UINSSC
UNIVERSITAS ISLAM NEGERI SIBER
SYEKH NURJATI CIREBON

KEBIJAKAN/PROSEDUR (SOP)

MANAJEMEN RISIKO TI

PUSAT TEKNOLOGI INFORMASI DAN KOMUNIKASI

UNIVERSITAS ISLAM NEGERI SIBER
SYEKH NURJATI CIREBON

LEMBAR PENGESAHAN

KEBIJAKAN/ PROSEDURE (SOP) MANAJEMEN RESIKO TI TAHUN 2025

Dokumen KEBIJAKAN/ PROSEDURE (SOP) MANAJEMEN RESIKO TI TAHUN 2025 ini telah diperiksa, disetujui, dan ditetapkan untuk digunakan sebagai acuan dalam pelaksanaan Sistem Manajemen Mutu di lingkungan UPT TIK Universitas Islam Negeri Siber Syekh Nurjati Cirebon.

Cirebon, 2 Maret 2025

Jabatan	Nama/TTD	Tanda Tangan
Penyusun	Tim UPT TIK	
Kepala UPT TIK	Riyanto, S.T. M.Kom.	
Sekretaris	Abdurrozaq Nasrudin, S.Kom., M.M.	
Wakil Rektor II	Prof. Dr. Jamali , M.Ag.	
Rektor	Prof. Dr. Aan Jaelani, M.Ag.	

BAB I
PENDAHULUAN

A. Latar Belakang

Seiring dengan percepatan transformasi digital di lingkungan pendidikan tinggi, pemanfaatan Teknologi Informasi (TI) di UIN Siber Syekh Nurjati Cirebon menjadi elemen krusial dalam mendukung kelancaran proses akademik, administratif, dan layanan publik. TI tidak hanya berperan sebagai alat bantu, tetapi telah menjadi infrastruktur utama yang menunjang efektivitas dan efisiensi tata kelola institusi.

Namun demikian, ketergantungan tinggi terhadap TI juga menghadirkan berbagai risiko yang dapat mengganggu stabilitas operasional, kerahasiaan dan integritas data, serta reputasi institusi. Gangguan teknis, serangan siber, kegagalan sistem, human error, hingga kurangnya kontrol akses merupakan sebagian dari risiko yang dapat berdampak signifikan terhadap layanan universitas.

Untuk itu, diperlukan suatu pendekatan manajemen risiko TI yang sistematis, terukur, dan terdokumentasi. Dengan adanya SOP ini, Pusat Teknologi Informasi dan Komunikasi (PUSTIKOM) sebagai leading sector memiliki acuan baku dalam mengidentifikasi, menganalisis, merespons, serta mengevaluasi risiko yang berkaitan dengan sistem dan layanan TI di kampus.

SOP ini juga sejalan dengan kebijakan tata kelola teknologi informasi nasional dan mendukung pencapaian visi UIN Siber Syekh Nurjati sebagai kampus digital berbasis keilmuan dan keislaman. Dengan pengelolaan risiko yang baik, institusi dapat lebih siap menghadapi dinamika teknologi dan potensi insiden yang muncul di masa depan.

B. Tujuan

SOP ini disusun dengan tujuan sebagai berikut:

1. Memberikan panduan yang terstandarisasi dalam pengelolaan risiko yang berkaitan dengan penggunaan Teknologi Informasi di lingkungan UIN Siber Syekh Nurjati Cirebon.

2. Meningkatkan kesadaran dan pemahaman seluruh pemangku kepentingan terhadap pentingnya pengendalian risiko TI dalam mendukung proses akademik, administratif, dan layanan digital kampus.
3. Mendorong terciptanya budaya pencegahan melalui identifikasi dini terhadap potensi risiko dan kelemahan sistem TI.
4. Menjamin keberlangsungan layanan TI kampus melalui tindakan mitigasi yang terencana dan sistematis.
5. Menyediakan mekanisme dokumentasi dan pelaporan yang akuntabel terhadap kejadian insiden TI dan langkah penanganannya.
6. Mendukung ketercapaian target transformasi digital kampus secara aman, efisien, dan sesuai dengan prinsip tata kelola TI yang baik.
7. Menjadi acuan bagi PUSTIKOM dalam menyusun kebijakan lanjutan, audit TI, dan peningkatan layanan berbasis data risiko aktual.

