JURNAL KHATULISTIWA INFORMATIKA VOL. 9 NO. 2 Desember 2021
p-ISSN: 2339-1928 e-ISSN: 2579-633X Halaman : 121-133

ANALISIS, EVALUASI, DAN MITIGASI RISIKO ASET TEKNOLOGI INFORMASI MENGGUNAKAN *FRAMEWORK OCTAVE* DAN *FMEA* (STUDI KASUS: UNIT PENGELOLA TEKNIS TEKNOLOGI INFORMASI DAN KOMUNIKASI UNIVERSITAS XYZ)

Rut Juniati Gagas[1]; **Ilhamsyah[2];** Ferdy Febryanto[3]

Jurusan Sistem Informasi [1][2][3]
Fakultas MIPA Universitas Tanjungpura
rut.juniati.gagas@student.untan.ac.id[1]; **ilhamsyah@sisfo.untan.ac.id[2]**; ferdyf@sisfo.untan.ac.i[3]

INFO ARTIKEL

Diajukan :
12 Juli 2021

Diterima :
30 Juli 2021

Diterbitkan:
01 Desember 2021

Kata Kunci :
aset kritis, FMEA, ISO/IEC 27001:2013, OCTAVE, Mitigasi Risiko

INTISARI

Unit Pengelola Teknis Teknologi Informasi dan Komunikasi Universitas XYZ (UPT. TIK XYZ) merupakan pengembang, pengelola, dan perencana TIK XYZ. Dalam meningkatkan pelayanan Tri Dharma Perguruan Tinggi, XYZ menggunakan layanan Teknologi Informasi (TI) sebagai strateginya. Ini menunjukan bahwa tantangan untuk UPT. TIK XYZ dalam pelaksanaan tersebut melibatkan banyak aset TI yang harus dikelola, dan memungkinkan muncul berbagai aset kritis yang berisiko. Dari uraian tersebut menunjukan pentingnya keamanan aset TI dan manajemen risiko aset TI sesuai framework dan standar yang membantu mengurangi atau menghilangkan dampak dari kegagalan akibat kerentanan yang ada pada aset yang kritis. Tujuan penelitian ini untuk mengetahui praktik keamanan yang digunakan, mengidentifikasi, dan menganalisis aset kritis menggunakan framework OCTAVE, kemudian mengevaluasi dan menilai dampak untuk mengukur nilai RPN risiko aset kritis menggunakan framework FMEA. Serta memberi rekomendasi praktik keamanan menggunakan OCTAVE Katalog Versi 2.0 dan rekomendasi mitigasi risiko menggunakan ISO/IEC 27001:2013 dan ISO/IEC 27002:2013. Hasilnya terdapat 10 praktik keamanan yang memiliki jawaban hasil "Tidak" dan/atau "Tidak Jelas". Kemudian terdapat 19 risiko dengan 22 kejadian ancaman, dimana level very high memiliki 2 risiko dengan nilai RPN sebesar 280, high memiliki 0 risiko, medium memiliki 3 risiko dengan nilai RPN sebesar 100-140, low memiliki 8 risiko dengan nilai RPN sebesar 30-70, dan very low memiliki 9 risiko dengan nilai RPN sebesar 1-18.

I. PENDAHULUAN

Institusi perguruan tinggi negeri saat ini banyak berusaha menjadi kampus digital dengan memanfaatkan Teknologi Informasi (TI) sebagai pendukung pelaksanaan Tri Darma Perguruan Tinggi. Pelaksanaan tiga poin tersebut tentunya bagi perguruan tinggi saat ini perlu menyediakan layanan TI yang menunjang pelaksanaan dengan beragam pengguna seperti mahasiswa, dosen, staf kampus, dan publik. Salah satunya Universitas XYZ yang merupakan Perguruan Tinggi yang berada di wilayah Kalimantan Barat, sebuah institusi pendidikan formal, XYZ dituntut untuk mengembangkan Teknologi Informasi dan Komunikasi (TIK) yang mampu mendukung strategi Universitas.

TIK XYZ sendiri ditangani oleh Unit Pengelola Teknis TIK XYZ (UPT. TIK XYZ) sebagai pengembang dan perencana TIK XYZ dimana terdapat 7 program utama yang direncanakan dan dilaksanakan dalam kurun waktu 2018-2022 sebagai bagian dari strategi XYZ. Ini memungkinkan muncul berbagai risiko aset TI, tantangan dan tuntutan untuk UPT. TIK XYZ dalam pelaksanaannya.

Dari uraian tersebut terlihat pentingnya mengelola keamanan aset TI yang ada di UPT.TIK XYZ dengan mengurangi atau menghilangkan dampak dari kegagalan atau risiko akibat kerentanan yang ada pada aset kritis, tentu ini menjadi tugas penting bagi UPT. TIK XYZ untuk memastikan aset TI yang ada sudah tertangani dengan benar. Masalah penting bagi seorang ahli keamanan saat menghadapi tugas untuk memperkenalkan langkah-langkah keamanan dalam bisnis dan organisasinya salah satunya mengidentifikasi dan menilai dampak organisasi dari implementasi rencana keamanannya (Vacca, 2017). Masalah tersebut menunjukan bahwa

pentingnya kesiapan UPT. TIK XYZ untuk melaksanakan manajemen risiko aset TI yang dapat mengidentifikasi dan menilai dampak dari implementasi keamanan yang dijalankannya, sesuai *framework* dan standar yang dapat membantu menangani dan memahami permasalahan dari implementasi TI yang ada.

Dalam penelitian ini peneliti tertarik untuk melakukan manajemen risiko aset TI menggunakan *framework* dan standar yang dapat mengukur pengetahuan praktik keamanan yang digunakan, mengidentifikasi, dan menganalisis aset kritis menggunakan *framework Operational Critical Threat, Asset, and Vulnerability Evaluation* (OCTAVE), kemudian mengevaluasi dan menilai dampak untuk mengukur nilai RPN risiko aset kritis menggunakan *framework Failure Mode Effect Analysis* (FMEA) pada UPT. TIK XYZ. Serta memberi rekomendasi praktik keamanan menggunakan OCTAVE Katalog Versi 2.0 dan rekomendasi mitigasi risiko menggunakan ISO/IEC 27001:2013 dan ISO/IEC 27002:2013.

II. BAHAN DAN METODE

Berdasarkan latar belakang tersebut hasil akhir penelitian akan melakukan perancangan dan pembuatan rekomendasi pengembangan praktik strategis dan praktik operasional berdasarkan OCTAVE Katalog versi 2.0 dan rekomendasi mitigasi risiko berdasarkan standar ISO/IEC 27001:2013 dan ISO/IEC 27002:2013. Rekomendasi yang dibuat selanjutnya diuji dengan membandingkan rekomendasi dengan penerapan praktik yang dilakukan saat ini oleh pihak UPT. TIK XYZ untuk melihat potensi penerapan rekomendasi yang sudah di buat dan dirancang berdasarkan hasil analisis wawancara, dan perhitungan nilai persenan hasil survei pengetahuan dari beberapa orang terkait pengetahuan mereka tentang praktik keamanan, yang dianalisis dan dievaluasi menggunakan *framework* OCTAVE. Selain itu berdasarkan evaluasi dan penilaian dampak risiko tersebut digunakan metode FMEA untuk mencari nilai RPN risiko. Berdasarkan hal itu peneliti menggunakan dua pendekatan kualitatif dan kuantitatif.

