

Modul Manajemen Risiko TI

APA ITU RISIKO TI?

Salah satu tugas di Subbag Perencanaan dan Kebijakan Teknologi Informasi adalah Pengelolaan Risiko Teknologi Informasi (TI). Bagi yang masih awam terhadap istilah Risiko TI, berdasarkan pengalaman dan pengetahuan dasar yang pernah diterima, kami akan coba untuk menjabarkan secara umum apa itu Risiko TI.

Risiko atau *Risk* dalam organisasi sering disandingkan dengan sebuah kesempatan, sehingga risiko dan kesempatan bagaikan mata uang dengan sisi yang berbeda. Semua organisasi harus melakukan pengelolaan risiko agar tujuan organisasi dapat tercapai. TI merupakan bagian dari organisasi, tentunya memiliki risiko-risiko baik dalam bentuk aset, proses bisnis, tentunya akan menjadi risiko dari bisnis. Jika dibiarkan tidak diatur, ketidakpastian dapat menyebar dengan cepat. Namun jika dikelola secara efektif, kerugian dapat dihindari dan pastinya ada manfaat yang akan diperoleh. Dalam Itjen saat ini, risiko memainkan peran penting. Secara efektif mengelola risiko adalah sebuah usaha yang sangat penting untuk kesuksesan organisasi.

Risiko TI

Risiko TI adalah komponen dari alam semesta keseluruhan risiko organisasi. Risiko lainnya contohnya risiko strategis, risiko lingkungan, risiko audit, risiko operasional dan risiko kepatuhan. Di banyak organisasi, risiko terkait TI dianggap komponen risiko operasional. Namun, risiko strategis dapat memiliki komponen TI, terutama di mana TI adalah *enabler* kunci dari inisiatif bisnis baru. Hal yang sama berlaku untuk risiko audit, di mana TI menjadi bagian dalam pelaksanaan pelaporan hasil audit. Seringkali, risiko TI (risiko yang terkait dengan penggunaan TI) terlupakan, padahal sebenarnya risiko TI sangat terkait dengan ketergantungan hirarkis di salah satu kategori risiko lain, dan juga TI memainkan peran sentral dalam organisasi sehingga dampak risiko TI terlalu besar untuk dapat diabaikan.

Ada beberapa dampak dari insiden risiko TI, dampak pertama secara signifikan merugikan pihak-pihak terkait baik internal maupun eksternal (*auditee*, pegawai unit eselon I lain, dan publik). Dampak selanjutnya dan yang lebih besar adalah dapat merusak reputasi Itjen, tidak hanya Bagian SIP sebagai unit pengelola TI namun juga Itjen secara umum.

Berdasarkan pengamatan kami, mayoritas risiko TI bukan karena masalah teknis, tetapi kegagalan proses pengawasan dan tata kelola TI Itjen, contohnya proses-proses pengambilan keputusan yang mengabaikan (baik sengaja maupun tidak) potensi konsekuensi pekerjaan dari risiko TI, serta kurangnya kesadaran pegawai Itjen terhadap risiko TI. Dalam hal ini, risiko TI bukan hanya masalah TI yang dipecahkan dengan teknologi dan keahlian pengelolaannya saja, namun inisiatif mitigasi risiko TI membutuhkan komitmen dari pimpinan organisasi termasuk berinvestasi dalam mengimplementasikan kontrol yang dibutuhkan.

Selanjutnya beberapa *framework* risiko yang dikenal di dunia TI antara lain *Risk IT* – ISACA, COSO, ISO 31000, ISO 27005 dan *framework* lain yang digunakan untuk TI. Pendekatan TI oleh ISACA dikenal dengan 3 domain pengelolaan resiko, terkait dengan *Governance*, Evaluasi dan Respon. Ketiga domain ini dikombinasikan dan dikomunikasikan untuk bisa mengelola resiko. *Framework* lain yang cukup terkenal adalah *COSO* dengan delapan pengelolaan komponen risiko, konteksnya adalah terkait dengan sifat dasar strategis, operasional, operasional dan *compliance*, komponen tersebut dikelola berdasarkan level-level di sisi *enterprise* atau sampai bisnis unit proses.

Manajemen Risiko TI

Sebagai bagian dari keamanan informasi, manajemen risiko adalah proses untuk mengidentifikasi risiko termasuk ancaman-ancaman terhadap kelangsungan Itjen dan bagaimana cara mengontrol ancaman-ancaman tersebut. Salah satu program dari manajemen risiko adalah pembuatan dan penerapan *contingency planning*. Sebelum berbicara *contingency planning* secara lebih dalam, maka harus dipahami dulu konsep manajemen risiko.

Proses untuk mengidentifikasi risiko dan mengontrol risiko yang mungkin akan terjadi disebut manajemen risiko. Jika risiko adalah kejadian yang dapat berdampak positif atau negatif pada suatu kegiatan, maka manajemen risiko TI adalah proses mengidentifikasi, menganalisa dan mengantisipasi risiko yang ditimbulkan dari pemanfaatan TI. Adapun prinsip dasar dari manajemen risiko ada yang bersifat proaktif (melakukan antisipasi, mengatasi penyebab, menyiapkan beberapa rencana penanggulangan terhadap kemungkinan-kemungkinan yang akan terjadi), bersifat kolektif (melibatkan semua pihak dan mempunyai tanggung jawab masing-masing dalam proses manajemen risiko), bersifat partisipatif (yang secara terbuka membahas potensi- potensi yang dapat terjadi agar kegiatan atau proyek dapat berjalan lancar), dan bersifat iteratif (belajar dari pengalaman kejadian yang sudah terjadi dan menjadikan evaluasi risiko untuk kedepannya).

