JISKa, Vol. 1, No. 3, Januari, 2017, Pp. 145 – 152
ISSN 2527 -5836

EVALUASI MANAJEMEN KESELAMATAN PADA PUSAT DATA (STUDI KASUS PERGURUAN TINGGI XYZ)

Aniq Noviciatie Ulfah [(1)], Wing Wahyu Winarno [(2)]
Magister Teknik Informatika Universitas Islam Indonesia[(1,2)]
Jl. Kaliurang Km 14,5 Sleman, Yogyakarta
e-mail : ang.noviciatie.ulfah@gmail.com[(1)], wingwahyuwinarno@gmail.com[(2)]

Abstract

Data center was developed related to data security as one of the assets of the organization in addressing the data management for operational purposes as secondary storage media and data distribution. Safety management is part of the framework of the data center that should be assessed by the manager to determine whether compliance with the standards so as to minimize the likelihood of the risk of adverse effects on the organization. This prompted the University XYZ to evaluate the safety management to determine the extent of the implementation of safety management in the data center in their environtment. In evaluating the safety management of the data center in the University XYZ is using the standard ISO 22301: 2012. ISO 22301 is a standard that specifically to plan, establish, implement, operate, monitor, review, maintain and improve a documented management system to protect or reduce the possibility of the risk, be on the alert, handle and recover the time of the incident. The sources of data was obtained from 9 respondents who are heads / staff from each division in the data center University XYZ. The data that have been obtained will be used to measure the maturity level of each clause of the ISO 22301: 2012 and as an evaluation tools. The results obtained in this study indicate that the University XYZ has been implementing safety management in the data center with a value for each clause 5, 6, 7, 8, and 9 are sequential ie 2:42, 2:41, 1:21, 1.67, and 1.65.

Keywords : data center, management safety, ISO 22301:2012

Pusat data dikembangkan terkait dengan pengamanan data sebagai salah satu aset organisasi dalam menangani pengelolaan data untuk kepentingan operasional sebagai media penyimpanan sekunder dan pendistribusian data. Manajemen keselamatan merupakan bagian kerangka pusat data yang harus diperiksa oleh pengelola apakah sudah memenuhi standar sehingga dapat meminimalisir kemungkinan terjadinya resiko yang mengakibatkan kerugian pada organisasi. Hal ini mendorong Perguruan Tinggi XYZ untuk melakukan evaluasi terhadap manajemen keselamatan untuk mengetahui sejauh mana penerapan manajemen keselamatan pada pusat data di Perguruan Tinggi XYZ. Dalam melakukan evaluasi terhadap manajemen keselamatan pusat data di Perguruan Tinggi XYZ menggunakan standar ISO 22301:2012. Standar ISO 22301 secara spesifik merencanakan, menetapkan, menerapkan, mengoperasikan, memantau, mengkaji ulang, memelihara dan meningkatkan sistem manajemen terdokumentasi untuk melindungi atau mengurangi kemungkinan terjadinya resiko, bersiap siaga, menangani dan memulihkan diri saat terjadinya insiden. Sumber data yang diperoleh berasal dari 9 responden yang merupakan kepala/staff dari masing-masing divisi pada pusat data Perguruan Tinggi XYZ. Data-data yang telah diperoleh akan digunakan untuk mengukur tingkat kematangan dari masing-masing klausal pada ISO 22301:2012 dan digunakan sebagai bahan evaluasi. Adapun hasil yang diperoleh dalam penelitian ini menunjukkan bahwa Perguruan Tinggi XYZ sudah menerapkan manajemen keselamatan pada pusat data dengan nilai untuk klausal 5, 6, 7, 8, dan 9 secara berurut yaitu 2.42, 2.41, 1.21, 1.67, dan 1.65.

Kata Kunci : pusat data, manajemen keselamatan, ISO 22301:2012

1. PENDAHULUAN

Keselamatan adalah sebuah proses perlindungan terhadap insiden yang tidak diinginkan yang terjadi sebagai akibat dari satu atau lebih kebetulan (Albrechtsen, 2003). Menurut Sayana (2003), untuk memperoleh jaminan keselamatan yang komprehensif dari sistem maka perlu

dilakukannya penilaian dan evaluasi semua aspek keamanan jaringan komputer, keamanan aplikasi, keamanan sistem operasi, keamanan basis data, keamanan fisik dan lingkungan sekitarnya. Sama halnya dengan kebutuhan evaluasi terhadap keselamatan dari sebuah pusat data, dikarenakan menurut Bullock (2009), pusat data merupakan kumpulan server atau ruang komputer di mana sebagian besar server dan penyimpanan data terletak, dioperasikan dan diatur sehingga dalam praktiknya juga membutuhkan adanya evaluasi yang dapat memberikan gambaran terkait keselamatan dari pusat data tersebut.

