IMPLEMENTASI *RISK ASSESSMENT* PADA DIVISI TEKNOLOGI INFORMASI DI PT. XYZ MENGGUNAKAN ISO 27005:2008

IMPLEMENTATION OF RISK ASSESSMENT ON INFORMATION TECHNOLOGY DIVISION IN PT. XYZ USES ISO 27005:2008

Muhammad Tsany Malik Atha Nur[1], Irfan Darmawan[2], Rokhman Fauzi [3]
[1,2,3] Prodi S1 Sistem Informasi, Fakultas Rekayasa Industri, Universitas Telkom
[1]**muhtsanymalik@student.telkomuniversity.ac.id** [2]**irfandarmawan@telkomuniversity.ac.id**
[3]**rokhmanfauzi@telkomuniversity.ac.id**

Abstrak

PT. XYZ merupakan perusahaan yang bergerak dalam pembuatan produk militer dan komersial di Indonesia. PT. XYZ memiliki penerapan manajemen risiko dalam pengelolaan TI (Teknologi Informasi) dan proses bisnis pada divisi TI. Akan tetapi, penerapan tersebut belum sepenuhnya menilai adanya ancaman pada aset TI di divisi TI dan menilai seberapa jauh kontrol yang sudah ada dapat mengurangi ancaman maupun risiko yang akan datang serta dampaknya. Implementasi dan penilaian *risk assessment* terhadap aset TI dilakukan menggunakan ISO 27005 yang difokuskan untuk melakukan pengelolaan/kontrol terhadap risiko TI. Penerapan *risk assessment* dilakukan dengan mengacu pada *risk scenario* pada ISO 27005. Penelitian ini dilakukan dengan mengidentifikasi *risk scenario* pada aset TI berdasarkan penilaian kontrol yang ada pada ISO 27001. Hasil pada penelitian ini berdasarkan latar belakang tersebut, *risk assessment* pada aset TI menghasilkan *level of risk* yang mempunyai nilai ekstrem 2, tinggi 4, moderat 24. *Risk response* terhadap 6 ancaman yang harus dimitigasi. *Risk treatment* seperti perencanaan dan penerapan *disaster recovery*, pengecekan fungsi keamanan fisik untuk mengurangi dampak kebakaran dan cek fungsi alarm di setiap ruangan, asuransi seluruh *hardware* untuk mengurangi biaya dampak kerusakan, dan menambahkan kapasitas dari *web hosting* atau dilakukannya pemakaian secara bergantian. Sebagai solusi yang menjadi rekomendasi untuk PT. XYZ sebagai panduan dalam mengelola aset TI.

Kata Kunci: ISO 27005, *risk assessment, risk scenario*, ISO 27001, *level of risk, risk treatment.*

Abstract

PT. XYZ is a company engaged in manufacturing military and commercial products in Indonesia. PT. XYZ has the application of risk management in the management of IT (Information Technology) and business processes in the IT division. However, the application has not fully assessed the threats to IT assets in the IT division and assessed the extent to which existing controls can reduce future threats and risks and their impact. Implementation and assessment of risk assessment of IT assets is carried out using ISO 27005 which is focused on managing / controlling IT risks. The application of risk assessment is carried out by referring to the risk scenario at ISO 27005. This study was conducted by identifying risk scenarios on IT assets based on the assessment of controls that exist at ISO 27001. The results of this study based on this background, risk assessment of IT assets generates level of risk has extreme values 2, high 4, moderate 24. Risk response to 6 threats that must be mitigated. Risk treatment such as planning and implementing disaster recovery, checking physical security functions to reduce the impact of fire and checking the alarm function in every room, insurance of all hardware to reduce the cost of damage, and adding capacity of web hosting or using it alternately. As a solution that becomes a recommendation for PT. XYZ as a guide in managing IT assets.

Keywords*: ISO 27005, *risk assessment, risk scenario*, ISO 27001, *level of risk, risk treatment.

