PEDOMAN MANAJEMEN RISIKO LAYANAN BERBASIS TEKNOLOGI INFORMASI

PENYELENGGARAAN SISTEM MANAJEMEN ATAS LAYANAN "APLIKASI REGISTRASI MATA KULIAH"

INSTITUT TEKNOLOGI TELKOM PURWOKERTO
Jl. DI Pandjaitan No 128
Purwokerto, 53147
Tel: +62-281 641629
Fax: +62-218 641630
Website: https://ittelkom-pwt.ac.id

No. : ITTel7254/IS-000/REK-02/IX/2022
Rev.00
Tgl Efektif: September 2022

DISUSUN OLEH	DISUSUN OLEH	DIAJUKAN OLEH:	DISETUJUI OLEH:
Hanu Handriadma.S.T.,M.T	Yudha Saintika, MTI	Tata Sambada, MBA	Dr. Arfianto Fahmi, MT., IPM
STAFF INTERNAL AUDIT	**UNIT IT SUPPORT**	**MANAGEMENT REPRESENTATIVE**	**REKTOR**

Internal Use Only

DAFTAR ISI

1 RUANG LINGKUP DAN TUJUAN KERANGKA MANAJEMEN RISIKO

1.1 Ruang Lingkup

Dokumen ini menguraikan manajemen risiko untuk aktivitas yang dilaksanakan di tim ITSUPPORT Institut Teknologi Telkom Purwokerto dalam aspek sistem manajemen layanan teknologi informasi . Dokumen ini menjelaskan bagaimana proses manajemen risiko yang dijalankan, metodologi yang digunakan, mekanisme pelaporan yang diterapkan, hingga penetapan tanggungjawab dalam implementasi manajemen risiko keamanan informasi. Manajemen risiko teknologi informasi merupakan bagian dari operasional ITTP yang dikendalikan oleh unit ITSUPPORT ITTP. Dokumen manajemen risiko disusun oleh Satuan Penjamin Mutu (SPM) ITTP yang bekerjasama dengan unit ITSUPPORT ITTP.

Pedoman manajemen risiko teknologi informasi disusun dan telah disesuaikan dengan kondisi internal dan eksternal unit ITSUPPORT ITTP. Pedoman manajemen risiko memberikan pendekatan yang melekat pada unit ITSUPPORT ITTP untuk mengelola semua risiko relevan yang akan ditetapkan, dinilai, diperlakukan dan dilaporkan sesuai cakupan kepemilikan risiko. Penerapan manajemen risiko oleh unit kerja dalam struktur organisasi dan tata kerja ITTP disesuaikan dengan kebutuhan spesifik, serta situasi yang terjadi pada masing-masing unit di dalam ITTP. Pelaksanaan monitoring manajemen risiko dilaksanakan oleh Satuan Penjamin Mutu dan Satuan Audit Internal melalui proses top-down (university wide) maupun bottom-up yang merupakan hasil assessment dari satuan kerja terkait. Adapun ruang lingkup risiko yang terdapat pada unit ITSUPPORT ITTP yaitu Information,People,Software,Physical, Service dan Intagible.

1.2 Tujuan Kerangka Manajemen Risiko

Tujuan dari manajemen risiko teknologi informasi Institut Teknologi Telkom Purwokerto untuk menyediakan proses formal yang diperlukan organisasi guna membantu manajemen institusi dalam aspek :

1. Mendorong pemahaman pimpinan satuan kerja beserta seluruh staf mengenai implikasi dampak dari risiko, opportunities dan manajemen risiko dalam menjalankan tupoksinya sehari-hari maupun dalam menjalankan kegiatan perencanaan operasional.
2. Mengembangkan dan menerapkan prosedur untuk memastikan bahwa proses manajemen risiko diidentifikasi serta dijalankan, dan memastikan bahwa langkah- langkah yang tepat telah diimplementasikan.
3. Mendokumentasikan tanggung jawab dan proses yang harus dijalankan.