Tujuan dari manajemen risiko TI ini adalah meminimalisir kerugian–kerugian yang dapat ditimbulkan dari pemanfaatan TI dan dapat meningkatkan keuntungan serta peluang dalam pemanfaatan TI.

Manajemen risiko TI merupakan tanggung jawab bersama, pimpinan TI harus dapat menjelaskan kepada pimpinan organisasi tentang konsekuensi risiko TI. Dan pimpinan TI harus menciptakan mekanisme pengambilan keputusan yang memungkinkan pembahasan risiko TI dari persepektif proses bisnis Itjen.

Adapun ruang lingkup dari proses manajemen risiko yaitu penentuan konteks atau objek yang akan dikelola risikonya, identifikasi risiko, analisis risiko, evaluasi risiko, pengendalian risiko, pemantauan dan telaah ulang, serta koordinasi dan komunikasi.

Penentuan Konteks Atau Objek Yang Akan Dikelola Risikonya

Kriteria informasi dari COBIT dapat digunakan sebagai dasar dalam mendefinisikan objektif TI. Terdapat tujuh kriteria informasi dari COBIT yaitu : *effectiveness, efficiency, confidentiality, integrity, availability, compliance, dan reliability.*

Identifikasi Risiko

Hingga saat ini, Subbag Perencanaan dan Kebijakan Teknologi Informasi sedang mengidentifikasi atau mengurai resiko, identifikasi risiko itu sendiri merupakan proses untuk mengetahui resiko. Sumber resiko bisa berasal dari :

- Manusia, proses dan teknologi
- Internal (dari dalam perusahaan) dan eksternal (dari luar perusahaan)
- Bencana (hazard), ketidakpastian (uncertainty) dan kesempatan (opportunity).

Dari ketiga sumber resiko tersebut dapat diketahui kejadian-kejadian yang dapat mengganggu perusahaan dalam mencapai objektifnya.

Analisis Risiko

Setelah diketahui apa saja risiko yang dapat terjadi, selanjutnya analisis tiap risiko apakah risiko itu akan berdampak sangat besar atau kecil dan apakah risiko tersebut dapat merugikan suatu organisasi.

Evaluasi Risiko

Lakukan evaluasi dari risiko–risiko yang sudah pernah terjadi, agar tidak terjadi lagi di masa sekarang maupun masa depan.

Pengendalian Risiko

Membuat sebuah rencana penanggulangan sebelum risiko terjadi, dan mengendalikan risiko yang telah terjadi. Dapat berupa implementasi mekanisme kontrol yang terintegrasi dalam prosedur kegiatan. Alternatif tindakan yang bisa dipilih : *accept* (terima jika masih dalam toleransi organisasi atau *risk appetite*), *avoid* (hindari dengan membatasi lingkup kegiatan), *transfer* (alihkan kepada

pihak lain termasuk dengan *outsourcing/subcontract/purchase* atau dengan asuransi), *mitigate* (menerapkan mekanisme untuk menurunkan peluang terjadinya atau meminimalisasi dampaknya sampai batas yang dapat ditolerir), *contingency* (menerapkan prosedur penanggulangan untuk meminimalkan dampak).

Pemantauan dan telaah ulang

Selalu melakukan pemantauan terhadap segala kegiatan. Misalnya kelambatan proses, peningkatan jumlah gangguan, jumlah pengerjaan ulang, dsb.

Koordinasi dan Komunikasi

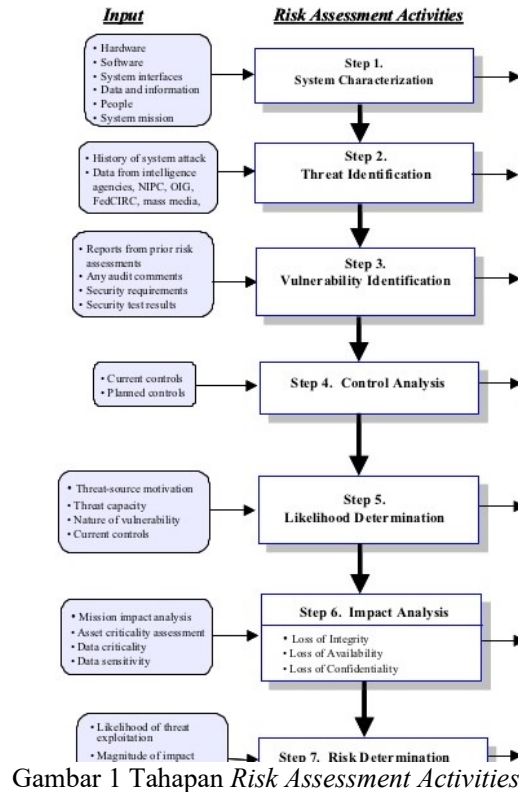
Selalu melakukan koordinasi dan komunikasi pada semua pihak yang bertanggung jawab terhadap kegiatan tersebut.

Konsep Manajemen Risiko IT Pada Organisasi

Menurut Emmett J. Vaughan dan Therese Vaughan dalam bukunya yang berjudul *Fundamentals Of Risk and Insurance* menyatakan bahwa *Risk Manajement* atau Manajemen risiko adalah : Manajemen risiko merupakan sebuah pendekatan ilmiah atau proses yang dilakukan untuk mengenali dan mengelola kejadian-kejadian atau risiko yang mungkin akan muncul serta membantu pemahaman organisasi tentang evaluasi penanganan risiko yang tepat sehingga meningkatkan kemungkinan peluang sukses dan mengurangi tingkat kegagalan.