Pusat data Perguruan Tinggi XYZ dikembangkan terkait kepentingan pengamanan data sebagai salah satu aset organisasi selain menangani pengelolaan data terkait kepentingan operasional sebagai media penyimpanan sekunder dan pendistribusian data. Dari hasil wawancara secara langsung dengan kepala pengelola pusat data tahun 2012-2016 mengatakan belum adanya evaluasi terhadap manajemen keselamatan dari pusat data Perguruan Tinggi XYZ, sehingga dimungkinkan sistem tersebut masih sangat rentan terhadap resiko-resiko yang ada

Manajemen keselamatan sangat penting dilakukannya evaluasi untuk meninjau apakah pusat data Perguruan Tinggi XYZ telah memenuhi standar keselamatan yang ada agar dapat menghidari terjadinya kecelakaan kerja dan keselamatan karyawan yang berada di dalam lingkungan pusat data. Terdapat beberapa framework atau kerangka kerja yang mengacu kepada referensi tata kelola teknologi informasi internasional yang telah diterima secara luas dan teruji implementasinya yaitu ISO 22301, COBIT dan ITIL, yang dapat diimplemetasikan sesuai dengan kondisi perusahaan yang berbeda-beda. Standar ini berfokus terhadap keamanan ataupun keselamatan informasi secara non-fisik (lingkungan yang mempengaruhi sistem).

Penelitian ini membantu organisasi dalam menganalisa manajemen keselamatan, standar yang digunakan adalah standar ISO 22301. Hal yang dijadikan pertimbangan mengapa standar ISO/IEC 22301 dipilih karena menurut BSN (2014), ISO 22301 standar ini secara spesifik merencanakan, menetapkan, menerapkan, mengoperasikan, memantau, mengkaji ulang, memelihara dan meningkatkan sistem manajemen terdokumentasi untuk melindungi atau mengurangi kemungkinan terjadinya resiko, bersiap siaga, menangani dan memulihkan diri dari insiden jika terjadi.

Dari permasalahan di atas maka diperlukan adanya penelitian untuk evaluasi keselamatan pada pusat data Perguruan Tinggi XYZ. Penelitian ini akan mengevaluasi keselamatan pada pusat data UIN Sunan Kalijaga menggunakan standar ISO 22301 bahan rekomendasi terhadap perbaikan pusat data Perguruan Tinggi XYZ dalam lingkup keselamatan pusat data.

Berdasarkan latar belakang masalah diatas dapat dirumuskan masalah sebagai berikut: Bagaimana penerapan keselamatan pada pusat data di Perguruan Tinggi XYZ dan sejauh mana penerapan keselamatan pada pusat data sesuai dengan standar ISO 22301, serta rekomendasi seperti apa yang cocok untuk meningkatkan keselamatan pada pusat data di Perguruan Tinggi XYZ?

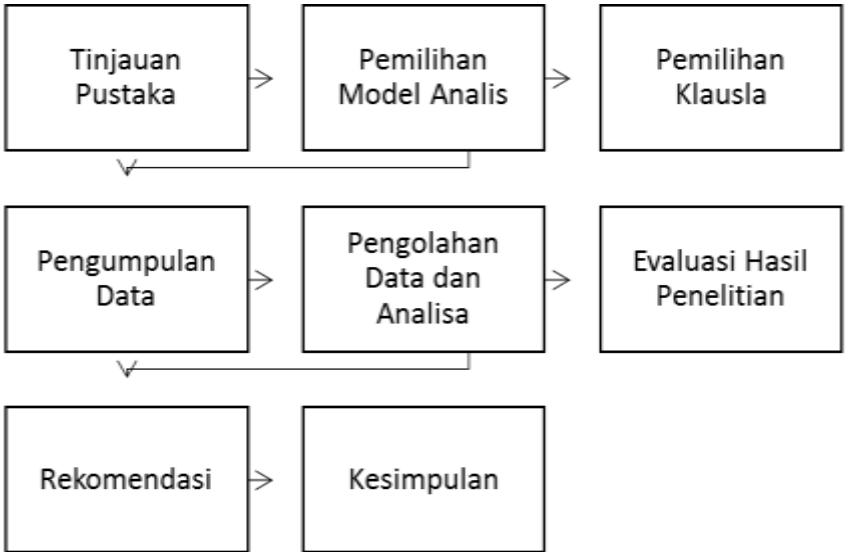
Penelitian ini bertujuan untuk memetakan dan memberikan rekomendasi perbaikan dalam manajemen keselamatan pada pusat data Perguruan Tinggi XYZ. Salah satu alat dalam melakukan penelitian adalah dengan melakukkan studi literatur, peneliti mengkaji beberapa penelitian yang berhubungan dengan penelitian yang akan dilakukan. Adapun beberapa penelitian yang dikajua adalah yaitu tentang manajemen keselamatan menggunakan ISO 22301 yang diteliti oleh Prasetyo (2016), mengenai evaluasi Business Continuity Plan and Disaster Recovery Plan menggunakan framework ISO 22301 pada Lembaga Negara XYZ. Hasil yang diperoleh berupa pemetaan Business Continuity Plan and Disaster Recovery Plan yang sesuai dengan kondisi perusahaan.