1. Pendahuluan

Penelitian ini membahas permasalahan yang ada di PT. XYZ. Berdasarkan data dari hasil wawancara kepada salah satu pegawai divisi teknologi informasi. Kondisi *risk assessment* yang ada yaitu sudah melakukan identifikasi ancaman pada proses bisnis yang terjadi sebelumnya, *treatment* yang dilakukan sebagai antisipasi terhadap ancaman yang terjadi sebelumnya, belum adanya penilaian kontrol *existing*, belum adanya penilaian dampak terhadap ancaman yang mungkin terjadi. Dalam menilai risiko berdasarkan *risk assessment* meliputi identifikasi risiko (aset, ancaman, kontrol *existing*, konsekuensi), analisis risiko (penilaian konsekuensi, penilaian kemungkinan ancaman, penentuan nilai risiko), evaluasi risiko, penanggulangan risiko.

PT. XYZ merupakan perusahaan BUMN (Badan Usaha Milik Negara) yang bergerak dalam pembuatan produk militer dan komersial di Indonesia dan memperkerjakan sekitar 3000 karyawan. Karena risiko permasalahan yang sering terjadi itu ada beberapa poin, yang pertama adalah tentang keamanan informasi yang kurang terjaga oleh

pihak *internal* maupun *eksternal*, seperti mendokumentasikan hal-hal yang ada di perusahaan ini. Padahal nyatanya perusahaan ini bersifat rahasia dan tidak boleh sembarang berfoto atau bervideo di dalam lingkungan perusahaan. Lalu poin selanjutnya adalah tentang kepatuhan terhadap *license* yang masih kurang disadari oleh para pegawai di dalamnya. PT. XYZ memiliki aset-aset penting di dalamnya, seperti yang dilampirkan pada tabel dibawah ini: [7]

Tabel 1. Daftar Aset Teknologi Informasi PT. XYZ

No.	Jenis Aset TI
1	Aset Dokumen
2	Aset *Hardware*
3	Aset *Software*

Berdasarkan Tabel 1 dapat dilihat bahwa PT. XYZ memiliki aset TI utama. Mengingat TI merupakan aset penting dalam operasional. Aset TI tersebut perlu diketahui nilai-nilai ancaman yang mungkin terjadi dan dikaitkan dengan penilaian kontrol existing, sehingga mengurangi kegagalan pencapaian tujuan dan misi perusahaan yang berdampak pada ketidakpercayaan publik atas pelayanan yang diberikan dan pada akhirnya akan mengakibatkan ketidakstabilan ekonomi secara sistematis.

2. Dasar Teori

2.1. ISO/IEC 27001

ISO/IEC 27001 merupakan dokumen Standar Sistem Manajemen Keamanan Informasi (SMKI) atau Information Security Management Systems (ISMS) yang memberikan gambaran secara umum mengenai apa saja yang seharusnya dilakukan dalam usaha pengimplementasian konsep-konsep keamanan informasi di perusahaan. Standar internasional ini telah dipersiapkan untuk menyediakan sebuah model pembangunan, penerapan, pengerjaan, pengawasan, peninjauan, pemeliharaan, peningkatan sebuah SMKI. Standar ini mengadopsi model Plan Do-Check-Act (PDCA) yang diterapkan untuk menyusun sebuah proses SMKI [1].

2.2. ISO/IEC 27005

Menurut ISO/IEC 27005 berfokus pada analisis risiko, selanjutnya tahapan menuju pemilihan terhadap kontrol keamanan. ISO/IEC 27001 dan ISO/IEC 27002 lebih menjelaskan tentang perencanaan, pelaksanaan dan operasi terhadap kontrol keamanan. Proses manajemen risiko keamanan informasi terdiri dari *context establishment*, *risk assessment*, *risk treatment*, *risk acceptance*, *risk communication*, *risk monitoring* and *review* [6].

2.3. *Risk Assessment*

Risk assessment menentukan nilai pada aset informasi, mengidentifikasi ancaman-ancaman dan kerentanan yang dapat terjadi, mengidentifikasi kontrol dan efeknya pada risiko yang teridentifikasi, menentukan konsekuensi potensial dan akhirnya memprioritaskan risiko yang telah diperoleh dan menggolongkan pada kriteria evaluasi risiko yang diatur dalam *establishment context*. Tahapan pada *risk assessment* terdiri dari identifikasi risiko, analisis risiko, evaluasi risiko [6].