Untuk mencapai tujuan dalam penelitian ini terdiri dari beberapa tahapan sebagai berikut:

1. *Preparation*:
   Melakukan persiapan untuk memastikan bahwa evaluasi sudah dicakup dengan benar, bahwa Kepala UPT.TIK XYZ mendukung evaluasi ini, dan bahwa setiap orang yang berpartisipasi dalam proses ini memahami perannya.
2. Fase 1 *Organizational View*: Proses 1 - Proses 4
   Mengidentifikasi pengetahuan anggota UPT. TIK XYZ dengan wawancara terkait aset yang berisiko, ancaman, kerentanan dan mengisi survei pengetahuan terkait praktik keamanan yang digunakan saat ini di UPT. TIK XYZ sehingga didapat profil ancaman aset TI dan kelemahan praktik keamanan dan profil risiko ancaman aset TI.
3. Fase 2 *Technological View*: Proses 5 - Proses 6
   Memeriksa infrastruktur komputasi yang terkait dengan profil ancaman aset kritis dengan mengevaluasi komponen aset TI sehingga hasil akhirnya ditemukan kerentanan komponen aset TI.
4. Fase 3 *Risk Analysis*: Proses 7 - 8 Dan Identifikasi Risiko
   Menganalisis komponen risiko ancaman aset, kerentanan aset, dan mengukur hasil survei praktik keamanan, dan melakukan identifikasi *potential cause* dan *potential effect* dari ancaman dan kerentanan serta mencari nilai RPN risiko berdasarkan FMEA.
5. Validasi Potensi Penerapan Rekomendasi Praktik Keamanan Dan Mitigasi Risiko
   Membuat rekomendasi mitigasi risiko berdasarkan standar ISO/IEC 27001:2013 dan ISO/IEC 27002:2013. Selain itu juga rekomendasi pengembangan praktik keamanan secara strategis dan operasional berdasarkan standar OCTAVE Katalog Praktik Versi 2.0. Setelah itu dilakukan pengecekan kesesuaian rekomendasi dengan keadaan UPT. TIK XYZ.

III. HASIL DAN PEMBAHASAN

Dari tahapan perancangan yang sudah dijelaskan sebelumnya, hasil dan pembahasan setiap tahapan dijelaskan sebagai berikut:

1. *Preparation*

Persetujuan dari manajemen senior untuk mendukung evaluasi yaitu Dr. Herry Sujaini, ST.MT selaku Kepala UPT.TIK XYZ, setelah itu dilakukan pemilihan tim analisis inti yang membantu peneliti yaitu Muhd. Rahmadi, S.T selaku pengelola Siakad, selanjutnya pengaturan ruang lingkup area operasional yaitu kepala UPT.TIK XYZ: pengelola sumber daya, pengelola sistem dan jaringan, dan pengelola siakad, dengan peserta evaluasi wawancara dan survei yaitu Dr. Herry Sujaini, ST. MT., Muanuddin, S. T., dan Muhd. Rahmadi, S. T.

2. Fase 1: Membangun Profil Ancaman Berbasis Aset (*Build Asset-Based Threat Profiles*).

1) Proses 1: *Identify Senior Management Knowledge.*

Tahap ini dilakukan wawancara langsung dengan kepala UPT. TIK XYZ untuk mengidentifikasi aset dan memilih aset yang paling penting menurut perspektif nya.

2) Proses 2: *Identify Operational Area Management Knowledge*

Tahap ini dilakukan wawancara langsung dengan admin database dan staf jaringan UPT. TIK XYZ untuk mengidentifikasi aset dan memilih aset yang paling penting menurut perspektif nya.

3) *Proses 3: Identify Staff Knowledge*

Tahap ini dilakukan wawancara langsung dengan admin database dan staf jaringan UPT. TIK XYZ untuk memilih aset yang paling penting menurut perspektif nya.

4) Proses 4: *Create Threat Profile*

Membuat profil ancaman berdasarkan hasil wawancara proses 1 sampai proses 3 dengan menentukan aset yang berdampak buruk besar jika keamanannya dilanggar bisa dilihat tabel berikut:

Tabel 5. Aset Kritis

No	Kategori	Aset
1.	Data / Informasi	Data nilai
2.	Sistem	Siakad
3.	*Hardware*	Server Jaringan
4.		Kabel
5.		Server database
6.	Orang	Admin database
7.		Operator Siakad/admin sistem
8.		Programmer
9.		Admin jaringan

Sumber: Hasil Penelitian (2021)

Selanjutnya mencatat alasan penetapan aset yang penting untuk dievaluasi dengan mempertimbangkan mengapa aset dianggap penting untuk memenuhi misi UPT.TIK XYZ bisa dilihat pada tabel berikut:

Tabel 6. Informasi Aset Kritis

Informasi Aset Kritis	
1. Aset: Data / informasi	**Data Nilai**
Alasan pemilihan sebagai aset penting	Data penting terkait layanan akademik untuk mahasiswa dan dosen.
Deskripsi singkat	Data yang krusial terkait penilaian dosen kepada mahasiswa sehingga membutuhkan data dan informasi yang valid untuk proses perkuliahan.
2. Aset: Sistem	**Siakad**
Alasan pemilihan sebagai aset penting	Sistem informasi akademik yang terkait langsung dengan layanan akademik yang merupakan core pendidikan.
Deskripsi singkat	Siakad memiliki runtutan proses yang saling memengaruhi untuk layanan penerimaan mahasiswa baru, daftar ulang mahasiswa, jadwal perkuliahan dan penilaian perkuliahan.
3. Aset: *Hardware*	**Server Jaringan**
Alasan pemilihan sebagai aset penting	Server sebagai jalur transmisi data jika tidak ada koneksi maka sistem akan gagal.
Deskripsi singkat	Server jaringan merupakan komputer dan komponen lainnya yang menggunakan mikro tik router sebagai server.
4. Aset: *Hardware*	**Kabel**
Alasan pemilihan sebagai aset penting	Kabel sebagai base jaringan dan listrik semua peralatan berhubungan dengan listrik dan tidak dapat berjalan tanpa listrik
Deskripsi singkat	Kabel sebagai base jaringan dan listrik semua peralatan berhubungan dengan listrik dan tidak dapat berjalan tanpa listrik
5. Aset: *Hardware*	**Server Database**
Alasan pemilihan sebagai aset penting	Sebagai alat agar sistem dapat berjalan karena terkait dengan data layanan mahasiswa dan dosen.
Deskripsi singkat	Server database merupakan komputer server dan perangkat lainnya yang mengolah dan menyimpan data Siakad.
6. Aset: Orang	**Admin Database**
Alasan pemilihan sebagai aset penting	Orang yang berkaitan langsung dengan sistem untuk memberikan layanan data dapat berjalan dengan baik.
Deskripsi singkat	Orang yang mengkondisikan, server database dapat berjalan dalam keadaan baik dan koneksi tersedia setiap saat dan bertanggung jawab menjaga keamanan data dalam memenuhi kebutuhan layanan data.
7. Aset: Orang	**Operator Siakad / Admin sistem**
Alasan pemilihan sebagai aset penting	Orang yang terkait langsung dengan sistem aplikasi Siakad dan dapat melakukan segala hal terkait dengan layanan akademik.
Deskripsi singkat	Admin orang yang mengelola aplikasi dan operator Siakad orang memiliki level otoritas yang berbeda-beda di fakultas atau Prodi bisa melakukan input, mengubah dan menghapus data terkait layanan akademik seperti penjadwalan, rencana studi, data nilai dan lain sebagainya.
8. Aset: Orang	**Admin Jaringan**
Alasan pemilihan sebagai aset penting	Keberhasilan sistem layanan yang berjalan di atas jaringan internet yang di kelola admin jaringan sangat mempengaruhi kecepatan akses sistem layanan yang diberikan, keberhasilan internet mendukung sistem yang baik.
Deskripsi singkat	Bertanggung jawab terkait berjalannya layanan internet yang mempunyai hak akses penuh dan kontrol atas dirinya sendiri dalam penanganan masalah jaringan yang putus dan lainnya.
9. Aset: Orang	**Programmer**
Alasan pemilihan	Pengembang sistem yang mempengaruhi performa layanan sistem, keamanan

sebagai aset penting	sistem, dan masalah penanganan yang cepat diatasi terkait dengan integritas programmer yang mengetahui celah kelemahan sistem dan bisa melakukan apa saja terhadap sistem.
Deskripsi singkat	Programmer di posisi kan sesuai *job desk* masing-masing sistem layanan dan memiliki tanggung jawab atas performa produk layanan yang dihasilkan untuk memenuhi kebutuhan, memperbaiki kekurangan dari masalah bug, antarmuka website.

