MODUL

BEST PRACTISE MANAJEMEN RISIKO TI MENGGUNAKAN NIST DAN COBIT 5

Oleh :

YULHENDRI

MANAJEMEN RISIKO TERHADAP SISTEM TEKNOLOGI INFORMASI MENGGUNAKAN *NIST* DAN COBIT 5

Risiko

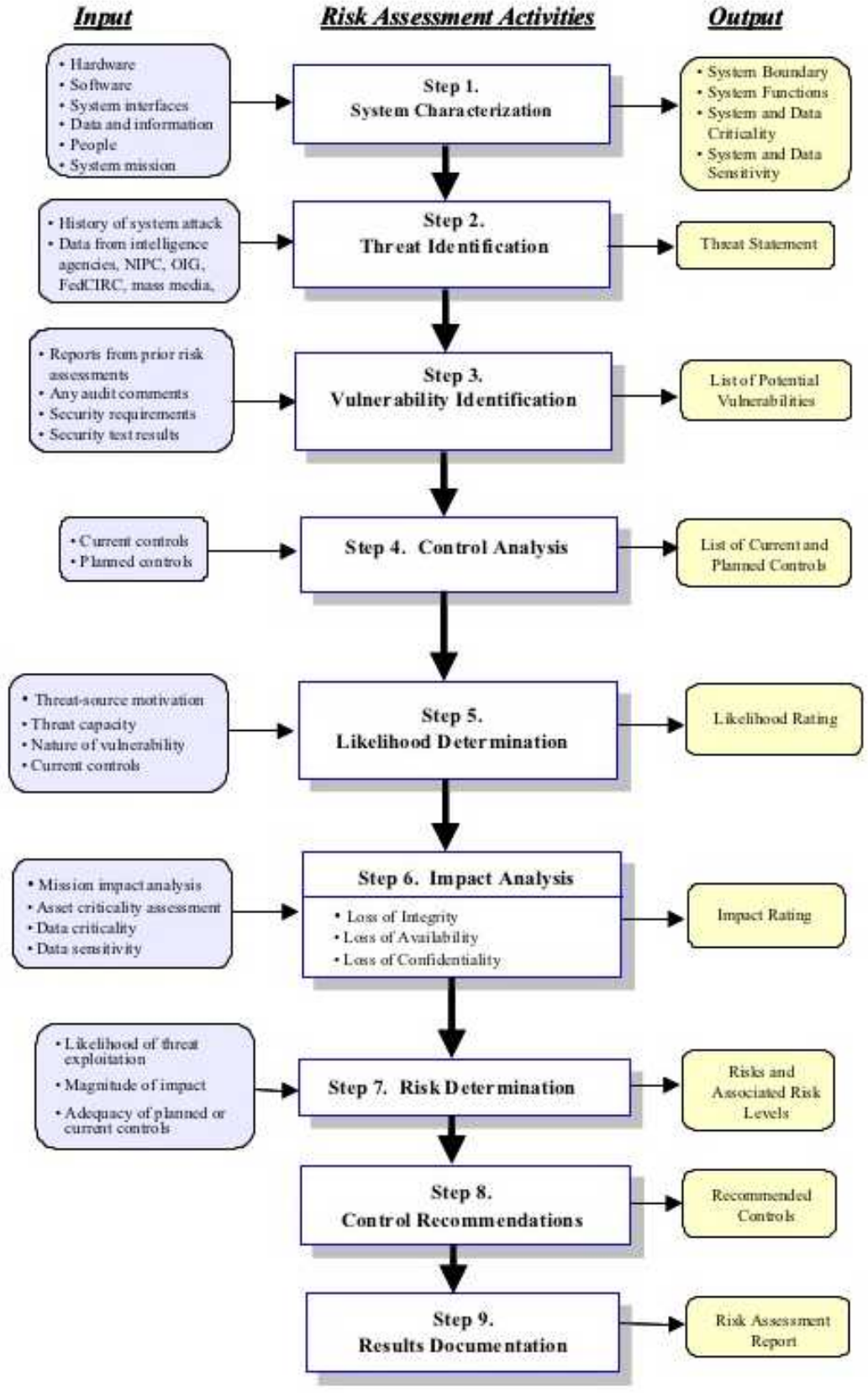
Dalam suatu organisasi pemerintahan risiko dapat didefinisikan sebagai segala sesuatu tindakan yang dapat berdampak pada tercapainya tujuan organisasi. Menurut para ahli Risiko dalam buku *Fundamentals of Risks Management : Understanding, Evaluating and Implementing Effective Risk Management* karya Paul Hopkin dapat di definisikan sebagai berikut *(*Hopkin, 2010:12*) :* Pengaruh ketidakpastian terhadap suatu tujuan. Dimana efek tersebut mungkin positif, negatif, atau penyimpangan dari yang diharapkan. Selain itu, risiko sering digambarkan menjadi sebuah peristiwa, sebuah perubahan keadaan atau konsekuensinya.