Dengan tujuan tersebut, SOP ini diharapkan mampu memperkuat kesiapan institusi dalam menghadapi tantangan digital dan mendorong kualitas layanan TI yang adaptif dan berkelanjutan.

C. Ruang Lingkup

SOP Manajemen Risiko Teknologi Informasi ini berlaku secara menyeluruh di lingkungan UIN Siber Syekh Nurjati Cirebon dan mencakup:

1. **Seluruh Unit Kerja Akademik dan Non-Akademik**

   Semua fakultas, program studi, biro, lembaga, dan unit pelaksana teknis yang menggunakan dan bergantung pada sistem dan layanan TI dalam pelaksanaan tugasnya.

2. **Sistem Informasi dan Aplikasi Digital Kampus**

   Termasuk namun tidak terbatas pada:

   - Sistem Informasi Akademik (Siakad)
   - Sistem Informasi Kepegawaian (SIMPEG)
   - Sistem Informasi Keuangan (SIMKEU)
   - Sistem Manajemen Surat dan Arsip Digital

- Helpdesk TI
- Website dan Portal Resmi Kampus
- Sistem Absensi Elektronik dan Learning Management System (LMS)

3. **Infrastruktur Teknologi Informasi**

   Mencakup server, jaringan internet dan intranet, perangkat penyimpanan (storage), firewall, dan perangkat keras lainnya yang dikelola oleh PUSTIKOM.

4. **Data dan Keamanan Informasi**

   Mencakup pengelolaan basis data mahasiswa, dosen, pegawai, arsip digital, email institusi, serta perlindungan terhadap integritas, ketersediaan, dan kerahasiaan informasi.

5. **Pengguna Sistem TI**

   Termasuk seluruh sivitas akademika yang menggunakan layanan TI kampus: mahasiswa, dosen, tenaga kependidikan, dan mitra kerja yang memiliki hak akses.

6. **Insiden, Gangguan, dan Ancaman TI**Baik yang bersifat teknis (kerusakan perangkat), non-teknis (human error), maupun eksternal (serangan siber, bencana alam, pemadaman listrik, dan sebagainya).

Dengan ruang lingkup ini, SOP bertujuan memberikan kepastian bahwa seluruh aspek layanan dan aset TI kampus tercakup dalam kerangka pengelolaan risiko yang terstandar dan terintegrasi.

BAB II
MANAJEMEN RESIKO TI

A. Definisi

Dalam dokumen ini, beberapa istilah yang digunakan memiliki pengertian sebagai berikut:

- **Risiko TI**: Kemungkinan terjadinya kejadian yang dapat menyebabkan gangguan atau kerugian terhadap sistem, layanan, dan aset teknologi informasi yang digunakan dalam penyelenggaraan kegiatan akademik, administratif, maupun layanan publik kampus.
- **Manajemen Risiko TI**: Suatu pendekatan sistematis yang digunakan untuk mengidentifikasi, menganalisis, mengevaluasi, dan merespon risiko yang berkaitan dengan aset dan layanan teknologi informasi, guna meminimalisir dampak negatif dan meningkatkan peluang keberhasilan operasional TI.
- **Insiden TI**: Suatu kejadian yang tidak direncanakan dan berdampak terhadap fungsi normal sistem TI, termasuk tetapi tidak terbatas pada gangguan jaringan, kerusakan sistem, akses ilegal, atau hilangnya data penting.
- **Kerentanan (Vulnerability)**: Kelemahan atau celah pada sistem informasi, jaringan, aplikasi, atau prosedur operasional yang dapat dimanfaatkan oleh ancaman untuk menimbulkan kerugian.
- **Ancaman (Threat)**: Potensi kejadian baik internal maupun eksternal yang dapat memanfaatkan kerentanan dan menyebabkan kerusakan atau gangguan pada sistem TI. Contoh: virus, malware, kesalahan pengguna, pemadaman listrik, bencana alam.
- **Dampak (Impact)**: Konsekuensi negatif yang terjadi jika risiko menjadi kenyataan, dapat berupa gangguan layanan, kerugian finansial, pencurian data, kerusakan reputasi, atau pelanggaran hukum.
- **Mitigasi Risiko**: Tindakan-tindakan yang dilakukan untuk mengurangi kemungkinan atau dampak dari suatu risiko TI. Mitigasi dapat bersifat teknis (seperti firewall), prosedural (seperti backup berkala), maupun organisatoris (seperti pelatihan pengguna).

