Evaluasi Kriteria Dampak, hasilnya dapat dilihat pada table berikut:

Tabel 2 Evaluasi Kriteria Dampak

No	Kiteria Dampak	Jenis Dampak	Level
1	Reputasi dan Kehilangan Aset	Reputasi	Sedang
		Kehilangan Aset	Tinggi
2	Keuangan	Biaya Operasional	Tinggi
3	Produktivitas	Jam Kerja	Tinggi
4	Kesehatan/ Keselamatan	Kesehatan / Keselamatan Pegawai	Sedang

2) Identifikasi Aset Organisasi

Proses ini mengidentifikasi aset-aset yang dimiliki oleh organisasi. Aset organisasi diidentifikasi menjadi dua (2) kelompok, yang pertama adalah aset informasi, sistem, dan aplikasi. Yang kedua adalah aset manusia, yaitu individu-individu dengan keterampilan khusus yang vital bagi organisasi. Lembar kerja yang diperlukan pada aktivitas ini adalah Lembar Kerja Identifikasi Aset dengan data hasil pengisian kueasioner dapat dilihat pada tabel-tabel lembar kerja berikut.

Tabel 3 Aset Informasi, Sistem, dan Aplikasi

Informasi, Sistem, dan Aplikasi			
Sistem	**Informasi**	**Aplikasi dan Layanan**	**Aset Lainnya**
Server	SOP dan Instruksi Kerja	SIAK	Perangkat Jaringan

Tabel 4 Aset Sumber Daya Manusia

Sumber Daya Manusia			
Sumber Daya Manusia	**Keterampilan dan Pengetahuan**	**Sistem terkait**	**Aset Terkait**
Sekretaris UPA TIK Undiksha dan Divisi Infrastruktur, Jaringan & keamanan.	Jaringan dan Pemrograman	OS, Windows, Linux, Tool Pemrograman	Komputer dan Laptop

3) Evaluasi Praktik Keamanan Organisasi

Proses mengevaluasi praktik keamanan organisasi yaitu mengevaluasi praktik keamanan. Aktivitas ini menentukan sejauh mana setiap praktik dalam survey digunakan oleh organisasi. Setelah survey dilakukan, selanjutnya adalah menetapkan status lampu merah (merah, kuning, hijau) untuk setiap area praktik keamanan. Status lampu merah ini harus mencerminkan seberapa baik kinerja organisasi di setiap area praktik keamanan.

Tabel 5 Evaluasi Praktik Keamanan Organisasi

NO	PRAKTIK KEAMANAN	STATUS STOPLIGHT		
		RED	YELLOW	GREEN
1.	Kesadaran dan Pelatihan Keamanan		[X]	
2.	Strategi Keamanan		[X]	
3.	Manajemen Keamanan		[X]	
4.	Peraturan dan Kebijakan Keamanan		[X]	
5.	Manajemen Keamanan Kolaboratif		[X]	
6.	Pemulihan Bencana		[X]	
7.	Pengendalian Akses Fisik		[X]	
8.	Pemantauan dan Audit Keamanan Fisik			[X]
9.	Manajemen Jaringan dan Sistem		[X]	
10.	Pemantauan dan Audit Keamanan TI		[X]	
11.	Otentikasi dan Otorisasi			[X]
12.	Manajemen Kerentanan		[X]	
13.	Enkripsi			[X]
14.	Perancangan dan Arsitektur Keamanan		[X]	
15.	Manajemen Insiden		[X]	

Penilaian pada aktivitas ini dilaksanakan dengan mengacu pada stoplight yang telah ditentukan oleh OCTAVE-S. Pemberian stoplight (status lampu merah) ditentukan berdasarkan hasil pengisian lembar kerja dengan menggunakan kuesioner yang sebelumnya telah dilakukan.

a. **Merah**: organisasi tidak menjalankan praktik keamanan di area tersebut sangat memerlukan perbaikan.
b. **Kuning**: organisasi menjalankan praktik keamanan namun masih ada ruang untuk perbaikan atau masih dibutuhkan perbaikan.
c. **Hijau**: organisasi menjalankan praktik keamanan di area tersebut dengan sangat baik; tidak ada perbaikan yang dibutuhkan.

4) Memilih Aset Kritis

UPA TIK Undiksha memiliki aset kritis yang berperan penting dalam menjalankan operasional harian mereka. Keberadaan aset-aset ini dinilai sangat vital untuk menjaga efisiensi dan keberlangsungan operasional di lingkungan UPA TIK Undiksha.

a. Server

Server merupakan pusat dari data dan sistem informasi sebagai jantungnya sebuah organisasi, server down hampir semua aktifitas tidak dapat berjalan dengan baik. Karena hampir semua kegiatan organisasi menggunakan sistem informasi. Terdapat aset yang terkait dengan server adalah Data civitas akademika dan semua sistem informasi yang dikembangkan oleh organisaasi (UNDIKSHA). Adapun pengguna server adalah admin database dan sistem informasi termasuk juga programmer dan admin jaringan dengan privileges sesuai kebutuhan masing-masing.

b. Perangkat Jaringan

Perangkat jaringan yang menjadi layanan inti dari lembaga kepada dosen, pegawai, dan mahasiswa terdapat potensi penyalahgunaan akses ke perangkat jaringan. Perangkat jaringan diperiksa satu (1) bulan sekali untuk mendeteksi adanya kerentanan. Dilakukan pemantauan dan evaluasi satu (1) bulan sekali terhadap prosedur keamanan yang diterapkan.

c. Sumber Daya Manusia; Sekretaris

Sekretaris UPA TIK Undiksha membantu kepala UPA TIK untuk memanajemen anggaran, sumber daya manusia, dan vendor.

Aset yang terkait dengan Sekretaris UPA TIK Undiksha dalam pekerjaannya sehari-hari adalah aset berupa laptop dan printer.

d. Sumber Daya Manusia; Divisi Infrastruktur, Jaringan & Keamanan

Divisi ini menjadi tim inti dalam organisasi, jika jaringan internet terputus maka layanan tidak akan tersedia. Selain itu juga divisi ini menjaga keamanan dari layanan yang diberikan. Divisi ini terdiri dari 1 kepala divisi dan 3 anggota divisi, total sebanyak 4 orang yang berada pada Divisi Infrastruutr, Jaringan & Keamanan. Adapun aset yang terkait dengan Divisi Infrastrukutr, Jaringan & Keamanan adalah aset infrastruktur seperti switch dan router.

e. SIAK

SIAK merupakan hal yang vital pada universitas karena semua data penunjang akademik, proses pembelajaran digunakan untuk mempermudah pengadministrasian pencatatan riwayat pembelajaran, dan diperlukan untuk dilaporkan ke pangkalan data pendidikan tinggi. Mulai dari mata kuliah, penawaran, kartu rencana studi, nilai matakuliah, perangkat pembelajaran (RPS, SPP, silabus), aktivitas kuliah mahasiswa, dan penunjang lainnya yang berhubungan dengan akademik. Adapun aset yang terkait dengan SIAK adalah aset informasi berupa data riwayat pembelajaran meliputi, data mata kuliah, data krs, data nilai mahasiswa, data Perangkat Pembelajaran, dan aset untuk mengetahui data mining, untuk memutuskan sesuatu yang berhubungan dengan akademik. Sistem Informasi Akademik (SIAK) ini digunkan oleh mahasiswa, dosen, dan peawai Universitas Pendidikan Ganesha.

f. SOP dan Instruksi Kerja

SOP dan Instruksi Kerja penting bagi organisasi karena pekerjaan dikerjakan berdasarkan SOP dan Instruksi Kerja (IK) yang sudah diterapkan. Adapun aset yang terkair dengan SOP dan Instruksi Kerja adalah dokumen SOP dan Instruksi Kerja, template SOP dan Instruksi Kerja, Log perubahan SOP dan Instruksi Kerja.

SOP digunakan oleh civitas akademika dan Instruksi Kerja digunakan oleh masing-masing divisi terkait.

5) Identifikasi Persyaratan Keamanan Aset Kritis

Persyaratam keamanan menggambarkan kualitas aset yang penting bagi organisasi. Terdapat tiga (3) persyaratan keamanan untuk aset kritis yaitu:

1. Kerahasiaan: kebutuhan untuk menjaga agar informasi hak milik, sensitif, atau pribadi tetap rahasia dan tidak dapat diakses oleh siapa pun yang tidak berwenang untuk melihatnya.
2. Integritas: keaslian, keakuratan, dan kelengkapan aset.
3. Ketersediaan: kapan atau seberapa sering suatu aset harus ada atau siap digunakan.
4. Lainnya: untuk persyaratan keamanan tambahan yang tidak termasuk dalam kategori kerahasiaan, integritas, dan ketersediaan.

Berikut merupakan data yang diperoleh dari aktivitas identifikasi persyaratan keamanan aset kritis pada lembar kerja yang telah disajikan pada tabel-tabel lembar kerja sebelumnya dimana aset kritis sudah diurutkan berdasarkan skala prioritas dan kerentanan.