Penelitian selanjutnya dilakukan Yanthestya & Gondodiyoto (2013), terkait evaluasi Business Continuity Plan and Disaster Recovery Plan menggunakan standar ISO 22301 dimana hasil penelitian yang dilakukan dapat digunakan oleh perusahaan dapat menanggulangi bencana. Penelitian lainnya mengenai evaluasi Business Continuity Plan dilakukan oleh Humdiana

(2010), yang menghasilkan pemetaan Business Continuity Plan dan rekomendasi yang sesuai pada PT. TAM.

2. METODE PENELITIAN

Dari kajian pustaka terhadap beberapa referensi diatas, peneliti menerapkan metode *maturity model* untuk menghitung tingkat kematangan manajemen keselamatan pusat data Perguruan Tinggi XYZ. Adapun dalam melakukan penelitian ini, peneliti menggunakan metodologi penelitian yang dapat dilihat pada Gambar 1.



Gambar 1. Metode Penelitian

3. HASIL DAN PEMBAHASAN

Menurut Bullock (2009), pusat data dikenal sebagai kumpulan server atau ruang komputer di mana sebagian besar server dan penyimpanan data terletak, dioperasikan dan diatur. Dalam memperoleh kondisi pusat data yang optimal maka perlu adanya manajemen kelangsungan usaha. Sistem Manajemen Kelangsungan Usaha (SMKU) dapat digunakan untuk menilai kemampuan suatu organisasi dalam memenuhi kewajiban dan kebutuhan kelangsungan usahanya. Tujuan SMKU ini agar organisasi dapat menjalin komunitas yang lebih luas dan dampak lingkungan organisasi terhadap organisasi, serta organisasi lainya mungkin perlu dilibatkan dalam proses pemulihan (BSN, 2014).

Peneliti menggukan standar ISO 22301 yang digunakan untuk mengidentifikasi dasar-dasar sistem manajemen keberlangsungan usaha, membangun proses, prinsip dan terminologi manajemen kontinuitas bisnis. Standar ini antara lain, bertujuan untuk dapat memberikan dasar acuan bagi suatu perusahaan atau organisasi, agar dapat memahami, mengembangkan, dan menerapkan manajemen kelangsungan binsis pada suatu organisasi bahwa organisasi tersebut dapat terus beroperasi walaupun sedang mengalami keadaan bencana. Dalam penerapannya peneliti menggunakan klausal 5, 6, 7, 8 dan 9 serta menggunakan 17 objektif kontrol. Hal ini dikarenakan klausal-klausal tersebut cocok untuk evaluasi manajemen keselamatan pada Perguruan Tinggi XYZ.

Dari 17 objektif kontrol tersebut diperoleh 66 kontrol yang digunakan peneliti untuk memperoleh data guna penelitian yang dilakukan. Data tersebut diperoleh dari hasil wawancara, observasi dan penyebaran kuisioner yang diberikan kepada 9 karyawan yang mengelola pusat pada Perguruan Tinggi XYZ.