3. Metodologi Penelitian

3.1. Model Konseptual

Model Konseptual adalah konsep yang digunakan penulis untuk membantu penelitiannya. Model konseptual pada Tugas Akhir ini adalah mengenai implementasi *risk assessment*. Model konseptual ini ini didasari oleh permasalahan yang terdapat pada divisi TI PT. XYZ, di mana permasalahan itu ialah belum adanya penilaian risiko serta belum adanya rekomendasi *risk treatment* yang sesuai. Pelaku yang terlibat dalam lingkungan ialah pegawai di divisi TI PT.XYZ. Untuk melakukan penelitian ini, digunakan dasar ilmu seperti manajemen risiko serta metode yang digunakan adalah ISO 27005. Penelitian ini akan menghasilkan implementasi *risk assessment* dengan ISO 27005. Untuk evaluasi adanya *checklist* ISO 27005.

3.2. Sistematika Penelitian

Sistematika penilitian merupakan suatu pemahaman untuk memecahkan masalah pada penelitian ini, Berikut adalah sistematika yang digunakan pada penelitian ini.

1) Tahap inisiasi dilakukan untuk penentuan ruang lingkup terhadap penelitian Tugas Akhir ini. Penentuan meliputi perumusan masalah, batasan,tujuan penelitian, studi lapangan melalui wawancara pada salah satu pegawai di divisi TI PT.XYZ, serta studi pustaka menggunakan ISO 27005:2008 dan ISO 27001:2005 sebagai pendukungnya.
2) Pada tahap pengumpulan data dilakukan pembuatan draf pertanyaan mengenai kondisi saat ini di divisi TI PT.XYZ. Setelah itu dilakukan verifikasi kepada PT.XYZ, apakah pertanyaan dapat diterima atau tidak. Jika pertanyaan diterima maka akan dilakukan wawancara serta perusahaan juga memberikan dokumen-dokumen yang berkaitan dengan penelitian.

3) Tahap pelaporan dilakukan setelah melakukan proses penilaian risiko, yaitu menyusun dokumen perbaikan yang berisikan tentang profil risiko berupa *level of risk* yang berisikan nilai risiko, *risk response* yang dikaitkan dengan dokumen *risk appetite* (selera risiko) dari perusahaan dengan maksud risiko mana yang dapat diterima oleh perusahaan dan risiko mana yang tidak dapat diterima, kemudian menentukan strategi *risk treatment* yang dapat mengurangi kemungkinan terjadi suatu ancaman atau dampak dari terjadinya ancaman yang menyebabkan kerugian bagi PT. XYZ.
4) Pada tahap ini dilakukan penilaian *risk assessment* berdasarkan ISO 27005:2008 dan untuk menentukan skenarionya menggunakan kontrol dari ISO 27001:2005. Proses *risk assessment* dilakukan dengan beberapa proses yaitu Penentuan *probability*, *Impact* dan identifikasi ancaman apa saja yang bakalan terjadi di divisi TI PT.XYZ setelah melihat kondisi saat ini. Selanjutnya tahap verifikasi dan validasi *risk assessment*. Verifikasi dilakukan untuk melihat *risk assessment* yang dilakukan sudah sesuai dengan standar yang dijadikan acuan atau tidak, sedangkan validasi dilakukan untuk memberikan hasil *risk assessment* kepada divisi TI PT.XYZ, untuk mengetahui apakah penilaian tersebut dapat diimplementasikan. Apabila *risk assessment* tersebut tidak disetujui oleh divisi TI PT.XYZ, maka dilakukan *risk assessment* kembali.
5) Setelah disetujui hasil *risk assessment* tersebut, maka tahap selanjutnya yaitu melakukan *level of risk* untuk setiap aset dan *risk treatment* untuk memberikan rekomendasi dari aset yang dimitigasi. Terakhir, dilakukan penarikan kesimpulan mengenai hasil dari penelitian yang dilakukan dan memberikan saran terhadap divisi TI PT.XYZ dan penelitian selanjutnya.