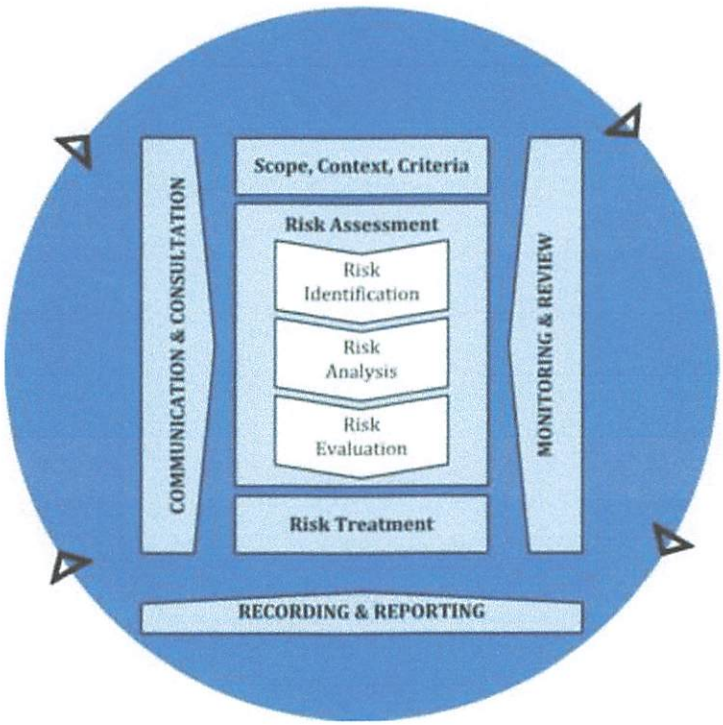
2. KERANGKA MANAJEMEN RISIKO LAYANAN TEKNOLOGI INFORMASI

2.1 Manajemen Risiko

Dalam kerangkan manajemen risiko Institut Teknologi Telkom Purwokerto, risiko didefiniskan sebagai peristiwa yang dapat memiliki dampak pada upaya pencapaian tujuan organisasi.Risiko dapat muncul faktor eksternal (seperti perubahan peraturan pemerintah, perubahan karakteristik demografi mahasiswa dan krisis ekonomi) maupun faktor internal (seperti pembukaan program studi baru, tantangan dalam penyediaan infrastruktur,penyediaan sumber daya manusia yang memadai dan lain-lain.

2.2 Kerangka dan Proses Manajemen Risiko Layanan Teknologi Informasi

Bentuk Kerangka Manajemen Risiko Teknologi Informasi di Institut teknologi Telkom Purwokerto berbasis pada ISO 31000: 2018.



Gambar 1 Kerangka Manajemen Risiko ISO 31000:2018

2.2.1 Komunikasi dan Konsultasi (Communication & Consultation)

Komunikasi dan konsultasi dengan unit ITSUPPORT dan manajemen representative untuk memastikan pemahaman tentang proses manajemen risiko teknologi informasi dan dilakukan tim manajemen risiko yang dibentuk dari tim satuan penjaminan mutu dan Sekpim,legal dan Internal Audit Institut Teknologi Telkom Purwokerto. Sekertaris pimpinan dan Internal Audit memfasilitasi operational review terhadap manajemen risiko teknologi informasi.

2.2.2 Menetapkan Ruang Lingkup, Konteks dan Kriteria (Scope, Context, Criteria)

Manajemen risiko dilakukan dalam upaya mencapai tujuan dan sasaran ITTP. Oleh karena itu, manajemen risiko harus ditempatkan dalam konteks strategik maupun operasional. Beberapa isu penting yang harus dipertimbangan dalam mengevaluasi strategic content, di antaranya adalah :

- Peluang dan ancaman yang berhubungan dengan lingkungan lokal, regional, global, sosial, politik, kultural, kebijakan dan kompetisi.
- Kekuatan dan kelemahan ITTP dalam rangka mencapai tujuan.

Berkaitan dengan operational context, identifikasi risiko melibatkan pemahaman terhadap kemampuan organisasi, tujuan, sasaran, kekuatan dan kelemahan dengan mempertimbangankan aspek :

- Struktur organisasi dan budaya organisasi
- Geografi dan demografi
- Keberadaan hambatan operasional.
- Tujuan dan KPI
- Isu terkait dengan manajemen perubahan atau audit reviews
- Kewajiban regulasi dan hambatan regulasi
- Sistem manajemen yang dijalankan Institut Teknologi Telkom Purwokerto.

2.2.3 Identifikasi Risiko (Risk Identification)

Identifikasi risiko merupakan langkah dalam konteks strategik dan operasional. Risiko dapat diidentifikasi melalui langkah berikut :

- Focus group discussion (*brainstorming approaches, SWOT analysis techniques dan project categories*).
- Workshops.
- Pengalaman organisasi lain.

- Interview dengan pihak ITSUPPORT.

Dari hasil identifikasi risiko maka akan menghasilkan *risk registers* yang dikategorikan sesuai dengan tabel 1 Kategori Risiko. Terdapat 6 kategori risiko yang melekat pada unit ITSUPPORT ITTP. Berikut Penjelasan dari masing-maing 6 Kategori risiko.

Tabel 1 Penjelasan Kategori Risiko

No	Kategori Risiko	Penjelasan
1	Information	Terkait pesan atau data yang mengalir di dalam sistem.
2	People	Terkait orang yang melaksanakan dan menjalankan sistem baik karyawan maupun outsourching
3	Software	Terkait Perangkat Lunak yang digunakan dalam sistem
4	Physical	Terkait Perangkat Fisik yang digunakan dalam sistem seperti komputer, jaringan, dsb
5	Service	Terkait layanan yang disediakan dan pelaksanaannya
6	Intagible	Terkait Reputasi Organisasi.

Berikut kategori risiko layanan teknologi informasi yang ditetapkan dalam mengkategorikan risk registers. Sub Kategori ditentukan berdasarkan hal-hal yang melekat pada masing-masing kategori risiko.Berikut tabel 2 mengenai sub kategori risiko.