Tahapan *Risk Management*

Risk assessment adalah proses pertama dalam melakukan manajemen risiko. Organisasi menggunakan penilaian risiko untuk mengetahui tingkat ancaman potensial dan risiko yang terkait dengan sistem TI secara keseluruhan. *Output* dari proses ini membantu mengidentifikasi pencegahan yang tepat untuk mengurangi atau menghilangkan risiko selama proses mitigasi risiko. Tahapan *Risk Assessment* terdiri dari sembilan tahapan utama, dapat di lihat pada Gambar 1



Risk Mitigation

Merupakan tahap kedua dari proses manajemen risiko yang dikeluarkan NIST melibatkan prioritisasi, evaluasi dan implementasi rekomendasi dari kontrol pengurangan risiko dari tahapan sebelumnya yaitu penilaian risiko.

Contoh Implementasi Manajemen Risiko pada Organisasi Menggunakan COBIT 5

1. Tahap Perencanaan

Langkah awal dari penelitian ini adalah melakukan tahap perencanaan, tahap perencanaan terdiri dari dua yaitu merumuskan masalah dan studi literatur. Merumuskan masalah dilakukan perumuskan permasalahan yang terjadi terkait dengan manajemen risiko TI. Dengan adanya perumusan masalah, maka akan menjadikan panduan untuk penelitian ini agar mendapatkan tujuan akhir seperti yang diharapkan. Studi literatur, pada tahap ini dilakukan studi dari berbagai pustaka yang relevan dengan kajian tesis.

2. Tahap Analisis Sistem Berjalan

Pada tahapan ini dilakukan observasi dan wawancara dengan tanya jawab dan pembagian kuesioner kepada beberapa pengelola teknologi informasi dan pejabat struktural seperti kepala bidang yang bertanggung jawab pada pengelolaan teknologi informasi.

Setelah tahapan menentukan manajemen risiko menggunakan NIST SP 800-30 selesai, kemudian dilakukan pemilihan proses dengan menggunakan *mapping* COBIT 5, domain yang di pilih adalah *deliver, service, and support* (DSS). Domain DSS mempunyai fokus pengiriman data, layanan dan dukungan yang diberikan untuk sistem informasi yang efektif dan efisien. Domain DSS memiliki enam proses yaitu :

1) *DSS01 Manage Operation*

Pada proses ini mengkoordinasikan dan melaksanakan kegiatan dan prosedur operasional yang dibutuhkan untuk memberikan layanan TI bagi internal termasuk juga pelaksanaan prosedur standar operasi dan kegiatan pemantauan yang dibutuhkan.

2) *DSS02 Manage Service Request and Incidents*

Proses ini memberikan respon yang tepat waktu dan efektif untuk permintaan pengguna dan resolusi semua jenis kejadian.

3) *DSS03 Manage Problems*

Proses ini mengidentifikasi dan mengklasifikasikan masalah, apa penyebab masalah tersebut, dan memberikan solusi yang terbaik.

4) *DSS04 Manage Continuity*

Pada proses ini membangun dan memelihara rencana yang memungkinkan proses bisnis TI menanggapi kejadian dan gangguan sehingga dapat melanjutkan proses operasi, dan menjaga ketersediaan informasi pada organisasi.

5) *DSS05 Manage Security Services*

Pada proses ini melindungi dan mengidentifikasi tingkat risiko sistem informasi organisasi dan mempertahankan risiko keamanan yang dapat diterima organisasi sesuai dengan kebijakan keamanan. Untuk mencapai hasil manajemen risiko yang optimal maka di dalam tahap ini akan digabungkan dengan kerangka kerja NIST SP 800-30.

6) *DSS06 Manage Business Process Controls*

Pada proses ini mendefinisikan dan mempertahankan kontrol proses bisnis yang tepat untuk memastikan bahwa informasi memenuhi syarat pengendalian informasi yang relevan.

Dalam penelitian ini proses DSS05 akan dikolaborasikan dengan kerangka kerja NIST SP 800-30 untuk lebih mengoptimalkan manajemen risiko sistem TI yang ada di BPSDM Provinsi Jawa Barat serta dapat memberikan pemecahan masalah terkait risiko yang

berhubungan dengan operasional yaitu gangguan pada *hardware* dan sistem TI yang ada di BPSDM Prov Jabar.

3. Tahap Manajemen Risiko

Pada tahap ini dilakukan penilaian risiko untuk mengetahui tingkat ancaman potensial dan risiko yang terkait dengan sistem TI secara keseluruhan. *Output* dari proses ini membantu mengidentifikasi pencegahan yang tepat untuk mengurangi atau menghilangkan risiko selama proses mitigasi risiko.

4. Analisis

Dalam tahapan analisi ini akan dilakukan pengukuran proses yang dipilih dengan melakukan pemetaan *capability level* dan analisis gap. Tujuan dari proses ini adalah dengan diketahuinya *nilai capability level* maka akan terlihat nilai kondisi manajemen risiko TI BPSDM Prov Jabar saat ini. Kemudian dengan menggunakan analisis gap, maka level tersebut akan dibandingkan dengan level yang ingin dicapai.

5. Membuat Rekomendasi

Setelah semua tahapan selesai yaitu melakukan asesmen risiko, pemetaan, dan analisis gap, kemudian akan dilanjutkan ke tahap membuat rekomendasi untuk penerapan manajemen risiko TI yang lebih efektif dan dapat mencapai level yang diharapkan.