- **Tingkat Risiko (Risk Level)**: Kombinasi dari kemungkinan terjadinya risiko dan tingkat dampaknya, biasanya dikategorikan sebagai rendah, sedang, atau tinggi.
- **Evaluasi Risiko**: Proses membandingkan tingkat risiko yang diidentifikasi dengan kriteria risiko organisasi untuk menentukan signifikansi dan prioritas penanganan.
- **Pengendalian Risiko**: Langkah-langkah strategis yang diterapkan untuk menangani risiko, termasuk menghindari, mengurangi, mentransfer, atau menerima risiko tersebut.

B. Tanggung Jawab Dan Peran

Tabel 2.1

Tanggung Jawab dan Peran User dalam Manajemen Risiko TI

Unit/Individu	Tugas dan Tanggung Jawab
PUSTIKOM	Sebagai leading sector dalam pelaksanaan SOP manajemen risiko TI
Tim Manajemen Risiko TI	Melakukan identifikasi, penilaian, mitigasi, dokumentasi dan pelaporan risiko
Operator Sistem	Melaporkan potensi gangguan dan insiden TI secara proaktif
Unit Pengguna	Memberikan informasi awal dan kolaborasi selama proses mitigasi risiko

C. Prosedur Manajemen Risiko TI

Prosedur manajemen risiko TI di lingkungan UIN Siber Syekh Nurjati Cirebon mencakup lima tahapan utama berikut:

1. Identifikasi Risiko

a. Dilakukan secara berkala (minimal 1x dalam satu semester) dan insidentil ketika terjadi gangguan.

b. Sumber informasi dapat berasal dari audit internal, laporan Helpdesk, masukan pengguna, hasil pemantauan sistem, serta laporan insiden sebelumnya.
c. Risiko diklasifikasikan berdasarkan:

- Jenis sistem atau layanan yang terdampak (akademik, keuangan, jaringan, dll)
- Aset yang berisiko (hardware, software, data, SDM)
- Sumber risiko (internal atau eksternal)

d. Output: Daftar risiko teridentifikasi beserta deskripsi, lokasi, dan potensi penyebabnya.

2. Analisis dan Penilaian Risiko

a. Setiap risiko dianalisis berdasarkan dua parameter utama:
   - **Kemungkinan Terjadi (Likelihood)**: Seberapa sering risiko tersebut mungkin terjadi.
   - **Tingkat Dampak (Impact Level)**: Seberapa besar konsekuensi yang ditimbulkan.

b. Hasil analisis dimasukkan ke dalam Matriks Risiko 3x3 atau 5x5:

Tabel 2.2
Matriks Risiko

Likelihood / Impact	Rendah	Sedang	Tinggi
Rendah	G	G	Y
Sedang	G	Y	R
Tinggi	Y	R	R

G: Green (Rendah), Y: Yellow (Sedang), R: Red (Tinggi)

c. Risiko dengan kategori Tinggi harus segera ditangani; risiko Sedang dimitigasi; risiko Rendah dimonitor secara berkala.