Tabel 2 Sub kategori Risiko

No	Kategori Risiko	Sub Kategori
1	Information	Database & data files
		Data Log & Audit
		Contract/Legal Documents
		Bussiness Process/Procedure
2	People	Pelaksana Teknis
		Pelaksana Non Teknis
		Tenaga Outsource
3	Software	Bussiness Aplication
		Database Engine
		Operating System
		System Utility
4	Physical	Server
		Network Devices
		Storage
		Laptop/Desktop
		Support Facility
5	Service	Data Communication Services
		Maintainance & Support Service
		Outsource Service

6	Intangible	Reputasi Organisasi

2.2.4 Analisa Risiko dan Evaluasi Risiko (Risk Analysis & Risk Evaluation)

Setelah Menentukan Risk Registers kemudian tim manajemen risiko akan melakukan analisis dan evaluasi. Analisis Risiko menggunakan metode dengan memperhatikan Likelihood (Kemungkinan) dan Impact(Dampak) dari semua risk registers. Kemudian di evaluasi dengan memperhatikan nilai risiko yang di dapatkan dari nilai *likehood*(Kemungkinan Risiko*)* dan *impact*(Dampak Risiko).

- Kriteria Likelihood

  Likelihood atau Frekuensi Kejadian adalah tingkat kemungkinan sebuah risiko terjadi- berapa sering,dibandingkan pada seluruh aktivitas dan/atau periode waktu tertentu,berdasarkan pengalaman historis dan/atau kemungkinan di masa depan.

Tabel 3 Kriteria Likelihood

Bobot	Skala	Kemungkinan
1	Sangat Rendah	Hampir Tidak mungkin terjadi (Rare)
2	Rendah	Kadang Terjadi(Unlikely)
3	Sedang	Mungkin tidak Terjadi(Moderate)
4	Tinggi	Sangat Mungkin Terjadi(Likely)
5	Sangat Tinggi	Hampir Pasti Terjadi(Almost Certain)

- Kriteria Impact

  Impact atau dampak adalah tingkat kerugian dan atau potensi kerugian/kerusakan yang terjadi, dari suatu kejadian/event, berdasarkan pengalaman historis dan/atau kemungkinan di masa depan.

Tabel 4. Kriteria Impact

Bobot	Skala	Kemungkinan
1	Sangat Rendah	Tidak Berpengaruh Signifikan(Insignificant)
2	Rendah	Minor
3	Sedang	Moderate
4	Tinggi	Berpengaruh(High)
5	Sangat Tinggi	Sangat Berpengaruh(Very High)

- Peta Risiko

  Peta Risiko merupakan Representasi grafis dari kejadian risiko atas dasar tingkatan Impact dan Likelihood/Probability dalam unit ITSUPPORT. Peta risiko terlampir pada tabel 5 tentang peta risiko.

IMPACT/DAMPAK							
	Very High/5	Sangat Tinggi	MEDIUM-5	MEDIUM-10	MEDIUM-15	HIGH-20	HIGH-25
	High/4	Tinggi	LOW-1	MINOR - 8	MEDIUM-12	HIGH-16	HIGH-20
	Moderate/3	Sedang	LOW-1	MINOR- 6	MINOR- 9	MEDIUM-12	MEDIUM-15
	Minor/2	Rendah	LOW-1	LOW-4	MINOR-6	MINOR-8	MEDIUM-10
	Insignificat 1	Sangat Rendah	LOW-1	LOW-2	LOW-3	LOW-4	MEDIUM-5
			Sangat Rendah	Rendah	Sedang	Tinggi	Sangat Tinggi
			RARE/1	UNLIKELY/2	MODERATE/3	LIKELY/4	ALMOST CERTAIN/5
			LIKELIHOOD/KEMUNGKINAN/PROBABILITAS				

Tabel 5 Peta Risiko

- Pengukuran Risiko
  Untuk mendapakan nilai Risiko didapatkan dengn formula sebagai berikut

$$Likelihood(Kemungkinan) x\ Impact(Dampak) = Nilai\ Risiko$$

Contoh tabel identifikasi risiko :

Risk No	Identifikasi Resiko			Nilai Risiko			
	Sub Kategori Risiko	Kemungkinan	Dampak	Kemungkinan	Dampak	Nilai Risiko	Status
PHY-01	Server	Kebakaran	Kehilangan perangkat akibat kebakaran	4	5	20	

2.2.5 Penanganan Risiko (Risk Threatment)

Penanganan risiko ini digunakan untuk pengambilan keputusan terkait risiko yang sudah di nilai. Apakah Avoid Risk, Accept Risk, Mitigate Risk dan Transfer Risk. Penjelasan masing- masing penanganan terdapat pada tabel 6 tentang penanganan Risiko.

Tabel 6 . Penanganan Risiko

Penanganan Risiko	Deskripsi
Avoid Risk	Tindakan pengendalian risik dengan tidak melakukan aktivitas atau memilih aktivitas lain dengan hasil (output) yang sama untuk menghindari risiko.
Accept Risk	Tindakan pengendalian risiko dengan menerima dampak dan kemungkinan terjadinya risiko
Mitigate Risk	Tindakan pengendalian risiko dengan mengurangi dampak atau kemungkinan terjadinya risiko melalui penerapan sistem, aturan atau program
Transfer Risk	Tindakan pengendalian risiko dengan mengalihkan seluruh atau sebagian tanggungjawab pelaksanaan suatu proses kepada pihak ketiga

Contoh tabel risk threatment

Risk Treatment(Penanganan Risiko)				
Rencana	**Tindakan**	**Penanganan Risiko**	**Pemilik Risiko**	**Diselesaikan Oleh**
Merencanakan pemasangan Fire extinguisher, smoke detector, fire supression pada ruang data center.	Pemasangan dan monitoring Fire extinguisher, smoke detector, fire supression pada ruang data center.	Mitigate Risk	ITSUPPORT(Data Center	Yudha Saintika

2.2.6 Monitoring dan Review

Monitoring dan review dari implementasi manajemen risiko dilakukan melalui proses audit internal yang dilaksanakan oleh satuan penjaminan mutu dan satuan audit internal karena termasuk dalam PIC Manajemen Risiko.