Sumber: Hasil Penelitian (2021)

Kemudian, meninjau persyaratan keamanan untuk setiap aset penting dan area perhatian untuk aset tersebut yang sudah diidentifikasi bisa dilihat pada tabel berikut:

Tabel 7. Persyaratan Keamanan

Aset Kritis	**Jenis Persyaratan Keamanan**	**Prioritas**	**Kebutuhan**
Data Nilai	Kerahasiaan *(Confidentiality)*		Akses hanya yang berwenang berdasarkan otorisasi nya.
	Integritas *(Integrity)*	**X**	Data akurat konsisten tidak berubah tanpa izin dari yang berhak memberi nilai.
	Ketersediaan *(Availability)*		Dapat diakses cepat, tepat, dan tersedia 24/7.
Siakad	Kerahasiaan *(Confidentiality)*		Akses hanya yang berwenang berdasarkan otoritas nya.
	Integritas *(Integrity)*		Data akurat konsisten tidak berubah tanpa izin.
	Ketersediaan *(Availability)*	**X**	Dapat diakses cepat, tepat dan tersedia 24/7.
Server Jaringan	Kerahasiaan *(Confidentiality)*		Data server hanya diketahui orang yang berwenang
	Integritas (*Integrity*)		Perangkat lunak asli dan berbayar.
	Ketersediaan *(Availability)*	**X**	Dapat diakses cepat, tepat dan tersedia 24/7
Kabel	Kerahasiaan *(Confidentiality)*		Kabel tidak ada kerahasiaan
	Integritas *(Integrity)*		Kabel original mengikuti standar jaringan.
	Ketersediaan *(Availability)*	**X**	Stok kabel cadangan tersedia 10% ketika dibutuhkan Kabel tetap tersambung dengan aman
Server Database	Kerahasiaan *(Confidentiality)*		Akses tersedia untuk yang berwenang.
	Integritas *(Integrity)*		Kondisi perangkat baik dan memiliki speck yang optimal.
	Ketersediaan *(Availability)*	**X**	Performa akses data cepat dan dapat diakses 24/7.
Admin Database	Kerahasiaan *(Confidentiality)*		Menjaga data rahasia dengan mendistribusikan data ke akses yang berwenang.
	Integritas *(Integrity)*	**X**	Berlaku jujur bertanggung jawab, dan memiliki kemampuan.
	Ketersediaan *(Availability)*		Dapat berkerja ketika dibutuhkan.
Operator Siakad / Admin Sistem	Kerahasiaan *(Confidentiality)*		Mengakses hanya bagian wewenang hak akses yang dimiliki.
	Integritas *(Integrity)*	**X**	Berlaku jujur dan bertanggung jawab atas validitas data dan cepat/tanggap dalam penanganan masalah sistem.
	Ketersediaan *(Availability)*		Dapat berkerja dimana saja ketika dibutuhkan.
Program-mer	Kerahasiaan *(Confidentiality)*		Menjaga data/informasi sistem yang rahasia.
	Integritas *(Integrity)*	**X**	Berlaku jujur bertanggung jawab, dan memiliki kemampuan.
	Ketersediaan *(Availability)*		Dapat berkerja dimana saja ketika dibutuhkan.
Admin Jaringan	Kerahasiaan *(Confidentiality)*		Menjaga data/informasi yang rahasia.
	Integritas *(Integrity)*	**X**	Berlaku jujur bertanggung jawab, dan memiliki kemampuan terhadap ketersediaan layanan internet.
	Ketersediaan *(Availability)*		Dapat berkerja dimana saja ketika dibutuhkan.

Sumber: Hasil Penelitian (2021)

Selanjutnya memetakan area yang menjadi perhatian atau potensi ancaman terhadap aset penting tersebut bisa dilihat pada tabel berikut:

Tabel 8. Area Perhatian

Area Perhatian Data Nilai
1. Penyingkapan data akibat akses menggunakan komputer umum yang dipasang aplikasi *spy.* 2. Data berubah akibat modifikasi oleh operator Siakad. 3. Data hilang atau terhapus akibat salah *setting* periode atau tahun ajaran pada aplikasi Siakad.
Area Perhatian Siakad
1. Akses layanan sistem lambat atau tidak tersedia akibat serangan DDoS, malware, atau kode berbahaya pada sistem. 2. Tampilan halaman utama web berubah akibat serangan deface. 3. Data login di ketahui orang yang tidak berhak dan berwenang.
Area Perhatian Server Jaringan
1. Data pada server di ketahui orang yang tidak berwenang. 2. Server mati atau rusak akibat masalah ketersediaan listrik yang tidak stabil. 3. Konektivitas jaringan putus akibat pemblokiran koneksi

ke *access point*.
4. IP konflik akibat serangan duplikasi alamat IP.
Area Perhatian Kabel
1. Kabel putus akibat *human error* saat beraktivitas tersentuh atau ditarik tidak sengaja. 2. Pemutusan kabel akibat pembangunan yang tanpa izin yang jelas.
Area Perhatian Server Database
1. Kinerja server tidak optimal atau sistem error akibat speck perangkat yang tidak memenuhi kebutuhan. 2. Server panas atau rusak akibat masalah listrik. 3. Masalah konfigurasi fisik akibat kabel lepas.
Admin Database
1. Melakukan perubahan data tanpa izin dari yang berwenang.
Operator Siakad/Admin Sistem
1. Melakukan perubahan data nilai tanpa izin dari yang berwenang.
Programmer
1. Masalah kesadaran keamanan sistem dan penanganan lambat terhadap layanan sistem yang bermasalah.
Admin Jaringan
1. Masalah kesadaran keamanan jaringan dan penanganan ketersediaan layanan internet yang putus.

Sumber: Hasil Penelitian (2021)

Kemudian memetakan area yang menjadi perhatian ancaman ke profil ancaman, dimana identifikasi profil ancaman berdasarkan kategori *human actor using physical access*, *human actor using network access*, *system problems* dan *other problems* bisa dilihat pada tabel berikut:

Tabel 9. Properti Ancaman yang Menjadi Perhatian

Area Perhatian	Properti Ancaman
1. Penyingkapan data akibat akses menggunakan komputer umum yang dipasang aplikasi *spy.*	Aset — data nilai Akses — fisik (akses Siakad menggunakan komputer umum yang dipasang aplikasi spy) Aktor — *inside* (user yang memiliki hak akses) Motif — kebetulan Hasil — penyingkapan (data dibobol dan di salah gunakan orang yang tidak berwenang)
2. Data berubah akibat modifikasi oleh operator Siakad.	Aset — data nilai Akses — jaringan (mengubah data langsung ke sistem aplikasi Siakad) Aktor — *inside* (operator yang memiliki hak akses) Motif — disengaja Hasil — modifikasi (data berubah)
3. Data hilang atau terhapus akibat salah *setting* periode atau tahun ajaran pada aplikasi Siakad.	Aset — data nilai Akses — jaringan (kesalahan setting periode atau tahun ajaran pada aplikasi Siakad) Aktor — *inside* (operator yang memiliki hak akses) Motif — kebetulan Hasil — gangguan (data hilang atau terhapus)
4. Akses layanan sistem lambat atau tidak tersedia akibat serangan DDoS, malware atau kode berbahaya pada sistem.	Aset — siakad Akses — jaringan Aktor — serangan DDoS, malware atau kode berbahaya (hacker) Motif — disengaja Hasil — gangguan (akses sistem lambat atau tidak tersedia)
5. Tampilan halaman utama web berubah akibat serangan *deface*.	Aset — Siakad Aktor — serangan *deface* (hacker) Hasil — modifikasi (Tampilan halaman utama web berubah)
6. Data login di ketahui orang yang tidak berhak dan berwenang	Aset — Siakad Akses — fisik (akses menggunakan komputer umum yang dipasang spy atau *sharing* email dan *password)* Aktor — *inside* (user yang memiliki hak akses) Motif — kebetulan dan disengaja Hasil — Penyingkapan (data login diketahui orang yang tidak berwenang dan penyalahgunaan data) dan Modifikasi (perubahan data LIRS, Login dll)
7. Data pada server di ketahui orang yang tidak berwenang.	Aset — server Jaringan (data server) Akses — fisik (*inside*) dan jaringan (*outside*) Aktor — i*nside* (staf yang tidak berwenang) dan *outside* (hacker) Motif — disengaja Hasil — Modifikasi (perubahan *setting* server) dan Gangguan (server *down*)
8. Server mati atau rusak akibat masalah ketersediaan listrik yang tidak stabil.	Aset — server jaringan Aktor — masalah ketersediaan listrik Hasil — kerugian, kehancuran (server panas atau rusak)
9. Konektivitas jaringan putus akibat pemblokiran koneksi ke *access point*.	Aset — server jaringan Aktor — serangan pemblokiran *access point* (hacker) Hasil — gangguan (koneksi internet putus)
10. IP konflik akibat serangan duplikasi alamat IP.	Aset — server jaringan Aktor — serangan duplikasi alamat IP (hacker) Hasil — gangguan (sistem crash atau error)
11. Kabel putus akibat *human error* saat beraktivitas tersentuh atau ditarik tidak sengaja.	Aset — kabel Akses — fisik (Kabel) Aktor — *human error* saat beraktivitas tersentuh atau ditarik (*inside* dan *outside*) Motif — kebetulan Hasil — gangguan (akses koneksi internet putus)
12. Pemutusan kabel akibat pembangunan yang tanpa izin yang jelas.	Aset — kabel Akses — fisik (Kabel *fiber optic*) Aktor — Pemutusan kabel akibat pembangunan yang tanpa izin yang jelas. *(outside)* Motif — disengaja Hasil — Gangguan (akses koneksi internet ke client atau server terputus) dan Kerugian, kehancuran (Kerugian secara finansial, waktu, tenaga dalam perbaikan infrastruktur yang hancur)
13. Kinerja server	Aset — server database

tidak optimal atau sistem error akibat speck perangkat yang tidak memenuhi kebutuhan.	Aktor — speck perangkat memory CPU, komputer tidak memenuhi layanan Hasil — gangguan (sistem *error* data terhapus atau tidak bisa disimpan)
14. Server panas atau rusak akibat masalah listrik.	Aset — server database Aktor — listrik tidak stabil Hasil — kerugian, kehancuran (server panas atau rusak)
15. Masalah konfigurasi fisik akibat kabel lepas.	Aset — server database Aktor — masalah konfigurasi fisik kabel lepas. Hasil — gangguan (akses jaringan terputus)
16. Melakukan perubahan data tanpa izin dari yang berwenang.	Aset — admin database Akses — fisik (melakukan perubahan data langsung ke database Siakad) Aktor — inside (admin database) Motif — disengaja Hasil — modifikasi (data tidak valid tanpa diketahui sebab atau jejak)
17. Melakukan perubahan data nilai tanpa izin dari yang berwenang.	Aset — operator siakad/admin sistem Akses — jaringan (melakukan perubahan data secara langsung ke sistem aplikasi Siakad) Aktor — inside (operator Siakad / admin sistem yang memiliki hak akses yang sah) Motif — disengaja Hasil — modifikasi (data tidak valid)
18. Masalah kesadaran keamanan sistem dan penanganan lambat terhadap layanan sistem yang bermasalah.	Aset —programmer Aktor — masalah kesadaran keamanan sistem dan penanganan lambat terhadap layanan sistem yang bermasalah. Hasil — gangguan (layanan sistem tidak tersedia)
19. Masalah kesadaran keamanan jaringan dan penanganan ketersediaan layanan internet yang putus.	Aset — admin jaringan Aktor — masalah kesadaran keamanan jaringan dan penanganan ketersediaan layanan internet yang putus. Hasil — gangguan (layanan internet tidak tersedia)

Sumber: Hasil Penelitian (2021)

3. Fase 2 *technological view*: proses 5 - proses 6.

1) Proses 5: Identifikasi Kelas Utama Komponen *(Identifying Key Components).*

Proses ini melihat aset dan ancaman penting dari fase 1 kaitannya dengan infrastruktur komputasi memeriksa jalur akses jaringan bisa dilihat pada tabel berikut:

Tabel 10. *Key Classes of Components*

Komponen	Deskripsi Kelas
Data: Nilai	Data yang penting untuk memberikan layanan akademik yang merupakan core layanan Universitas XYZ dalam layanan teknologi informasi oleh UPT.TIK XYZ.
Server	Komputer (host), atau perangkat lain dalam infrastruktur teknologi informasi UPT. TIK XYZ yang menyediakan layanan teknologi informasi untuk layanan sistem akademik.
Perangkat Jaringan	Perangkat yang penting untuk akses jaringan layanan teknologi informasi (mis., komponen nirkabel seperti router dan kabel).
People	SDM yang berpengaruh besar terhadap berjalannya layanan dimana posisinya tidak dapat digantikan jika dibutuhkan dan dituntut berintegritas dan profesional (mis., admin database, operator Siakad/admin sistem, programmer dan admin jaringan)

Sumber: Hasil Penelitian (2021)

2) Proses 6: Mengevaluasi Komponen yang dipilih *(Evaluate Selected Components).*

Mengevaluasi kerentanan aset yang sebelumnya sudah diidentifikasi dengan menggabungkan seluruh data informasi yang diperoleh bisa dilihat tabel berikut:

Tabel 11. Kerentanan Aset

Aset	Kerentanan
Data: Nilai	Kesadaran keamanan yang kurang
	Ancaman orang dalam
Sistem	Serangan DDoS, *malware* atau kode berbahaya
	Serangan *deface*
	Kesadaran keamanan yang kurang
Server	Kesadaran keamanan yang kurang
	Terlalu panas
	Serangan pemblokiran *access point*
	Serangan duplikasi alamat IP
	kerentanan terhadap penyimpanan yang tidak dilindungi
	Ancaman orang dalam
Perangkat jaringan	Ancaman orang dalam dan luar
	Jalur komunikasi yang tidak terlindungi (tidak ada kebijakan izin pemutusan kabel dan ganti rugi yang jelas ke pihak UPT. TIK XYZ)
Server	Kesadaran keamanan yang kurang
	Terlalu panas
	Serangan pemblokiran *access point*
	Serangan duplikasi alamat IP
	kerentanan terhadap penyimpanan yang tidak dilindungi
	Ancaman orang dalam
Perangkat jaringan	Ancaman orang dalam dan luar
	Jalur komunikasi yang tidak terlindungi (tidak ada kebijakan izin pemutusan kabel dan ganti rugi yang jelas ke pihak UPT. TIK XYZ)
People	Ancaman orang dalam
	Kesadaran keamanan dan penanganan masalah lambat.