3. Penanganan Risiko

Berdasarkan hasil klasifikasi, strategi penanganan risiko mencakup:

a. **Eliminasi Risiko**: Menghapus sumber risiko, misalnya menghentikan penggunaan sistem rentan.
b. **Mitigasi Risiko**: Mengurangi kemungkinan atau dampak melalui:

   - Peningkatan keamanan (patch, firewall, enkripsi)
   - Penjadwalan backup
   - Pembaruan SOP

c. **Transfer Risiko**: Memindahkan beban risiko kepada pihak ketiga, misalnya asuransi TI atau layanan cloud.
d. **Penerimaan Risiko**: Risiko diterima tanpa tindakan, dilakukan jika biaya mitigasi lebih tinggi dari dampaknya.

4. Monitoring dan Review

a. Proses pengawasan risiko dilakukan secara berkelanjutan melalui dashboard monitoring sistem dan laporan berkala Helpdesk.
b. Evaluasi efektivitas mitigasi risiko dilakukan triwulanan.
c. Peninjauan ulang daftar risiko dan SOP dilakukan secara periodik oleh PUSTIKOM.
d. Setiap temuan baru ditambahkan dalam sistem manajemen risiko.

5. Pelaporan dan Dokumentasi

a. Seluruh aktivitas manajemen risiko harus terdokumentasi secara elektronik.
b. Template pelaporan risiko mencakup informasi: tanggal, sistem terdampak, penanggung jawab, penanganan, status terkini.
c. Laporan dikompilasi dan diserahkan secara berkala ke Wakil Rektor II dan Unit Audit Internal.

D. Format Laporan Risiko

Pelaporan risiko TI merupakan bagian penting dalam siklus manajemen risiko yang bertujuan untuk memberikan dokumentasi yang sistematis dan dapat ditindaklanjuti oleh pihak-pihak terkait, khususnya oleh manajemen dan pengambil kebijakan di lingkungan UIN Siber Syekh Nurjati Cirebon. Laporan ini berfungsi sebagai alat pemantauan terhadap risiko yang terjadi, efektivitas penanganan, serta sebagai bahan evaluasi dan perencanaan strategis layanan TI.

Setiap risiko yang telah diidentifikasi, dianalisis, dan ditangani wajib dilaporkan dalam format baku yang terdiri dari:

No	Tanggal Temuan	Unit/Sistem Terdampak	Deskripsi Risiko	Dampak Potensial	Tingkat Risiko	Penanggung Jawab	Tindakan Penanganan	Status Risiko	Tanggal Pemutakhiran

Penjelasan Kolom:

- **No**: Nomor urut entri risiko
- **Tanggal Temuan**: Waktu awal risiko terdeteksi
- **Unit/Sistem Terdampak**: Nama unit kerja atau sistem/aplikasi TI yang terdampak
- **Deskripsi Risiko**: Ringkasan kejadian atau potensi gangguan
- **Dampak Potensial**: Penjabaran akibat dari risiko jika tidak segera ditangani (misal: kehilangan data, layanan terhenti)
- **Tingkat Risiko**: Kategori (rendah, sedang, tinggi) hasil dari penilaian likelihood x impact
- **Penanggung Jawab**: PIC (Person in Charge) yang menangani risiko tersebut
- **Tindakan Penanganan**: Langkah mitigasi atau solusi yang diambil

- **Status Risiko**: Selesai / Dalam Penanganan / Belum Ditangani / Berulang
- **Tanggal Pemutakhiran**: Waktu terakhir data risiko diperbarui

Laporan risiko ini dapat dikompilasi dalam bentuk:

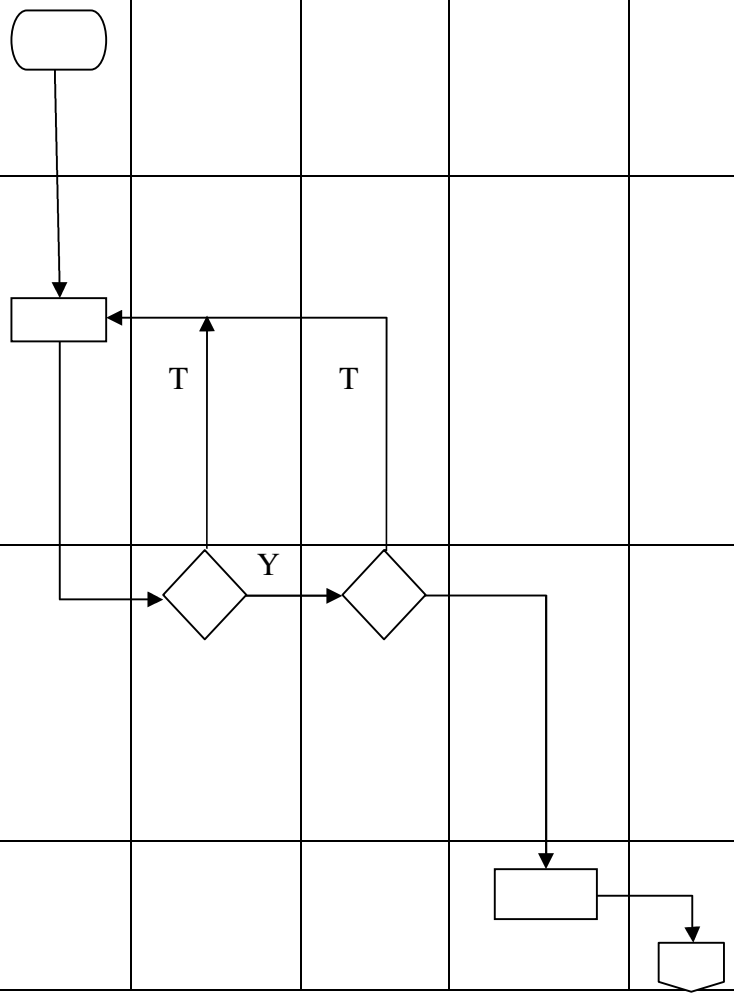
1. **Laporan bulanan internal PUSTIKOM** untuk keperluan evaluasi teknis.
2. **Laporan triwulanan ke pimpinan universitas** (Warek II, Kepala SPI) sebagai bahan monitoring dan pengambilan keputusan strategis.
3. **Lampiran dokumentasi insiden** sebagai bagian dari proses audit dan penguatan kebijakan keamanan informasi.

Semua laporan risiko disimpan secara elektronik dalam sistem informasi manajemen risiko PUSTIKOM, serta diarsipkan dalam bentuk dokumen PDF di repositori internal yang aman.

Dasar Hukum	Kualifikasi Pelaksana
Persyaratan ISO 27001	1. Mempunyai pengetahuan dibidang pengelolaan perguruan Tingg 2. Mempunyai pengetahuan dan memahami sistem mutu perguruan tinggi, standar, prinsip jaminan mutu, dan peraturan-peraturan yang digunakan. 3. Mempunyai kemampuan komunikasi yang baik. 4. Mempunyai kemampuan melaksanakan fungsi manajemen. 5. Mempunyai kemampuan berinovasi dan berwawasan luas. 6. dll
Keterkaitan :	**Peralatan/Perlengkapan :**
Semua SOP	ATK, Komputer dan Printer
Peringatan	**Pencatatan dan Pendataan**
Mengidentifikasi dan menetapkan konteks pengelolaan risiko disusun supaya dapat digunakan sebagai panduan mengenai kriteria penilaian tingkat risiko serta strategi penanganan risiko agar dalam penilaian resiko pada proses utama BAK, BUK dan BPHM memberikan informasi yang tepat	1. Surat undangan 2. Daftar hadir rapat 3. Notulen hasil rapat kaji ulang manajemen