Tabel 7. Penanggung Jawab Monitoring Manajemen Risiko

No	Unit	Tanggung Jawab
1.	Unit Penjaminan Mutu	a. Memegang penuh tanggungjawab terhadap proses manajemen risiko di universitas.

		b. Bertanggung Jawab untuk menentukan tingkat risiko yang siap terima berdasarkan isu yang dihadapi c. Bertanggungjawab untuk patuh pada peraturan perundangan yang berlaku dalam rangka mengkoordinasikan proses.
2.	Wakil Rektor 1,2,3	a. Bertanggungjawab dalam konteks kepemimpinan dalam implementasi manajemen risiko. b. Mengawasi praktik manajemen risiko.
3.	PIC Manajemen Risiko	a. Bertanggungjawab untuk mengelola proses identifikasi dan monitoring risiko. b. Mengelola Risk Register. c. Melaksanakan *risk management framework.* d. Memberikan masukan tentang alat yang dapat digunakan untuk membantuk implementasi manajemen risiko.
4.	Risk Owner	a. Memonitor status risiko di unit kerjanya, b. Memberikan masukan tentang respon yang tepat pada risiko maupun control yang harus ditetapkan. c. Mengkonfirmasi bahwa control telah diterapkan.

3 PENUTUP

Pedoman manajemen risiko layanan teknologi informasi institut teknologi telkom purwokero ini mulai berlaku sejak tanggal ditetapkan. Pedoman ini dapat direview dan dimutakhirkan secara berkala untuk dilihat kesesuaiannya dan apabila diperlukan maka akan dilakukan perubahan dan/atau penyempurnaan guna menjamin keselarasan dengan praktik-praktik terbaik di bidang manajemen risiko, audit internal, perubahan lingkungan organisasi, dan perkembangan praktik-praktik penyelenggaraan tugas dan fungsi unit ITSUPPORT. Pedoman manajemen risiko ini dapat dijadikan dasar bagi Pimpinan institusi untuk mengevaluasi kegiatan strategis Institut Teknologi Telkom Purwokerto. Seluruh Program Studi dan Unit dihimbau untuk menyusun, mengontrol dan mengevaluasi manajemen risiko layanan teknologi informasi.

4 RISK REGISTERS

INFORMATION			
No	**Sub Kategori Risiko**	**Risiko**	**Dampak**
1.	Database & data files	Penyingkapan informasi kepada pihak yang tidak berwenang	Ketiadaan Kebijakan Keamanan Informasi
2.	Database & data files	Perubahan/penghilangan Informasi/data secara tidak sah	Ketiadaan Kebijakan Keamanan Informasi
3.	Database & data files	Penyingkapan informasi kepada pihak yang tidak berwenang	Ketidaksempurnaan penerapan Kebijakan Keamanan Informasi di lingkungan ITTP
4.	Database & data files	Perubahan/penghilangan Informasi/data secara tidak sah	Ketidaksempurnaan penerapan Kebijakan Keamanan Informasi di lingkungan organisasi
5.	Database & data files	Ketidakpahaman pegawai akan pentingnya keamanan informasi	Ketidakcukupan perjanjian kerahasiaan
6.	Database & data files	Kedatangan pihak ketiga ke area Data Center	Ketidakcukupan perjanjian kerahasiaan
7.	Database & data files	Information/data sniffing	Kurangnya pengamanan pada sistem/network customer yang terhubung ke network organisasi
8.	Database & data files	Data tapping oleh pihak ketiga	Ketidaksempurnaan kontrol keamanan informasi terhadap pihak ketiga
9.	Database & data files	Ketidakjelasan siapa yang bertanggung jawab utama atas ancaman keamanan informasi terhadap aset	Ketidakjelasan kepemilikan aset
10.	Database & data files	Banyaknya jumlah informasi yang dikelola oleh organisasi	Bercampurnya informasi rahasia dengan informasi lainnya
11.	Database & data files	Banyaknya jumlah informasi yang dikelola oleh organisasi	Ketidakjelasan penanganan informasi rahasia
12.	Database & data files	Pemrosesan informasi yang tidak sah	Informasi masih bisa diakses oleh pegawai yang sudah tidak bekerja di ITTP (pensiun / mutasi / mengundurkan diri)
13.	Database & data files	Kehilangan / pencurian informasi/data	Ketidaksempurnaan terhadap proteksi perangkat penyimpan informasi saat dibawa keluar data center
14.	Database & data files	Kehilangan / pencurian informasi/data	Ketidaksempurnaan aturan penggunaan ulang media