Untuk mengukur tingkat kematangan dari data yang diperoleh maka peneliti menggunakan salah satu alat ukur dari kinerja suatu sistem adalah model kematangan (maturity level). Model

kematangan untuk pengolahan dan pengendalian pada proses sistem didasarkan pada metode evaluasi organisasi sehingga dapat mengevaluasi sendiri dari level 0 (tidak ada) hingga level 5 (sempurna). Model kematangan dirancang sebagai profil proses teknologi informasi, sehingga organisasi akan dapat mengenali sebagai deskripsi kemungkinan keadaan sekarang dan mendatang (ISACA, 2007). Gambar 2 dibawah ini merupakan urutan tingkat kematangan teknologi informasi dalam perusahaan (ISACA, 2007)

Gambar 2. Urutan Tingkat Kematangan

Jika dikelompokkan berdasarkan nilai level kematangan maka dapat dirinci seperti Tabel 1 dibawah ini:

Tabel 1. Level Kematangan Teknologi Informasi

Indeks Kematangan	Level Kematangan
0,00 – 0,49	0 - *Non Exisient* (tidak ada proses)
0,50 – 1,49	1 - *Initial /ad-hoc* (dilakukan tetapi tidak ada prosedur)
1,50 – 2,49	2 - *Repeatable but intuitive* (dilakuakn tetapi belum baku)
2,50 – 3,49	3 - *Defined process* (dilakuakan dan sudah baku)
3,50 – 4,49	4 - *Managed and measurement* (dilakukan, ada prosedur, baku serta ada monitoring)
4,50 – 5.00	5 - *Optimized* (sempurna, IT berjalan dengan baik dan organisasi dapat beradaptasi terhadap perubahan)

Perhitungan tingkat kematangan yang dilakuakan terdiri dari kematangan saat ini, tingkat kematangan yang diharapkan dan analisis kesenjangan.

Perhitungan kematangan saat ini menggunakan metode Capability Maturity Model for System Security Engineering (SSE-CMM). Rumus Pers (1) yang digunakan untuk menghitung tingkat kematangan setiap kontrol.

$$\text{Indeks } 1 = \frac{\Sigma(jumlah\ nilai\ jawaban)}{\Sigma(jumlah\ responden)} \quad (1)$$

Perhitungan tingkat kematangan Pers (2) setiap objektif kontrol.

$$\text{Indeks } 2 = \frac{nilai\ maturity\ level\ setiap\ kontrol}{jumlah\ kontrol} \quad (2)$$

Perhitungan tingkat kematangan Pers (3) setiap klausal.

$$\text{Indeks } 3 = \frac{nilai\ maturity\ level\ setiap\ objektif kontrol}{jumlah\ objektif\ kontrol} \quad (3)$$

Perhitungan tingkat kematangan yang diharapkan bertujuan untuk memeberikan acuan pengembangan manajemen keamanan pada pusat data di Perguruan Tinggi XYZ. Proses dilakukan berdasarkan nilai masing-masing kontrol model kematangan untuk kemudian proses dinilai. Penilaian tingkat kematangan manajemen keamanan yang diharapkan diperoleh dari hasil wawancara yang telah dilakukan.

Setelah tingkat kematangan keamanan untuk saat ini dan tingkat kematangan keamanan yang diharapkan diperoleh, kemudian dilakukuan analisis kesenjangan (gap analysis) terhadap tingkat kematangan tersebut. Analisis ini bertujuan untuk memberikan perbaikan pada manajemen keamanan pusat data melalui kontrol model kematangan mengenai proses mana saja yang memiliki kesenjangan dan membutuhkan perbaikan. Rumus yang digunakan yaitu:

$$Indeks\ 4 = nilai\ yang\ diharapkan - nilai\ saat\ ini \quad (4)$$

Tabel 2 dibawah ini menunjukkan hasil perhitungan kuisioner untuk mendapatkan tingkat kematangan manajemen keselamatan.

Tabel 2. Hasil Perhitungan Tingkat Kematangan Manajemen Keselamatan

Klausal	Nilai	Lv	Kondisi
5	2.42	2	*Repeatable but intuitive*
6	2.41	2	*Repeatable but intuitive*
7	1.21	1	*Initial /ad-hoc*
8	1.67	2	*Repeatable but intuitive*
9	1.65	2	*Repeatable but intuitive*

Berdasarkan hasil tingkat kematangan dari hasil penyebaran kuisioner, kemudian dihitung nilai kesenjangan antara tingkat kematangan saat ini dengan tingkat kematangan yang diharapkan. Tabel 3 menunjukkan nilai kesenjangan keamanan informasi di pusat data Perguruan Tinggi XYZ.