HASIL ANALISIS DAN PEMBAHASAN

1. Pemetaan NIST SP 800-30 dengan COBIT 5

domain DSS

Sesuai dengan permasalahan yang terjadi pada bab sebelumnya maka penelitian ini menggunakan NIST SP 800-30 dan COBIT 5. Kerangka kerja NIST SP 800-30 dipetakan pada proses domain DSS, yaitu proses DSS 05 *Manage security services* sebagai dasar dalam melakukan manajemen risiko serta evaluasi terhadap layanan TI saat ini. Hasil manajemen risiko dan mitigasi risiko dengan menggunakan kerangka kerja NIST SP 800-30 ini yang menjadi nilai tambah dalam pengukuran keberhasilan proses layanan TI yang ada di BPSDM Prov Jabar dalam sistem pendaftaran diklat secara online.

2. Risk Assessment (Penilaian Risiko)

a) System Characterization (Karakteristik Sistem)

System Characterization pada sistem teknologi informasi aplikasi pendaftaran secara online BPSDM Provinsi Jawa Barat meliputi : perangkat keras, perangkat lunak, peralatan jaringan, data/informasi, dan sebagainya.

Tabel 1 Klasifikasi karakter sistem BPSDM Prov Jabar

No.	Nama	Keterangan
1.	PC Bidbangdiklatjabar1	
2.	Server cent OS	
3.	Server jaringan	
4.	Wifi TP link cisco	
5.	Printer	
No	Nama Software	Keterangan
6.	Windows 8 .1	
7.	Ubuntu	
8.	Microsoft office	
9.	Database mysql dengan PHPmyadmin	
10.	Microsoft acces	
11.	Php myadmin	
12.	Antivirus smadav , avast	
No	<i>System Interfaces</i>	Keterangan
13.	Pendaftaran Diklat secara Online BPSDM Prov Jabar	
14.	Admin, <i>stakeholder</i> , calon peserta diklat, Staf	
15.	Untuk membantu calon peserta mendaftar untuk mengikuti diklat	

b) *Threat Identification* (Identifikasi Ancaman)

Pada tahap ini akan dilakukan identifikasi ancaman yang mungkin terjadi pada sistem dan lingkungannya. Sumber ancaman terbagi menjadi beberapa kategori, ancaman yang berasal dari alam, manusia, maupun teknologi.

Tabel 2 Identifikasi Ancaman

NO	Uraian Kejadian	<i>Threat Source</i>	Motivation	<i>Threat Action</i>
1	Pemadaman listrik secara mendadak menyebabkan server mati karena tidak ada sumber listrik cadangan	Teknologi <i>disaster</i>	Ketidak sengajaan	Tidak tersedianya UPS
2	AC di ruang server yang padam menyebabkan server <i>overheat</i> dan mati	Teknologi <i>disaster</i>	Ketidak sengajaan	Usia AC yang sudah tua sehingga terjadi kerusakan
3	AC di ruang server yang dimatikan	<i>Human disaster</i>	Ketidak sengajaan	Mematikan AC karena ketidaktahuan
4	Pencurian 2 buah komputer yang memiliki data-data penting	<i>Human disaster (Computer</i>	Faktor ekonomi	Tindakan pencurian dengan motif ekonomi

NO	Uraian Kejadian	<i>Threat Source</i>	Motivation	<i>Threat Action</i>
		<i>criminal</i>)		
5	Komputer terkena malware sehingga sistem <i>blank</i>	<i>Human disaster (insider)</i>	ketidaksengajaan	Komputer digunakan untuk mendownload sehingga terkena malware
6	Komputer terkena virus	<i>Human disaster</i>	ketidaksengajaan	Menggunakan <i>Flasdisk</i> untuk mengcopy data
7	<i>Hacker</i> pada saat lomba web dicurangi pesaing melakukan <i>hacking</i> supaya web dinas kalah dalam lomba	<i>Human Disaster (industrial espionage)</i>	Keunggulan kompetisi	Peretasan pada web yang sedang di lobbakan dengan merubah tampilan menu dalam web
8	Terputus jaringan kondisi eksisting	<i>Human disaster</i>	ketidaksengajaan	Akibat orang yang tidak tau dan kabel putus akibat tikus
9	Banjir karena daerah pelajar pejuang ketika hujan sering tergenang oleh air	<i>Natural disaster</i>		bisa mengakibatkan server mati mitigasi server harus benar-benar ditempat yang lebih aman
10	Gempa meskipun kota bandung jauh dari pantai tapi tetap ketika ada gempa besar kadang terkena dampaknya	<i>Natural disaster</i>		

c) *Vulnerability Identification* (Identifikasi Kerentanan)

Pada tahapan identifikasi kerentanan dilakukan proses identifikasi berdasarkan sumber-sumber ancaman dengan cara menganalisis kerentanan atau kelemahan yang dimiliki sistem informasi pendaftaran diklat secara online dan berpotensi terjadi di masa depan.

