Journal of Information Technology and Computer Science (INTECOMS)
Volume 3 Nomor 2, Desember 2020
e-ISSN : 2614-1574
p-ISSN : 2621-3249

ANALISIS MANAJEMEN RISIKO IT DAN KEAMANAN ASET MENGGUNAKAN METODE OCTAVE-S

IT RISK MANAGEMENT ANALYSIS AND ASSET SECURITY USING OCTAVE-S METHOD

Arif Fathur Rohman, Awalludiyah Ambarwati, Eman Setiawan
Sistem Informasi, Fakultas Ilmu Komputer, Universitas Narotama
arif.fathur@mhs.fasilkom.narotama.ac.id

ABSTRACT

This study aims to determine the analysis results of IT risk management and asset security using Octave-S method at Vocational High School Raden Paku Wringinom. This study uses a literature study approach. The literature study was carried out by looking for references on information technology risk management analysis using the OCTAVE-S method, books related to research material, and research journals as support for the writing of this research proposal. Theory taken from the reference, especially about OCTAVE-S method. Preliminary research data were collected from observations and interviews about the story of events that occurred in 2019, namely the TU (Administration) office which spent several Personal Computers (PCs) and important documents in it. The results of this study are related to the risk mitigation process that the researchers carried out on Vocational High School Raden Paku Wringinom, it was obtained 8 risks and 20 incidents of risk that could have more than one risk event due to different causes. The results of the assessment that have been carried out are concluded in a category, i.e very high, high, medium, low, very low. Very high, at this level the researcher has 4 risks with the highest RPN of 94.The low level has 2 risks with the highest RPN of 32. Very low has the risk of having 8 controls that the researcher input according to the ISO 27001 standard which can be used as a reference for recommendations of risk mitigation.

***Keywords**: Asset Security, Risk Management, Octave-S method*

ABSTRAK

Penelitian ini bertujuan mengetahui hasil analisis manajemen risiko IT dan keamanan aset menggunakan metode Octave-S di SMK Raden Paku Wringinanom. Penelitian ini menggunakan pendekatan studi literatur. Studi literatur dilakukan dengan mencari referensi tentang analisis manajemen risiko teknologi informasi menggunakan metode OCTAVE-S, buku yang terkait materi penelitian, dan jurnal penelitian sebagai pendukung pada penulisan proposal penelitian ini. Teori yang diambil dari refensi terutama tentang metode OCTAVE-S. Data awal penelitian dikumpulkan dari hasil observasi dan wawancara tentang cerita kejadian yang telah terjadi pada tahun 2019 yaitu kebakan pada kantor TU (Tata Usaha) yang menghabiskan beberapa Personal Computer (PC) dan dokumen penting di dalamnya. Hasil penelitian ini terkait proses mitigasi risiko yang peneliti lakukan terhadap Sekolah Menengah Kejuruan Raden Paku Wringinanom diperoleh 8 risiko dan 20 kejadian dari risiko yang dapat memiliki kejadian risiko lebih dari satu dikarenakan berbedanya penyebab yang ada. Pada hasil penilaian yang telah dilakukan disimpulkan pada sebuah kategori yaitu sangat tinggi, tinggi, sedang, rendah, sangat rendah. Sangat tinggi, pada level ini peneliti memiliki 4 risiko dengan RPN tertinggi sebesar 94. Level rendah memiliki 2 risiko dengan RPN tertinggi sebesar 32. Sangat rendah memiliki risiko terdapat 8 kontrol yang peneliti masukan sesuai dengan standar iso 27001 di mana dapat dijadikan sebuah acuan untuk rekomendasi dari mitigasi risiko.

Kata Kunci: Keamanan Asset, Manajemen Risiko, Metode Octave-S.

PENDAHULUAN

Komputasi bagi proses bisnis perusahaan, instansi pemerintahan, maupun pendidikan dirasa cukup membantu dalam menyelesaikan kegiatan yang mereka jalankan. Terdapat kelebihan dan kelemahan (TI) Teknologi informasi di setiap masing-masing

perusahaan maupun sekolah. Beberapa kelemahan TI seperti dari hilangnya data, virus dan ancaman keamanan aset TI tersebut(Setyawan & Wijaya, 2018). Bencana merupakan salah satu bentuk ancaman yang tidak bisa kita prediksi kapan terjadi, baik bencana alami maupun bencana yang secara tidak sengaja terjadi. Penyebab bencana atau risiko ini bermacam-macam, seperti bencana alami yang diakibatkan siklus alam dan bencana yang diakibatkan oleh suatu ancaman, baik ancaman yang bersumber dari alat itu sendiri maupun bersumber dari faktor manusia sebagai pengguna. Risiko dari bencana tersebut tetap memiliki kerugian bagi kelangsungan proses bisnis yang sedang dijalankan dengan tingkat dampak yang berbeda-beda, baik dampak pendek maupun dampak panjang(Nasution, 2020).

Instansi pendidikan seperti sekolah juga menerapkan komputasi dalam hal pembelajaran, pembayaran, maupun operasional sekolah. Beberapa alat komputasi yang dimiliki termasuk dalam aset TI. Terdiri mulai dari *hardware*, *software*, hingga manusia itu sendiri merupakan bagian aset bagi sebuah organisasi yang sebisa mungkin dilindungi. Sekolah Menengah Kejuruan Raden Paku Wringinanom adalah Sekolah yang berada di wilayah Wringinanom, Kabupaten Gresik. Sekolah Menengah Kejuruan Raden Paku berdiri pada tahun 2011 dan berada dalam naungan Yayasan Pendidikan Islam Raden Paku (YASPIRU). Dengan H. Fadkhur Rohman, S.Pd.I sebagai kepala sekolah saat ini. SMK Raden Paku memiliki empat bidang kompetensi keahlian yaitu, Teknik Komputer & Jaringan, teknik permesinan, teknik sepeda motor dan teknik instalasi tenaga listrik. SMK Raden Paku Wringinanom menggunakan infrastruktur TI dalam membantu proses belajar mengajar dan kegiatan operasional sekolah.