Tabel 6 Data Aset Kritis

No	Aset Kritis	Kebutuhan Keamanan	Keterangan
1.	Server	Kerahasiaan	Server hanya dapat diakses oleh orang-orang tertentu saja dengan role yang sudah disesuaikan dengan kebutuhan dengan semua akses harus melewati server tunnel.
		Ketersediaan	Ketersediaan server yang dapat diakses selama 24 jam.

2.	Perangkat jaringan	Kerahasiaan	Pengaturan dan data konfigurasi jaringan harus hanya diakses oleh personel jaringan yang berwenang.
		Integritas	Monitoring jaringan pada lingkup organisasi, termasuk menjaga perangkat agar tidak dimodifikasi secara tidak sah.
		Ketersediaan	Perangkat harus beroperasi secara optimal dan dapat diakses kapan saja untuk memastikan konektivitas jaringan yang konsisten.
3.	Sekretaris UPA TIK Undiksha	Kerahasiaan	Sekretaris harus menjaga bahwa informasi dan data sensitif yang dikelola tidak boleh diakses oleh pihak yang tidak berwenang.
		Integritas	Sekretaris harus memastikan bahwa informasi yang diakses dan disimpan pada peralatan teknologi informasi serta server tetap utuh dan akurat.
		Ketersediaan	Akses ke sistem dan data harus selalu tersedia sesuai dengan kebutuhan operasional. Sekretaris dan staf pendukung harus siap memberikan dukungan teknis kapan saja untuk memastikan kelancaran operasional.
4.	Divisi Infrastruktur, Jaringan & Keamanan	Kerahasiaan	Divisi Infrastruktur, Jaringan & Keamanan memastikan kerahasiaan data yang dimiliki.
		Ketersediaan	Divisi Infrastruktur, Jaringan & Keamanan memastikan data yang diperlukan tersedia.

5.	SIAK	Otentikasi	Setiap pengguna SIAK yang mencoba mengakses sistem harus diverifikasi identitasnya. Ini bisa dilakukan melalui kata sandi yang kuat, biometrik, otentikasi multi-faktor, atau sertifikat digital.
		Otorisasi	Pengguna yang telah terotentikasi hanya diberikan akses sesuai dengan hak mereka. Ini membatasi apa yang dapat dilakukan pengguna di dalam sistem SIAK.
6.	SOP dan Instruksi Kerja	Kerahasiaan	Kerahasiaan dokumen harus dijaga, namun ada beberapa SOP yang harus dipublish di ketahui civitas akademik seperti SOP permintaan layanan SI/TI
		Ketersediaan	Ketersediaan harus bisa diakses dengan mudah juga oleh staff UPA TIK.

Berikut merupakan data persyaratan keamanan paling penting aset kritis yang telah ditentukan sebelumnya.

Tabel 7 Data Persyaratan Keamanan Paling Penting

No	Aset	Persyaratan keamanan paling penting
1.	Sever	Kerahasiaan
		Ketersediaan
2.	Perangkat jaringan	Kerahasiaan
		Integritas
		Ketersediaan

3.	SDM; Sekretaris UPA TIK Undiksha	Kerahasiaan
		Integritas
		Ketersediaan
4.	SDM; Divisi Infrastruktur, Jaringan & Keamanan	Kerahasiaan
		Ketersediaan
5.	SIAK	Integritas
6.	SOP dan instruksi kerja	Kerahasiaan
		Ketersediaan

6) Identifikasi Ancaman Terhadap Aset Kritis

Ancamann terhadap aset kritis organisasi dapat terjadi melalui tiga (3) akses, yaitu akses jaringan, akses fisik, dan masalah sistem. Pada akses jaringan dan fisik tersebut terdapat dua aktor yang memiliki kemungkinan menjadi ancaman, yaitu aktor yang berasal dari dalam organisasi (*internal*) dan aktor yang berasal dari luar organisasi (*external*), pada masalah sistem terdapat aktor kerusakan perangkat lunak, kegagalan sistem, kerusakan perangkat keras, dank kode berbahaya. Adapun motif ancaman dari aktor/pelaku terbagi menjadi dua (2) yaitu, ancaman yang dilakukan secara sengaja dan ancaman yang dilakukan secara tidak sengaja. Dari adanya motif pelaku tersebut memungkinkan dapat terjadinya pengungkapan/penyingkapan, modifikasi, kehilangan dan kerusakan, serta gangguan (interupsi).

Pada lembar kerja aktivitas identifikasi ancaman pada aset kritis organisasi, dilakukan penilaian terhadap aset kritis yaitu, Server, Perangkat Jaringan, Sumber Daya Manusia; Sekretaris dan Divisi Infrastruktur, Jaringan, & Keamanan, SIAK, SOP dan Instruksi Kerja

berdasarkan lembar kerja OCTAVE-S. Dalam lembar kerja untuk mengidentifikasi ancaman terhadap aset kritis, terdapat kolom pertanyan untuk mengetahui pelaku, jalur akses, motif serta dampak yang ditimbulkan. Dari pertanyaan-pertanyaan tersebut, menghasilkan diagram pohon profil ancaman pada aset kritis UPA TIK Undiksha. Diagram pohon profil ancaman pada aset kritis UPA TIK Undiksha menggunakan akses jaringan, akses fisik, dan masalah sistem.

Berikut merupakan penjelasan mengenai pohon profil ancaman UPA TIK Undiksha:

1. Server

Server merupakan aset yang penting bagi suatu organisasi juga UPA TIK Undiksha dimana akses server *database* dipegang oleh Divisi Pusat Data & Informasi dan akses server web dipegang oleh Divisi Infrastruktur, Jaringan, & Keamanan. Akses fisik ke ruang server sudah menggunakan sidik jari dan hanya orang-orang tertentu saja yang memiliki akses serta ruang server dilengkapi dengan CCTV. Berikut merupakan penjelasan ancaman terhadap server melalui jalur akses.

a. Jalur akses jaringan

Pada jalur akses jaringan, aktor yang memiliki ancaman terhadap server adalah pihak UPA TIK Undiksha (*internal*) dan pihak luar UPA TIK Undiksha (*external*) dengan motif sengaja dan tidak sengaja. Motif utama pelaku *external* adalah secara sengaja menyerang server adalah untuk men-*down*-kan server dan mencuri data yang mengakibatkan gangguan pada server. Serangan dari pihak *external* memiliki riwayat 1 bulan mendapat satu (1) kali serangan DDos dengan tingkat kekuatan ancaman rendah.

Pihak *internal* UPA TIK Undiksha juga memliki potensi ancaman pada server dengan dampak kehilangan, kerusakan yaitu kehiangan data yang diakibatkan oleh *human error* atau kerusakan *hard drive* (HD) dengan tingkat kemungkinan yang rendah. Dilakukan pengecekan setiap hari pada server untuk mendeteksi

kemungkinan terjadi serangan dan jika ditemukan kerentanan akan segera di antisipasi agar tidak terjadi gangguan kembali pada server.

b. Jalur akses fisik

Pada jalur fisik, aktor yang memiliki ancaman pada server secara fisik adalah pihak *internal* yaitu Divisi Infrastruktur, Jaringan & Keamanan yang menyebabkan terjadinya gangguan yaitu kesalahan pegawai dalam penanganan kerusakan server secara fisik. Dalam hal ini, tidak ada riwayat ancaman fisik terhadap server.

Pihak *external* yaitu bencana alam yang menyebabkan adanya gangguan pada server memiliki potensi ancaman dengan tingkat ancaman yang rendah. Pemeliharaan fisik ruang server untuk memastikan keamanan dilakukan 1 kali perminggunya. Sejauh ini tidak ada insiden ataupun pernah terjadi risiko fisik terhadap server.

c. Jalur masalah sistem

Kerusakan perangkat lunak yaitu kerusakan sistem pada server menakibatkan terjadinya gangguan pada server sehingga menyebabkan gagal *log in* ke sistem operasi dan terjadi masalah dalam sistem operasi yang menyebabkan tidak bisa menyimpan data di *hard disk*. Kerusakan perangkat lunak pada server sebanyak dua (2) kali dalam kurun waktu lima (5) tahun.

Kegagalan sistem pada server dapat menyebabkan gangguan sehingga operasinal sistem terganggu atau terhenti, sehingga akses ke data atau layanan tidak bisa dilakukan. Gangguan ini terjdi satu (1) kali dalam kurun waktu lima (5) tahun.

Kerusakan perangkat keras server seperti kerusakan *hard disk* dan *processor* yang dapat menyebabkan gangguan pada server yaitu *hard disk* dan *processor* tidak berfungsi dengan baik. Kerusakan perangkat keras pada server terjadi sebanyak tiga (3) kali dalam kurun waktu lima (5) tahun.

Kode berbahaya yang menyerang server seperti kode tidak legal masuk ke server dapat menyebabkan gangguan terhadap operasonal sistem. Selain kode berbahaya, serangan DDos dan juli *online* juga

dapat menyebabkan server terganggu. Ancaman kode berbahaya terjadi lima (5) kali dalam lima (5) tahun.