4. Pengolahan Data

4.1. Penetapan Konteks

Penetapan konteks merupakan ruang lingkup terhadap kajian risiko yang akan dilakukan pada *risk assessment*. *Assessment* yang dilakukan yaitu pada aset TI. Aset TI yang akan dibahas berdasarkan data yaitu aset-aset kritikal seperti dokumen, *hardware*, *software*. Penetapan konteks akan dilakukan pengelompokkan aset dengan unit kerja sebagai penentuan nilai aset. Kemudian, penentuan kriteria perhitungan dalam melakukan *assessment* berupa analisis tingkat kemungkinan kejadian saat ini dan penilaian dampak terhadap aset perusahaan. Dalam melakukan *assessment*, kriteria perhitungan risiko mencakupi *likelihood* dan *impact* yang digunakan untuk mendapatkan nilai risiko terhadap aset TI di divisi TI PT.XYZ. Kemudian, nilai risiko dari hasil perhitungan akan disesuaikan dengan selera risiko di perusahaan yaitu *risk appetite* (selera risiko) untuk menentukan risk *response* terhadap suatu risiko.

4.2. Identifikasi Risiko

Tujuan dari identifikasi risiko adalah untuk menentukan apa yang bisa terjadi untuk menyebabkan potensi kerugian, dan untuk mendapatkan wawasan tentang bagaimana, dimana dan mengapa kerugian mungkin terjadi. Dalam mengidentifikasi risiko, berdasarkan ISO 27005 memiliki tahapan diantaranya: identifikasi aset dan identifikasi ancaman.

4.2.1. Identifikasi Aset

Proses penilaian pada aset TI dilakukan dengan melakukan wawancara pada salah satu pegawai divisi TI, yang dimiliki oleh PT. XYZ. Berikut daftar aset TI dengan hubungan proses bisnis yang dicantumkan pada tabel 2. sebagai berikut:

Tabel 2. Data Aset Teknologi Informasi

Aset	Jenis
Dokumen	Strategis
	Teknis
	Administratif
Hardware	Server
	Network
Software	*Software* berlisensi
	Software non lisensi

4.2.2. Identifikasi Ancaman

Ancaman yang digunakan untuk melakukan implementasi dan penilaian *risk assessment* mengacu pada *risk scenario* menurut ISO 27005:2008 yang telah disesuaikan dengan jenis aset TI di perusahaan, sebagai berikut:

Tabel 3. Daftar Ancaman Aset TI
(Sumber: ISO 27005:2008)

Jenis Ancaman	Skenario Ancaman	*Threat ID*
Kerusakan Fisik	Kebakaran	T1
	Kerusakan karena kebocoran	T2
	Perusakan pada peralatan atau media	T3
Peristiwa Alam	Badai	T4
	Gempa bumi	T5
	Banjir	T6
Kehilangan layanan yang penting	Hilangnya pasokan listrik	T7
	Kegagalan peralatan telekomunikasi	T8
Kompromi Akan Informasi	Memata-matai dari jauh	T9
	Menguping	T10
	Pencurian media atau dokumen	T11
	Data dari sumber yang tidak dapat dipercaya	T12
	Gangguan perangkat keras	T13
	Gangguan perangkat lunak	T14
Kegagalan Teknis	Kegagalan peralatan	T15
	Kerusakan peralatan	T16
	Kejenuhan sistem informasi	T17
	Kerusakan perangkat lunak	T18
	Pelanggaran pemeliharaan sistem informasi	T19

5. Hasil dan Pembahasan

5.1. Penilaian Risiko

Penilaian risiko yang digunakan ialah *level of risk* yang dikaitkan antara *likelihood* dengan *impact* yang telah disesuaikan dengan penilaian kerentanan, risiko dan kontrol *existing*. Untuk mengetahui nilai *level of risk*, berdasarkan nilai dampak sebagai pengaruh ancaman terhadap kegiatan operasional perusahaan. *Level of risk* dapat diketahui dengan menyesuaikan peta tingkat risiko perusahaan pada bab mengenai penetapan konteks sebelumnya. Maka, diperoleh hasil sebagai berikut:

a) Aset Dokumen

Level of risk didapati dari rekomendasi dan kesepakatan dengan pihak PT. XYZ, dengan cara membandingkan ancaman, kerentanan, kontrol *existing* dan risiko. Berdasarkan perbandingan tersebut bisa kita dapatkan nilai *likelihood* X *impact*. Berikut tabel nilai risiko pada aset dokumen:

Tabel 4. Nilai Risiko Pada Aset Dokumen

Jenis Aset	*Threat ID*	Ancaman	*Level Of Risk*
Strategis, Teknis, dan Administratif	T4	Badai	[16] Tinggi
	T5	Gempa Bumi	[20] Ekstrem
	T6	Banjir	[5] Moderat
	T9	Memata-matai dari jauh	[8] Moderat
	T10	Menguping	[8] Moderat
	T11	Pencurian media atau dokumen	[4] Moderat
	T12	Data dari sumber yang tidak dapat dipercaya	[4] Moderat

b) Aset *Hardware*

Level of risk didapati dari rekomendasi dan kesepakatan dengan pihak PT. XYZ, dengan cara membandingkan ancaman, kerentanan, kontrol *existing* dan risiko. Berdasarkan perbandingan tersebut bisa kita dapatkan nilai *likelihood* X *impact*. Berikut tabel nilai risiko pada aset *hardware*:

Tabel 5. Nilai Risiko Pada Aset *Hardware*

Jenis Aset	*Threat ID*	Ancaman	*Level Of Risk*
Server	T4	Badai	[16] Tinggi
	T5	Gempa Bumi	[20] Ekstrem
	T6	Banjir	[5] Moderat
	T1	Kebakaran	[12] Tinggi
	T2	Kerusakan karena kebocoran	[10] Tinggi
	T3	Perusakan pada peralatan atau media	[4] Moderat
	T10	Menguping	[8] Moderat
	T13	Gangguan perangkat keras	[4] Moderat
Network	T7	Hilangnya pasokan listrik	[4] Moderat
	T8	Kegagalan peralatan telekomunikasi	[4] Moderat
	T9	Memata-matai dari jauh	[8] Moderat
	T11	Pencurian media atau dokumen	[4] Moderat

c) Aset *Software*

Level of risk didapati dari rekomendasi dan kesepakatan dengan pihak PT. XYZ, dengan cara membandingkan ancaman, kerentanan, kontrol *existing* dan risiko. Berdasarkan perbandingan tersebut bisa kita dapatkan nilai *likelihood* X *impact*. Berikut tabel nilai risiko pada aset *software*:

Tabel 6. Nilai Risiko Pada Aset *Software*

Jenis Aset	*Threat ID*	Ancaman	*Level Of Risk*
Software berlisensi	T9	Memata-matai dari jauh	[8] Moderat
	T10	Menguping	[8] Moderat
	T11	Pencurian media atau dokumen	[8] Moderat
	T18	Kerusakan perangkat lunak	[8] Moderat
	T19	Pelanggaran pemeliharaan sistem informasi	[8] Moderat
Software non lisensi	T14	Gangguan perangkat lunak	[5] Moderat
	T7	Hilangnya pasokan listrik	[4] Moderat
	T8	Kegagalan peralatan telekomunikasi	[8] Moderat
	T15	Kegagalan peralatan	[8] Moderat

Jenis Aset	*Threat ID*	Ancaman	*Level Of Risk*
	T16	Kerusakan peralatan	[8] Moderat
	T17	Kejenuhan sistem informasi	[8] Moderat

5.2. *Risk Treatment*

Rekomendasi *Risk Treatment* terhadap hasil nilai risiko yang perlu dimitigasi. Penentuan *treatment* berdasarkan jenis ancamannya sebagai kontrol untuk mengurangi kemungkinan terjadinya ancaman dan dampak kejadian suatu ancaman. Maka, *treatment* yang diusulkan sebagai berikut:

1. Aset Dokumen
   Hasil akhir dari *level of risk* yaitu menentukan *risk response* untuk setiap ancamannya. Untuk *risk response* yang ada pada aset dokumen hanya ada 2 tipe yaitu *mitigate* atau upaya mengurangi risiko dan *retention* atau menerima risiko tersebut. *Risk treatment* didapati berdasarkan hasil rekomendasi dan kesepakatan pada pihak divisi TI PT. XYZ. Berikut tabel rekomendasi *risk treatment* pada aset dokumen:

Tabel 7. *Risk Treatment* Aset Dokumen

Threat ID	Ancaman	*Level Of Risk*	*Risk Response*	*Risk Treatment*
T4	Badai	[16] Tinggi	*Mitigate*	Perencanaan dan penerapan *disaster recovery* baik virtualisasi atau fisik dengan lokasi penyimpanan di tempat lain.
T5	Gempa Bumi	[20] Ekstrem	*Mitigate*	Perencanaan dan penerapan *disaster recovery* baik virtualisasi atau fisik dengan lokasi penyimpanan di tempat lain. Penanggulangan terhadap risiko dapat mengurangi efek pada dampak dan organisasi masih dapat berjalan seperti biasanya.
T6	Banjir	[5] Moderat	*Mitigate*	Perencanaan dan penerapan *disaster recovery* baik virtualisasi atau fisik dengan lokasi penyimpanan di tempat lain.

2. Aset *Hardware*
   Hasil akhir dari *level of risk* yaitu menentukan *risk response* untuk setiap ancamannya. Untuk *risk response* yang ada pada aset *hardware* hanya ada 2 tipe yaitu *mitigate* atau upaya mengurangi risiko dan *retention* atau menerima risiko tersebut. *Risk treatment* didapati berdasarkan hasil rekomendasi dan kesepakatan pada pihak divisi TI PT. XYZ. Berikut tabel rekomendasi *risk treatment* pada aset *hardware*:

Tabel 8. *Risk Treatment* Aset *Hardware*

Threat ID	Ancaman	*Level Of Risk*	*Risk Response*	*Risk Treatment*
T4	Badai	[16] Tinggi	*Mitigate*	• Perencanaan dan penerapan *disaster recovery* baik virtualisasi atau fisik dengan lokasi penyimpanan di tempat lain. • Asuransi seluruh *hardware* untuk mengurangi biaya dampak kerusakan.
T5	Gempa Bumi	[20] Ekstrem	*Mitigate*	• Perencanaan dan penerapan *disaster recovery* baik virtualisasi atau fisik dengan lokasi penyimpanan di tempat lain. Penanggulangan terhadap risiko dapat mengurangi efek pada dampak dan organisasi masih dapat berjalan seperti biasanya. • Asuransi seluruh *hardware* untuk mengurangi biaya dampak kerusakan.
T6	Banjir	[5] Moderat	*Mitigate*	• Perencanaan dan penerapan *disaster recovery* baik virtualisasi atau fisik dengan lokasi penyimpanan di tempat lain. • Asuransi seluruh *hardware* untuk mengurangi biaya dampak kerusakan.

Threat ID	Ancaman	*Level Of Risk*	*Risk Response*	*Risk Treatment*
T1	Kebakaran	[12] Tinggi	*Mitigate*	• Perencanaan dan penerapan disaster recovery baik virtualisasi atau fisik dengan lokasi penyimpanan di tempat lain. • Pengecekan fungsi keamanan fisik (FAP, FM200, APAR) untuk mengurangi dampak kebakaran dan cek fungsi alarm di setiap ruangan. • Asuransi seluruh h*ardware* untuk mengurangi biaya dampak kerusakan.
T2	Kerusakan karena kebocoran	[10] Tinggi	*Mitigate*	• Perencanaan dan penerapan disaster recovery baik virtualisasi atau fisik dengan lokasi penyimpanan di tempat lain. • Pengecekan fungsi keamanan fisik (FAP, FM200, APAR) untuk mengurangi dampak kebakaran dan cek fungsi alarm di setiap ruangan. • Asuransi seluruh h*ardware* untuk mengurangi biaya dampak kerusakan.