Tabel 3 Identifikasi Kerentanan

No.	<i>Theat Source</i>	<i>Vulnerability</i>	Keterangan
1	Virus	Anti Virus sudah diinstal tapi tidak pernah digunakan	Kemungkinan terjadinya sangat tinggi karena sering ada personil yang menggunakan <i>USB PC client</i>
2	Listrik mati	Tidak adanya cadangan sumber listrik (UPS)	Kemungkinan terjadinya tinggi karena bila server mati karena listrik mati maka akan terjadinya kerusakan dan kehilangan data
3	Malware	Belum ada penghalang malware	Kemungkinan terjadinya <i>low</i> karena jarang dilakukan <i>upgrade</i>
4	<i>Hacker</i>	Belum ada pencegahan supaya tidak terjadi <i>hacking</i>	Kemungkinan <i>medium</i> karena admin yang sudah tidak bekerja pernah

No.	<i>Theat Source</i>	<i>Vulnerability</i>	Keterangan
		ke sistem	memegang <i>password</i>
5	<i>Insider</i>	Masih banyak pegawai yang tidak paham atau tidak mengerti sama sekali tentang TI	Kemungkinan terjadi tinggi karena 80 % pegawai lulusan SMA, dan tidak bisa menjalankan perangkat komputer
6	Bencana banjir	Lokasi yang sering tergenang air	Kemungkinan terjadi sedang karena kantor punya pompa penyedot dan tanggul air
7	Kebakaran	masih ada yang merokok di dalam ruangan	Kemungkinan terjadi rendah karena sudah ada larangan merokok
8	Tikus (aliran listrik)	Pernah beberapa kali kabel listrik terputus digigit tikus	Meskipun jarang tetapi harus jadi perhatian karena jika kabel terputus sangat beresiko
9.	Jaringan internet mati	Sering terjadi pemutusan jaringan	Akibat terjadinya pemutusan jaringan internet maka terhambatnya koneksi internet yang menyebabkan sistem tidak bisa diakses

d) *Control Analysis* (Analisis Kontrol)

Pada tahap ini tujuan yang dihasilkan adalah identifikasi langkah-langkah kontrol apa saja yang dilakukan pada risiko yang telah teridentifikasi oleh langkah sebelumnya.

Tabel 4 Analisis Kontrol

No.	<i>Control</i>	Implementasi
1	Setiap ruangan simulasi dipasang <i>doorclock</i> yang menggunakan <i>finger print</i> maupun <i>access code</i>	Melakukan pemasangan <i>doorlock</i> dan memberikan akses kepada orang-orang yang berkepentingan
2	Ada larangan tidak boleh merokok dan makan diruangan tetapi tidak dalam bentuk tertulis dan tidak ada sangksi yang diberikan	Ketidakhahaman pegawai akan bahaya merokok sembarangan yang bisa terjadi kebakaran
3	Pemasangan lantai panggung di ruang server dari bahan yang didatangkan dari jerman untuk anti api	Ruang server lebih aman dari kebakaran karena lantai anti api tetapi hanya pada servernya saja, disisi yang lainnya menggunakan lantai panggung
4	Mengubah <i>password</i> secara rutin	Untuk melindungi komputer server maupun sistem yang lain untuk waktu yang akan datang wajib melakukan ganti <i>password</i> secara rutin supaya tidak siapa saja yang menggunakan komputer
5	Springkler	Ada 1 di depan ruang server

No.	Control	Implementasi
6	Tralis	Harus ada tralis yang melindungi ruang server untuk meningkatkan keamanan
7	UPS	UPS belum tersedia untuk membantu jika terjadi pemadaman listrik
8	Induksi	Induksi harus dilakukan untuk menjaga keamanan listrik
9	Atap belum pakai <i>aquaproof</i>	Atap masih banyak yang bocor ketika hujan besar, mitigasi menggunakan <i>aquaproof</i>

e) *Likelihood Determination* (Pengenalan Kecenderungan)

Pada langkah *Likelihood Determination* tujuannya adalah untuk menentukan derajat kemungkinan terjadinya suatu risiko dari sistem teknologi informasi. Derajat kemungkinan tersebut dibagi menjadi tiga, yaitu *High*, *Medium*, dan *Low*.

Tabel 5 Level Kemungkinan Risiko

No.	Risiko	Threat	Vulnerability	Risk likelihood evaluation	Keterangan
1	Virus	<i>PC client</i> atau <i>PC server</i>	Anti Virus sudah diinstal tapi tidak pernah digunakan	<i>High</i>	Kemungkinan terjadinya sangat tinggi karena sering ada personil yang menggunakan <i>USB PC client</i>
2	Listrik mati	<i>Server</i>	Tidak adanya cadangan sumber listrik (UPS)	<i>High</i>	Kemungkinan terjadinya tinggi karena bila server mati karena listrik mati maka akan terjadinya kerusakan dan kehilangan data
3	Malware		Belum ada penghalang malware	<i>Low</i>	Kemungkinan terjadinya <i>low</i> karena jarang dilakukan <i>upgrade</i>
4	<i>Hacker</i>	<i>Website, Server</i>	Belum ada pencegah <i>hacking</i> ke sistem	<i>Medium</i>	Kemungkinan <i>medium</i> karena admin yang sudah tidak bekerja pernah memegang <i>password</i>
5	<i>Insider</i>	SDM non IT	Masih banyak pegawai yang tidak mengerti sama sekali tentang TI	<i>High</i>	Kemungkinan terjadi tinggi karena 80 % pegawai lulusan SMA

No.	Risiko	Threat	Vulnerability	Risk likelihood evaluation	Keterangan
6	Bencana banjir	PC server	Lokasi yang sering tergenang air	Medium	Kemungkinan terjadi sedang karena kantor punya pompa penyedot dan tanggul air
7	Kebakaran		masih ada yang merokok di dalam ruangan	Low	Kemungkinan terjadi rendah karena sudah ada larangan merokok
8	Tikus (aliran listrik)	Kabel listrik	Pernah beberapa kali kabel listrik terputus digigit tikus	Medium	Meskipun jarang tetapi harus jadi perhatian karena jika kabel terputus sangat beresiko
9.	Jaringan internet mati	Jaringan	Sering terjadi pemutusan jaringan	Medium	Akibat terjadinya pemutusan jaringan internet maka terhambatnya koneksi internet yang menyebabkan sistem tidak bisa diakses

f) *Impact Analysis* (Analisis Dampak)

Tahapan *Impact Analysis* bertujuan untuk menentukan tingkat dari dampak risiko yang dihasilkan oleh kerentanan.