4. Fase 3 *risk analysis*: proses 7 - 8 dan identifikasi risiko.

1) Proses 7: Melakukan Analisis Risiko *(Conducting the Risk Analysis)*

Melakukan analisis komponen risiko ancaman, aset dan kerentanan pada aset secara teknologi dengan memetakan kerentanan, *potential cause* dan *potential effects* untuk perhitungan FMEA pada tahap selanjutnya bisa dilihat pada tabel berikut:

Tabel 12. *Potential Cause dan Potential Effects*

Kode	Aset	Kerentanan	Ancaman	***Potential Cause***	***Potential Effects***
R1.1	Data: Data Nilai	Kesadaran keamanan yang kurang	Data dibobol dan di salah gunakan orang yang tidak berwenang	Akses menggunakan komputer umum yang dipasang aplikasi *spy*	Kebocoran informasi
R1.2		Ancaman orang dalam	Data berubah	Mengubah data langsung ke sistem aplikasi Siakad	Data tidak valid
R.1.3		Ancaman orang dalam	Data hilang atau tidak tersedia	Kesalahan *setting* periode atau tahun ajaran pada aplikasi Siakad	Data hilang atau terhapus
R2.1	Sistem	Serangan DDoS, *malware* atau kode berbahaya	Akses sistem lambat atau tidak tersedia	Serangan DDoS, *malware* atau kode berbahaya (*hacker*)	Akses layanan sistem lambat atau tidak tersedia
R2.2		Serangan *deface*	Tampilan halaman utama web berubah	Serangan *deface* (hacker)	Tampilan halaman utama web berubah
R2.3		Kesadaran keamanan yang kurang	Data login diketahui orang yang tidak berwenang dan penyalahgunaan data	Akses menggunakan komputer umum yang dipasang spy atau *sharing* email dan *password*	Kebocoran informasi
R2.4		Kesadaran keamanan yang kurang	Perubahan data LIRS, *login* dll	Akses menggunakan komputer umum yang dipasang *spy* atau *sharing* email dan *password*	Perubahan data Siakad (LIRS, login dll).
R3.1	*Hardware*: Server Jaringan	Kesadaran keamanan yang kurang.	Perubahan pengaturan (*setting)* server	Data pada server di ketahui orang yang tidak berwenang	Perubahan pengaturan (*setting)* server
R3.2		Kesadaran keamanan yang kurang.	Server *down*	Data pada server di ketahui orang yang tidak berwenang	Server down
R3.3		Terlalu panas	Server panas atau rusak	Listrik tidak stabil	Server panas atau rusak
R3.4		Serangan pemblokiran *access point*	Koneksi internet putus.	Serangan pemblokiran *access point* (hacker)	koneksi internet putus
R3.5		Serangan duplikasi alamat IP	*Sistem crash atau error*	Serangan duplikasi alamat IP (hacker)	Sistem *crash* atau *error*
R4.1	Server Database	kerentanan terhadap penyimpanan yang tidak dilindungi	Sistem error data terhapus atau tidak bisa disimpan	*Speck* perangkat memori CPU, komputer tidak memenuhi layanan	Sistem *error* data terhapus atau tidak bisa disimpan
R4.2		Terlalu panas	Server panas atau rusak	Listrik tidak stabil	Server panas atau rusak
R4.3		Ancaman orang dalam	Akses jaringan terputus	Masalah konfigurasi fisik kabel lepas	Akses jaringan terputus
R5.1	Perangkat jaringan	Ancaman orang dalam dan luar	Akses koneksi internet terputus	*Human error* kabel tersentuh atau ditarik saat beraktivitas	Akses koneksi internet terputus

				menyebabkan kabel putus	
R5.2		Jalur komunikasi yang tidak terlindungi (tidak ada kebijakan izin pemutusan kabel dan ganti rugi yang jelas ke pihak UPT. TIK XYZ)	Akses koneksi internet ke *client* atau server terputus	Pembangunan yang memutuskan kabel tanpa izin yang jelas	Akses koneksi internet ke client atau server terputus
R5.3		Jalur komunikasi yang tidak terlindungi (tidak ada kebijakan izin pemutusan kabel dan ganti rugi yang jelas ke pihak UPT. TIK XYZ)	Rugi secara *finansial*, waktu, tenaga dalam perbaikan infrastruktur yang hancur	Pembangunan yang Memutuskan kabel tanpa izin yang jelas	Kerugian secara finansial, waktu, tenaga dalam perbaikan infrastruktur yang hancur
R6.1	*People*	Ancaman orang dalam	Data tidak valid tanpa diketahui sebab atau jejak	Melakukan perubahan data langsung ke database Siakad	Data tidak valid tanpa diketahui sebab atau jejak
R6.2		Ancaman orang dalam	Data tidak valid	Melakukan perubahan data secara langsung ke sistem aplikasi Siakad	Data tidak valid
R6.3		Kesadaran keamanan dan penanganan masalah lambat.	Layanan sistem tidak tersedia	Masalah kesadaran keamanan sistem dan penanganan lambat terhadap layanan sistem yang bermasalah.	Layanan sistem tidak tersedia.
R6.4		Kesadaran keamanan dan penanganan masalah lambat.	Layanan internet tidak tersedia	Masalah kesadaran keamanan jaringan dan penanganan ketersediaan layanan internet yang putus.	Layanan internet tidak tersedia

Sumber: Hasil Penelitian (2021)

2) Proses 8: Strategi dan Tindakan *(Strategies and Actions)*

Konsolidasi interpretasi atau pandangan dan pengetahuan berdasarkan hasil survei proses 1 sampai 3, jawaban narasumber yang menjawab dilakukan perhitungan persentase jawaban "Ya", "Tidak", dan "Tidak Tahu" dengan menggunakan rumus:

$$(\%) = \frac{Jumlah\ Jawaban}{Jumlah\ Total\ Jawaban} \times 100\% \dots\dots\dots\dots\dots\dots\dots\dots\dots (1)$$

Sehingga didapat angka-angka persentase jawaban. Beberapa hasil perhitungan survei bisa dilihat pada tabel berikut:

Tabel 13. Hasil survei

Kesadaran dan Pelatihan Keamanan: Hasil Survei				
Pernyataan Survei	*Jawaban*	Ya	Tidak	Tidak Tahu
Anggota staf UPT. TIK XYZ memahami peran dan tanggung jawab keamanan mereka. Ini didokumentasikan dan diverifikasi.	*Kepala UPT.TIK*	1 100%	0 0%	0 0%
	Staf Jaringan	1 100%	0 0%	0 0%
	Admin Database	1 100 %	0 0 %	0 0 %
Ada keahlian internal yang memadai untuk semua layanan, mekanisme, dan teknologi yang didukung (misalnya, logging, pemantauan, atau enkripsi), termasuk	*Kepala UPT.TIK*	1 100%	0 0%	0 0%
	Staf Jaringan	1 100%	0 0%	0 0%
	Admin Database	1 100 %	0 0 %	0 0 %

keamanan pengoperasian. Ini didokumentasikan dan diverifikasi.				
Kesadaran akan keamanan, pelatihan, dan pengingat berkala disediakan untuk semua personel. Pemahaman staf didokumentasikan dan kesesuaian diverifikasi secara berkala.	*Kepala UPT.TIK*	1 100%	0 0%	0 0%
	Staf Jaringan	1 100%	0 0%	0 0%
	Admin Database	1 100 %	0 0 %	0 0 %

Sumber: Hasil Penelitian (2021)