15.	Database & data files	Kesalahan pemrosesan informasi/data	Ketiadaan dokumentasi prosedur operasional
16.	Database & data files	Ketidaksempurnaan backup	Ketiadaan dokumentasi prosedur operasional
17.	Database & data files	Terinfeksi malicious code/virus/worm	Ketiadaan malicious data/traffics monitoring dan surveilance
18.	Database & data files	Terinfeksi malicious code/virus/worm	Ketidaksempurnaan kontrol keamanan terhadap penggunaan internet
19.	Database & data files	Terinfeksi malicious code/virus/worm	Penggunaan software yang tidak diotorisasi (bajakan / freeware yang tidak dikenal)
20.	Database & data files	Pemrosesan informasi yang tidak sah	Ketidaksempurnaan penanganan mobile code
21.	Database & data files	Kehilangan / pencurian informasi/data	Ketidakteraturan backup data/informasi
22.	Database & data files	Bencana alam	Ketidakteraturan backup data/informasi
23.	Database & data files	Kegagalan backup	Ketidakcukupan backup testing
24.	Database & data files	Pertukaran informasi/data via network	Ketidaksempurnaan kontrol jaringan
25.	Database & data files	Removable media digunakan sembarangan (dicolokkan ke komputer/ laptop manapun tanpa kontrol)	Ketiadaan otentikasi removable media
26.	Database & data files	Kehilangan / pencurian informasi/data	Ketidaksempurnaan aturan pembuangan media
27.	Database & data files	Information/data sniffing	Ketidaksempurnaan jalur komunikasi digital
28.	Database & data files	Penyingkapan informasi kepada pihak yang tidak berwenang	Ketidaksempurnaan perjanjian pertukaran Informasi
29.	Database & data files	Kehilangan/pencurian perangkat/media	Ketidaksempurnaan pengamanan perangkat penyimpan informasi selama pengangkutan
30.	Database & data files	Pengiriman informasi rahasia via email	Alamat email tujuan keliru
31.	Database & data files	Information sharing	Ketidaksempurnaan pengamanan interkoneksi sistem informasi
32.	Database & data files	Penyalahgunaan ID/otentikasi	Ketiadaan access control policy
33.	Database & data files	Penyalahgunaan ID/otentikasi	Ketidaksempurnaan proses registrasi user
34.	Database & data files	Penyalahgunaan ID/otentikasi	Ketidaksempurnaan pembagian privilege user
35.	Database & data files	Password cracking	Ketiadaan standar password yang digunakan
36.	Database & data files	Pencurian password	Kerahasiaan password tidak dijaga oleh pemiliknya

37.	Database & data files	Komputer/laptop ditinggalkan aktif tanpa pengamanan	Belum ada clean screen policy
38.	Database & data files	Pencurian informasi/data	Penggunaan mobile phone / smart phone di dalam data center
39.	Database & data files	Bencana alam / kebakaran	Ketidakcukupan Business Continuity Plan
40.	Data Log & Audit	Penyingkapan informasi kepada pihak yang tidak berwenang	Ketiadaan Kebijakan Keamanan Informasi
41.	Data Log & Audit	Perubahan/penghilangan Informasi/data secara tidak sah	Ketiadaan Kebijakan Keamanan Informasi
42.	Data Log & Audit	Penyingkapan informasi kepada pihak yang tidak berwenang	Ketidaksempurnaan penerapan Kebijakan Keamanan Informasi di lingkungan ITTP
43.	Data Log & Audit	Perubahan/penghilangan Informasi/data secara tidak sah	Ketidaksempurnaan penerapan Kebijakan Keamanan Informasi di lingkungan ITTP
44.	Data Log & Audit	Ketidakjelasan siapa yang bertanggung jawab utama atas ancaman keamanan informasi terhadap aset	Ketidakjelasan kepemilikan aset
45.	Data Log & Audit	Banyaknya jumlah informasi yang dikelola oleh ITTP	Bercampurnya informasi rahasia dengan informasi lainnya
46.	Data Log & Audit	Banyaknya jumlah informasi yang dikelola oleh ITTP	Ketidakjelasan penanganan informasi rahasia
47.	Data Log & Audit	Ketidaksempurnaan backup	Ketiadaan dokumentasi prosedur operasional
48.	Data Log & Audit	Kehilangan / pencurian informasi/data	Ketidakteraturan backup data/informasi
49.	Data Log & Audit	Bencana alam	Ketidakteraturan backup data/informasi
50.	Data Log & Audit	Kegagalan identifikasi gangguan keamanan Informasi	Perangkat CCTV tidak berfungsi
51.	Data Log & Audit	Kegagalan identifikasi gangguan keamanan Informasi	Ketidaksempurnaan pengisian data log
52.	Data Log & Audit	Kedatangan pihak ketiga ke Data Center	Ketidaksempurnaan proteksi log
53.	Data Log & Audit	Kegagalan identifikasi gangguan keamanan Informasi	Waktu komputer dan perangkat pemroses informasi tidak sinkron
54.	Data Log & Audit	Information/data sniffing	Ketidaksempurnaan secure configuration sistem access control
55.	Contract / legal documents	Penyingkapan informasi kepada pihak yang tidak berwenang	Ketiadaan Kebijakan Keamanan Informasi
56.	Contract / legal documents	Perubahan/penghilangan Informasi/data secara tidak sah	Ketiadaan Kebijakan Keamanan Informasi
57.	Contract / legal documents	Penyingkapan informasi kepada pihak yang tidak berwenang	Ketidaksempurnaan penerapan Kebijakan Keamanan Informasi di lingkungan ITTP