Tabel 3. Nilai Kesenjangan Manajemen Keselamatan

Klausal	Tingkat Kematangan		Nilai Kesenjangan
	Saat ini	Yang diharapkan	
5	2.42	5.00	2.58
6	2.41	5.00	2.59
7	1.21	5.00	3.79
8	1.67	5.00	3.33
9	1.65	5.00	3.35

Nilai kesenjangan antara nilai tingkat kematangan saat ini dengan nilai tingkat kematangan yang diharapkan dapat dilihat pada Gambar 3.

Gambar 3. Perbandingan Nilai Tingkat Kematangan yang diharapkan dan saat ini

Berdasarkan hasil tingkat kematangan yang diperoleh dari penyebaran kuisioner yang diolah untuk mendapatkan nilai tingkat kematangan dari evaluasi yang dilakukan, didapatkan beberapa analisa yaitu terdapat dua tingkat kematangan yaitu Repeatable But Intuitive dan initial/ ad hoc.

Nilai yang diperoleh pada klausal 5, 6, 8, dan 9 berada pada tingkat Repeatable But Intuitive dengan nilai tingkat kematangan 2.42, 2.41, 1.67, dan 1.65. Hal ini menandakan bahwa pusat data pada Perguruan Tinggi XYZ berada pada kondisi dimana prosedur yang ada dilakukan tetapi tidak baku. Prosedur yang ada belum dikomunikasikan dengan baik, belum adanya pelatihan tanggap darurat untuk karyawan serta tanggung jawab yang diserahkan kepada individu yang dianggap memiliki kemampuan dan pengetahuan dalam tanggung jawab tersebut sehingga untuk kesalahan-kesalahan masih sering terjadi.

Prosedur yang ada pada pusat data Perguruan Tinggi XYZ sebagai berikut:

- Klausal 5 (kepemimpinan) kebijakan dan komitmen organisasi sudah berjalan dengan baik namun dokumentasi penerapan dan pemeriharaan terhadap resiko masih kurang,
- Klausal 6 (perencanaan) perencanaan terhadap resiko sudah dilakuakan tapi prosedur dan dokumentasi masih belum baku,
- Klausal 8 (operasi) pengendalian resiko dan dampak dari resiko yang dihasilkan belum dikelola dengan baik serta stategi yang akan dilakukan kedepan belum dirancang dengan baik serta pelatihan dan pengujian terhadap kejadian yang mungkin terjadi belum ada,
- Klausal 9 (evaluasi kinerja) belum di evaluasi secara berkala dan dilakukan pembenahan atau pengkajian ulang terhadap apa yang belum dibuat dalam organisasi.

Nilai yang diperoleh pada klausal 7 berada pada tingkat Initial/ ad hoc dengan nilai tingkat kematangan 1.21. Hal ini menandakan bahwa pusat data pada pusat data Perguruan Tinggi XYZ berada pada kondisi dimana segala kegiatan dilakukan tanpa adanya prosedur yang jelas. Kegiatan yang dilakukan sesuai dengan kompetansi individu dan tidak ada dokumentasi serta tidak terorganisir. Pada klausal 7 kompetensi dan kesadaran terhadap keadaan organisasi belum dipahami dengan baik oleh seluruh karyawan, komunikasi yang baik belum dilakukan, serta belum ada dokumentasi untuk seluruh kegiatan.

Berdasarkan hasil analisis yang dilakukan pada pusat data Perguruan Tinggi XYZ, maka nilai-nilai temuan akan dicocokan pada kondisi kematangan pada masing-masing kontrol ISO 22301:2012. Rekomendasi perbaikan yang diajukan peneliti sebaiknya organisasi memperbaiki manajemen dengna tingkat kematangan yang paling rendah terlebih dahulu kemudian sampai tingkat kematangan yang tertinggi. Mengingat resiko sangat mungkin terjadi jika manajemen

keselamatan yang ada pada organisasi itu bernilai rendah. Secara berurut rekomendasi yang disarankan penulias yaitu:

- Klausal 7

Manajemen perlu menanamkan kesadaran kepada seluruh karyawan mengenai pentingnya tujuan organisasi dan melakukan pelatihan penanganan gangguan kepada karyawan sesuai dengan kompetensi yang dimiliki, manajemen perlu menyediakan dan menjalin komunikasi dengan pihak dalam dan pihak luar yang relevan untuk memenuhi kelangsungan usaha yang dijalankan, manajemen perlu membuat dokumentasi dari setiap insiden yang terjadi dan dibuat serinci mungkin sehingga hal ini dapat digunakan sebagai acuan dalam penentuan kelangsungan usaha dimasa yang akan datang Manajemen harus melengkapi segaa kebutuhan sesuai dengan rencana kelangsungan usaha yang dijalankan.