Di tahun 2019, Sekolah Menengah Kejuruan Raden Paku mengalami musibah kebakaran yang terjadi di ruang (TU) Tata Usaha yang menghabiskan *Personal Computer* (PC*)* yang berada di ruang tersebut. Data fisik maupun *digital* habis terbakar akibat peristiwa kebakaran tersebut. Kurangnya antisipasi dalam penanganan kejadian risiko seperti tidak adanya alat pemadam api ringan (APAR) di lokasi-lokasi infrastruktur TI dan belum adanya pencadangan (*back up*) data merupakan ancaman bagi SMK Raden Paku. Kebakaran merupakan salah satu bencana alami yang dapat mengancam peralatan komputer, yang dapat menyebabkan kehilangan data dan termasuk dalam salah satu wujud risiko(Santoso & Ernawati, 2017). Peristiwa yang berkaitan dengan ketidakpastian serta ancamaan atau bahaya yang bersifat merugikan merupakan risiko(Driantami & Suprapto, 2018).

Sekolah Menengah Kejuruan Raden Paku hingga saat ini belum pernah melakukan penilaian analisis risiko, serta minimya kebijakan yang jelas berkaitan dengan keamanan TI. Sehingga Sekolah Menengah Kejuruan Raden Paku tidak tahu pasti sampai sejauh mana kesiapan untuk menghadapi ancaman-ancaman yang ada. Tindakan untuk meminimalisir kemungkinan terjadinya risiko aset TI pada Sekolah Menengah Kejuruan Raden Paku perlu dilakukan, yaitu analisis manajamen risiko TI dan penyusunan dokumen SOP infrastruktur TI(Putra, dkk., 2019).

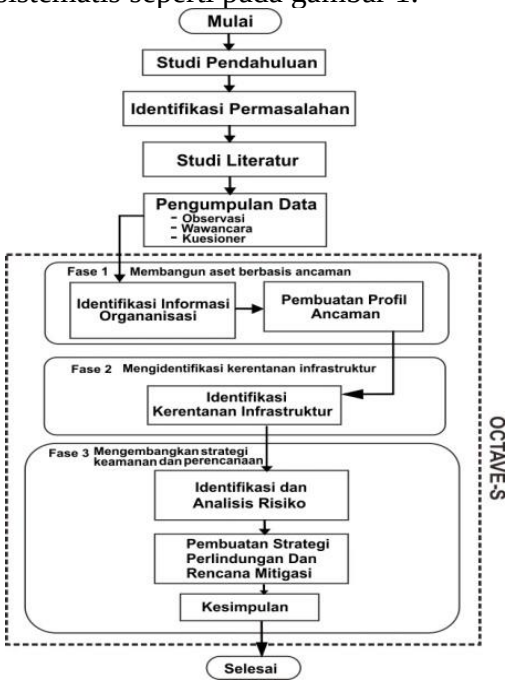
Banyak *framework* yang telah disediakan untuk menghadapi risiko-risiko ancaman yang kemungkinan terjadi bagi sebuah organisai. Salah satunya yaitu *Operationally Critical Threat, Asset, and Vulnerability*

Evaluation (OCTAVE) merupakan metode yang dapat digunakan untuk mengidentifikasi ancaman yang dapat menimbulkan risiko TI(Putri & Kusumawati, 2017). Dalam praktiknya OCTAVE-S juga dapat membantu dalam melakukan evaluasi risiko, identifikasi aset TI yang penting sesuai organisasi, juga melakukan identifikasi kerentanan dan ancaman terhadap aset TI tersebut serta melakukan evaluasi potensi jika ancaman tersebut terjadi(Moteff, 2005). Metode yang akan dipakai dalam penelitian ini yaitu OCTAVE-S(Setyawan & Wijaya, 2018). Metode OCTAVE-S yang telah di rancang khusus untuk organisasi yang terdiri dari sekitar 100 orang atau kurang. Dengan kondisi *existing* seluruh SDM SMK Raden Paku yang kurang dari 100. Oleh karena itu metode OCTAVE-S merupakan metode yang cocok bagi organisai dengan lingkup kecil. Dengan implemetasi dari hasil metode OCTAVE-S diharapkan dapat menghasilkan evaluasi risiko dari tiap aset TI yang dimiliki serta menghasilkan dokumen SOP infrastruktur TI berdasarkan hasil mitigasi risiko. Berdasarkan paparan data tersebut, peneliti tertarik membahas mengenai, "Analisis Manajemen Risiko IT dan Keamanan Aset Menggunakan Metode Octave-S (Studi Kasus: SMK Raden Paku Wringinanom)" dengan tujuan menjabarkan implementasi TI, identifikasi aset-aset TI dan profil risiko ancaman-ancaman yang kemungkinan terjadi, serta menghasilkan dokumen SOP terkait pemakaian infrastruktur TI yang teratur, sistematis, sesuai dengan kebijakan dan peraturan yang berlaku di Sekolah Raden Paku Wringinanom().