Konsep Manajemen Risiko IT Pada Organisasi

Menurut Emmett J. Vaughan dan Therese Vaughan dalam buku nya 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



Gambar 1 Tahapan *Risk Assessment Activities*

Risk Mitigation

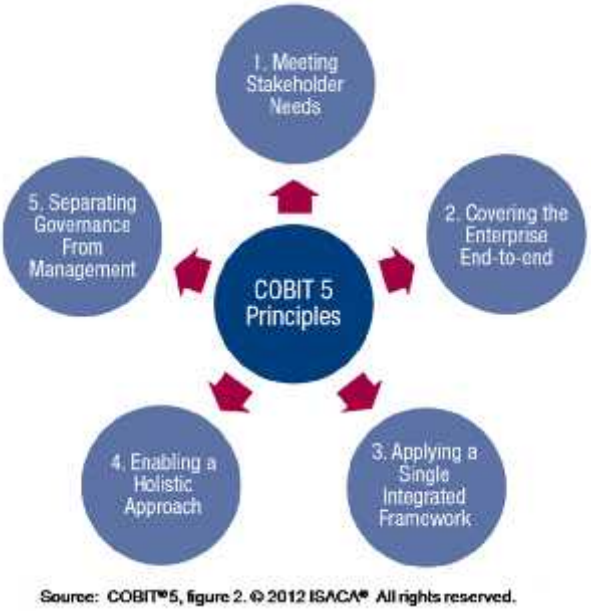
Merupakan tahap kedua dari proses manajemen risiko yang dikeluarkan NIST melibatkan prioritasisasi, evaluasi dan implementasi rekomendasi dari kontrol pengurangan risiko dari tahapan sebelumnya yaitu penilaian risiko.

COBIT 5

COBIT 5 Menyediakan kerangka kerja komprehensif yang membantu Organisasi dalam mencapai tujuan mereka untuk *governance* dan pengelolaan Organisasi TI. Secara sederhana, ini membantu Organisasi menciptakan nilai optimal dari TI dengan menjaga keseimbangan antara mewujudkan manfaat dan mengoptimalkan tingkat risiko dan penggunaan sumber daya.

Prinsip COBIT 5

COBIT 5 didasarkan pada lima prinsip utama digunakan untuk *governance* dan pengelolaan TI Organisasi, seperti pada Gambar 2 di bawah ini:



Gambar 2 Prinsip COBIT 5
(Sumber COBIT 5, 2012 : 13)

Domain dan Proses COBIT 5

COBIT 5 memiliki 5 domain yang terbagi ke dalam domain tata kelola dan manajemen. Setiap domain memilikki proses yang membantu dalam mencapai tujuan. Satu domain menangani tata kelola dan 4 domain mencakup area manjemen. Domain tata kelola, yaitu *Evaluate, Direct dan Monitor* (EDM). Domain manajemen terdiri 4 area, yaitu :

1. *Align, Plan and Organize* (APO) : 13 proses
2. *Build, Acquire and Implement* (BAI) : 10 proses
3. *Deliver, Service and Support* (DSS) : 6 proses
4. *Monitor, Evaluate and Assess* (MEA) : 3 proses

Area *governance* terdiri dari 5 proses, yaitu EDM01 Memastikan Pengaturan Kerangka Kerja Tata Kelola dan Pemeliharaan, EDM02 Memastikan Penyampaian Manfaat, EDM03 Optimasisasi Risiko, EDM04 Optimasisasi Sumber Daya dan EDM05 Transparansi *Stakeholder.* (ISACA, 2012 : 12)