Tabel 6 Level Dampak Risiko

No.	Risiko	Impact	keterangan
1	Virus	Medium	Jika server terkena virus dan tidak bisa di cegah oleh antivirus maka dampaknya <i>medium</i> karena harus menginstal ulang server dan data beresiko hilang
2	Listrik mati	High	Jika terjadi pemadaman listrik dampaknya <i>high</i> karena server akan mati dan kemungkinan terjadi kerusakan dan kehilangan data akibat mati secara mendadak dan tidak terdapat sumber daya cadangan listrik seperti UPS.
3	Malware	Medium	Jika server terkena malware dampaknya <i>medium</i> karena sistem pendaftaran tidak dapat berjalan, sehingga calon peserta harus kembali mendaftar secara manual.
4	Hacker	Low	Kemungkinan sistem terkena <i>hack</i> dampaknya <i>low</i> karena hanya terdapat data yang umum
5	Insider	High	Dampak yang ditimbulkan tinggi, karena dengan tingkat pendidikan di kalangan staf hanya lulusan SMA dan sebagian lagi adalah orang-orang yang tidak paham tentang teknologi sehingga sangat beresiko terhadap sistem
6	Bencana banjir	Low	Karena terletak di daerah jalan pelajar pejuang dengan dataran yang cukup tinggi, walau terjadi hujan yang lebat kemungkinan untuk banjir sangat kecil

7	Kebakaran	<i>Low</i>	Bila terjadi kebakaran dampaknya rendah karena telah tersedia alat pemadam api dan juga jarak dinas kebakaran letaknya tidak begitu jauh
8	Tikus (aliran listrik)	<i>Medium</i>	Jika kabel listrik terputus akibat tikus dampaknya <i>medium</i> , tetapi untuk perbaikannya yang memerlukan usaha ekstra
9	Jaringan internet mati	<i>Medium</i>	Jika jaringan terputus maka dampaknya <i>medium</i> karena untuk memperbaikinya tinggal menghubungi teknisi dari pihak jaringan

g) *Risk Determination* (Penentuan Risiko)

Bertujuan untuk menentukan tingkat risiko pada sistem teknologi informasi.

Tabel 7 Level Risiko

No.	Resiko	Likelihood	Impact	Risk
1	Virus	<i>High (1.0)</i>	<i>Medium (50)</i>	<i>Medium</i> ($50 \times 1.0 = 50$)
2	Listrik mati	<i>High (1.0)</i>	<i>High (100)</i>	<i>High</i> ($100 \times 1.0 = 100$)
3	<i>Malware</i>	<i>Low (0.1)</i>	<i>Medium (50)</i>	<i>Low</i> ($50 \times 0.1 = 5$)
4	<i>Hacker</i>	<i>Medium (0.5)</i>	<i>Low (10)</i>	<i>Low</i> ($10 \times 0.5 = 5$)
5	<i>Insider</i>	<i>High (1.0)</i>	<i>High (100)</i>	<i>High</i> ($100 \times 1.0 = 100$)
6	Bencana banjir	<i>Medium (0.5)</i>	<i>Low (10)</i>	<i>Low</i> ($10 \times 0.5 = 5$)
7	Kebakaran	<i>Low (0.1)</i>	<i>Low (10)</i>	<i>Low</i> ($10 \times 0.1 = 1$)
8	Tikus (aliran listrik)	<i>Medium (0.5)</i>	<i>Medium (50)</i>	<i>Medium</i> ($50 \times 0.5 = 25$)
9	Jaringan internet mati	<i>Medium (0.5)</i>	<i>Medium (50)</i>	<i>Medium</i> ($50 \times 0.5 = 25$)

h) *Control Recommendation* (Rekomendasi Kontrol)

Pada tahapan ini bertujuan untuk memberikan rekomendasi pengendalian risiko yang dapat mengurangi atau menghilangkan risiko yang telah ditentukan pada tahap sebelumnya.

Tabel 8 Rekomendasi Kontrol

No.	Risiko	Risk level	Control Recommendations
1	Virus	<i>Medium</i>	a. Menginstal anti virus yang otomatis b. Menjadikan <i>USB port disable</i> sehingga tidak bisa menggunakan USB
2	Listrik mati	<i>High</i>	a. Memasang sumber listrik cadangan seperti

No.	Risiko	Risk level	Control Recommendations
			<i>uninterruptible power supply</i> (UPS) dan menyediakan genset.
3	<i>Malware</i>	<i>Low</i>	a. Menginstal malware b. Dilarang melakukan hal apapun pada komputer
4	<i>Hacker</i>	<i>Low</i>	a. Mengecek konten web setiap waktu
5	<i>Insider</i>	<i>High</i>	a. Memberi larangan kepada orang awan b. Menyeleksi petugas yang akan bekerja di server
6	Kebakaran	<i>Low</i>	a. Pelatihan menanggulangi kebakaran b. Penyediaan alat pemadam c. Pendeteksi otomatis jika ada api
7	Kabel putus	<i>Medium</i>	a. Dilarang mengganggu kabel b. Admin server selalu berjaga di kantor dan sering memeriksa
8	Banjir	<i>Low</i>	a. Memindahkan ruangan server b. Meninggikan lantai c. Membuat drynase d. Membuat saluran air
9	Jaringan internet mati	<i>Medium</i>	a. Menghubungi pihak teknisi dari penyedia jaringan

i) *Result Documentation* (Dokumentasi Hasil)

Tahap ini adalah tahap terakhir dari *risk assessment*, hasil dari proses *risk assessment* didokumentasikan kedalam bentuk sebuah laporan yang berisi strategi secara keseluruhan yang dimulai dari tahap karakterisasi sistem sampai tahap rekomendasi kontrol yang diperlukan. Sehingga nantinya akan bermanfaat untuk membantu membuat keputusan tentang kebijakan manajemen teknologi informasi di BPSDM Prov Jabar.