METODE

Alur Penelitian

Metodologi Penelitian dalam bentuk *flowchart* agar tahap pengerjaan penelitian dapat berjalan terarah dan sistematis seperti pada gambar 1.



Gambar 1. *Flowchart* Metodologi

Identifikasi Permasalahan

Pada tahap identifikasi masalah ini, peneliti melakukan wawancara dan observasi ke SMK Raden Paku Wringinanom untuk menganalisis risiko apa yang telah terjadi disana. Berdasarkan observasi dan wawancara awal yang dilakukan, peneliti mendapatkan cerita kejadian yang telah terjadi pada tahun 2019 yaitu kebakan pada kantor TU (Tata Usaha) yang menghabiskan beberapa *Personal Computer* (PC) dan dokumen penting di dalamnya.

Pendekatan Penelitian

Penelitian ini menggunakan pendekatan studi literatur. Studi literatur dilakukan dengan mencari referensi tentang analisis manajemen risiko teknologi informasi menggunakan metode OCTAVE-S, buku yang terkait materi penelitian, dan jurnal penelitian sebagai pendukung pada penulisan proposal penelitian ini. Teori yang diambil dari refensi terutama tentang metode OCTAVE-S.

Populasi dan Sampel Penelitian

Teknik Pengumpulan Data

Pada penelitian ini dilakukan pengumpulan data yang dibutuhkan seperti data primer dan data sekunder. Data primer diperoleh dari SMK Raden Paku Wringinanom terkait kejadian risiko yang pernah terjadi, profil, aset-aset yang digunakan dan visi dan misi SMK Raden Paku Wringinanom. Data sekunder yang dibutuhkan seperti jurnal, buku dan informasi yang berhubungan dengan analisis manajemen risiko TI dan keamanan aset menggunakan metode OCTAVE-S(Saputra, dkk., 2020).

Tahap-tahap pengumpulan data dilakukan dengan: (1) Observasi. Pada tahap ini peneliti melakukan survei langsung dengan mengunjungi SMK Raden Paku Wringinanom untuk melihat dan mengamati aset teknologi informasi yang digunakan, risiko yang pernah dialami dan bagaimana proses yang dijalankan pihak SMK Raden Paku Wringinanom dalam mendukung proses pembelajaran maupun operasional yang berlangsung. (2) Kuesioner. Kuesioner dilakukan dengan data angket pertanyaan terbuka dan pertanyaan tertutup dengan poin-poin pertanyaan dari OCTAVE–S agar dapat mengadaptasi lingkungan organisasi SMK Raden Paku Wringinanom. (3) Wawancara. Wawancara dilakukan untuk mengetahui masalah dan risiko yang pernah dialami SMK Raden Paku Wringinanom. Responden yang akan diwawancara meliputi Kepala Sekolah, Wakil Kepala Sekolah, Ketua Kurikulum, Kepala lab/staff TI, operator sekolah dan staff tata usaha. Pertanyaan yang diajukan terkait manajemen risiko teknologi informasi dan keamanan aset.

Analisis Data

Membangun Aset Berbasis Profil Ancaman

Fase pertama adalah membangun profil ancaman berdasarkan aset. Terdapat dua proses yaitu proses mengidentifikasi informasi organisasi dan proses pembuatan profil ancaman. Pada proses mengidentifikasi informasi organisasi terdapat tiga aktivitas.

Tahap analisis data pada penelitian ini yakni: (1) Aktivitas pertama yaitu menetapkan kriteria pengaruh evaluasi. Pada aktivitas ini terdapat sebuah aturan yang sudah ditetapkan sebagai acuan kriteria dan apa saja yang akan dievaluasi. (2) Aktivitas kedua yaitu mengidentifikasi aset organisasi. Mengidentifikasi aset-aset teknologi apa saja yang dimiliki SMK Raden Paku Wringinanom. (3) Aktivitas ketiga yaitu mengevaluasi pelatihan keamanan organisasi. Mengidentifikasi area praktik keamanan apa saja yang telah dilakukan pada SMK Raden Paku Wringinanom. Acuan area praktik kemananan telah di paparkan di panduan implementasi OCTAVE-S.

Pada proses kedua yaitu pembuatan profil ancaman yang terdapat tiga aktivitas yakni: (1) Aktivitas pertama yaitu memilih aset yang berharga, pada SMK Raden Paku Wringinanom yang berhubungan dengan informasi baik berupa data, *hardware, sofware,* jaringan maupun *user*. (2) Aktivitas kedua yaitu mengidentifikasi syarat-syarat keamanan untuk aset berharga. Identifikasi syarat-syarat berharga pada SMK Raden Paku Wringinanom adalah cara memberikan pengamanan pengamanan pada aset tersebut. (2) Aktivitas ketiga mengidentifikasi ancaman-ancaman untuk aset berharga. Pada aktivitas ini mencatat apa saja ancaman-ancaman yang sering terjadi pada beberapa aset dan juga sumber ancaman.

Data yang digunakan adalah hasil kuesioner dan hasil wawancara pada aktivitas OCTAVE–S. Hasil dari identifikasi aset, risiko dan ancaman dituliskan dalam *worksheet* OCTAVE-S.