58.	Contract / legal documents	Perubahan/penghilangan Informasi/data secara tidak sah	Ketidaksempurnaan penerapan Kebijakan Keamanan Informasi di lingkungan ITTP
59.	Contract / legal documents	Ketidakpahaman pegawai akan pentingnya keamanan informasi	Ketidakcukupan perjanjian kerahasiaan
60.	Contract / legal documents	Ancaman keamanan informasi terhadap aset tidak dapat dipetakan dengan baik	Ketidaksempurnaan dalam pendataan aset
61.	Contract / legal documents	Ketidakjelasan siapa yang bertanggung jawab utama atas ancaman keamanan informasi terhadap aset	Ketidakjelasan kepemilikan aset
62.	Contract / legal documents	Banyaknya jumlah informasi yang dikelola oleh ITTP	Bercampurnya informasi rahasia dengan informasi lainnya
63.	Contract / legal documents	Banyaknya jumlah informasi yang dikelola oleh ITTP	Ketidakjelasan penanganan informasi rahasia
64.	Contract / legal documents	Kedatangan pihak ketiga ke area kerja	Ketidakcakapan staf keamanan
65.	Contract / legal documents	Kedatangan pihak ketiga ke area kerja	Ketidaksempurnaan proteksi informasi/data/dokumen
66.	Contract / legal documents	Bencana Alam / kebakaran	Ketidaksempurnaan proteksi informasi/data/dokumen
67.	Contract / legal documents	Kudeta / gejolak politik / demonstrasi	Ketidaksempurnaan proteksi informasi/data/dokumen
68.	Contract / legal documents	Kedatangan pihak ketiga ke area kerja	Ketidakjelasan pembagian area berdasarkan tingkat keamanannya
69.	Contract / legal documents	Dokumen terletak di sembarang tempat	Belum ada clean desk policy
70.	Business Process/ Procedure	Bencana Alam	Ketidakcukupan Business Continuity Plan
71.	Business Process/ Procedure	Bencana Alam	Ketidaksempurnaan terhadap proteksi penyimpanan
72.	Business Process/ Procedure	Akses ilegal terhadap dokumen (termasuk Spionase/mata-mata dan pencurian)	Housekeeping yang kurang baik
73.	Business Process/ Procedure	Akses ilegal terhadap dokumen (termasuk Spionase/mata-mata dan pencurian)	Ketidaksempurnaan akses kontrol fisik
74.	Business Process/ Procedure	Akses ilegal terhadap dokumen (termasuk Spionase/mata-mata dan pencurian)	Ketidakjelasan pembagian area berdasarkan tingkat keamanannya
75.	Business Process/ Procedure	Akses ilegal terhadap dokumen (termasuk Spionase/mata-mata dan pencurian)	Belum diterapkannya Clean Desk & Clean Screen Policy
76.	Business Process/ Procedure	Pengungkapan Informasi yang tidak sah	Belum diterapkannya Clean Desk & Clean Screen Policy
77.	Business Process/ Procedure	Pengungkapan Informasi yang tidak sah	ketidaksempurnaan dalam penghapusan Data/Informasi pada media/disks/USB Flashdisk

78.	Business Process/ Procedure	Akses ilegal terhadap dokumen (termasuk Spionase/mata-mata dan pencurian)	Ketidaksempurnaan/inkonsistensi pelaksanaan aturan pembuangan media
79.	Business Process/ Procedure	Penyalahgunaan dokumen dari Pihak Eksternal (legal)	Inkonsistensi pelaksanaan NDA
80.	Business Process/ Procedure	Kehilangan Data/informasi	Ketidaksempurnaan kontrol terhadap askes fisik ke ruang kerja/premises
81.	Business Process/ Procedure	Kehilangan Data/informasi	USB Flashdisk yang belum dikontrol penggunaannya
82.	Business Process/ Procedure	Terinfeksi malicious code/virus	Ketidakcukupan anti virus/anti mal-code control

PEOPLE			
No	**Sub Kategori Risiko**	**Risiko**	**Dampak**
1.	Manajemen	Kudeta / gejolak politik / demonstrasi	Lokasi yang berada di area yang "high risk"
2.	Manajemen	Kudeta / gejolak politik / demonstrasi	Ketiadaan kontak dengan pihak berwenang (kepolisian)
3.	Manajemen	Api / kebakaran	Ketiadaan kontak dengan pihak berwenang (pemadam kebakaran)
4.	Manajemen	Api / kebakaran	Ketidaksempurnaan sistem deteksi dan pemadaman api
5.	Manajemen	Api / kebakaran	Penyuluhan tentang Keselamatan dan Kesehatan Kerja (K3) yang kurang intensif
6.	Manajemen	Ketidakpahaman manajemen akan pentingnya keamanan informasi	Ketidakcukupan materi awareness
7.	Manajemen	Bencana alam / kebakaran	Penyuluhan tentang pertolongan pertama kondisi darurat yang kurang intensif
8.	Pelaksana Teknis	Kudeta / gejolak politik / demonstrasi	Lokasi yang berada di area yang "high risk"
9.	Pelaksana Teknis	Api / kebakaran	Ketidaksempurnaan sistem deteksi dan pemadaman api
10.	Pelaksana Teknis	Api / kebakaran	Penyuluhan tentang Keselamatan dan Kesehatan Kerja (K3) yang kurang intensif
11.	Pelaksana Teknis	Perubahan organisasi dalam perusahaan	Ketidakjelasan pembagian tanggung jawab / instruksi kerja
12.	Pelaksana Teknis	Kesalahan seleksi pegawai	Ketidaksempurnaan proses rekrutmen
13.	Pelaksana Teknis	Kesalahan seleksi pegawai	Ketidaksempurnaan perjanjian kerja pegawai dengan instansi
14.	Pelaksana Teknis	Ketidakpahaman pegawai akan pentingnya keamanan informasi	Ketiadaan orientasi/induksi
15.	Pelaksana Teknis	Ketidakpahaman pegawai akan pentingnya keamanan informasi	Ketidakcukupan materi awareness