2. Perangkat Jaringan

Divisi Infrastruktur, Jaringan & Keamanan memiliki tanggung jawab dalam mengelola dan memelihara keamanan perangkat jaringan. Akses ke perangkat jaringan sudah dikendalikan dengan baik. Berikut merupakan penjelasan ancaman terhadap perangkat jaringan melalui jalur akses.

a. Jalur akses jaringan

Pada jalur akses jaringan, aktor yang memiliki ancaman terhadap perangkat jaringan adalah pihak luar UPA TIK Undiksha (*external*). Motif utama pelaku *external* adalah secara sengaja melakukan serangan untuk mencuri data dan untuk mengambil alih jaringan dengan tingkat ancaman yang tinggi. Serangan DDos dan judi *online* sering terjadi pada perangkat jaringan dengan tingkat ancaman tinggi. Pemeliharaan perangkat jaringan dilkukan secara berkala yaitu satu (1) bulan sekali.

b. Jalur akses fisik

Pada jalur akses fisik, aktor yang memiliki potensi ancaman pada server adaah pihal *external* yang secara secara sengaja untuk melalukan pencurian perangkat keras suku cadang dengan tingkat ancaman sedang. Pihak *internal* UPA TIK Undiksha juga memiliki ancaman terhadap perangkat jaringan karena ketidaktahuan pihak *internal* dengan asal memasang kabel jaringan ke perangkat jaringan sehingga menyebabkan *loop* dan jaringan menjadi *error*.

c. Jalur akses masalah sistem

Kerusakan perangkat lunak bisa menyebabkan data atau informasi yang dapat diakses atau terjadi penyingkapan informasi atau data, kehilangan akses sistem, dan gangguan ketika mengakses layanan. Kerusakan perangkat lunak bisa terjadi karena perangkat lunak tidak pernah di*update*. Kerusakan perangkat lunak bisa terjadi

satu (1) bulan bisa sampai dua (2) atau tiga (3) kali dan perlu ditangani selama satu (1) jam.

Kegagalan sistem bisa menyebabkan gangguan terhadap layanan, sehingga pengguna tidak dapat mengakses layanan. Kegagalan sistem dapat terjadi karena *switch* atau *router* tidak dapat dipakai. Kegagalan sistem perangkat jaringan jarang terjadi yaitu satu (1) tahun sekali dalam kurun waktu satu (1) jam.

Kerusakan perangkat keras seperti *switch* atau *router* mati dapat menyebabkan ancaman gangguan sehingga operasional sistem terganggu atau terhenti, sehingga akses ke data atau layanan tidak bisa dilakukan. Kerusakan perangkat keras jaringan jarang terjadi yaitu satu (1) tahun terkadang satu (1) kali selama (1) jam.

Serangan DDos menyebabkan gangguan sehingga membuat *bandwith* penuh dan layanan tidak dapat diakses dan terjadi peningkatan *bandwidth* yang cukup tinggi.

3. SDM; Sekretaris UPA TIK Undiksha

   Pengambilan cuti sementara oleh Sekretaris UPA TIK Undiksha tidak memiliki dampak atau pengaruh terhadap kelancaran operasionalnya sehari-hari karena pekerjaannya bisa dikerjakan secara *online*.

   Jika Sekretaris UPA TIK Undiksha meninggalkan organisasi secara permanen (misalnya pensiun atau pindah kerja) tidak memiliki dampak pada operasional organisasi karena semua dokumentasi terarsip dengan baik, proses peralihan juga sudah disiapkan.

   Sampai saat ini, tidak pernah ada ancaman pihak ketiga pada tugas sekretaris UPA TIK Undiksha sehingga pihak ketiga tidak mempengaruhi kinerja sekretaris UPA TIK Undiksha.

4. SDM; Divisi Infrastruktur, Jaringan & Keamanan

   Jika staf Divisi Infrastruktur, Jaringan & Komunikasi mengambil cuti sementara (misalnya karena sakit atau keperluan diluar organisasi), hal ini tidak berdampak pada operasional sehari-

hari karena tugas-tugas yang bersangkutan telah dialihkan kepada staf lain yang tidak sedang cuti. Divisi Infrastruktur, Jaringan & Keamanan jarang mengambil cuti, satu (1) bulan terkadang satu (1) kali.

Jika staf Divisi Infrastruktur, Jaringan & Keamanan meninggalkan oeganisasi secara permanen (misalnya karena pensiun atau pindah kerja), hal ini tidak berdampak pada operasional sehari-hari karena ketika ada staf yang pindah secara permanen, akan diminta aksesnya dan dokumentasi yang selama ini dipegang kemudian menonaktifkan semua akses yang dimiliki. Sampai saat ini, tidak pernah ada pergantian staf Divisi Infrastruktur, Jaringan & Keamanan.

Pihak ketiga (misalnya vendor) tidak memiliki akses ke server. Kendala yang mungkin disesbabkan oleh pihak ketiga adalah ketidaktersediaan layanan, seperti internet yang mati atau ketika listrik mati.

5. Sistem Informasi Akademik (SIAK)

Sistem Informasi Akademik (SIAK) merupakan aset penting karena semua aktivitas perkuliahan dan penunjang lainnya berhubungan dengan akademik ditunjang oleh SIAK. Berikut merupakan penjelasan ancaman terhadap SIAK selalui jalur akses.

a. Jalur akses jaringan

Pihak *external* yaitu mahasiswa menjadi ancaman terjadinya modifikasi data yaitu merubah nilai yang dilakukan oleh mahasiswa sendiri karena memberikan akun sistem. Selain mahasiswa, pihak *external* lainnya yang dapat mengancam SIAK adalah peretas yang mencoba masuk ke dalam sistem SIAK untuk tujuan keuangan, sabotase, atau hanya mencari tantangan. Peretas bisa memanfaatkan kelemahan dalam keamanan jaringan atau perangkat lunak untuk mencuri atau merusak data. Tingkat ancaman yang berasal dari pihak *external* berada pada tingkat ancaman tinggi.

Pihak *internal* UPA TIK Undiksha juga menjadi ancaman terhadap SIAK karena pada SIAK lama yaitu modifikasi data oleh staf UPA TIK Undiksha yang sebenarnya tidak sesuai dengan kebijakan. Namun, karena adanya persetujuan dari pimpinan, perubahan tersebut tetap dilakukan meskipun melanggar aturan atau prosedur yang seharusnya. Tingkat ancaman yang berasal dari pihak *internal* berada pada tingkat ancaman sedang.

Sistem Informasi Akademik (SIAK) mengalami gangguan jaringan yang terjadi akibat banyaknya akses secara bersamaan, sehingga menyebabkan sistem mengalami down. Untuk mengatasi dan mencegah ancaman keamanan, pemeliharaan dilakukan satu (1) kali setiap enam (6) bulan, yang disesuaikan dengan tingkat kepadatan akses. Akses jaringan ke sistem SIAK pun sudah dikendalikan dengan baik. Divisi Infrastruktur, Jaringan & Keamanan yang bertanggung jawab dalam mengelola akses jaringan ke SIAK.

b. Jalur akses fisik

Pada jalur akses jaringan, aktor yang memiliki ancaman terhadap SIAK adalah pihak UPA TIK Undiksha (*internal*) dan pihak luar UPA TIK Undiksha (*external*) dengan motif sengaja dan tidak sengaja. Motif utama pelaku *internal* secara tidak sengaja human error, kesalahan *query* yang menyebabkan kehilangan data sehingga organisasi mengalami kerugian operasional yang signifikan, termasuk downtime sistem, kehilangan informasi penting, dan gangguan dalam layanan akademik. Jika perangkat rusak secara fisik, waktu dan biaya pemulihan bisa tinggi. Tingkat ancaman pihak *internal* terhadap SIAK melalui jalur akses fisik tinggi karena jika ada motivasi seperti kepentingan pribadi, ketidakpuasan kerja, atau balas dendam, aktor internal dengan akses fisik bisa mencoba mengeksploitasi sistem. Contohnya, seorang pegawai yang merasa tidak puas atau terancam dengan perubahan kebijakan dapat termotivasi untuk menyalahgunakan aksesnya.

Pihak *external* seperti tamu atau vendor memiliki potensi ancaman terhadap SIAK motifnya melakukan pencurian data untuk dijual atau bahkan sabotase untuk tujuan tertentu. Pihak *external* dengan akses fisik dapat menyusup ke perangkat jaringan untuk mencuri data atau informasi sensitif. Penyusupan ini bisa berupa akses langsung ke server atau perangkat untuk mencuri data. Kebocoran data sensitif seperti data pribadi mahasiswa, informasi akademik, atau detail login dapat dieksploitasi oleh pihak eksternal untuk tujuan kriminal atau pencurian identitas. SIAK pernah mengalami serangan DDos, ini sengaja dilakukan agar sistem sulit untuk di akses dari pihak luar (saingan) dan juga pernah mengalami *down database* karena akses membludak. Langkah yang telah diterapkan untuk mengamankan akses fisik ke perangkat adalah pemindahan ke server *docker* dari server *cluster*, pemasangan Port Git, dan *update dependency* pada sistem.

c. Jalur akses masalah sistem

Kerusakan perangkat lunak pada Sistem Informasi Akademik (SIAK) bisa berdampak sangat signifikan pada operasional harian di lingkungan pendidikan, terutama karena SIAK merupakan sistem inti yang mengelola data akademik dan administrasi. Terjadi kegagalan sistem atau *downtime* pada SIAK karena pemeliharaan perangkat keras atau perangkat lunak yang tidak terjadwal dapat mengakibatkan kegagalan sistem. Ketika SIAK tidak dapat diakses, kegiatan akademik seperti pengisian KRS dan pengambilan nilai dapat terganggu. SIAK mengalami gangguan terjadi satu (1) tahun dua (2) kali karena padatnya akses saat kegiatan penyusunan KRS terjadi dan juga karena aktivitas lain terjadi secara berbarengan.