Contoh Penerapan Manajemen Risiko TI pada BPSDM Jabar

Profil Badan Pengembangan Sumber Daya Manusia Prov. Jabar

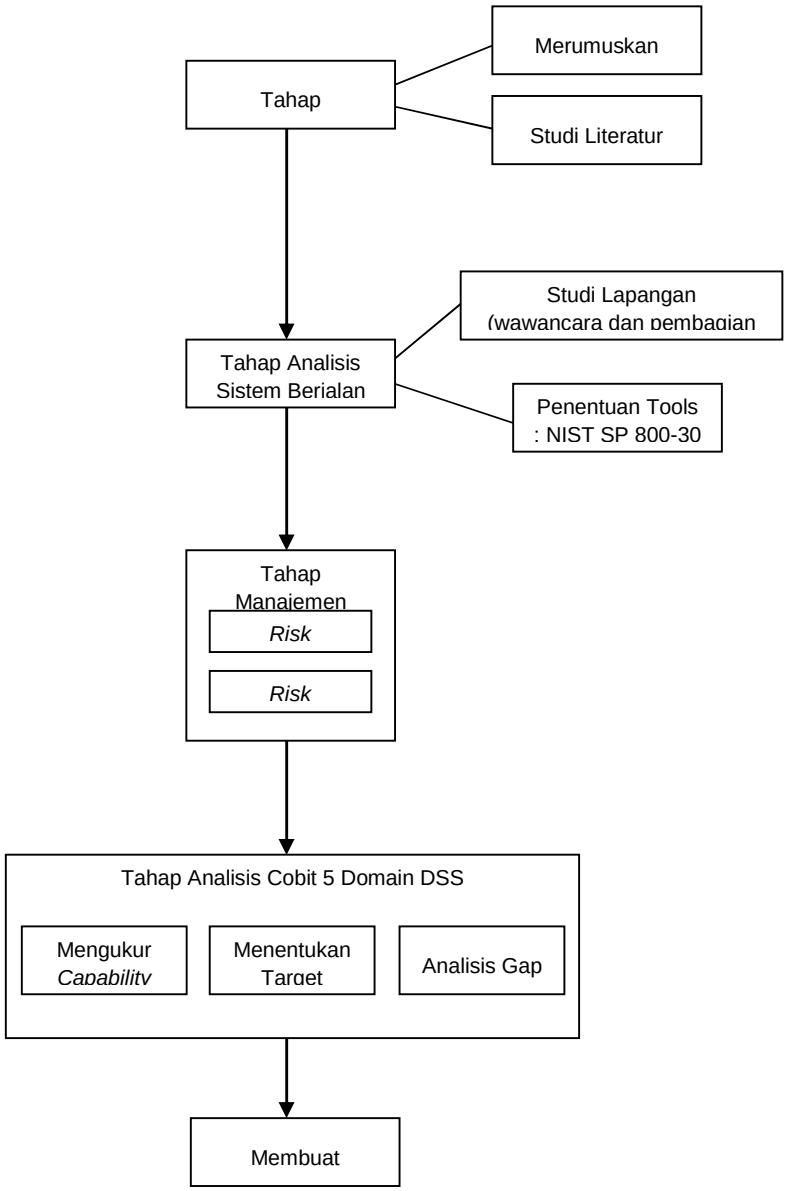
Badan Sumber Daya Manusia Provinsi Jawa Barat (BPSDM) sebelumnya bernama Badan Pendidikan dan Pelatihan Provinsi Jawa Barat pertama kali dibentuk pada Tahun 1968. Lembaga ini pada awalnya bernama Pusat Pendidikan dan Latihan Pemerintah Daerah Tingkat I Jawa Barat yang beralamat di Jl. Windu Nomor 26 Bandung.

Aplikasi Sistem Informasi BPSDM (Pendaftaran Diklat Secara Online)

Aplikasi daftar diklat secara online ini dibuat bagi para Pegawai Negeri Sipil (PNS), CPNS, maupun Aparatur Sipil Negara (ASN) lainnya yang ingin mendaftar untuk mengikuti diklat. Pengelola dari aplikasi ini adalah Bidang Pengembangan Kompetensi teknis subtantif, Bid Pengembangan kompetensi teknis umum, dan Bid pengembangan kompetensi Manajerial.