Selanjutnya dilakukan penilaian risiko menggunakan metode FMEA, dengan pemberian skor *Severity* (S), *Occurrence* (O) dan *detection* (D) sesuai standar FMEA yang sudah ditetapkan tim analisis dan perhitungan RPN dengan rumus:

$$RPN = (S) \times (O) \times (D) \dots\dots\dots\dots\dots\dots\dots\dots\dots (2)$$

Hasil perhitungan RPN risiko dapat dilihat pada tabel berikut:

Tabel 14. Tabel Pengkategorian RPN

Kode	Risiko	Penyebab	RPN	Kategori
R6.3	Layanan sistem tidak tersedia	Masalah kesadaran keamanan sistem dan penanganan lambat terhadap layanan sistem yang bermasalah.	280	Very High
R6.4	Layanan internet tidak tersedia	Masalah kesadaran keamanan jaringan dan penanganan ketersediaan layanan internet yang putus.	280	Very High
R5.2	Akses koneksi internet ke client atau server terputus	Pembangunan yang memutuskan kabel tanpa izin yang jelas	140	Medium
R5.3	Rugi secara finansial, waktu, tenaga dalam perbaikan infrastruktur yang hancur	Pembangunan yang Memutuskan kabel tanpa izin yang jelas	140	Medium
R6.1	Data tidak valid tanpa diketahui sebab atau jejak	Melakukan perubahan data langsung ke database Siakad	100	Medium
R1.2	Data berubah	Mengubah data langsung ke sistem aplikasi Siakad	70	Low
R6.2	Data tidak valid	Melakukan perubahan data secara langsung ke sistem aplikasi Siakad	70	Low
R2.1	Akses sistem lambat atau tidak tersedia	Serangan DDoS, malware atau kode berbahaya (hacker)	60	Low
R2.2	Tampilan halaman utama web berubah	Serangan deface (hacker)	48	Low
R2.3	Data login diketahui orang yang tidak berwenang dan penyalahgunaan data	Akses menggunakan komputer umum yang dipasang spy atau sharing email dan password	40	Low
R2.4	Perubahan data LIRS, login dll	Akses menggunakan komputer umum yang dipasang spy atau sharing email dan password	40	Low
R4.1	Sistem error data terhapus atau tidak bisa disimpan	Speck perangkat memori CPU, komputer tidak memenuhi layanan	36	Low
R5.1	Akses koneksi internet terputus	Human error kabel tersentuh atau ditarik saat beraktivitas menyebabkan kabel putus (Inside dan outside)	30	Low
R4.3	Akses jaringan terputus	Masalah konfigurasi fisik kabel lepas	18	Very Low
R1.3	Data hilang atau tidak tersedia	Kesalahan setting periode atau tahun ajaran pada aplikasi Siakad	14	Very Low
R1.1	Data dibobol dan di salah gunakan orang yang tidak berwenang	Akses menggunakan komputer umum yang dipasang aplikasi spy	10	Very Low
R3.1	Perubahan setting server	Data pada server di ketahui orang yang tidak berwenang	10	Very Low
R3.2	Server down	Data pada server di ketahui orang yang tidak berwenang	10	Very Low
R3.4	Koneksi internet putus	Serangan pemblokiran access point (hacker)	10	Very Low
R3.3	Server panas atau rusak	Listrik tidak stabil	7	Very Low

R4.2	Server panas atau rusak	Listrik tidak stabil	7	Very Low
R3.5	Sistem crash atau error	Serangan duplikasi alamat IP (hacker)	1	Very Low

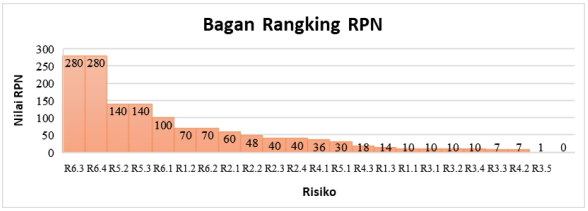
Sumber: Hasil Penelitian (2021)

Tabel 15. Jumlah Penilaian Risiko

Level RPN	Jumlah
Very High	2 Risiko
High	0 Risiko
Medium	3 Risiko
Low	8 Risiko
Very Low	9 Risiko

Sumber: Hasil Penelitian (2021)

Dari hasil pengkategorian level RPN diatas didapat level RPN dan jumlah risiko, kemudian RPN risiko diklasifikasikan dengan grafik batang pada bagan pareto untuk membantu menemukan permasalahan yang terpenting untuk segera diselesaikan nilai RPN bisa dilihat pada gambar berikut:



Sumber: Hasil Penelitian (2021)

Gambar 1. Bagan Rangking RPN

Berdasarkan hasil jawaban survei setiap tingkat organisasi yang diubah dalam bentuk angka sebagai indikator preferensi atau kecenderungan dari pilihan responden. Disimpulkan bahwa 75 persen atau lebih responden menjawab "ya" menyatakan bahwa praktik yang digunakan cukup tinggi dan menunjukkan praktik tersebut yang paling kemungkinan digunakan. Responden menjawab "Tidak" 75 persen atau lebih menyatakan bahwa suatu praktik tidak digunakan cukup tinggi dan menunjukkan bahwa praktik tersebut kemungkinan besar tidak digunakan. Kemudian "Tidak jelas" menyatakan tidak satu pun dari dua kriteria persentase "ya" dan "tidak" memenuhi ambang batas 75 persen. Artinya tidak jelas apakah praktiknya digunakan atau tidak ini menujukan kemungkinan beberapa orang di UPT.TIK XYZ menggunakan praktik ini sedangkan yang lain tidak. Beberapa hasil kecenderungan praktik keamanan bisa dilihat pada tabel berikut ini:

Tabel 16. Konsolidasi Hasil Survei

Kesadaran dan Pelatihan Keamanan: Hasil Survei			
Pernyataan Survei	*Kepala UPT.TIK*	*Staf Jaringan*	*Admin Database*
Anggota staf UPT. TIK XYZ memahami peran dan tanggung jawab keamanan mereka. Ini didokumentasikan dan diverifikasi.	Ya	Ya	Ya
Ada keahlian internal yang memadai untuk semua layanan, mekanisme, dan teknologi yang didukung (misalnya, logging, pemantauan, atau enkripsi), termasuk keamanan pengoperasian. Ini didokumentasikan dan diverifikasi.	Ya	Ya	Ya
Kesadaran akan keamanan, pelatihan, dan pengingat berkala disediakan untuk semua personel. Pemahaman staf didokumentasikan dan kesesuaian diverifikasi secara berkala.	Ya	Ya	Ya

Sumber: Hasil Penelitian (2021)

Selanjutnya berdasarkan hasil dari penanggung jawab aset dan risiko atau ancaman yang ada, didapat respon perlakuan terhadap risiko yang dilakukan dengan wawancara langsung dengan staf pemilik risiko respon risiko dapat dilihat pada tabel berikut ini:

Tabel 17. Jumlah Hasil Respon Risiko

Kode	Risiko	Respon Risiko
R6.3	Layanan sistem tidak tersedia	Hindari/Mitigasi
R6.4	Layanan internet tidak tersedia	Hindari/Mitigasi
R5.2	Akses koneksi internet ke *client* atau server terputus	Hindari/Mitigasi
R5.3	Rugi secara *finansial*, waktu, tenaga dalam perbaikan infrastruktur yang hancur	Hindari/Mitigasi
R6.1	Data tidak valid tanpa diketahui sebab atau jejak	Hindari/Mitigasi
R1.2	Data berubah	Hindari/Mitigasi
R6.2	Data tidak valid	Hindari/Mitigasi
R2.1	Akses sistem lambat atau tidak tersedia	Hindari/Mitigasi
R2.2	Tampilan halaman utama web berubah	Hindari/Mitigasi
R2.3	Data login diketahui orang yang tidak berwenang dan penyalahgunaan data	Hindari/Mitigasi
R2.4	Perubahan data LIRS, *login* dll	Hindari/Mitigasi
R4.1	Sistem error data terhapus atau tidak bisa disimpan	Hindari/Mitigasi
R5.1	Akses koneksi internet terputus	Hindari/Mitigasi
R4.3	Akses jaringan terputus	Hindari/Mitigasi
R1.3	Data hilang atau tidak tersedia	Hindari/Mitigasi
R1.1	Data dibobol dan di salah gunakan orang yang tidak berwenang	Hindari/Mitigasi
R3.1	Perubahan *setting* server	Hindari/Mitigasi