PROSEDUR MANAJEMEN RISIKO

No	Uraian Prosedur	Pelaksana					Baku Mutu			Ket
		Staf	Kasubbag	Kabag	Kabiro	WMM	Persyaratan / Kelengkapan	Waktu	Output	
1	Melakukan Identifikasi, penilaian, pengkajian dan penanganan risiko sesuai dengan tabel pada masing-masing proses						Ada proses yang dijalankan	15 menit	Analisa Potensi Moda Kegagalan dan Dampaknya	
4	Menetapkan tingkat dampak serta munculnya peluang dan menetap tingkat resikonya. Jika ditemukan tingkat risiko yang tidak dapat diterima, maka diusulkan tindakan rencana kerja untuk menghilangkan risiko atau menurunkan risiko pada tingkat yang dapat diterima						Tabel 1 . Nilai Kemungkinan Tabel 2 . Nilai Konsekuensi Dampak atau Keparahan	15 menit	Analisa Potensi Moda Kegagalan dan Dampaknya	
5	Menyerahkan draf dokumen analisisi risiko untuk diverifikasi ke Kasubbag, Kabag dan Kabiro untuk kajian akhir. Jika ditemukan isi yang belum disetujui, maka draf dokumen tersebut dikembalikan untuk diperbaiki						Analisa Potensi Moda Kegagalan dan Dampaknya	1 hari	Analisa Potensi Moda Kegagalan dan Dampaknya	
6	Menyerahkan dokumen analisis risiko yang telah disetujui kepada WMM untuk dikompilasi						Analisa Potensi Moda Kegagalan dan Dampaknya	30 menit	Analisa Potensi Moda Kegagalan	



									dan Dampaknya	
7	Mengkompilasi dokumen analisis risiko dan mengesahkan						Analisa Potensi Moda Kegagalan dan Dampaknya	1 hari	Analisa Potensi Moda Kegagalan dan Dampaknya	
8	Melakukan pengkajian secara rutin analisa risiko pada proses rutin yang dijalankan						Analisa Potensi Moda Kegagalan dan Dampaknya	Menyesuaikan pada proses yang dijalankan	Analisa Potensi Moda Kegagalan dan Dampaknya	

TABEL RISIKO

1. Nilai Kemungkinan

   Kemungkinan terjadinya adalah probabilitas dari suatu peristiwa yang terjadi. Kemungkinan risiko, perlu mempertimbangkan baik probabilitas dan frekuensi kejadian. BAK, BUK dan BPHM menggunakan peringkat kemungkinan berikut.

Tabel 1 . Nilai Kemungkinan

Nilai	Kemungkinan	Deskripsi	Kuantifikasi / Frekuensi
1	Sangat Jarang	Peristiwa mungkin terjadi tetapi hanya dalam keadaan luar biasa. Tidak ada riwayat kejadian masa lalu.	Sekali setiap 5 tahun atau lebih
2	Jarang	Peristiwa mungkin terjadi dalam beberapa keadaan. Tidak ada riwayat kejadian masa lalu.	Sekali dalam 2 tahun.
3	Mungkin	Peristiwa mungkin terjadi dalam beberapa waktu. Adanya beberapa tanda-tanda peringatan sebelumnya atau riwayat kejadian sebelumnya	Sekali dalam 1 tahun
4	Lebih mungkin	Peristiwa akan kemungkinan terjadi. Beberapa kejadian masalalu terulang.	Sekali dalam 6 bulan
5	Hampir selalu	Peristiwa diperkirakan terjadi dalam situasi normal. Telah sering terjadi kejadian masalalu.	Sekali setiap 1 bulan atau lebih frekuensi nya.

2. Nilai Keparahan atau Konsekuensi

   Penilaian “Severity” atau “konsekuensi” merupakan dampak dari resiko tersebut, yang dapat diukur dari (atau kombinasi nya):

   - Dampak pada kegiatan organisasi
   - Dampak finansial
   - Reputasi pada organisasi.