Mengidentifikasi Kerentanan Infrastruktur

Pada fase kedua ini yaitu mengidentifikasi kerentanan infrastruktur teknologi informasi. Hanya terdapat satu proses saja dalam fase ini yaitu melakukan perhitungan aset kritis yang terkait dengan aset di SMK Raden Paku Wringinanom. Pada tahap berikut ini yang akan dilakukan yaitu menganalisa terkait kerentanan, infrastruktur dan jalur akses yang telah digunakan dalam mengakses data maupun informasi

Mengembangkan Strategi Keamanan dan Perencanaan

Fase ketiga, mengembangkan strategi keaman dan perencanaan. Terdapat dua proses yaitu (idetifikasi dan analisis risiko) dan (pembuatan strategi perlindungan dan rencana mitigasi).

Pada proses identifikasi dan analisis risiko terdapat tiga aktivitas. Aktivitas pertama yaitu mengevaluasi dampak-dampak dari ancaman. Pengaru-pengaruh yang terjadi dari ancaman yang dapat menimbulkan kerugian material maupun finansial, seperti sabotase atau penggunan aset tidak sesuai *job desk* masing-masing. Oleh karena itu harus dapat memininalkan risiko-risiko yang terjadi. Aktivitas kedua yaitu membangun kriteria evaluasi yang berkaitan erat dengan kejadian yang akan terjadi. Nilai kemungkinan ancaman diukur berdasarkan ukuran kualitatif (*high, medium, low*). Aktivitas ketiga mengevaluasi kemungkinan-kemungkinan ancaman berdasarkan frekuensi yang telah ditetapkan.

Kriteria ini berdasarkan waktu harian, mingguan, bulanan atau tahunan. Dari situ dapat ditemukan risiko yang dapat mengancam serta rekomendasi untuk meminimalkan risiko yang ada.

Pada proses kedua yaitu pembuatan strategi perlindungan dan rencana mitigasi. Data yang digunakan adalah hasil kuesioner dan hasil wawancara pada akvifitas OCTAVE–S. Tujuan dari akvifitas ini adalah mengevaluasi strategi keamanan orgnisasi dan membentuk perencanaan mitigasi risko. Evaluasi strategi keamanan berfokus pada perbaikan strategi yang dapat diterapkan oleh SMK Raden Paku Wringinanom. Perencanaan mitigasi risiko dilakukan dengan memodifikasi *worksheet* mitigasi risiko OCTAVE-S sesuai dengan kebutuhan di SMK Raden Waru Wringinanom(Prabawati, dkk., 2018).

HASIL DAN PEMBAHASAN

Hasil

Organizational View

Fase ini merupakan tahapan untuk membuat profil ancaman (threat profile) dengan cara menentukan aset yang penting bagi organisasi dan kebutuhan pengamanannya. Penentuan aset yang penting dilakukan melalui pengumpulan informasi tentang aset, kebutuhan keamanan, ancaman, dan kekuatan serta kelemahan organisasi. Hasil dari fase ini adalah pendefinisian kebutuhan keamanan informasi dan profil ancaman untuk aset-aset penting.

Daftar Aset Kritis

Penentuan aset yang penting dilakukan melalui pengumpulan informasi tentang aset, kebutuhan keamanan, ancaman, dan kekuatan serta kelemahan organisasi dari beberapa tingkatan manajemen yaitu operasional dan staf TU dapat dilihat pada tabel 4.1

Tabel 1. Aset Kritis Organisasi

No.	Aset	Kategori Aset
1.	Komputer	*Hardware*
2.	Server	
3.	Printer	
4.	Genset	
5.	Perangkat Jaringan	*Network*
6.	Kepala Staff IT	*People*

Kebutuhan Aset Kritis

Dalam sebuah keamanan informasi merupakan perlindungan dari setiap informasi dari segala ancaman yang mana akan memungkinkan terjadi guna memastikan keberlangsungan akan proses bisnis, memaksimalkan pengembalian investasi, meminimalisir risiko bisnis, memanfaatkan peluang yang ada. Tabel kebutuhan keamanan aset kritis dapat dilihat pada tabel 2 berikut:

Tabel 2. Kebutuhan Keamanan Aset Kritis

Aset Kritis	Kebutuhan Keamanan	Keterangan
Server	Integritas	Server tidak boleh diakses oleh pihak yang tidak berwenang
	Kerahasiaan	Hanya diakses oleh pihak tertentu
	Ketersediaan	Akses tersedia selama 24 jam penuh dalam 1 minggu, *maintenance* 2 jam sekali tiap minggu
Komputer & Printer	Kerahasiaan	Ketersediaan untuk akses oleh beberapa pihak seperti siswa, guru, dan staff
Genset	Ketersediaan	Dapat digunakan ketika dibutuhkan
	Integritas	Melakukan monitoring guna pemastian daya kerja ketika listrik anjlok
	Kerahasiaan	Hanya digunakan oleh pihak berwenang
Perangkat Jaringan	Integritas	Monitoring jaringan pada lingkup sekolah, memastikan semua dapat berkomunikasi dengan lancar
	Kerahasiaan	Adanya keamanan filtering IP Address guna memastikan tidak ada pelanggaran
	Ketersediaan	Terpasangnya alat monitoring peralatan jaringan agar selalu bisa dipergunakan
Kepala Staff IT Staff TU	Integritas	Staff IT memastikan sumber daya pada peralatan khususnya IT dan server berjalan dengan semestinya
	Kerahasiaan	Staff IT dan Staff TU menjaga bahwa karyawan tidak boleh memberikan akses kepada pihak yang tidak berkewenangan
	Ketersediaan	Kurangnya staff TU dalam melakukan managemen