3. Aset *Software*

Hasil akhir dari *level of risk* yaitu menentukan *risk response* untuk setiap ancamannya. Untuk *risk response* yang ada pada aset *software* hanya ada 2 tipe yaitu *mitigate* atau upaya mengurangi risiko dan *retention* atau menerima risiko tersebut. *Risk treatment* didapati berdasarkan hasil rekomendasi dan kesepakatan pada pihak divisi TI PT. XYZ. Berikut tabel rekomendasi *risk treatment* pada aset *software*:

Tabel 9. *Risk Treatment* Aset *Software*

Threat ID	Ancaman	*Level Of Risk*	*Risk Response*	*Risk Treatment*
T14	Gangguan perangkat lunak	[5] Moderat	*Mitigate*	Menambahkan kapasitas dari *web hosting* atau dilakukannya pemakaian secara berkala.

6. Kesimpulan

Berdasarkan seluruh proses penilaian *risk assessment* pada divisi teknologi informasi di PT. XYZ menggunakan ISO 27005:2008, dapat disimpulkan bahwa:

a. Hasil dari *risk assessment* berupa *level of risk*, dimana dalam *level of risk* terhadap ancaman yang perlu dimitigasi berdasarkan peta tingkat risiko di PT. XYZ yaitu:
Pada jenis aset dokumen, diketahui ancaman yang perlu dimitigasi seperti badai dengan nilai risiko 16, gempa bumi dengan nilai risiko 20, banjir dengan nilai risiko 5. Pada jenis aset *hardware*, diketahui ancaman yang perlu dimitigasi seperti badai dengan nilai risiko 16, gempa bumi dengan nilai risiko 20, banjir dengan nilai risiko 5, kebakaran dengan nilai risiko 12, kerusakan karena kebocoran dengan nilai risiko 10. Pada jenis aset *software*, diketahui ancaman yang perlu dimitigasi seperti gangguan perangkat lunak dengan nilai risiko 5. Nilai-nilai risiko di atas (16,20,5,16,20,5,12,10) adalah hasil perkalian level likelihood terhadap level impact.

b. Berdasarkan nilai risiko yang perlu dimitigasi terhadap masing-masing aset, maka akan dilakukan rekomendasi *treatment* sebagai kontrol yang dapat mengurangi tingkat kemungkinan ancaman terjadi dan dampaknya yaitu:
Perencanaan dan penerapan *disaster recovery* pada aset dokumen. Perencanaan dan penerapan *disaster recovery*, pengecekan fungsi keamanan fisik (FAP, FM200, APAR) untuk mengurangi dampak kebakaran dan cek fungsi alarm di setiap ruangan, lalu asuransi seluruh *hardware* untuk mengurangi biaya dampak kerusakan pada aset *hardware*. Menambahkan kapasitas dari *web hosting* atau dilakukannya pemakaian secara bergantian pada aset *software*. *Risk Treatment* ini adalah bagian dari penanganan yang bersifat *risk mitigate* (*control*).

Daftar Pustaka:

[1] 27035:2011. (2011). *INTERNATIONAL STANDARD ISO / IEC Information technology — Security techniques — Information security incident management*. *2011*.

[2] Departemen Teknik Informatika, U. T. (2015). *Analisis Risiko Teknologi Informasi Berbasis Risk Management Menggunakan ISO 31000*. *2*(2), 1–8. Retrieved from https://openlibrary.telkomuniversity.ac.id/pustaka/files/102538/jurnal_eproc/analisis-risiko-teknologi-informasi-berbasis-risk-management-menggunakan-iso-31000-studi-kasus-i-gracias-telkom-university.pdf

[3] ISACA. (2013). COBIT 5 For Risk. USA.

[4] ISO/IEC. (2014). *INTERNATIONAL STANDARD ISO / IEC 17788 E Information technology — Security techniques — Information security management systems — Overview and Vocabulary 2014*. *2014*(E).

[5] Iso, B. S. (2011). Risk management — Principles and guidelines. *Engineering*, *2009*.

[6] ISO, I. S. O., 1, J. T. C. I. J., Technology, I., & Subcommittee SC 27, I. S. techniques. (2008). *Iso/Iec 27005:2008*. *3*, 61. Retrieved from http://www.iso.org

[7] XYZ. (2019). SKEP.16.P.BD.II.2019_Pedoman Penerapan Manajemen Risiko.