Metodologi Penelitian

Metodologi penelitian merupakan serangkaian cara atau langkah untuk memecahkan suatu masalah. Metodologi penelitian terdiri dari merumuskan masalah, analisis manajemen risiko dengan menggunakan NIST SP 800-30 dan COBIT 5, membuat rekomendasi berdasarkan hasil analisis dan diakhiri dengan dokumentasi. Metodologi penelitian yang digunakan terlihat pada Gambar 3



Gambar 3 Metodologi Penelitian

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 memungkian 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 mancapai 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 anlisis 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	***System Interfaces***	**Keterangan**
13.	Pendaftaran Diklat secara Online BPSDM Prov Jabar	
14.	Admin, *stakeholder*, 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**	***Threat Source***	**Motivation**	***Threat Action***
1	Pemadaman listrik secara mendadak menyebabkan server mati karena tidak ada sumber listrik cadangan	Teknologi *disaster*	Ketidak sengajaan	Tidak tersedianya UPS
2	AC di ruang server yang padam menyebabkan server *overheat* dan mati	Teknologi *disaster*	Ketidak sengajaan	Usia AC yang sudah tua sehingga terjadi kerusakan
3	AC di ruang server yang dimatikan	*Human disaster*	Ketidak sengajaan	Mematikan AC karena ketidaktahuan
4	Pencurian 2 buah komputer yang memiliki data-data penting	*Human disaster (Computer criminal)*	Faktor ekonomi	Tindakan pencurian dengan motif ekonomi
5	Komputer terkena malware sehingga sistem *blank*	*Human disaster (insider)*	ketidaksengajaan	Komputer digunakan untuk mendownload sehingga terkena malware
6	Komputer terkena virus	*Human disaster*	ketidaksengajaan	Menggunakan *Flasdisk* untuk mengcopy data
7	*Hacker* pada saat lomba web dicurangi pesaing melakukan *hacking* supaya web dinas kalah dalam lomba	*Human Disaster (industrial espionage)*	Keunggulan kompetisi	Peretasan pada web yang sedang di lombakan dengan merubah tampilan menu dalam web
8	Terputus jaringan kondisi eksisting	*Human disaster*	ketidaksengajaan	Akibat orang yang tidak tau dan kabel putus akibat tikus
9	Banjir karena daerah pelajar pejuang ketika hujan sering tergenang oleh air	*Natural disaster*		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	*Natural disaster*		

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.	***Theat Source***	***Vulnerability***	**Keterangan**
1	Virus	Anti Virus sudah diinstal tapi tidak pernah digunakan	Kemungkinan terjadinya sangat tinggi karena sering ada personil yang menggunakan USB *PC client*
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 *low* karena jarang dilakukan *upgrade*
4	*Hacker*	Belum ada pencegahan supaya tidak terjadi *hacking* ke sistem	Kemungkinan *medium* karena admin yang sudah tidak bekerja pernah memegang *password*
5	*Insider*	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.	*Control*	Implementasi
1	Setiap ruangan simulasi dipasang *doorclock* yang menggunakan *finger print* maupun *acces code*	Melakukan pemasangan *doorlock* 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	Ketidakpahaman 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 *password* secara rutin	Untuk melindungi komputer server maupun sistem yang lain untuk waktu yang akan datang wajib melakukan ganti password secara rutin supaya tidak siapa saja yang menggunakan komputer
5	Springkler	Ada 1 di depan ruang server
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 *aquaproof*	Atap masih banyak yang bocor ketika hujan besar, mitigasi menggunakan *aquaproof*

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	*PC client* atau *PC server*	Anti Virus sudah diinstal tapi tidak pernah digunakan	*High*	Kemungkinan terjadinya sangat tinggi karena sering ada personil yang

No.	Risiko	*Threat*	*Vulnerability*	*Risk likelihood evaluation*	Keterangan
					menggunakan USB *PC client*
2	Listrik mati	*Server*	Tidak adanya cadangan sumber listrik (UPS	*High*	Kemungkinan terjadinya tinggi karena bila server mati karena listrik mati maka akan terjadinya kerusakan dan kehilangan data
3	Malware		Belum ada penghalang malware	*Low*	Kemungkinan terjadinya *low* karena jarang dilakukan *upgrade*
4	*Hacker*	*Website, Server*	Belum ada pencegah *hacking* ke sistem	*Medium*	Kemungkinan *medium* karena admin yang sudah tidak bekerja pernah memegang *password*
5	*Insider*	SDM non IT	Masih banyak pegawai yang tidak mengerti sama sekali tentang TI	*High*	Kemungkinan terjadi tinggi karena 80 % pegawai lulusan SMA
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 *medium* karena harus menginstal ulang server dan data beresiko hilang
2	Listrik mati	*High*	Jika terjadi pemadaman listrik dampaknya *high* 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 *medium* karena sistem pendaftaran tidak dapat berjalan, sehingga calon peserta harus kembali mendaftar secara manual.
4	*Hacker*	*Low*	Kemungkinan sistem terkena *hack* dampaknya *low* 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	*Low*	Bila terjadi kebakaran dampaknya rendah karena telah tersedia alat pemadam api dan juga jarak dinas kebakaran letaknya tidak begitu jauh
8	Tikus (aliran listrik)	*Medium*	Jika kabel listrik terputus akibat tikus dampaknya *medium*, tetapi untuk perbaikannya yang memerlukan usaha ekstra
9	Jaringan internet mati	*Medium*	Jika jaringan terputus maka dampaknya *medium* 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	*High (1.0)*	*Medium (50)*	*Medium (50 x 1.0 = 50)*
2	Listrik mati	*High (1.0)*	*High (100)*	*High (100 x 1.0 = 100)*
3	*Malware*	*Low (0.1)*	*Medium (50)*	*Low*