Mitigasi risiko

Proses kedua manajemen risiko adalah pencegahan risiko yang melibatkan sebuah prioritas, evaluasi, dan penerapan pengendalian dan pengurangan risiko yang sesuai untuk direkomendasikan dari proses penilaian risiko. Karena untuk menghilangkan semua risiko biasanya tidak praktis atau tidak mungkin. Pencegahan risiko merupakan tanggung jawab manajemen senior dan manajer fungsional untuk menerapkan kontrol yang paling tepat untuk mengurangi risiko misi ke tingkat yang dapat diterima, dengan meminimalkan dampak buruk pada sumber daya dan misi organisasi.

Proses Penilaian Level Kapabilitas COBIT 5

Untuk menentukan dan melakukan penilaian terhadap level kapabilitas setiap domain yang terdapat pada COBIT 5, maka masing-masing proses yang terdapat dalam domain tersebut diidentifikasi dan dianalisis secara bertahap, serta dinilai apakah proses tersebut telah memenuhi syarat untuk berada pada level tertentu atau belum, dimulai dari level 1 sampai level 5.

Tabel 9 Skala *Capability Level*

Kode	Deskripsi Skala	% Pencapaian
N	<i>Not Achieved</i>	0% - 15%
P	<i>Partially Achieved</i>	>15% - 50%
L	<i>Largely Achieved</i>	> 50% - 85%
F	<i>Fully Achieved</i>	>85% - 100%

Penilaian Level Kapabilitas Saat Ini

Proses yang pertama adalah DSS01 yang berfokus untuk mengkoordinasikan dan melakukan kegiatan operasional serta prosedur operasional yang diperlukan sistem untuk memberikan sebuah layanan TI secara internal, dan *outsorce*. Pada Tabel 10 dapat dilihat hasil perhitungan presentase kapabilitas dari domain DSS01 level 1.

Tabel 10 Nilai Kapabilitas Proses DSS01 Level 1

Proses	Pertanyaan	Jawaban	Konversi	Rata-rata	Dalam %
DSS01	P1	Ya	1	0,11	11%
	P2	Ya	1	0,11	11%
	P3	Ya	1	0,11	11%
	P4	Ya	1	0,11	11%
	P5	Ya	1	0,13	13%
	P6	Ya	1	0,08	8%
	P7	Ya	1	0,13	13%
	P8	ya	1	0,09	9%
			Total		86%

Proses DSS01 terdapat 8 pertanyaan yang ditunjukkan dengan kode P1 sampai P8, dari 10 responden yang memberikan jawaban rata-rata responden memberi jawaban “Ya”, dan sebagian memberikan jawaban “Tidak”. Konversi merupakan nilai atas jawaban kuesioner “Ya” bernilai 1 sedangkan “Tidak” bernilai 0. Nilai rata-rata diperoleh dari nilai konversi dibagi dengan total jumlah pertanyaan, kemudian dibuatkan dalam bentuk persen dan dilakukan proses pembulatan.

Hasil dari perhitungan kapabilitas level pada domain DSS01 level 1 memperoleh nilai 86% maka masuk dalam kategori *Fully Achieved* sehingga dapat dilanjutkan pada tahap perhitungan level 2.

Tabel 11 Penilaian DSS01 atribut proses PA 2.1 *Performance Management*

No	Responden	Nilai DSS01	Skala PA
1	R1	40	80%
2	R2	44	88%
3	R3	42	84%
4	R4	43	86%
5	R5	41	82%
6	R6	44	88%
7	R7	46	92%
8	R8	44	88%
9	R9	40	80%
10	R10	44	88%
Total		428	86%

Tabel 12 Penilaian DSS01 atribut proses PA 2.2 *Work Product Management*

No	Responden	Nilai DSS01	Skala PA
1	R1	40	80%
2	R2	41	82%
3	R3	43	86%

No	Responden	Nilai DSS01	Skala PA
4	R4	42	84%
5	R5	44	88%
6	R6	44	88%
7	R7	46	92%
8	R8	42	84%
9	R9	44	88%
10	R10	41	82%
Total		427	85%

Setelah melakukan perhitungan maka didapat hasil penilaian kapabilitas BPSDM Prov Jabar pada DSS01 level 2 berada di tingkat *Fully Achieved*, karena level 2 proses PA 2.1 yaitu *Performance Management* mencapai 86% dan untuk PA 2.2 yaitu *Work Product Management* mencapai 85% sehingga dapat dilanjutkan perhitungan level 3.