Kegagalan sistem pada Sistem Informasi Akademik (SIAK) dapat memberikan dampak yang serius pada operasional sehari-hari di institusi pendidikan, karena sistem ini berperan penting dalam pengelolaan data akademik, administrasi, dan layanan kepada

mahasiswa, dosen, serta staf. Secara keseluruhan, kegagalan sistem pada SIAK berdampak negatif pada efisiensi, keamanan data, serta kepuasan pengguna, sehingga penting bagi institusi untuk memastikan ketahanan sistem, keamanan data, dan prosedur pemulihan yang cepat untuk meminimalkan risiko dan dampak dari kegagalan sistem. Kegagalan sistem bisa terjadi karena ketika secara bersamaan terjadi aktivitas yang berbeda, seperti saat KRS dilakukan berbarengan dengan pendaftaran wisuda, mengunduh nominatife wisuda, mengunduh ijazah, dan mengunduh transkrip nilai. SIAK mengalami gangguan kegagalan sistem biasanya terjadi setiap semester yaitu satu (1) tahun dua (2) kali. Skalabilitas dan ketahanan sistem perlu diperbaiki, SIAK perlu dibangun agar mampu menangani lonjakan beban, khususnya saat periode pendaftaran atau pengumuman nilai. Kegagalan skalabilitas dapat menyebabkan sistem tidak merespons di waktu-waktu kritis.

Kerusakan perangkat keras pada Sistem Informasi Akademik (SIAK) dapat memberikan ancaman pada operasional sistem terganggu. Kerusakan perangkat keras pernah terjadi satu (1) tahun sebanyak dua (2) kali.

Kode berbahaya, seperti virus, *worm, Trojan horse, dan backdoor*, dapat memberikan dampak serius pada Sistem Informasi Akademik (SIAK) yang digunakan dalam lingkungan pendidikan. Jenis-jenis kode berbahaya ini sering kali menyusup ke dalam sistem melalui jaringan yang terhubung ke internet, email, atau perangkat eksternal, yang pada akhirnya dapat mengganggu operasional harian SIAK. SIAK mengalami gangguan serangan kode berbahaya terjadi lima (5) tahun sekali. Kode berbahaya dapat memengaruhi SIAK dalam berbagai cara mulai dari penyingkapan data, modifikasi yang tidak sah, kehilangan data yang tidak dapat dipulihkan, hingga gangguan operasional yang menghambat akses ke layanan penting. Untuk meminimalkan risiko, institusi perlu menerapkan langkah-langkah keamanan seperti *firewall, antivirus, backup* data secara

berkala, dan pemantauan sistem untuk mendeteksi dan mengatasi ancaman sebelum terjadi kerusakan lebih lanjut.

6. SOP dan Instruksi Kerja

SOP dan Instruksi Kerja (IK) merupakan asset penting bagi UPA TIK Undiksha karena memulai pekerjaan berdasarkan SOP dan IK yang sudah ditetapkan. Tidak ada kemungkinan tidak sah pada SOP dan IK karena dilakukan diskusi untuk melakukan perubahan namun perubahan tidak pernah tercatat atau pembaharuan di daftar dokumen SOP yang dimiliki UPA TIK Undiksha. Dalam menjaga dokumen SOP dan IK tetap aman dari akses yang tidak berwenang, SOP dan IK disimpan pada *google drive* dan tidak memberikan akses ke semua orang, akses diberikan sesuai dengan divisi masing-masing. Berikut merupakan penjelasan ancaman terhadap SOP dan Instruksi Kerja (IK) melalui jalur akses.

a. Jalur akses jaringan

Pada jalur akses jaringan, aktor yang memiliki ancaman terhadap SOP dan Instruksi Kerja (IK) adalah pihak *internal* UPA TIK Undiksha yang secara tidak sengaja menyebabkan gangguan pemeliharaan sistem yaitu kesalahan dalam pemeliharaan atau pembaruan sistem yang menyimpan SIP dan IK dapat mengakibatkan ketidakmampuan karyawan untuk mengakses dokumen tersebut secara efisien. Hal ini bisa menghambat pelaksanaan SOP di lapangan. Tigkat ancaman perubahan atau modifikasi tidak sah pada okumen SOP dan IK tinggi. Terlebih lagi SOP dan IK belum dilindungi oleh kontrol akses jaringan, namun belum ada insiden terkait ancaman jaringan terhadap SOP dan IK sebelumnya. Pihak *external* UPA TIK Undiksha juga memiliki potensi ancaman melalui jalur akses jaringan yang dilakukan secara sengaja yaitu melakukan pencurian data untu kepentingan pihak ketiga.

b. Jalur akses fisik

Pihak *internal* UPA TIK Undiksha memiliki ancaman terhadap dokumen SOP dan IK yang disimpan secara fisik yaitu secara tidak sengaja kemungkinan hilang atau lupa tempat menyimpan dokumen, namun UPA TIK Undiksha sudah menyimpan dokumen di tempat yang aman yaitu di lemari penyimpanan yang terkunci. Sehingga tingkat ancaman pihak *internal* terhadap dokumen SOP dan IK rendah. Belum ada insiden terkait dengan ancaman secara fisik terhadap dokumen SOP dan IK bahkan pengecekan fisik dokumen dilakukan satu (1) bulan satu (1) kali untuk memastikan keamanan dokumen SOP dan IK.

LEMBAR PERTANDATANGANAN

INFORMASI PELAKSANAAN KONFIRMASI TEMUAN HASIL ANALISIS PENELITIAN "ANALISIS MANAJEMEN RISIKO KEAMANAN INFORMASI MENGGUNAKAN *FRAMEWORK* OCTAVE-S DAN ISO 27001:2022"			
Peneliti	:	Hardiyanti Rohmania	
Hari, Tanggal	:	Rabu, 5 februari 2025	
Lokasi	:	UPA TIK Undiksha	
DITANDATANGANI OLEH:			**Tanda Tangan**
Nama	:	I Ketut Resika Arthana, S.T., M.Kom.	
NIP	:	1984120120121210	
Instansi	:	UPA TIK Undiksha	
Jabatan	:	Kepala UPA TIK Undiksha	
Nama	:	Ida Komang Widhiarjaya, S.T.	
NIP	:	198108032006041002	
Instansi	:	UPA TIK Undiksha	
Jabatan	:	Sekretaris UPA TIK Undiksha	

Lampiran 18. Berita Acara Serah Terima Dokumen Rekomendasi

BERITA ACARA SERAH TERIMA DOKUMEN

Berita Acara Serah Terima Dokumen ("Berita Acara") ini dibuat pada hari ini, Selasa tanggal 6 bulan Mei tahun 2025, oleh dan diantara:

(1) Nama : Hardiyanti Rohmania
NIM : 2015091018
Program Studi : S1 Sistem Informasi

-selanjutnya ini disebut sebagai "**Pihak Pertama**"

(2) Nama : Ida Komang Widhiarjaya, S.T.
NIP : 198108032006041002
Jabatan : Sekretaris UPA TIK Undiksha
Instansi : Unit Penunjang Akademik Teknologi Informasi & Komunikasi

-selanjutnya disebut sebagai "**Pihak Kedua**"

Pihak Pertama dan Pihak Kedua secara bersama-sama selanutnya disebut sebagai "Para Pihak". Para Pihak dengan ini menerangkan dan menyatakan hal-hal sebagai berikut:

1. Bahwa, sebelumnya Pihak Pertama telah melaksanakan penelitian dengan jududl "**Analisis Manajemen Risiko Keamanan Informasi Menggunakan *Framework* OCTAVE-S dan ISO 27001:2022**";
2. Bahwa salah satu alur penelitian mewajibkan untuk melaksanakan penyerahan Dokumen Rekomendasi, maka Pihak Pertama dengan ini menyerahkan Dokumen kepada Pihak Kedua sebagaimana Pihak Kedua dengan ini menerima Dokumen tersebut dari Pihak Pertama;
3. Bahwa dengan telah dilakukannya serah terima dokumen berdasarkan Berita Acara ini, maka demikian kewajiban Pihak Pertama untuk menyerahkan Dokumen kepada Pihak Kedua dan Pihak Kedua untuk menerima Dokumen tersebut dari Pihak Pertama telah dilaksanakan;
4. Bahwa Berita Acara ini merupakan bagian dari pelaksanaan Penelitian dan sekaligus sebagai Tanda Terima Dokumen diantara Para Pihak.

Demikian Berita Acara ini dibuat pada waktu sebagaimana telah disebutkan pada bagian awal Berita Acara ini.