   BAK, BUK dan BPHM akan menggunakan penilaian konsekuensi berikut:

Tabel 2 . Nilai Konsekuensi Dampak atau Keparahan

Nilai	Konsekuensi	Dampak Kegiatan Organisasi	Dampak Finansial	Dampak Reputasi
1	Tidak signifikan	Gangguan biasa yang terjadwal. Gangguan yg tak terjadwal kurang dari 2 jam.	Kerugian yang lebih kecil, dengan nilai > Rp. 100.000 ,-	Dampak yang sangat kecil – pengaruh pada inetrnal organisasi itu sendiri

2	Minor	Aktivitas utama terganggu hingga ½ hari	Kerugian secara kecil, dengan nilai > Rp. 500.000 ,-	Dampak yang terbatas – pengaruh pada media lokal.
3	Moderat / Sedang	Aktivitas utama terganggu hingga 1 hari	Kerugian secara lokal, dengan nilai > Rp.1.000.000,-	Dampak yang pantas dipertimbangkan – pengaruh media lokal. Dampak terhadap lisensi nasional
4	Major	Aktivitas utama terganggu hingga 2 hari	Kerugian yang luas dengan nilai > Rp. 5.000.000,-	Dampak Nasional – pengaruh media nasional. Dampak terhadap lisensi nasional
5	Katastropik	Aktivitas utama terganggu hingga > 2 hari	Luasan kerugian – substansi atau total kerugian operasional > Rp. 10.000.000,-	Dampak internasional – pengaruh media internasional. Dampak terhadap lisensi internasional.

3. Penilaian Resiko

Penilaian resiko ditentukan dengan perkalian antara nilai dampak dengan nilai kemungkinan. Tingkat resiko tersebut menentukan bagaimana tindak lanjut penanganan resiko. Tabel berikut dibawah menggambarkan tingkat resiko yang digunakan oleh BAK, BUK dan BPHM.

Tabel 3 . Tingkat Resiko

	Kemungkinan				
Konsekuensi	**1** Sangat jarang	**2** jarang	**3** mungkin	**4** Lebih mungkin	**5** Hampir selalu
5 Katastropik	**Sangat Besar 5**	**Ekstrim 10**	**Ekstrim 15**	**Ekstrim 20**	**Ekstrim 25**
4 Major	**Medium 4**	**Sangat Besar 8**	**Sangat Besar 12**	**Eksrim 16**	**Ekstrim 20**
3 Moderat	**Medium 3**	**Besar 6**	**Besar 9**	**Sangat Besar 12**	**Ekstrim 15**
2 Minor	**Kecil 2**	**Medium 4**	**Besar 6**	**Besar 8**	**Sangat Besar 10**
1 Tidak signifikan	**Kecil 1**	**Kecil 2**	**Kecil 3**	**Medium 4**	**Medium 5**

4. Evaluasi Resiko

Penialain resiko melibatkan komparasi nilai resiko yang muncul dan analisa proses prioritas dan persyaratan yang ada.

Strategi penanganan resiko sebagai berikut :

- Ekstrim : memerlukan tindakan segera karena sebaran potensi resiko memungkinkan hancurnya organisasi.

  Resiko tersebut dapat di alihkan ke pihak lain atau di hindari oleh BAK, BUK dan BPHM.
- Sangat Besar: memerlukan tindakan cepat [maksimal 3 bulan], karena potensi dampak nya melemahkan organisasi. Prosedur atau Instruksi kerja pada aktivitas terkait proses ini diperlukan.

  Resiko tersebut dapat di alihkan ke pihak lain atau di hindari oleh BAK, BUK dan BPHM.

  Besar : Memerlukan penanganan dengan rencana tindakan [antara 3 – 6 bulan].

  Resiko tersebut dapat diterima, namun diperlukan usaha untuk menurunkan kemungkinan munculnya penyebab kegagalan proses, atau menurunkan potensi dampak kegagalan proses.
- Medium : Merupakan batas resiko yang dapat diterima oleh BAK, BUK dan BPHM., namun selalu memantau dan mengevaluasi resiko tersebut.

  Menerima resiko dengan informasi yang diterima, namun ada upaya untuk memperbaiki.
- Kecil : Dikaji, dipantau dan dievauasi minimal setahun sekali.