16.	Pelaksana Teknis	Bencana alam / kebakaran	Penyuluhan tentang pertolongan pertama kondisi darurat yang kurang intensif
17.	Pelaksana Teknis	Pelanggaran aturan keamanan informasi	Ketidaktegasan penerapan aturan
18.	Pelaksana Non Teknis	Kudeta / gejolak politik / demonstrasi	Lokasi yang berada di area yang "high risk"
19.	Pelaksana Non Teknis	Api / kebakaran	Ketidaksempurnaan sistem deteksi dan pemadaman api
20.	Pelaksana Non Teknis	Api / kebakaran	Penyuluhan tentang Keselamatan dan Kesehatan Kerja (K3) yang kurang intensif
21.	Pelaksana Non Teknis	Perubahan organisasi dalam perusahaan	Ketidakjelasan pembagian tanggung jawab / instruksi kerja
22.	Pelaksana Non Teknis	Kesalahan seleksi pegawai	Ketidaksempurnaan proses rekrutmen
23.	Pelaksana Non Teknis	Kesalahan seleksi pegawai	Ketidaksempurnaan perjanjian kerja pegawai dengan instansi
24.	Pelaksana Non Teknis	Ketidakpahaman pegawai akan pentingnya keamanan informasi	Ketiadaan orientasi/induksi
25.	Pelaksana Non Teknis	Ketidakpahaman pegawai akan pentingnya keamanan informasi	Ketidakcukupan materi awareness
26.	Pelaksana Non Teknis	Bencana alam / kebakaran	Penyuluhan tentang pertolongan pertama kondisi darurat yang kurang intensif
27.	Pelaksana Non Teknis	Pelanggaran aturan keamanan informasi	Ketidaktegasan penerapan aturan
28.	Tenaga Outsource	Api / kebakaran	Ketidaksempurnaan sistem deteksi dan pemadaman api
29.	Tenaga Outsource	Api / kebakaran	Penyuluhan tentang Keselamatan dan Kesehatan Kerja (K3) yang kurang intensif
30.	Tenaga Outsource	Ketidakpahaman tenaga outsource akan pentingnya keamanan informasi	Ketiadaan orientasi/induksi
31.	Tenaga Outsource	Ketidakpahaman tenaga outsource akan pentingnya keamanan informasi	Ketidakcukupan materi awareness
32.	Tenaga Outsource	Kesalahan dalam seleksi tenaga outsource	Ketidaksempurnaan HR policies
33.	Tenaga Outsource	Kesalahan dalam menangani Security Incident	Kurangnya koordinasi serta tidak jelasnya peran dan tanggung jawab setiap personnel berkaitan dengan keamanan Informasi

SOFTWARE			
No	**Sub Kategori Risiko**	**Risiko**	**Dampak**
1.	Business Application	Penyalahgunaan aplikasi	Ketiadaan Kebijakan Keamanan Informasi
2.	Business Application	Penyalahgunaan aplikasi	Ketidaksempurnaan penerapan Kebijakan Keamanan Informasi di lingkungan ITTP
3.	Business Application	Hacking	Kelemahan sistem yang tidak diketahui oleh custodian/owner
4.	Business Application	Ketidakjelasan siapa yang bertanggung jawab utama atas ancaman keamanan informasi terhadap aset	Ketidakjelasan kepemilikan aset
5.	Business Application	Berakhirnya masa kerja pegawai (pensiun / mutasi / mengundurkan diri)	Ketidaksempurnaan HR policy
6.	Business Application	Instalasi software yang tidak sempurna	Ketidakcukupan Change Control/Management
7.	Business Application	Perubahan fitur aplikasi dalam pengembangan	Ketidakcukupan Change Control/Management
8.	Business Application	Penanaman kode/version	Ketidaksempurnaan review source code
9.	Business Application	Aplikasi yang dikembangkan belum sempurna / belum dites	Bercampurnya fasilitas development, test, dan operational
10.	Business Application	Terinfeksi malicious code/virus/worm	Ketiadaan malicious data/traffics monitoring dan surveilance
11.	Business Application	Terinfeksi malicious code/virus/worm	Ketidaksempurnaan kontrol keamanan terhadap penggunaan internet
12.	Business Application	Penyalahgunaan ID/otentikasi	Ketiadaan access control policy
13.	Business Application	Penyalahgunaan ID/otentikasi	Ketidaksempurnaan proses registrasi user
14.	Business Application	Penyalahgunaan ID/otentikasi	Ketidaksempurnaan pembagian privilege user