Para Pihak

Pihak Pertama	**Pihak Kedua**
Hardiyanti R	Ida Komang Widhiarjaya

DOKUMEN REKOMENDASI HASIL ANALISIS PENELITIAN

"ANALISIS MANAJEMEN RISIKO KEAMANAN INFORMASI MENGGUNAKAN FRAMEWORK OCTAVE-S DAN ISO 27001:2022"

Presented for :
UPA TIK UNDIKSHA

Presented by :
HARDIYANTI ROHMANIA
(2015091018)

Berdasarkan hasil analisis dan setelah dilakukan konfirmasi temuan dan hasil temuan telah ditandatangani, selanjutnya adalah meyusun rekomendasi mitigasi yang mengacu pada ISO 27001:2022. Rekomendasi dapat digunakan untuk melakukan perbaikan pada Unit Penunjang Akademik Teknologi Informasi dan Komunikasi (UPA TIK) Universitas Pendidikan Ganesha. Rekomendasi diberikan terhadap praktik keamanan organisasi dan asset organisasi dengan Klausul dan Annex dimana klausul membantu memberikan landasan bagi organisasi untuk membangun kerangka kerja yang sesuai dan Annex adalah kontrol spesifik yang dapat langsung diterapkan.

1. Rekomendasi area praktik keamanan organisasi

No	Aspek	Klausul dan Pengendalian berdasarkan ISO 27001:2022	Rekomendasi
1.	Praktik keamanan Kesadaran dan Pelatihan Keamanan	• Klausul 5.3 Peran, Tanggung Jawab dan Wewenang Organisasi • Klausul 7.3 Kesadaran • A 6.1 Skrining • A 6.3 Kesadaran, pendidikan dan pelatihan keamanan informasi	• Membuat kebijakan keamanan informasi yang jelas • Berikan pelatihan kesadaran keamanan informasi • Melakukan pemeriksaan kompetensi dan kesadaran terhadap calon staff mengenai keamanan informasi
2.	Praktik keamanan Strategi Keamanan	• Klausul 5.2 Kebijakan • Klausul 7.1 Sumber Daya • Klausul 7.2 Kompetensi • A 6.1 Skrining • A 8.6 Manajemen Kapasitas	• Tinjau dan sesuaikan kebijakan keamanan dengan strategi dan tujuan bisnis • Berikan pelatihan kesadaran keamanan informasi untuk staf • Implementasikan teknologi keamanan yang sesuai

No	Aspek	Klausul dan Pengendalian berdasarkan ISO 27001:2022	Rekomendasi
3.	Praktik keamanan Manajemen Keamanan	• Klausul 5.3 Peran, Tanggung jawab, dan Wewenang • Klausul 7.1 Sumber Daya • A 5.30 Kesiapan TIK untuk kontinuitas bisnis • A 6.3 Kesadaran, pendidikan, dan pelayihan keamanan informasi	• Mengalokasikan sumber daya, pastikan alokasi sumber daya yang cukup • Tentukan peran dan tanggung jawab keamanan
4.	Praktik keamanan Peraturan dan Kebijakan Keamanan	• Klausul 5.2 Kebijakan • Klausul 9.2 Audit internal • Klausul 10.2 Ketidaksesuaian dan tindakan korektif • A 5.1 Kebijakan keamanan informasi • A 5.31 Persyaratan legal, statutri, regulatori, dan kontraktual • A 5.36 Kepatuhan terhadap kebijakan, aturan, dan standar keamanan informasi	• Buat kebijakan keamanan informasi yang terdokumentasi • Dokumentasi kebijakan keamanan informasi • Maninjau dan memperbarui kebijakan keamanan informasi

No	Aspek	Klausul dan Pengendalian berdasarkan ISO 27001:2022	Rekomendasi
		• A 5.37 Prosedur operasi terdokumentasi	
5.	Praktik keamanan Manajemen Keamanan Kolaboratif	• Klausul 5.3 Peran, tanggung jawab, dan wewenang organisasi • Klausul 6.1.2 Asesmen risiko keamanan informasi • Klausul 7.4 Komunikasi	• Membuat dan menentukan prosedur keamanan untuk kerja sama internal • Dokumentasi kebijakan keamanan informasi • Pantau akses keamanan informasi
6.	Praktik keamanan Pemulihan Bencana	• Klausul 7.2 Kompetemsi • Klausul 7.3 Kesadaran • Klausul 8.1 Perencanaan dan pengontrolan operasional • Klausul 8.3 Penanganan risiko keamanan informasi • A 5.29 Keamanan informasi selama disrupsi	• Dokumentasikan rencana kontinjensi dan pemulihan bencana yang mencakup tindakan mitigasi darurat, prosedur pemulihan, dan daftar kontak penting. • Jadwalkan uji coba (simulasi) secara rutin untuk memastikan rencana tersebut dapat berjalan dengan baik. • Adakan pelatihan rutin bagi staf untuk memahami tanggung jawab mereka dalam situasi darurat atau bencana. • Lakukan backup data secara otomatis dan berkala ke lokasi penyimpanan yang terpisah *(off-site)*.

No	Aspek	Klausul dan Pengendalian berdasarkan ISO 27001:2022	Rekomendasi
		• A 5.2 Peran dan tanggung jawab keamanan informasi • A 8.13 Pencadangan informasi	• Verifikasi integritas dan pemulihan cadangan data secara berkala untuk memastikan data dapat diakses saat dibutuhkan.
7.	Praktik keamanan Pengendalian Akses Fisik	• Klausul 7.5 Informasi terdokumentasi • Klausul 8.1 Perencanaan dan pengontrolan operasional • A 7.2 Entri fisik • A 7.3 Mengamankan kantor, ruangan, dan fasilitas • A 7.5 Memproteksi dari ancaman fisik dan lingkungan	• Ganti kunci manual untuk lab komputer dengan sistem akses elektronik, seperti smart card atau pemindai sidik jari, untuk meningkatkan keamanan fisik dan mengurangi risiko akses oleh pihak yang tidak berwenang. • Gunakan sistem log untuk merekam aktivitas akses ke area kerja dan perangkat keras • Lakukan audit secara berkala terhadap catatan log untuk mengidentifikasi aktivitas yang mencurigakan • Perketat pengawasan terhadap pengunjung, termasuk penerapan peraturan untuk akses ke area sensitif seperti lab komputer.

No	Aspek	Klausul dan Pengendalian berdasarkan ISO 27001:2022	Rekomendasi
8.	Praktik keamanan Manajemen Jaringan dan Sistem	• Klausul 6.2 Sasaran keamanan informasi dan perencanaan untuk mencapainya • A 8.8 Manajemen kerentanan teknis • Klausul 8.3 Penanganan risiko keamanan informasi • Klausul 7.5 Informasi terdokumentasi • A 8.20 Keamanann Jaringan	• Jadwalkan pembaruan rutin pada rencana keamanan jaringan dan sistem minimal setiap 6 bulan, atau sesuai kebutuhan berdasarkan hasil analisis risiko. • Libatkan semua pihak terkait dalam proses pembaruan untuk memastikan cakupan keamanan yang menyeluruh. • Implementasikan kebijakan pembaruan sistem yang mencakup seluruh perangkat secara berkala • Tetapkan SLA untuk memprioritaskan pembaruan pada sistem yang kritis • Lakukan audit layanan aktif secara berkala, identifikasi layanan yang tidak diperlukan, dan segera non-aktifkan untuk mengurangi potensi exploitasi
9.	Praktik keamanan Pemantauan dan Audit Keamanan TI	• Klausul 9.3 Tinjauan manajemen • A 5.21 Memanajemeni keamanan informasi dalam rantai pasokan TIK	• Susun rencana audit berbasis risiko dengan mengidentifikasi aset kritis terlebih dahulu. • Pastikan audit mencakup analisis risiko yang telah diidentifikasi dalam kerangka manajemen risiko

No	Aspek	Klausul dan Pengendalian berdasarkan ISO 27001:2022	Rekomendasi
		• Klausul 6.1 Tindakan untuk menangani peluang • A 8.15 Membuat log • Klausul 10.2 Ketidak sesuaian dan tindaka korektif • A 8.8 Manajemen kerentanan teknis	• Terapkan sistem real-time monitoring untuk mendeteksi aktivitas mencurigakan pada jaringan dan sistem • Simpan log pemantauan secara aman untuk referensi dan analisis lebih lanjut • Lakukan pengukuran kerentanan secara berkala untuk mengidentifikasi risiko sebelum menjadi kejadian • Tetapkan langkah-langkah mitigasi jangka panjang untuk mencegah kerentanan berulang.
10.	Praktik keamanan Manajemen Kerentanan	• Klausul 8.2 Penilaian risiko keamanan informasi • Klausul 8.3 Penanganan risiko keamanan informasi • A 8.8 Manajemen kerentanan teknis • A 8.29 Pengujian keamanan dalam pengembangan dan penerimaan	• Melakukan analisis risiko untuk menentukan sistem prioritas yang perlu diuji • Mengumumkan rencana mitigasi terhadap kerentanan yang ditentukan • Terapkan proses manajemen kerentanan yang mencakup identifikasi, penilaian, dan perbaikan kerentanan di semua sistem atau server.