Identifikasi Ancaman Terhadap Aset Kritis

Pada tahapan ini proses pengidentifikasi ancaman terhadap aset kritis merupakan gabungan dari semua informasi yang telah diperolah ketika proses identifikasi terhadap staff TU, dan staff IT kemudian membuat sebuah ancaman profil terhadap aset kritis, dapat dilihat pada tabel 2 berikut:

Tabel 2. Ancaman terhadap aset Kritis

Aset Kritis	Ancaman
Server	Kesalahan ketika konfigurasi
	Server overload
	Server dapat dibobol dan diakses oleh pihak yang bukan wewenangnya
	Memori server penuh
	AC dalam ruangan server bermasalah sehingga membuat temperature panas
Komputer, Printer	Perusakan peralatan
	Korosi, debu
	pencurian
	Terserang virus
	Maintenance yang kurang
Genset	Perusakan terhadap peralatan
	Maintenance yang kurang

Perangkat Jaringan	Kabel LAN digigit tikus
	Access Point rusak karena diserang semut
	Jaringan Lan lama
	Koneksi terputus
	Kesalahan pemberian alamat IP Address
Kepala Staff IT	SDM yang tidak memenuhi tanggung jawab
Staff TU	Penyalahgunaan jabatan

View Technological

Pada tahap ini dilakukannya pengidentifikasian proses bisnis dan profil ancaman terhadap aset kritis yang telah didukung oleh layanan teknologi informasi pada lingkup SMK Raden Paku Wringinanom dan identifikasi terhadap kelemahan dalam skala infrastruktur.

Identifikasi Kunci Komponen

Pada proses ini hanya berfungsi sebagai penggali informasi yang lebih detail lagi terhadap pelayanan teknologi dan informasi. Pada tahapan berikutnya merupakan *system of interest* merupakan sistem yang mana merupakan inti dari pada analisis risiko yang dilakukan, sistem yang menjadi inti dari setiap analisis risiko pada penelitian penulis ini berupa layanan teknologi dan informasi pada lingkup SMK. Dapat dilihat pada tabel 3 berikut :

Tabel 3. *System of Interest & Key Classes*

Layanan Teknologi Informasi	
System of interest	Pemantauan website sekolah pada SMK guna melakukan pemantauan informasi yang disediakan oleh pihak sekolah
Key classes of components	Data pengadaan barang yang ada pada smk
	Komputer
	Server
	Printer
	Perangkat Jaringan

Identifikasi Kerentanan Suatu Aset

Kerentanan merupakan kondisi di mana tidak adanya suatu prosedur keamanan, kontrol teknik, kontrol fisik atau lainnya yang dapat di eksploitasi oleh suatu ancaman lainnya. Kerentanan akan teridentifikasi berdasarkan *key classes of compinen* dan aset kritis. Tabel kerentanan aset dapat dilihat pada tabel 4 berikut.

Tabel 4. Kerentanan Asset

Aset	**Kerentanan**
Server	Beban kerja yang server lakukan terlalu tinggi
	listrik yang tidak stabil
	Konsleting listrik
Perangkat jaringan	Sambungan Kabel Lan yang buruk
	Manajemen jaringan yang tidak memadai (routing jaringan)
	Kualitas kabel kurang baik
	Tidak adanya pelindung kabel
Komputer	Pemeliharaan atau maintenance yang kurang
	Kurangnya penggantian komponen alat
	Korosi
Staff IT, Staff Tata Usaha	Seringnya absen karyawan
	Pelatihan terhadap teknologi dan informasi kurang memadai
	Kurangnya kesadaran karyawan akan keamanan yang ada
	Kurangnya kesadaran akan mekanisme pemantauan

Identifikasi Risiko

Pada tahapan ini merupakan tahapan di mana penilaian sebuah risiko melalui beberapa tahapan seperti penilaian risiko berserta mitigasi terhadap aset kritis terhadap teknologi dan informasi pada SMK, Raden Paku Wringinanom berikut merupakan penjelasan dari tahapan-tahapan identifikasi risiko.

Identification Potentional Cause

Pada tahapan ini merupakan tahapan di mana penyebab dari terjadinya risiko

dari identifikasi kerentanan serta ancaman dari aset informasi pada lingkup SMK Raden Paku Wringinanom yang telah penulis paparkan pada sub bab sebelumnya, tabel potentional cause dapat dilihat pada tabel 5 sebagai berikut.

Tabel 5. *Potential Cause*

Aset	Kerentanan	Ancaman	Potentional cause
Perangkat Keras: Komputer Server	1.Kurangnya pergantian perangkat keras secara rutin 2.kurangnya kesadaran dalam penerapan prosedur pemeliharaan	1.perusakan peralatan 2. Korosi, debu 3. penyadapan pada server	1. maintenance yang tidak teratur 2.Kerusakan fisik pada server
Perangkat pada jaringan	1.Sambungan kabel yang tidak teratur 2.ketahanan terhadap routing jaringan yang kurang memadai 3.sumber daya manusia yang kurang memadai	1.konektivitas jaringan lambat 2. Jaringan Lan yang buruk 3.koneksi terputus	1.kerusakan terhadap infrastruktur pada jaringan 2.gangguan dari provider yang terkadang lambat 3.kabel lan tergigit oleh tikus
Karyawan / Staff	Ketidak hadiran dari staff	Kekurangan tenaga kerja	Adanya karyawan yang kurang mematuhi aturan (share login)
	Pelatihan terhadap teknologi dan informasi yang kurang	Kesalahan menggunakan perangkat	Kurangnya kesadaran dalam penggunaan media IT
	Bekerja tanpa pengawasan	Pencurian barang	Kurangnya mekanisme dalam pemantauan keamanan