R3.2	Server *down*	Hindari/Mitigasi
R3.4	Koneksi internet putus	Hindari/Mitigasi
R3.3	Server panas atau rusak (jaringan)	Berbagi/Mitigasi

Sumber: Hasil Penelitian (2021)

Selanjutnya pemilihan praktik strategi dan praktik operasional dan sub kontrol yang disesuaikan dengan hasil jawaban kecenderungan praktik keamanan yang hasilnya "Tidak" yang berarti praktik tidak digunakan cukup tinggi ini menunjukan kemungkinan besar tidak digunakan dan "Tidak Jelas" yang berarti apakah praktiknya digunakan atau tidak ini menujukan kemungkinan beberapa orang di UPT.TIK XYZ menggunakan praktik ini sedangkan yang lain tidak yang berarti praktik di UPT.TIK. Hasilnya ada 10 bidang praktik dengan Pemilihan praktik strategi dan praktik operasional dan sub kontrol nya bisa dilihat tabel sebagai berikut:

Tabel 18. Memilih Praktik Strategis dan Praktik Operasional

No.	**Praktik Strategi/ Praktik Operasional**	**Sub Praktik Strategis/ Praktik Operasional**	**Hasil Kecenderungan Praktik Keamanan**		
			Kepala UPT. TIK	*Staf Jaringan*	*Admin Database*
1.	Strategi Keamanan (SP2)	Praktik strategi (SP2.3)	Ya	Ya	Tidak
2.	Kebijakan dan Peraturan Keamanan (SP4)	Praktik strategi (SP4.1)	Tidak	Ya	Tidak Jelas
		Praktik strategi (SP4.2)	Ya	Ya	Tidak Jelas
		Praktik strategi (SP4.3)	Ya	Ya	Tidak Jelas
		Praktik strategi (SP4.5)	Ya	Ya	Tidak Jelas
3.	Manajemen Keamanan Kolaboratif (SP5)	Praktik strategi (SP5.1)	Ya	Tidak Jelas	Ya
4.	Perencanaan Kontingensi / Pemulihan Bencana (SP6)	Praktik strategi (SP6.2)	Ya	Ya	Tidak Jelas
		Praktik strategi (SP6.3)	Ya	Ya	Tidak Jelas
5.	Keamanan Fisik (OP1) Rencana dan Prosedur Keamanan Fisik (OP1.1)	Praktik operasional (OP1.1.1)	Tidak	Tidak Jelas	Tidak Jelas
		Praktik operasional (OP1.1.4)	Ya	Tidak Jelas	Tidak Jelas
		Praktik operasional (OP1.1.5)	Ya	Tidak Jelas	Tidak Jelas
6.	Keamanan Fisik (OP1) Kontrol Akses Fisik (OP1.2)	Praktik operasional (OP1.2.2)	Ya	Tidak Jelas	Tidak Jelas
		Praktik operasional (OP1.2.4)	Ya	Tidak Jelas	Ya
7.	Keamanan Fisik (OP1) Pemantauan dan Audit Keamanan Fisik (OP1.3)	Praktik operasional (OP1.3.3)	-	Tidak Jelas	Ya
8.	Keamanan Teknologi Informasi (OP2) Pemantauan dan Audit Keamanan TI (OP2.3)	Praktik operasional (OP2.3.1)	-	Tidak Jelas	Ya
9.	Keamanan Staf (OP3) Manajemen Insiden (OP3.1)	Praktik operasional (OP3.1.2)	Tidak	Ya	Ya
		Praktik operasional (OP3.1.3)	Tidak	Ya	Tidak Jelas
10.	Keamanan Staf (OP3) Praktik Staf Umum (OP3.2)	Praktik operasional (OP3.2.3)	Ya	Ya	Tidak Jelas

Sumber: Hasil Penelitian (2021)

Rencana mitigasi risiko menggunakan standar internasional yaitu ISO/IEC 27001:2013 sebagai standar sistem manajemen keamanan yang disesuaikan berdasarkan risiko di UPT.TIK XYZ dan penyebabnya secara objektif. Penentuan klausul dan kontrol objektif bisa dilihat pada tabel berikut:

Tabel 19. Memilih Klausul dan Kontrol Objektif

Kode	**Risiko**	**Penyebab**	**Klausul**	**Kontrol Objektif**	**Sub Kontrol Objektif**
R6.3	Sistem layanan tidak sesuai	Masalah kesadaran keamanan dan penanganan masalah lambat	A.7 Keamanan Sumber Daya Manusia A.16 Manajemen insiden keamanan informasi	A.7.2 Selama Berkerja	A.7.2.2 Kesadaran, pendidikan dan pelatihan keamanan informasi
					A.7.2.3 Proses disipliner
				A.16.1 Manajemen insiden dan peningkatan keamanan informasi	A.16.1.1 Tanggung jawab dan prosedur

Sumber: Hasil Penelitian (2021)

Rekomendasi pengembangan praktik yang diberikan terdiri dari dua yaitu praktik strategis dan praktik operasional yang sudah dilakukan dengan menyesuaikan hasil survei sebelumnya. Rekomendasi yang dibuat sesuai dengan standar OCTAVE Katalog Versi 2.0 sebagai rencana mengembangkan strategis yang harus diterapkan beberapa rekomendasi pengembangan praktik UPT.TIK XYZ bisa dilihat pada tabel berikut:

Tabel 20. Pengembangan Praktik

Praktik Strategis Strategi Keamanan (SP2)	
SP2.3	Strategi, sasaran, dan tujuan keamanan didokumentasikan dan secara rutin ditinjau, diperbarui, dan dikomunikasikan kepada UPT.TIK XYZ.

Sumber: Hasil Penelitian (2021)

Selanjutnya mitigasi risiko dari pemilihan klausul dan kontrol objektif yang sudah dilakukan sebelumnya berdasarkan ISO/IEC 27001:2013 ditambah dengan rekomendasi implementasi dari klausul dan kontrol objektif berdasarkan ISO/IEC 27002:2013. Dilakukan dengan menyesuaikan penyebab dari masing-masing risiko untuk mengurangi risiko berdasarkan hasil identifikasi dan analisis risiko. Penjelasan mitigasi risiko yang dibuat bisa dilihat tabel berikut ini:

Tabel 21. Pengembangan Praktik

Kode Risiko	R6.3
Kategori	*People* (programmer)
Risiko	Sistem layanan tidak sesuai
Penyebab	Masalah kesadaran keamanan dan penanganan masalah lambat
Kontrol Objektif	**A.7.2.2 Kesadaran, pendidikan dan pelatihan keamanan informasi** Semua staf programmer dan, jika relevan, programmer kontrak harus menerima pendidikan dan pelatihan kesadaran yang sesuai dan pembaruan rutin dalam kebijakan dan prosedur UPT.TIK XYZ, yang relevan dengan fungsi pekerjaan mereka.
	A.7.2.3 Proses disipliner Harus ada proses disipliner formal dan yang dikomunikasikan kepada programmer untuk mengambil tindakan yang telah melakukan pelanggaran kebijakan yang sudah ditetapkan oleh UPT.TIK XYZ.
	A.16.1.1 Tanggung jawab dan prosedur Tanggung jawab dan prosedur manajemen harus ditetapkan pada setiap programmer untuk memastikan respons yang cepat, efektif dan teratur terhadap insiden keamanan informasi atau masalah sistem layanan yang dilaporkan ke pihak UPT.TIK XYZ terkait masalah sistem layanan.
Implementasi	1. Menjalankan dan mengembangkan program pendidikan dan pelatihan keamanan informasi yang dilakukan secara berkala untuk meningkatkan kepedulian (*awareness*) programmer. 2. Adanya proses mendisiplinkan formal terhadap pelanggaran yang dilakukan secara benar dan adil bagi programmer. 3. Buat prosedur untuk perencanaan dan persiapan tanggap insiden untuk programmer. 4. Buat prosedur untuk memantau, mendeteksi, dan melaporkan kejadian dan insiden. Buat prosedur untuk mencatat kegiatan manajemen insiden oleh programmer. 5. Buat prosedur untuk respons pemulihan terkontrol dari suatu insiden dan komunikasi.