No	Aspek	Klausul dan Pengendalian berdasarkan ISO 27001:2022	Rekomendasi
			• Jadwalkan uji kerentanan secara berkala, mencakup semua sistem, termasuk yang jarang digunakan • Lakukan pengujian kerentanan sebelum sistem baru diimplementasikan. • Prosedur perbaikan uji kerentanan agar mencakup server dengan prioritas rendah sekalipun
11.	Praktik keamanan Perancangan dan Arsitektur Keamanan	• Klausul 6.1.3 Penanganan risiko keamanan informasi • Kalusul 8.1 Perencanaan dan pengendalian operasional • A 5.8 Keamanan informasi dalam manajemen proyek • A 8.25 Siklus hidup pengembangan yang aman • A 8.27 Arsitektur sistem aman dan prinsip rekayasa	• Menentukan control keamanan yang harus diterapkan pada arsitektur baru • Membuat prosedur keamanan yang diterapkan dalam pengembangan sistem baru • Dokumentasikan persyaratan keamanan sistem, termasuk ancaman dan risiko yang mungkin terjadi • Terapkan kebijakan pengembangan yang aman yang mencakup semua siklus hidup sistem, mulai dari perancangan hingga implementasi • Gunakan prinsip rekayasa yang aman

No	Aspek	Klausul dan Pengendalian berdasarkan ISO 27001:2022	Rekomendasi
12.	Praktik Keamanan Manajemen Insidenn	• Klausul penanganan risiko keamanan informasi • Klausul 9.1 pemantauan, pengukuran, analisis, dan evaluasi • A 5.24 Informasi manajemen insiden keamanan perencanaan dan persiapan	• Meningkatkan efektivitas prosedur manajemen kejadian • Mengevaluasi efektivitas respons terhadap kejadian keamanan

2. Rekomendasi aset

No	Aset	Jalur akses	Klausul dan pengendalian berdasarkan ISO 27001:2022	Rekomendasi mitigasi
1.	Server	Jaringan	• Klausul 6.1 Penilaian risiko keamanan informasi • Klausul 8.1 Perencanaan dan pengontrolan operasional • A 8.23 Penyaringan web • A 8.16 Pengontrolan aktivitas • Klausul 7.2 Kompetensi • Klausul 6.1.3 Penanganan risiko keamanan informasi • A 8.14 Pencadangan informasi • A 8.15 Membuat log • A 8.16 Pemonitoran aktivitas	• Pasang *firewall*, dapat memblokir lalu lintas mencurigakan yang mencoba menyerang server dan gunakan *firewall* bawaan sistem operasi atau dari penyedia layanan internet • Pantau aktivitas server berkala seperti lakukan pengecekan log server untuk melihat apakah ada aktivitas mencurigakan, seperti serangan DDoS • Batasi akses ke server seperti hanya izinkan akses ke server dari alamat IP yang terpercaya dan hindari penggunaan jaringan publik saat mengakses server. • *Backup* data secara rutin setiap minggu atau sebelum perubahan besar dilakukan dan simpan Salinan data penting di tempat lain seperti di *hard drive* eksternal atau *cloud*. • Lakukan pembaruan sistem operasi, aplikasi, dan firmware (penghubung antara perangkat keras dan perangkat lunak, mengatur dan mengontrol operasi dasar perangkat)

No	Aset	Jalur akses	Klausul dan pengendalian berdasarkan ISO 27001:2022	Rekomendasi mitigasi
				• Lakukan pelatihan keamanan informasi kepada staf untuk meningkatkan kesadaran terhadap prosedur kerja yang aman
		Masalah sistem	• Klausul 8.3 Penanganan risiko keamanan sistem informasi • A 8.13 Pencadangan Informasi • Klausul 8.1 Perencanaan dan pengendalian operasional • A 7.5 Memproteksi dari ancaman fisik dan lingkungan • A 8.6 Manajemen kapasitas • Klausul 8.1 Perencanaan dan pengontrolan operasional • A 8.20 Keamanan jaringan • A 5.26 Respons terhadap insiden keamanan informasi	• Sediakan server cadangan untuk mengalihkan operasi saat server utama mengalami kerusakan perangkat lunak dan pastikan data dan konfigurasi perangkat lunak selalu disinkronkan antara server utama dan server cadangan • Siapkan prosedur dokumentasi pemulihan untuk meminimalkan *downtime* saat sistem gagal • Pastika server diletakkan di ruanan dengan control lingkungan (seperti AC) • Menerapkan perlindungan fisik seperti kartu akses untuk mencegah adanya sabotase • Pantau secara berkala kondisi perangkat keras server • Perbarui secara berkala perangkat lunak server • Terapkan firewall untuk memblokir serangan DDos • Jadwalkan audit keamanan sistem secara berkala
2.	Perangkat jaringan	Jaringan	• Klausul 6.1.2 Penilaian risiko keamanan informasi • Klausul 8.1 Perencanaan dan pengontrolan operasional	• Melakukan penilaian risiko untuk mengidentifikasi ancaman dari aktor eksternal yang melakukan serangan DDoS dan judi *online*

No	Aset	Jalur akses	Klausul dan pengendalian berdasarkan ISO 27001:2022	Rekomendasi mitigasi
			• A 8.20 Keamanan jaringan • A 8.23 Penyaringan web • A 8.16 Kegiatan pemantauan	• Terapkan sistem filtering untuk memnlokir akses ke situs web berbahaya atau tidak sah • Gunakan *firewall* dan *proxy* untuk mengelola lalu lintas jaringan • Enkripsi semua data yang dikirimkan melakui jaringan untuk melindunginya dari *interepsi* (mencegat atau mengambil data yang sedang dikirimkan melalui suatu jalur komunikasi tanpa seizin pengirim atau penerima) • Mengimplementasikan sistem pemanatauan jaringan secara *real-time* untuk mendeteksi serangan, seperti DDoS • Gunakan alat seperti IDS/IPS (*Intrusion Detection/Prevention Systems*) untuk melindungi jaringan.
		Fisik	• Klausul 7.3 Kesadaran • A 7.3 Mengamankan kantor, ruangan, dan fasilitas • A 7.4 Pemantaua keamanan fisik • A 7.5 Melindungi dari ancaman fisik dan lingkungan	• Pasang CCTV di area akses fisik ke perangkat kritis (misalnya, ruang server) dan pastikan berfungsi dengan baik • Lakukan pemantauan akses fisik secara teratur untuk mendeteksi aktivitas mencurigakan • Selalu berikan akses perangkat keras jaringan hanya kepada staff yang berwenang

No	Aset	Jalur akses	Klausul dan pengendalian berdasarkan ISO 27001:2022	Rekomendasi mitigasi
				• Lindungi perangkat keras dari risiko lingkungan seperti kelembapan dan panas • Buat dan perbarui secara berkala kebijakan perangkat keras secara berkala untuk mencegah kerusakan.
		Masalah sistem	• Klausul 8.1 Perencanaan dan pengontrolan operasional • A 8.8 Manajemen kerentanan teknis • A 8.16 Pemonitoran aktivitas • A 8.15 Membuat log • A 8.13 Informasi cadangan	• Lakukan pembaruan perangkat lunak secara rutin untuk mengurangi kerentanan • Lakukan analisis kerentanan secara berkala untuk mendeteksi dan memperbaiki celah keamanan • terapkan alat pemantauan log untuk mencatat dan menganalisis kesalahan sistem • buat laporan insiden dan gunakan temuan untuk meningkatkan keamanan sistem • dokumentasikan semua kesalahan sistem, termasuk langkah-langkah yang diambil untuk memperbaiki masalah dan pastikan pencatatan kesalahan mudah diakses oleh staf • cadangkan data dan simpan di lokasi yang aman, baik secara fisik maupun *cloud*
3.	SDM, Divisi infrastruktur, jaringan & keamanan	Ancaman dari pihak ketiga	• klausul 7.4 Komunikasi • A 5.30 Kesiapan TIK untuk keberlangsungan bisnis	• Menyediakan alternatif penyedia layanan internet atau listrik untuk menghindari ketergantungan pada satu pihak

No	Aset	Jalur akses	Klausul dan pengendalian berdasarkan ISO 27001:2022	Rekomendasi mitigasi
				• Memastikan bahwa ada langkah-langkah yang jelas dan rencana pemulihan yang dapat diterapkan ketika layanan pihak ketiga terganggu
4.	SIAK	Jaringan	• Klausul 7.3 Kesadaran • A 6.3 Kesadaran keamanan informasi, pendidikan dan pelatihan • Klausul 9.1 Pemonitoran, pengukuran, analisis, dan evaluasi • A 5.15 Kontrol akses • A 5.18 Hak akses • A 8.3 Informasi pembatasan akses	• Implementasikan kebijakan pengendalian akses yang ketat, termasuk pembatasan akses fisik ke perangkat jaringan. • Lakukan pelatihan keamanan untuk pegawai internal tentang pentingnya keamanan data dan mengurangi kesalahan manusia. • Implementasikan pemantauan terhadap akses jaringan untuk mendeteksi aktivitas mencurigakan.
		Fisik	• Klausul 6.1 Tindakan untuk menangani risiko dan peluang • A 5.15 Kontrol akses • A 7.5 Melindungi dari ancaman fisik dan lingkungan • A 5.37 Prosedur operasional yang terdokumentasi	• Untuk aktor internal; Batasi akses fisik ke perangkat keras, server, dan data sensitif hanya kepada personel yang membutuhkan akses untuk menjalankan tugas mereka • Untuk aktor internal; Implementasikan prosedur keluar dan masuk yang ketat (misalnya, log pengunjung dan penggunaan akses yang tercatat) untuk meminimalkan risiko penyalahgunaan oleh aktor internal yang tidak puas atau memiliki motivasi pribadi.