Analisa Potensi Moda Kegagalan dan Dampaknya

Tahapan Proses	Persyaratan	Moda Potensi Kegagalan	Potensi Dampak Kegagalan	Level Dampak	Penyebab Potensi Kegagalan	Peluang Terjadi	Kendali Pencegahaan [Saat Ini]	Resiko	Rekomenda-si Tindakan	Penanggung Jawab & Target Selesai	Hasil Tindakan			
											Status Tindakan & Tanggal Selesai	Level Dampak	Peluang Terjadi	Resiko

Residu resiko

Tahapan proses sesuai alur

Persyaratan terkait proses atau output

Potensi kegagalan proses

Potensi dampak gagalnya proses

Dampak gagal proses **Tabel 2**

Potensi penyebab kegagalan proses

Peluang muncul penyebab gagal proses **Tabel 1**

Kendali sekarang mencegah penyebab kegagalan proses

Resiko = Dampak x Peluang

Rencana tindakan untuk resiko: Ekstrim, Sangat Besar, Besar, **Tahap 6**

BAB III
KESIMPULAN DAN RENCANA TINDAK LANJUT

A. Kesimpulan

Manajemen risiko Teknologi Informasi merupakan elemen kunci dalam menjaga keberlangsungan dan keamanan sistem digital di lingkungan UIN Siber Syekh Nurjati Cirebon. Melalui penyusunan SOP ini, PUSTIKOM sebagai leading sector bertanggung jawab untuk:

1. Menyusun pendekatan sistematis dalam mengidentifikasi, menganalisis, menangani, dan memantau risiko TI yang berpotensi mengganggu proses bisnis kampus.
2. Menjamin keterlibatan seluruh unit dalam proses pelaporan dan pengendalian risiko melalui mekanisme terstandarisasi.
3. Menyediakan format pelaporan dan pemantauan risiko yang akuntabel, terdokumentasi, dan dapat diakses sebagai bahan evaluasi dan pengambilan kebijakan TI.
4. Menumbuhkan budaya kerja yang sadar risiko (risk-aware) demi meningkatkan ketahanan sistem dan mutu layanan digital universitas.

B. Rencana Tindak Lanjut

Sebagai bentuk implementasi SOP ini, dirumuskan beberapa langkah lanjutan sebagai berikut:

1. **Sosialisasi dan Pelatihan**
    - Melaksanakan pelatihan teknis dan sosialisasi SOP Manajemen Risiko TI kepada seluruh unit kerja.
    - Menyediakan materi edukasi untuk meningkatkan pemahaman sivitas akademika terkait potensi ancaman dan langkah mitigasi TI.
2. **Pembentukan Tim Risiko TI**
    - Membentuk Tim Manajemen Risiko TI yang terdiri dari perwakilan PUSTIKOM dan unit-unit terkait.
    - Menetapkan PIC risiko di masing-masing sistem atau unit layanan TI utama.
3. **Integrasi ke Sistem Helpdesk dan Audit Internal**
    - Menambahkan fitur pelaporan risiko ke dalam sistem helpdesk TI.
    - Memastikan laporan risiko menjadi bagian dari agenda rutin audit internal dan perencanaan teknologi kampus.
4. **Pemutakhiran Berkala SOP dan Daftar Risiko**
    - Menetapkan jadwal review SOP setiap 12 bulan atau saat terjadi perubahan signifikan dalam infrastruktur TI.

- Melakukan update daftar risiko berdasarkan hasil monitoring insiden dan feedback pengguna.

5. **Penyediaan Infrastruktur Pendukung**
    - Menyiapkan repositori elektronik risiko TI dan dashboard pemantauan risiko berbasis web.
    - Menyediakan sistem backup dan pemulihan data yang teruji serta prosedur pemulihan bencana (disaster recovery plan).

Dengan pelaksanaan rencana tindak lanjut ini, diharapkan seluruh aktivitas digital kampus dapat berjalan secara lebih aman, adaptif, dan berkelanjutan dalam menghadapi dinamika ancaman TI.