- Klausal 9

Manajemen harus memantau kegiatan kelangsungan usaha secara berkala sehingga dapat mengurangi dampak yang dihasilkan akibat gangguan, manajemen perlu melakukan audit internal sehingga kelangsungan usaha yang dijalankan tetap sesuai dengan tujuan organisasi, manajemen perlu mengkaji ulang kegiatan kelangsungan usaha yang dijalankan.

- Klausal 8

Manajemen harus melengkapi segala kebutuhan sesuai denga nrencana kelangsungan usaha yang dijalankan, manajemen perlu melakukan analisis terhadap insiden-insiden yang terjadi serta dampak dari insiden tersebut sehingga tidak terjadi insiden serupa dikemudian hari, manajemen harus membuat strategi kelangsunganan usaha yang baik yang berdasarkan atas analisis dampak dan penilaian resiko yang dilakukan, manajemen perlu mengevalusi kelangsungan usaha yang dijalankan, Manajemen harus melakukan pelatihan dan pengujian terhadap prosedur kelangsungan usaha.

- Klausal 6

Manajemen perlu meninjau secara berkala kelangsungan usaha yang dijalankan sehingga kelangsungan usaha dapat berjalan secara efisien, manajemen perlu membuat dan mengkomunikasikan kebijakan kelangsungan usaha kepada seluruh karyawan.

- Klausal 5

Manajemen perlu melakukan standarisasi keselamatan pusat data sehingga manajemen keselamtan yang ada dapat diakui secara naisonal maupun internasional, manajemen harus membuat dokumentasi terkait resiko yang ada dalam kelangsungan bisnis, manajemen harus memastikan pembagian peran, tanggung jawab dan wewenang karyawan secara jelas serta dikomunikasikan kepada seluruh karyawan.

4. KESIMPULAN

Berdasarkan hasil penelitian yang dilakukan, maka didapatkan kesimpulan bahwa Perguruan Tinggi XYZ sudah menerapkan manajemen keselamatan. Hal ini dapat dilihat dari hasil tingkat kematangan pada manajemen keselamatan untuk klausal 5, 6, 7, 8, dan 9 secara berurut yaitu 2.42, 2.41, 1.21, 1.67, dan 1.65. Hal ini menunjukkan bahwa prosedur-prosedur yang terdapat pada kontrol-kontrol manajemen keselamatan sudah disampaikan dan dukungan telah dikembangkan dalam proses-proses untuk menangani tugas dan diikuti oleh setiap orang yang terlibat didalamnya. Tanggung jawab pelaksanaan diserahkan kepada setiap karyawan dimana kepercayaan terhadap karyawan sangat tinggi, sehingga kesalahan sangat mungkin terjadi.
Rekomendasi yang diberikan membutuhkan pemahaman tentang organisasi yang berkaitan dengan keselamatan pusat data dan merujuk pada standar ISO ISO 22301:2012.

DAFTAR PUSTAKA

Albrechtsen, E. (2003). Security vs safety. Retrieved October 8, 2016, from http://www.iot.ntnu.no/users/albrecht/rapporter/notat safety v security.pdf

BSN. (2014). Keamanan Masyarakat - Sistem Manajemen Kelangsungan Usaga - Persyaratan. Jakarta: BSN.

Bullock, M. (2009). Data Center Definition and Solutions. Retrieved October 10, 2016, from http://www.datacenterscanada.com/pdf/CIO - Data Center Definition and Solutions.pdf

Humdiana. (2010). Perancangan Business Continuity Plan : Studi Kasus pada PT. PAM. Jurnal Informatika Dan Bisnis, 1–9.

ISACA. (2007). CoBIT 4.1. IT Governance Institute, 1–29. https://doi.org/10.1016/S0167-4048(97)84675-5

Prasetyo, D. B. (2016). Perancangan Business Continuity Plan & Disaster Recovery Plan pada Lembaga Negara XYZ Menggunakan ISO 22301. Jakarta.

Sayana, B. S. A. (2003). Approach to Auditing Network Security. Information System Control Journal, 5, 1–3.

Yanthestya, L. M., & Gondodiyoto, S. (2013). Evaluasi Business Continuity Plan dan Disaster Recovery Plan dengan Menggunakan Standarisasi ISO 22301 pada PT Sigma Cipta Caraka. Jakarta.