No	Aset	Jalur akses	Klausul dan pengendalian berdasarkan ISO 27001:2022	Rekomendasi mitigasi
				• Untuk aktor internal; Lakukan audit dan pemantauan terhadap akses fisik secara rutin untuk mendeteksi adanya aktivitas mencurigakan • Untuk aktor eksternal; Batasi akses fisik dari pihak eksternal ke lokasi perangkat keras dan data sensitif dengan menggunakan pengawasan ketat (misalnya, menggunakan petugas keamanan dan kontrol akses yang ketat) • Pastikan hanya vendor yang terverifikasi dan tamu yang memerlukan akses dapat memasuki area yang dilindungi. • Pastikan bahwa semua perangkat yang digunakan oleh pihak eksternal telah dipindai dan aman sebelum dihubungkan dengan jaringan internal • Pastikan bahwa perangkat yang rusak atau tidak terpakai dimusnahkan dengan aman, dan pastikan bahwa data yang ada dalam perangkat tersebut dihapus dengan benar
		Masalah sistem	• Klausul 6.1 Penilaian dan perlakukan terhadap risiko • A 5.30 Kesiapan TIK untuk kelangsungan bisnis • A 8.7 Perlindungan terhadap *malware*	• Lakukan uji ketahanan sistem secara berkala, terutama saat periode pendaftaran KRS dan pengumuman nilai • Implementasikan solusi *load balancing* untuk menangani lonjakan beban

No	Aset	Jalur akses	Klausul dan pengendalian berdasarkan ISO 27001:2022	Rekomendasi mitigasi
				• Siapkan rencana pemulihan bencana yang mencakup prosedur cadangan dan pemulihan otomatis untuk memastikan ketersediaan sistem • Implementasikan kebijakan pemeliharaan perangkat keras yang mencakup pemeriksaan berkala dan penggantian perangkat keras yang sudah usang • Miliki cadangan perangkat keras untuk meminimalkan dampak kerusakan perangkat keras yang tidak terduga • Lakukan pembaruan sistem secara berkala untuk mengurangi kerentanannya • Terapkan prosedur *backup* data secara berkala untuk menghidari kehilangan data akhibat *malware*
5.	SOP dan Instruksi Kerja	Jaringan	• Klausul 8.3 Penanganan risiko keamanan informasi • A 5.15 Kontrol akses • A 5.14 Transfer informasi • A 6.3 Kesadaran keamanan informasi, pendidikan dan pelatihan	• Buat prosedur standar untuk pemeliharaan dan pembaruan sistem yang menyimpan SOP dan IK • Gunakan enkripsi data untuk melindungi SOP dan IK selama proses transmisi melalui jaringan • Lakukan pelatihan kepada staf internal untuk meminimalkan kesalahan operasional dan meningkatkan kesadaran risiko
		Fisik	• Klausul 7.2 Kompetensi • A 5.13 Pelabelan Informasi • A 7.2 Masuk secara fisik	• Pastikan lemari penyimpanan dokumen memiliki pengamanan tambahan, seperti kunci kombinasi atau biometrik

No	Aset	Jalur akses	Klausul dan pengendalian berdasarkan ISO 27001:2022	Rekomendasi mitigasi
			• A 7.10 Media penyimpanan	• Scan dan arsipkan SOP dan IK dalam bentuk digital dengan perlindungan akses berbasis jaringan • Tingkatkan frekuensi pengecekan fisik dari sebulan sekali menjadi dua minggu sekali untuk memastikan dokumen dalam kondisi aman • Berikan label unik pada dokumen SOP dan IK untuk memudahkan pelacakan dan identifikasi • Lakukan pelatihan untuk staf agar memahami pentingnya keamanan dokumen fisik dan prosedur pelaporan jika terjadi kehilangan

Lmpiran 19. Referensi Dokumen ISO 27001:2022

Referensi dokumen mandatory ISO 27001:2022 dapat diakses pada link berikut: **https://drive.google.com/drive/folders/1C4WE7KkaW9hn6AOdZfiOZZvOGigYfnoY?usp=drive_link**

1. **Dokumen Komitmen Keamanan Informasi/ISMS Guideline**

   Dokumen Komitmen Keamanan Informasi/ISMS Guideline digunakan untuk mengcover / dijadikan sebagai evidence pemenuhan klausa ISO 27001 (clause 4 – clause 10).

   Contoh isi dari dokumen komitmen keamanan informasi adalah sebagai berikut.

   Bagian depan

   1) Judul dokumen
   2) Nomor dokumen
   3) Tanggal efektif berlaku dokumen
   4) Versi dokumen
   5) Pengesahan dokumen

   Bab I Masalah dan Harapan Pihak-pihak yang Berkepentingan

   1) Masalah internal dan eksternal (internal & external issues)
   2) Kebutuhan dan harapan pihak-pihak yang berkepentingan

   Bab II Cakupan, Antarmuka dan Dependensi

   1) Ruang lingkup implementasi ISO 27001
   2) Interface & Dependencies

   Bab III Roles & Responsibilities

   Bab IV Tujuan keamanan

   Bab V Sumber daya dan kompetensi

   1) Sumberdaya
   2) kompetensi

   Bab VI Awareness dan Komunikasi

   1) Awareness
   2) Komunikasi

   Bab VII Evaluasi Kinerja

   1) Pemantauan, Pengukuran, Analisis dan Evaluasi
   2) Audit internal ISO 27001

3) Tinjauan Management

Bab VIII Perbaikan (Ketidaksesuaian dan tindakan korektif)

Lampiran

2. Dokumen Statement of Applicability

Dokumen SoA (Statement of Applicability) merupakan kumpulan dari beberapa kontrol yang terdapat pada bagian Annex yang diterapkan dan yang tidak akan diterapkan dalam rangka menerapkan risk treatment. Untuk mengetahui kontrol mana saja yg dapat diterapkan dan yg tidak dapat diterapkan, diperlukan analisa mendalam mengenai kesesuaian antara lain bisnis proses, kontrol yg terdapat dibagian Annex dan ruang lingkup sertifikasi.

Seluruh aktivitas analisa tiap klausul harus dituangkan ke dalam bentuk dokumen yang akan menampilkan kontrol-kontrol apa saja yang dapat diterapkan/tidak diterapkan, beserta penjelasan singkat mengenai kontrol tersebut di dalam sistem. Dokumen SoA merupakan salah satu dokumen yang wajib tersedia dalam rangka pemenuhan sertifikasi ISO/IEC 27001, dimana jika tidak ditemukannya dokumen ini dapat berdampak terhadap proses pengurusan sertifikasi.

3. Risk Register

Dokumen ini berisi list risiko yang teridentifikasi pada ruang lingkup implementasi ISO 27001. Selain itu juga berisi identifikasi resiko, analisis resiko, tipe resiko, evaluasi resiko, penanganan risiko danpemantauan resiko.

4. Asset register

Dokumen asset register berisi list aset yang terkait dengan ruang lingkup implementasi ISO 27001 berisi primary asset dan supporting asset. Aset yang dimaksud oleh ISO 27001 adalah segala sesuatu yang memiliki nilai bagi perusahaan, dapat berupa barang fisik, perangkat keras (hardware), perangkat lunak (software), informasi, orang/personel/karyawan.

5. Nondisclosure Agreement (NDA)

Dokumen NDA bisa diartikan sebagai perjanjian kerahasiaan. Dikutip dari laman Institute of Compliance Professional Indonesia (ICoPI), Non-Disclosure Agreement merupakan perjanjian yang digunakan untuk menjaga informasi yang bersifat rahasia. NDA sendiri memiliki fungsi yang penting diantaranya:

a. Melindungi informasi sensitive

Orang yang menandatangani NDA, baik itu karyawan maupun partner perusahaan, menunjukkan bahwa mereka sudah menyetujui ketentuan yang ada di dalam perjanjian tersebut. Jika melanggar perjanjian tersebut, pihak yang dirugikan bisa saja membawa permasalahan tersebut ke jalur hukum.

b. Menjaga hak paten

Jika semua orang menaati NDA yang telah ditandatangani, besar kemungkinan orang yang membuat produk tersebut mendapatkan hak patennya.

c. Memberi batasan yang jelas

Di dalam NDA, terdapat penjelasan mengenai informasi apa yang sifatnya rahasia, dan apa yang masih bisa dibicarakan seperti biasa. Dengan begitu, orang yang menandatangani perjanjian kerahasiaan tersebut bisa benar-benar tahu apa yang bisa dibicarakan dan apa yang harus dirahasiakan dari siapa pun itu.