No.	Resiko	*Likelihood*	*Impact*	*Risk*
				(50 x 0.1 = 5)
4	*Hacker*	*Medium (0.5)*	*Low (10)*	*Low (10 x 0.5 = 5)*
5	*Insider*	*High (1.0)*	*High (100)*	*High (100 x 1.0 = 100)*
6	Bencana banjir	*Medium (0.5)*	*Low (10)*	*Low (10 x 0.5 = 5)*
7	Kebakaran	*Low (0.1)*	*Low (10)*	*Low (10 x 0.1 = 1)*
8	Tikus (aliran listrik)	*Medium (0.5)*	*Medium (50)*	*Medium (50 x 0.5 = 25)*
9	Jaringan internet mati	*Medium (0.5)*	*Medium (50)*	*Medium (50 x 0.5 = 25)*

h) *Control Recomendation* (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	*Medium*	a. Menginstal anti virus yang otomatis b. Menjadikan *USB port disable* sehingga tidak bisa menggunakan USB
2	Listrik mati	*High*	a. Memasang sumber listrik cadangan seperti *uninterruptible power supply* (UPS) dan menyediakan genset.
3	*Malware*	*Low*	a. Menginstal malware b. Dilarang melakukan hal apapun pada komputer
4	*Hacker*	*Low*	a. Mengecek konten web setiap waktu
5	*Insider*	*High*	a. Memberi larangan kepada orang awan b. Menyeleksi petugas yang akan bekerja di server
6	Kebakaran	*Low*	a. Pelatihan menanggulangi kebakaran b. Penyediaan alat pemadam c. Pendeteksi otomatis jika ada api
7	Kabel putus	*Medium*	a. Dilarang menggangu kabel b. Admin server selalu berjaga di kantor dan sering memeriksa
8	Banjir	*Low*	a. Memindahkan ruangan server b. Meninggikan lantai c. Membuat drynase d. Membuat saluran air

No.	Risiko	*Risk level*	*Control Recommendations*
9	Jaringan internet mati	*Medium*	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 Penlaian Level Kapabilitas COBIT 5

Untuk menentukan dan melakukan penilaian terhadap level kapabiltas setiap domain yang terdapat pada COBIT 5, maka masing-masing proses yang terdapat dalam domain tersebut diidentifikasikan 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	*Not Achieved*	0% - 15%
P	*Partially Achieved*	>15% - 50%
L	*Largely Achieved*	> 50% - 85%
F	*Fully Achieved*	>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 *outsource.* 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 ditunjukan dengan kode P1 sampai P8, dari 10 responden yang memberikan jawaban rata-rata responden memberi jawaban “Ya”, dan sebagian memberikan jawaban “Tidak”. Konversi menupakan 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%
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	*Manage Problems*									
	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 – *Manage operations*	3	3	0
DSS02 - *Manage Service Requests and Incidents*	3	1	2
DSS03 - *Manage Problems*	3	1	2
DSS04 - *Manage Continuity*	3	1	2
DSS05 - *Manage Security Services*	3	1	2
DSS06 - *Manage Business Process Controls*	3	1	2

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

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

Keterangan :

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

Z : Jumlah proses yang dievaluasi

$$\textit{Capability level} = \frac{(1*5)+(2*0)+(3*1)+(4*0)+(5*0)}{6}$$

$$= \frac{(5)+(3)}{6}$$

$$= \frac{8}{6} = 1{,}3$$

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

Proses	Rekomendasi	Perbaikan
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 cacatan 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. b. Organisasi perlu menindaklanjuti terhadap setiap laporan pengolahan informasi proses bisnis.	a. Menjadwalkan perawatan untuk sistem TI agar terhindar dari kesalahan dalam mengelola proses bisnis. b. Melakukan tindakan dari setiap laporan dalam pengolahan informasi proses bisnis.