Tabel 13 Penilaian DSS01 atribut proses PA 3.1 *Process Definition*

No	Responden	Nilai DSS01	Skala PA
1	R1	35	64%
2	R2	33	60%
3	R3	34	62%
4	R4	31	56%
5	R5	31	56%
6	R6	31	56%
7	R7	31	56%
8	R8	31	56%
9	R9	34	62%
10	R10	34	62%
Total		325	59%

Tabel 14 Penilaian DSS01 atribut proses PA 3.2 *Work Process Deployment*

No	Responden	Nilai DSS01	Skala PA
1	R1	27	49%
2	R2	29	53%
3	R3	29	53%
4	R4	25	45%
5	R5	28	51%
6	R6	27	49%
7	R7	27	49%
8	R8	27	49%
9	R9	26	47%
10	R10	26	47%
Total		271	49%

Setelah melakukan perhitungan maka didapat hasil penilaian kapabilitas BPSDM Prov Jabar pada DSS01 level 3 berada di tingkat *Largely Achieved*, karena level 3 proses PA 3.1 yaitu *Process Definition* mencapai 59% dan untuk PA 3.2 yaitu *Work Process Deployment* 49% maka DSS01 ini masih berada pada level 3 dijelaskan pada Tabel 14.

Tabel 15 Pencapaian Level Kapabilitas DSS01

Tujuan	<i>Manage Problems</i>									
	Level 0	Level 1	Level 2		Level 3		Level 4		Level 5	
DSS01		PA 1.1	PA 2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2	PA 5.1	PA 5.2
Pencapaian level kapabilitas	100%	100%	86%	85%	59%	49%				

Analisis GAP

Untuk mengetahui berapa Gap (jarak) yang ada diantara hasil pengukuran level kapabilitas yang telah ditentukan dengan level yang telah ditargetkan oleh BPSDM Prov Jabar. Table 15 di bawah ini menunjukkan Gap antara level saat ini dengan target level.

Tabel 16 Analisis Gap

Proses	Target Level	Level saat ini	Gap (Jarak)
DSS01 – <i>Manage operations</i>	3	3	0
DSS02 - <i>Manage Service Requests and Incidents</i>	3	1	2
DSS03 - <i>Manage Problems</i>	3	1	2
DSS04 - <i>Manage Continuity</i>	3	1	2
DSS05 - <i>Manage Security Services</i>	3	1	2
DSS06 - <i>Manage Business Process Controls</i>	3	1	2

Untuk mengetahui besarnya rata-rata kapabiliti level yang telah dicapai menggunakan perhitungan rata-rata sebagai berikut :

$$Capability\ level = \frac{(1*Y1)+(2*Y2)+(3*Y3)+(4*Y4)+(5*Y5)}{Z}$$

Keterangan :

Yn (Y0 s.d Y5) : Jumlah proses yang berada di level n

Z : Jumlah proses yang dievaluasi

$$\begin{aligned} Capability\ level &= \frac{(1*5)+(2*0)+(3*1)+(4*0)+(5*0)}{6} \\ &= \frac{(5)+(3)}{6} \\ &= \frac{8}{6} = 1,3 \end{aligned}$$

Hasil dari perhitungan diatas diperoleh rata-rata level kapabilitas berdasarkan hasil kuesioner adalah sebesar 1,3 dan analisis gap sebesar 1,7 untuk mencapai target level 3 sebagai target yang ingin dicapai pada sistem pendaftaran diklat secara online di BPSDM Prov Jabar.

Rekomendasi Perbaikan Domain DSS

Bagi domain DSS yang masih berada di level 1 membutuhkan rekomendasi perbaikan supaya dapat maju ketahap selanjutnya, rekomendasi tersebut dapat dilihat pada Tabel 17.

Tabel 17 Rekomendasi Domain DSS

Proses	Rekomendasi	Perbaikan
DSS02	a. Organisasi perlu membuat jadwal untuk melakukan pengecekan secara berkala terhadap suatu insiden atau kejadian, agar tidak terulang kembali.	a. Menentukan jenis insiden yang sering terjadi. b. Membuat daftar prioritas insiden yang harus ditangani terlebih dahulu.
DSS03	a. Organisasi perlu memiliki peta klasifikasi masalah, serta membuat laporan terhadap status masalah yang sudah ditangani.	a. Membuat peta klasifikasi masalah yang terjadi. b. Bila suatu masalah telah berhasil ditangani maka harus membuat laporan secara tertulis.
DSS04	a. Organisasi perlu peninjauan secara berkala atas rencana pengelolaan sistem TI b. Organisasi perlu melakukan pemantauan terhadap kemampuan dan kompetensi seluruh pegawai atas perkembangan sistem TI	a. Dilakukan peninjauan berkala bagi rencana pengelolaan sistem TI di BPSDM Prov Jabar b. Melakukan pelatihan terhadap pegawai yang kurang berkompeten dalam pengembangan sistem TI
DSS05	a. Organisasi perlu memberikan kebijakan untuk pencegahan ancaman perangkat lunak yang berbahaya terhadap sistem TI b. Setelah organisasi melakukan uji kerentanan terhadap sistem TI perlu adanya sebuah catatan hasil.	a. Memberikan kebijakan dan peraturan terhadap pemakaian teknologi informasi sebagai pencegahan ancaman dari perangkat lunak yang berbahaya. b. Membuat laporan setelah melakukan uji kerentanan terhadap sistem TI.
DSS06	a. Organisasi perlu membuat rekomendasi perbaikan terhadap kesalahan dalam mengelola pengendalian proses bisnis.	a. Menjadwalkan perawatan untuk sistem TI agar terhindar dari kesalahan dalam

Proses	Rekomendasi	Perbaikan
	b. Organisasi perlu menindaklanjuti terhadap setiap laporan pengolahan informasi proses bisnis.	mengelola proses bisnis. b. Melakukan tindakan dari setiap laporan dalam pengolahan informasi proses bisnis.