6. Bukti kemampuan/kompetensi

Organisasi sebaiknya menentukan kompetensi yang dibutuhkan bagi penanggung jawab yang melakukan aktivitas terkait SMKI dan kontrol keamanan yang dapat mempengaruhi smki. Dokumen ini berisikan pelatihan sebelumnya, serta jika memungkinkan tindakan yang dilakukan untuk memperoleh kompetensi yang diperlukan untuk evaluasi keefektifan tindakan yang diambil.

7. Risk Assessment dan proses penilaian resiko

Dokumen ini digunakan untuk menentukan metodologi penilaian dan pengelolaan risiko informasi pada organisasi dan untuk menentukan tingkat resiko yang dapat diterima sesuai dengan standar ISO 27001. Dokumen ini berisikan:

Cover:

1) Logo organisasi
2) Judul dokumen
3) Kode dokumen
4) Versi dokumen

5) Tanggal pembuatan dokumen
6) Tingkat kerahasiaan
7) Tanda tangan pihak-pihak berkepentingan

Isi:

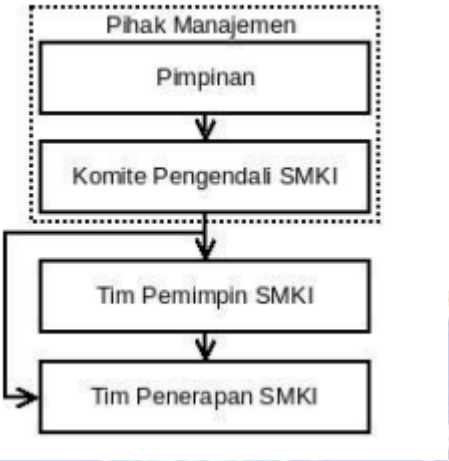
1) Tujuan
2) Ruang lingkup
3) Pengguna
4) Referensi
5) Penilaian resiko dan metodologi pengelolaan risiko
6) Dokumen penunjang dan penyimpanan dokumen
7) Status perubahan
8) Lampiran

8. Rencana perawatan resiko

Dokumen ini berisikan pemilihan penanganan risiko yang tepat yang mengacu terhadap hasil penilaian resiko. Dokumen ini berisi tujuan, ruang lingkup, komunikasi dan konsultasi, pengawasan dan peninjauan dan laporan proses penanganan risiko.

Lampiran 20. Struktur Tim SMKI

Tim pengelola SMKI tugas utamanya adalah menyiapkan, menjamin dan/atau melakukan seluruh kegiatan dalam tahapan penerapan SMKI agar dapat terlaksana dengan baik sesuai rencana. Berikut adalah struktur Tim Pengelola SMKI.



Rincian gambar struktur tim pengelola SMKI

A. Pimpinan (*top management*)

Pimpinan adalah orang atau kelompok orang yang memimpin dan mengontrol organisasi di tingkat tertinggi organisasi. Pimpinan bertanggung jawab terhadap visi, keputusan strategis dan mengkoordinasikan aktivitas untuk memimpin dan mengontrol organisasi. Pimpinan dapat termasuk *Chief Executive Officer (CEO), Chief Operating Officer (coo), president* (ketua/direktur/rector) atau yang serupa. Berikut ini adalah peran dan tanggung jawab pimpinan terhadap SMKI:

1. Memastikan kebijakan dan sasaran keamanan informasi telah ditetapkan dan sesuai dengan arah strategis organisasi.
2. Memastikan integrasi persyaratan SMKI kedalam proses organisasi.
3. Memastikan tersedianya sumber daya yang dibutuhkan untuk SMKI.
4. Mengkomunikasikan pentingnya patuh terhadap persyaratan SMKI dan manajemen keamanan informasi yang efektif.

5. Mengarahkan dan mendukung pemangku kepentingan untuk berkontribusi dalam keefektifan SMKI.
6. Memastikan SMKI mencapai hasil yang diharapkan dan memajukan peningkatan berkelanjutan.
7. Mendukung peran pihak manajemen terkait lainnya untuk menunjukkan kepemimpinannya yang termasuk area tanggung jawab mereka.

B. Komite pengendali SMKI (*ISMS steering committee*)

Komite pengendali SMKI berperan memimpin SMKI dan menangani aset informasi di organisasi. Komite ini merupakan landasan untuk mendiskusikan persoalan apapun yang berhubungan dengan SMKI dan keamanan informasi secara umum. Komite pengendali SMKI idealnya dapat terdiri dari:

- Chairman/ketua: bertanggung jawab untuk memastikan sasaran SMKI sejalan dengan sasaran strategis organisasi. Ketua sebaiknya ditetapkan dari jajaran manajemen atas. Contohnya jika Chief Information Security Officer (CISO) ditetapkan sebagai ketua, idealnya CISO sebaiknya berada di manajemen atas dan melaporkan secara langsung kepada CEO organisasi
- Line manager (contohnya kepala unit organisasi): bertanggung jawab terhadap setiap unit dan operasional bisnis, serta memastikan hasil dari aktivitas penilaian risiko menyatu dalam setiap aktivitas operasional.
- Pemilik aset dan/atau proses: bertanggung jawab untuk memastikan kontrol yang tepat diterapkan dan setiap aset terlindungi.

Berikut ini contoh peran dan tanggung jawab komite pengendali SMKI terhadap SMKI:

1. Memastikan kesesuaian penerapan kebijakan dan sasaran keamanan informasi.
2. Melaksanakan tinjauan manajemen.

3. Memastikan peningkatan berkelanjutan dilakukan dengan segera tanpa penundaan.
4. Memastikan kecukupan langkah yang diambil secara teratur untuk meningkatkan keamanan informasi pada organisasi.
5. Menyediakan arahan yang jelas pada strategi SMKI organisasi dalam mengelola keamanan informasi.
6. Memperlihatkan komitmen dalam mendukung pimpinan untuk mencapai sasaran strategis organisasi.

C. Tim pemimpin SMKI (*ISMS lend team*)

Tim pemimpin SMKI sebaiknya yang memiliki pengetahuan yang dalam dan/atau berpengalaman dalam keamanan informasi, memahami SMKI secara luas baik penerapan SMKI dan pengelolaan risiko keamanan informasi. Berikut ini adalah peran dan tanggung jawab tim pemimpin SMKI:

1. Merencanakan, menggerakkan, dan mengatur aktivitas yang berhubungan dengan SMKI.
2. Mengelola risiko keamanan informasi secara berkala.
3. Mengkoordinasi aktivitas secara umum yang berhubungan dengan SMKI, komite pengendali SMKI dan program keamanan informasi lainnya dalam organisasi.

D. Tim penerapan SMKI (*ISMS implementation team*)

Tim penerapan SMKI adalah yang bertanggung jawab untuk melakukan aktifitas SMKI yang direncanakan oleh tim pemimpin SMKI. Bergantung dari ruang lingkup SMKI dan struktur organisasi, tim penerapan SMKI dapat terdiri dari karyawan dari departemen/divisi seperti:

- Pihak manajemen resiko: bertanggung jawab terhadap standar atau kerangka kerja manajemen risiko organisasi.
- Bagian *human resource*: bertanggung jawab secara keseluruhan terhadap karyawan di organisasi, termasuk persyaratan perekrutan, pemberhentian, dan pelatihan bagi karyawan.

- Bagian TIK: bertanggung jawab terhadap keamanan sistem TIK organisasi, dan seluruh sumber daya TIK yang dibutuhkan untuk penerapan SMKI.
- Bagian keuangan dan akuntansi: bertanggung jawab terhadap manajemen anggaran belanja secara keseluruhan dalam penerapan SMKI.
- Bagian administrasi bangunan dan fasilitas: bertanggung jawab terhadap keamanan fisik dan administrasi umum tempat fisik organisasi.
- Auditor: bertanggung jawab dalam pelaksanaan audit SMKI. Pemimpin tim auditor yang bertanggung jawab dalam perencanaan program audit SMKI.

Lampiran 21. Dokumentasi

RIWAYAT HIDUP PENULIS

Hardiyanti Rohmania lahir di Batumarta pada tanggal 26 juni 2002. Penulis lahir dari pasangan suami istri Bapak M Ridwan dan Ibu Musrifah. Penulis berkebangsaan Indonesia dan beragama Islam. Kini penulis beralamat di Desa Batumarta VI, Kecamatan Madang Suku III, Kabupaten Ogan Komering Ulu Timur (OKU Timur), Provinsi Sumatera Selatan. Penulis menyelesaikan Pendidikan Dasar di SD Negeri 2 Batumarta VI pada tahun 2014. Kemudian penulis melanjutkan sekolah menengah di SMP Negeri 1 Madang Suku III dan lulus pada tahun 2017. Pada tahun 2020, penulis lulus dari SMA Negeri 1 Madang Suku III Jurusan Matematika dan Ilmu Pengetahuan Alam (MIPA) dan melanjutkan ke Sarjana Program Studi Sistem Informasi di Universitas Pendidikan Ganesha. Pada semester akhir tahun 2025 penulis telah menyelesaikan Skripsi yang berjudul **"*ANALISIS MANAJEMEN RISIKO KEAMANAN INFORMASI MENGGUNAKAN FRAMEWORK OCTAVE-S DAN ISO 27001:2022.*"**