Sumber: Hasil Penelitian (2021)

5. Validasi potensi penerapan rekomendasi praktik keamanan dan mitigasi risiko

Selanjutnya melakukan pengujian atau validasi potensi penerapan dengan memastikan bahwa rekomendasi pengembangan praktik dan mitigasi risiko sesuai dengan kondisi dan harapan UPT.TIK XYZ dapat dilihat pada tabel berikut:

Tabel 22. Pengujian Rekomendasi Pengembangan Praktik

No	**Strategi Praktik (SP) / Strategi Operasional (OP)**	**Sub Strategi Praktik (SP) / Strategi Operasional (OP)**	**Tujuan**	**Potensi Penerapan**
1.	Strategi Keamanan (SP2)	Praktik strategi (SP2.3)	Strategi, sasaran, dan tujuan keamanan didokumentasikan dan secara rutin ditinjau, diperbarui, dan dikomunikasikan kepada Organisasi.	Dapat diterapkan UPT. TIK XYZ dengan menyusun praktik strategi, sasaran dan tujuan keamanan yang dilakukan untuk dibagikan dan dikomunikasikan kepada setiap staf agar mengerti.

Sumber: Hasil Penelitian (2021)

Tabel 23. Pengujian Rekomendasi Mitigasi Risiko

No	**Kontrol Objektif**	**Sub Kontrol Objektif**	**Tujuan**	**Implementasi**	**Potensi Penerapan**
1	A.5.1 Arahan manajemen untuk kea	A.5.1.1	Serangkaian kebijakan untuk keamanan informasi terkait perizinan pembanguna n yang	Membuat kebijakan strategi bisnis, peraturan, perunda	Dapat diterapkan UPT. TIK dengan menyusun dokumen terkait

	man an infor masi		melibatkan aset XYZ, ganti rugi yang melibatkan kerusakan infrastruktur jaringan internet XYZ dan data nilai harus ditetapkan, disetujui oleh manajemen, dipublikasikan dan dikomunikasikan kepada staf UPT.TIK XYZ dan pihak eksternal terkait.	ng-undangan dan kontrak, lingkungan ancaman yang mendefinisikan keamanan informasi, tujuan dan prinsip yang memandu kegiatan yang berkaitan dengan keamanan aset terkait pembangunan.	kebijakan terkait strategi bisnis dan kebijakan untuk keamanan informasi dan aset terkait pembangunan yang melibatkan aset XYZ, ganti rugi dll.

Sumber: Hasil Penelitian (2021)

KESIMPULAN

Kesimpulan dari penelitian ini yang sudah dilakukan identifikasi aset kritis diperoleh 19 risiko dan 22 kejadian ancaman dengan demikian terdapat risiko yang memiliki kejadian ancaman lebih dari satu karena memiliki lebih dari satu dampak. Kemudian dari proses identifikasi pengetahuan juga dilakukan survei terkait praktik yang digunakan di UPT.TIK XYZ menggunakan standar OCTAVE yang dilakukan dengan beberapa perwakilan diperoleh 10 praktik keamanan yang memiliki jawaban hasil "Tidak" dan/atau "Tidak Jelas". "Tidak" yang berarti praktik tidak digunakan cukup tinggi ini menunjukan kemungkinan besar tidak digunakan dan "Tidak Jelas" yang berarti apakah praktiknya digunakan atau tidak ini menujukan kemungkinan beberapa orang di UPT.TIK XYZ menggunakan praktik ini sedangkan yang lain tidak yang berarti praktik di UPT.TIK.

Selanjutnya dari hasil penilaian RPN menggunakan FMEA dikategorikan ke empat level penilaian risiko *very high* memiliki 2 risiko dengan nilai RPN sebesar 280, *high* memiliki 0 risiko, *medium* memiliki 3 risiko dengan nilai RPN sebesar 100-140, *low* memiliki 8 risiko dengan nilai RPN sebesar 30-70 dan *very low* memiliki 9 risiko dengan nilai RPN sebesar 1-18.

Kemudian dari hasil survei praktik terdapat 10 praktik strategi (SP) atau praktik operasional (OP) dalam OCTAVE Katalog Versi 2.0 yang dijadikan acuan standar. Rekomendasi Pengembangan Praktik atau praktik yang harus dikembangkan di UPT.TIK XYZ seperti strategi keamanan (SP2), kebijakan dan peraturan keamanan (SP4), manajemen keamanan kolaboratif (SP5), perencanaan kontingensi atau pemulihan bencana (SP6), rencana dan prosedur keamanan fisik (OP1.1), kontrol akses fisik (OP1.2), pemantauan dan audit keamanan fisik (OP1.3), pemantauan dan audit keamanan TI (OP2.3), manajemen insiden (OP3.1), dan praktik staf umum (OP3.2).

Dari hasil identifikasi risiko terdapat 10 kontrol dan 26 klausul dalam ISO 27001:2013 dan ISO 27002:2013 yang dijadikan acuan standar rekomendasi mitigasi risiko dan implementasi seperti A.5 kebijakan keamanan informasi, A.6 organisasi keamanan informasi, A.7 keamanan sumber daya manusia, A.9 akses kontrol, A.10 kriptografi, A.11 keamanan fisik dan lingkungan, A.12 keamanan operasi, A.13 keamanan komunikasi, A.15 hubungan pemasok, dan A.16 manajemen insiden keamanan informasi.

REFERENSI

AIAG-VDA Failur Mode And Effects Analysis (FMEA) Handbook First Edition. (2017). Southfield: AIAG.

Carlson, C. S. (2014). *Understanding and Applying the Fundamentals of FMEAs.* Tucson: AR&MS Tutorial Notes.

FMEA Handbook Version 4.2. (2011). Dearborn: Ford Motor Company.

FMEA HANDBOOK VERSION 4.2. (2011). DEARBORN: Ford Motor Company.

ISO/IEC 27001 Information Technology Security Techniques Information Security Management System Requirements. (2013). Switzerland: ISO/IEC 2013.

ISO/IEC 27002 Information technology Security techniques Code of practice for information security. (2013). Switzerland: ISO/IEC 2013.

Putri, A. H., & Kusumawati, Y. (2017). Strategi Mitigasi Risiko Aset Kritis Teknologi Informasi . *Techno.COM*, Vol. 16, No. 4, November 2017 : 367-3777.

Stebbins, E. J., & Turgeon, A. (2018). *Guide to Risk Assement and Response.* Wheelock : The University of Vermont.

Vacca, J. R. (2017). *Computer and Information Security Handbook Third Edition.* Cambridge: Morgan Kaufmann.