KESIMPULAN DAN SARAN

Kesimpulan

Berdasarkan rumusan masalah yang terdapat pada BAB I, maka dapat disimpulkan bahwa :

1. Pengukuran manajemen risiko TI BPSDM Prov Jabar perlu meningkatkan keamanan sistem teknologi informasinya untuk mencegah terjadinya risiko kerusakan dengan cara mengimplementasikan kontrol yang tersedia pada hasil *risk mitigation* dalam panduan NIST SP 800-30.
2. Memetakan kapabiliti level manajemen risiko TI berdasarkan hasil analisis secara umum BPSDM Prov Jabar berada di level 1 yaitu DSS02, DSS03, DSS04, DSS05, DSS06. BPSDM Prov Jabar sudah menjalankan proses manajemen risiko TI namun belum berjalan dengan optimal karena masih ditemukan banyak permasalahan terkait pengelolaan dan manajemen TI yang berdampak pada operasional.
3. Berdasarkan hasil analisis GAP maka secara umum BPSDM Prov Jabar berada di level 1 terdapat gap/jarak sebesar 2 untuk mencapai level 3 pada semua proses DSS. Berikut rekomendasi untuk dapat meningkatkan kapabilitas level manajemen risiko TI BPSDM Prov Jabar :
   a) BPSDM perlu melengkapi semua proses di level 1 pada doamian DSS02 sampai DSS06, setelah itu melakukan *assessment* kembali untuk mengetahui apakah kelima proses tersebut telah mencapai level 1 dengan capaian *Fully Achieved* (F).
   b) Jika level 1 sudah terpenuhi maka dapat melanjutkan ke level selanjutnya yaitu level 2 dan level 3.

Saran

Penelitian ini fokus pada manajemen risiko dengan NIST SP 800-30 secara lengkap dan COBIT 5 pada domain proses DSS. Oleh karena itu, untuk penelitian selanjutnya dapat mengembangkan penelitian ke domain COBIT 5 lainnya.

Saran bagi BPSDM Prov Jabar adalah untuk meningkatkan keamanan dari risiko dengan mengacu pada hasil mitigasi risiko NIST SP 800-30 yang telah tersedia, serta melakukan peningkatan terhadap proses bisnis dan melakukan penyesuaian untuk mencapai level kapabilitas yang diharapkan dari manajemen risiko TI.

DAFTAR PUSTAKA

Hopkin, Paul. 2010. *Fundamentals of Risks Management : Understanding, Evaluating and Implementing Effective Risk Management*. Kogan Page. London.

ISACA. 2012. COBIT 5: *A Business Framework for the Governance and Management of Enterprise IT*. ISACA

ISACA. 2012. *COBIT 5 Toolkit: COBIT and GRC*. ISACA

ISACA. 2012. *Process Assessment Model (PAM): Using COBIT 5*. ISACA

Khanyile, Slindile. Abdullah, Hanifa. *COBIT 5: An Evolutionary Framework and Only Framework to Address The Governance and Management of Enterprise IT*. UNISA.

Maulana, Muhammad Mahreza. Supangkat, Suhono Harso. 2006. Prosiding Konferensi Nasional Teknologi Informasi dan Komunikasi untuk Indonesia. Pemodelan *Framework* Manajemen Resiko TI untuk Organisasi di Negara Berkembang.

Nugraha, Ucu. 2016. Seminar Nasional Telekomunikasi dan Informatika (SELISIK) . Manajemen Risiko Sistem Informasi Pada Perguruan Tinggi Menggunakan Kerangka Kerja NIST SP 800-30

Stoneburner, Gary, Alice Goguen, dan Alexis Feringa. 2002. *Risk Management Guide for Information Technology System*. NIST SP 800-30

Syafitri, Wenni. 2016. Penilaian Risiko Keamanan Informasi Menggunakan Metode NIST 800-30 (Studi Kasus: Sistem Informasi Akademik Universitas XYZ). Jurnal CoreIT. Vol.2 No. 2

Vaughan, Emmet J. Vaughan, Therese M. 2008. *Fundamentals of Risk and Insurance*. John Wiley & Sons. USA

ISACA. 2013. Mapping to COBIT 5. Melalui http://www.isaca.org/Certification/CGEIT-Certified-in-the-Governance-of Enterprise-IT/Prepare-for-the-Exam/Mappin-to-COBIT/Pages/default.aspx. 12 juni 2017 pukul 11.30