Identification risk

Setelah melalui tahapan sebelumnya selanjutnya hal yang perlu dilakukan adalah melalui tahapan identifikasi sebuah risiko di mana identifikasi ini bermaksud untuk mengetahui risiko-risiko apa saja yang dapat mengancam sebuah aset informasi dari pihak SMK. Risiko yang dimaksud merupakan kejadian di mana suatu kejadian tersebut bersinanggungan dengan probabilitas untuk terjadi bahkan yang sering terjadi baik disebabkan oleh faktor eksternal maupun faktor internal, yaitu dapat berupa gangguan umum, bencana alam, sosial dan gangguan operasional, tabel identifikasi risiko dapat dilihat pada tabel 6 sebagai berikut:

Tabel 6. Identification Risk

Aset	Cause Potential	Risiko
Perangkat keras : Server Komputer	Tidak teraturnya manajemen maintenance yang baik Server yang overheat sehingga merusak server Kerusakan pada fisik server	Kesalahan pada hardware (malfungsi)
	Konsleting listrik	Kebakaran
	Pemadaman pada listrik	Kegagalan pada sistem sumber tenaga listrik
	Kapasitas pada server yang tidak mampu menampung daya kebutuhan	Sumber memori dari server penuh
Perangkat jaringan (AP, Router, Kabel LAN)	Kurangnya mekanisme dalam pemantauan terhadap gangguan yang terjadi Gangguan pada provider yang mengakibatkan	Kegagalan dalam masalah internet

	gagalnya beberapa koneksi	
	Kesalahan dalam konfigurasi AP	
	Kabel LAN digigit tikus	
	AP dikerumuni Semut	
Staff atau karyawan	Tidak bijaknya karyawan melakukan pembagian share login	Penyalahgunaan hak pada karyawan maupun staff
	Tidak adanya pengaturan dalam manajemen hak akses	
	Kurangnya kesadaran terkait regulasi pada karyawan	Pelanggaran terhadap aturan karyawan di sekolah
	Kurangnya pemantauan terhadap karyawan	Pencurian informasi atau barang

Risk Assessment

Pada tahapan penilaian risiko merupakan penentuan tingkat dari 3 hal berikut yaitu *occutance, severity dan detection.* Pada tahapan penialain ini dilakukan dengan cara melakukan pendeskripsian pada informasi yang tadinya telah diterima kemudian diolah secara lebih dalam terhadap risiko yang telah dilakukan identifikasi sebelumnya. Pada hasil ini nantinya akan menghasilkan RPN yaitu *Risk priority number* di mana pada paramenet dari *occurance, severity* dan *detection*. Pada proses penilaian ini akan penulis terapkan metode perhitungan FMEA yaitu failur*e mode and effect analysis* di mana nantinya akan didapatkan sebuah risiko yang akan mempunyai nilai skor tertinggi hingga rendah. Penulis membaginya menjadi beberapa bagian nilai yaitu sangat tinggi, tinggi, sedang, rendah, sangat rendah RPN merupakan perkalian dari *rating Occurrence* (O), *Severity* (S) dan *Detectability* (D). Rumus RPN: RPN = O x S x D. Tabel skala RPN dapat dilihat pada tabel 7 berikut:

Tabel 7. RPN Skala

Skala	Level
>151	Sangat tinggi
100 - 150	Tinggi
51- 100	Sedang
20 – 50	Rendah
0 - 20	Sangat rendah

Setelah itu penulis akan menjelaskan skala level dari identifikasi risiko yang telah dibuat sebelumnya dapat dilihat pada tabel 8 berikut:

Tabel 8. Penilaian Terhadap Identifikasi Risiko

Risiko	Cause Potential	Sv	Oc	Dc	Rpn	Level
Kegagalan dalam hardware	Tidak teraturnya dalam melakukan maintenance	8	2	2	32	Rendah
	Server kelebihan beban	8	2	6	96	Sedang
	Kerusakan fisik pada perangkat keras	9	1	3	27	Rendah
Kegagalan pada software	Kesalahan saat melakukan coding pada software fungsional yang ada	6	3	4	72	Sedang
Kegagalan pada jaringan	Kecepatan pada koneksi internet lemah	9	5	8	360	Sangat Tinggi

	Tidak adanya mekanisme pemantauan	8	2	4	64	Sedang
Kegagalan pada sumber tenaga	Listrik padam	9	9	5	405	Sangat Tinggi
Tidak adanya backup data	Kurangnya kesadaran melakukan pencadangan data	5	5	5	125	Tinggi
Human error	Salah input data	4	4	4	64	Sedang
kebakaran	Konsleting listrik	9	2	6	108	Tinggi
Memori penuh	Kapasitas server kurang	9	7	2	108	Tinggi

Pembahasan

TI menjadi basis yang diperlukan bagi perusahaan untuk bertahan dalam persaingan bisnis. Banyak perusahaan mengubah sistemnya menjadi sistem terkomputerisasi. Sistem yang terkomputerisasi akan banyak memberikan manfaat bagi perusahaan seperti efisiensi sumber daya manusia, waktu dan anggaran, serta validitas dalam kinerja perusahaan serta dapat membantu manajemen dalam mengambil keputusan. Menurut Moteff (2005) penilaian risiko akan melibatkan integrasi ancaman, kerentanan, konsekuensi informasi, dan memutuskan bagaimana strategi untuk mengurangi risiko terjadi dan juga menginformasikan alokasi sumber daya yang hemat biaya untuk mengurangi risiko. Ada beberapa cara untuk mengurangi risiko yang terjadi dan setiap cara memberikan tindakan penanggulangan potensial yang mungkin ada untuk aset tertentu, analis harus melakukan kelayakan tindakan penanggulangan tersebut. Menurut Walewski (2003), penilaian risiko dapat berdampak pada struktur sekitarnya yang terdaftar dan dinilai sesuai dengan kemungkinan dan konsekuensinya dengan dianalisis, tindakan eliminasi dan penghitungan ulang pengukuran yang diadopsi.