15.	Business Application	Password cracking	Ketiadaan standar password yang digunakan
16.	Business Application	Pencurian password	Kerahasiaan password tidak dijaga oleh pemiliknya
17.	Business Application	Password cracking	Ketiadaan password management system
18.	Business Application	Cookie/session replay	Ketiadaan session timeout
19.	Business Application	Hacking	Ketidaksempurnaan software patch
20.	Business Application	Hacking	Prosedur penanganan insiden keamanan informasi yang belum disahkan
21.	Business Application	Hacking	Ketidaksempurnaan secure configuration aplikasi
22.	Database Engine	Database failure	Kelemahan sistem yang tidak diketahui oleh custodian/owner
23.	Database Engine	Terinfeksi malicious code/virus/worm	Tidak dilakukannya malicious data/traffics monitoring dan surveilance
24.	Database Engine	Penyalahgunaan ID/otentikasi	Ketiadaan access control policy
25.	Database Engine	Penyalahgunaan ID/otentikasi	Ketidaksempurnaan pembagian privilege user
26.	Database Engine	Password cracking	Ketiadaan standar password yang digunakan
27.	Database Engine	Pencurian password	Kerahasiaan password tidak dijaga oleh pemiliknya
28.	Operating System	Hacking	Kelemahan sistem yang tidak diketahui oleh custodian/owner
29.	Operating System	OS failure	Kelemahan sistem yang tidak diketahui oleh custodian/owner
30.	Operating System	Kesalahan penggunaan sistem	Ketidakcukupan dokumentasi standar

			prosedur penggunaan sistem
31.	Operating System	Instalasi software yang tidak sempurna	Ketidakcukupan Change Control/Management
32.	Operating System	Perubahan fitur aplikasi dalam pengembangan	Ketidakcukupan Change Control/Management
33.	Operating System	Penyalahgunaan ID/otentikasi	Ketidaksempurnaan access control policies
34.	Operating System	Terinfeksi malicious code/virus/worm	Ketiadaan malicious data/traffics monitoring dan surveilance
35.	Operating System	Terinfeksi malicious code/virus/worm	Ketidaksempurnaan kontrol keamanan terhadap penggunaan internet
36.	Operating System	Sistem memroses informasi rahasia/sensitif	Ketiadaan prosedur log-on
37.	Operating System	Dictionary attack	Ketidaksempurnaan penanganan failed log-on
38.	Operating System	Sistem memroses informasi rahasia/sensitif	Ketiadaan user account policy
39.	Operating System	Password cracking	Ketiadaan standar password yang digunakan
40.	Operating System	Cookie/session replay	Ketiadaan Session timeout
41.	Operating System	Penyebaran worm/virus	Ketiadaan atau keterlambatan patch
42.	Operating System	Hacking	Ketiadaan atau keterlambatan patch
43.	System Utility	Penyalahgunaan system utility	Ketiadaan kontrol penggunaan system utility
44.	System Utility	Kegagalan system utility	Update system utility yang terlambat
45.	System Utility	Kegagalan system utility	Menggunakan system utility yang tidak terotorisasi
46.	System Utility	Kegagalan system utility	Tidak terdapat maintenance perangkat lunak

SERVICE			
No	**Sub Kategori Risiko**	**Risiko**	**Dampak**
1.	Data communication services	Ketidaksempurnaan layanan vendor	Ketidakjelasan standar layanan yang disepakati
2.	Data communication services	Penyingkapan informasi kepada pihak yang tidak berwenang	Ketiadaan komitmen pihak ketiga dalam menjaga keamanan informasi
3.	Data communication services	Ketidaksempurnaan layanan vendor	Ketidaksempurnaan review layanan
4.	Maintenance & support services	Ketidaksempurnaan layanan vendor	Ketidakjelasan standar layanan yang disepakati
5.	Maintenance & support services	Penyingkapan informasi kepada pihak yang tidak berwenang	Ketiadaan komitmen pihak ketiga dalam menjaga keamanan informasi
6.	Maintenance & support services	Ketidaksempurnaan layanan vendor	Ketidaksempurnaan review layanan
7.	Outsource Service	Penyingkapan informasi kepada pihak yang tidak berwenang	Ketiadaan komitmen pihak ketiga dalam menjaga keamanan informasi
8.	Outsource Service	Kesalahan dalam seleksi tenaga outsource	Ketidaksempurnaan HR policies
9.	Outsource Service	Kesalahan dalam menangani Security Incident	Kurangnya koordinasi serta tidak jelasnya peran dan tanggung jawab setiap personnel berkaitan dengan keamanan Informasi

INTANGIBLE			
No	**Sub Kategori Risiko**	**Risiko**	**Dampak**
1.	Reputasi Organisasi	Terjadi pelanggaran keamanan informasi	Ketiadaan Kebijakan Keamanan Informasi
2.	Reputasi Organisasi	Terjadi pelanggaran keamanan informasi	Ketidaksempurnaan penerapan Kebijakan Keamanan Informasi di lingkungan organisasi
3.	Reputasi Organisasi	Terganggunya proses bisnis yang menjadi tanggung jawab organisasi	Ketidaksempurnaan layanan vendor
4.	Reputasi Organisasi	Bencana Alam / kebakaran	Ketidakcukupan Business Continuity Plan
5.	Reputasi Organisasi	Pelanggaran aturan keamanan informasi	Ketidaktahuan pegawai akan peraturan
6.	Reputasi Organisasi	Pelanggaran HAKI	Penggunaan software bajakan di komputer/laptop organisasi