Dari analisis pada identifikasi aset kritis maka selanjutnya adalah peneliti melakukan tahapan terakhir yaitu tahapan mitigasi risiko. Mitigasi risiko dilakukan dengan standar ISO 27001 di mana standar ini akan menghasilkan penliaian risiko dari beberapa kontrol secara objektif dari standar ISO 27001, beberapa rekomendasi kontrol yang telah peneliti berikan sesuai dengan risiko-risiko yang ada yaitu: (1) Tidak adanya *backup*. Biasanya data tidak dilakukan pencadangan karena memori atau kapasitas yang digunakan sudah tidak sanggup untuk menampung data terbaru sehingga dilakukannya Tindakan pencadangan secara berkala baik sehari sekali maupun dalam seminggu sekali sehingga pada kapasitas dapat termonitoring secara baik. (2) Identifikasi *human error*. Pada identifikasi kesalahan pada *human error* terutama pada pengoprasian sistem baik secara perangkat keras maupun pada perangkat lunak dapat menganggu kegiatan operasional maka perlu dilakukannya pelatihan pada keamanan informasi terhadap karyawan ataupun staff sehingga dapat memahami pentingnya keamaanan yang telah ditetapkan oleh pihak sekolah sehingga dapat mengurangi terjadinya kesalahan. (3) Identifikasi risiko kapasitas memori penuh. Terjadinya kapasitas penuh karena kurangnya dilakukannya pencadangan secara rutin, salah satu cara agar mengurangi risiko ini adalah dengan melakukan pencadangan secara berkala sehingga memori akan terasa lega kembali. (4) Identifikasi kegagalan

dalam perangkat keras. Kesalahan ini biasanya terjadi karena beberapa hal seperti virus, server yang terserang *malware* maupun *maintenance* yang tidak dilakukan secara rutin serta kesalahan konfigurasi yang dilakukan oleh para staf sehingga akan berdampak pada kehilangan data. Agar terhindar dari hal tersebut perlunya diterapkan pemeliharaan serta control yang berkala terhadap *hardware.* (5) Identifikasi kegagalan pada perangkat lunak. Pada kegagalan ini biasanya disebabkan oleh kurangnya para staf maupun karyawan yang kurang memahami, ataupun dapat terjadi karena kegagalan dari *coding* yang terjadi, ataupun serangan dari virus atau program yang tidak semestinya ada sehingga perlunya diterapkan pentingnya menggunakan antivirus yang tepat agar terhindar dari malware, virus, *trojan* serta *maleware* agar sesuai dengan standar prosedur. (6) Identifikasi pada kegagalan sumber daya tenaga. Penyebab dari gagalnya ini merupakan berasal dari kesalahan pada konsleting arus listrik yang berdampak pada kerusakan peralatan *hardware* ataupun PC dan *server* yang mati secara tiba-tiba dan menyebabkan hilangnya beberapa data, salah satu cara adalah dengan menerapkan perlindungan secara fisik dan penggunaan genset agar dapat menunjang pasokan sumber daya yang cukup agar dapat dilakukannya backup sebelum server atau PC mati total. (7) Identifikasi terhadap kegagalan jaringan. Penyebab kerusakan ini adalah berasal dari jaringan internal yang berdampak pada kegiatan operasional terhadap staff yang ada di mana para staff terhubung pada jaringan internet melalui kabel LAN dan internet terhenti maka perlunya dilakukan *control monitoring* secara rutin dan pemeliharaan keamanan pada sistem yang ditinjau secara rutin. (8) Identifikasi terhadap kebakaran. Penyebab dari risiko ini adalah hubungan arus pendek listrik dan terbakarnya genset yang berdampak tidak dapatnya staff mengoprasikan server dan perangkat hardware lainnya sehingga kegiatan operasional pada smk lumpuh dan memunculkan waktu serta biaya lebih untuk perbaikan sehingga perlunya Tindakan seperti perlindungan secara fisik dan peninjauan terhadap perangkat yang ada.

Menurut World Bank Group (1999), penilaian risiko ini akan menggabungkan eksposur dan respon untuk menghitung estimasi risiko seperti jumlah orang, yang diprediksi mengalami dan risiko menggambarkan ketidakpastian dalam perhitungan dan memberikan informasi lain untuk membantu hasil analisis. Penilaian risiko yang efektif harus memiliki ruang lingkup yang ditentukan dengan baik tergantung pada tujuan analisis, dan tujuan tersebut harus mengidentifikasi poin paling sehat dari orang-orang yang terkena dampak.

Elemen kunci dari setiap analisis risiko yang valid adalah memiliki prosedur untuk menentukan konsekuensi dan tingkat kemungkinan yang sesuai. Untuk penilaian risiko ini akan menggunakan pendekatan Octave-S sebagai metode. Menurut Alberts (2005), persiapan Octave-S penting untuk mensukseskan evaluasi, dan sebelum itu, ada beberapa faktor kunci keberhasilan: (1) mendapatkan sponsor manajemen senior untuk evaluasi (2) memilih tim analisis untuk memimpin evaluasi (3) menetapkan ruang lingkup evaluasi. Menetapkan pendekatan Octave-S membutuhkan pengembangan pemahaman bersama tentang evaluasi tujuan; tujuan ini dapat mengurangi risiko insiden besar di masa depan dan membantu menetapkan ekspektasi serta memberikan informasi berharga ketika tim analisis selanjutnya menetapkan ruang lingkup evaluasi yang bagus

digunakan teruma di SMK Raden Paku Wringinanom. Apalagi Octave-S dirancang untuk organisasi besar dan mengoptimalkan proses penilaian risiko keamanan informasi sehingga organisasi dapat memperoleh hasil yang memadai dengan investasi waktu yang kecil, orang dan sumber lain.

SIMPULAN

Berdasarkan paparan hasil di atas, peneliti lakukan ditarik beberapa buah kesimpulan antara lain: (1) Dari proses mitigasi risiko yang peneliti lakukan terhadap Sekolah Menengah Kejuruan Raden Paku Wringinanom diperoleh 8 risiko dan 20 kejadian dari risiko yang dapat memiliki kejadian risiko lebih dari satu dikarenakan berbedanya penyebab yang ada. (2) Pada hasil penilaian yang telah dilakukan disimpulkan pada sebuah kategori yaitu sangat tinggi, tinggi, sedang, rendah, sangat rendah: (a) Sangat tinggi. Pada level sangat tinggi peneliti memiliki 2 risiko dengan RPN tertinggi sebesar 405. (b) Tinggi. Pada level tinggi peneliti memliki 3 risiko dengan RPN tertinggi sebesar 125. (c) Sedang. Pada level sedang peneliti memiliki 4 risiko dengan RPN tertinggi sebesar 94. (d) Rendah. Pada level rendah peneliti memiliki 2 risiko dengan RPN tertinggi sebesar 32. (e) Sangat rendah. Pada level sangat rendah peneliti tidak memiliki kemungkinan terjadinya risiko dengan RPN yang dimiliki adalah 0. Dari hasil identifikasi risiko terdapat 8 kontrol yang peneliti masukan sesuai dengan standar iso 27001 di mana dapat dijadikan sebuah acuan untuk rekomendasi dari mitigasi risiko.

Rekomendasi yang dapat peneliti berikan terkait metode OCTAVE-S yang telah peneliti terapkan, karena keterbatasan akses yang peneliti lakukan karena pandemi yang sedang terjadi maka untuk penelitian selanjutnya diperlukannya pertimbangan guna melakukan penggalian informasi terhadap keseluruhan staff yang terlibat pada organisasi.

DAFTAR PUSTAKA

Alberts, C., Dorofee, A., Stevens, J., & Woody, C. (2005). *OCTAVE-S implementation guide, Version 1.0*. Manuel électronique. Pittsburg, PA,: Software Engineering Institute, Carbegie Mellon university.

Driantami, H. T. I., & Suprapto, A. R. P. (2018). Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 (Studi kasus: Sistem Penjualan PT Matahari Department Store Cabang Malang Town Square). *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer e-ISSN*, *2548*, 964X.

Moteff, J. (2005, February). *Risk management and critical infrastructure protection: Assessing, integrating, and managing threats, vulnerabilities and consequences*. Library of Congress Washington DC Congressional Research Service.

Nasution, M. H. (2020). Telaah Kritis Berbagai Risiko Sdm Dalam Mempertahankan Kelangsungan Perusahaan. *Jurnal BONANZA: Manajemen dan Bisnis*, *1*(1), 32-42.

Prabawati, V. A., Rachmadi, A., & Perdanakusuma, A. R. (2018). Analisis Risiko Teknologi Informasi Berbasis Risk Management Menggunakan Kerangka Kerja OCTAVE-S pada Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer Universitas Brawijaya. *Jurnal Pengembangan*

Teknologi Informasi dan Ilmu Komputer e-ISSN, 2548, 964X.

Putri, A. H., & Kusumawati, Y. (2017). Strategi Mitigasi Risiko Aset Kritis Teknologi Informasi Menggunakan Metode Octave Dan FMEA. *Techno. Com*, *16*(4), 367-377.

Saputra, R. R., Ambarwati, A., & Setiawan, E. (2020). Manajemen Risiko Teknologi Informasi Menggunakan Octave Allegro Pada PT. HD. Jurnal Sains dan Teknologi Industri, 17(1), 1-10.

Santoso, H. B., & Ernawati, L. (2017). Manajemen Risiko Pada Pusat Data Perguruan Tinggi Dengan Kerangka Kerja NIST 800-30 (Studi Kasus: Universitas Kristen Duta Wacana). *Jurnal Informatika Dan Sistem Informasi (JUISI) Universitas Ciputra*, *3*(02), 8-17.

Setyawan, A. A., & Wijaya, A. F. (2018). Analisis Manajemen Risiko Teknologi Informasi Pada Diskominfo Kota Salatiga Menggunakan Metode Octave-S. *SESINDO 2018*, 2018.

Walewski, J., & Gibson, E. G. (2003). *International Project Risk Assessment: Methods. Procedures, and Critical Factors, Center Construction Industry Studies Report, 31*.

World Bank Group. (1999). *Comparative Risk Assesement*, in Pollution Prevention and Abatement Handbook pp 45-53.