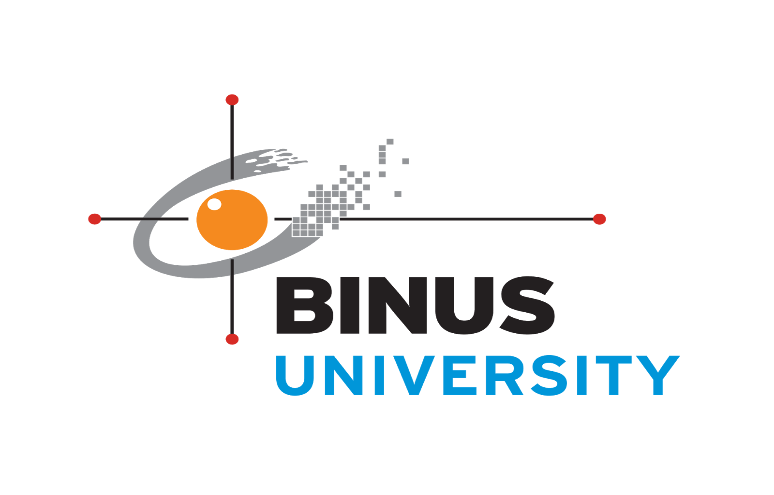
Tugas Review 5 Artikel



Disusun oleh:

Mozari Putri

2001847843

***Binus Graduate Program***

***Magister Management Of Information System***

***Binus University***

Rencana topik thesis: IS Research (IS Risk Management)

Sub-topik: Melakukan penelitian analisa resiko di satu perusahaan

Referensi paper:

1. **Penulis:**

Nugraha, U. (2016). MANAJEMEN RISIKO SISTEM INFORMASI PADA PERGURUAN TINGGI MENGGUNAKAN KERANGKA KERJA NIST SP 800-300. *Seminar Nasional Telekomunikasi dan Informatika (SELISIK 2016),* 122-126. http://jitter.widyatama.ac.id/index.php/Selisik2016/article/view/118/96

**Area masalah:**

* Mengidentifikasi, menganalisis, mengelola risiko sistem informasi akademik
* Mengembangkan strategi keamanan sistem informasi untuk meningkatkan keamanan sistem informasi, dan membuat kebijakan manajemen risiko yang mendukung misi dan prioritas organisasi untuk mengurangi dampak kerugian akibat kerusakan sistem informasi

**Pertanyaan penelitian:**

* Risiko apa saja yang dapat terjadi pada sistem informasi perguruan tinggi
* Apa saja sumber ancaman yang dapat menimbulkan risiko pada sistem informasi perguruan tinggi
* Bagaimana menggunakan kerangka kerja NIST SP 800-300 untuk melakukan penilaian risiko sistem informasi perguruan tinggi

**Metodologi:** Menggunakan framework NIST SP 800-300 untuk melakukan penilaian risiko

**Konklusi:**

* Hasil dari penilaian risiko didapat beberapa sumber ancaman yang dapat menimbulkan risiko pada sistem informasi, diantaranya keamanan sistem yang memiliki tingkat risiko tinggi, *backup* server *hang* yang memiliki tingkat risiko tinggi, dan *password* yang memiliki tingkat risiko sedang.
* Proses peringanan risiko yang dilakukan di perguruan tinggi, dengan menambah server sebagai cadangan, untuk mengantisipasi kerusakan server dan dapat melindungi data-data sensitif.
* Evaluasi kegiatan manajemen risiko sistem informasi perguruan tinggi belum dilaksanakan sesuai prosedur yang sudah ditetapkan. Untuk menghindari ancaman yang dapat menimbulkan risiko terhadap sistem informasi baru dilaksanakan secara rutin proses *backup* data saja.
* Manajemen risiko dengan menggunakan kerangka kerja NIST SP 300-80, dapat mendeskripsikan profil risiko yang dapat mengancam keberlangsungan sistem informasi.

**Rekomendasi:**

Penelitian manajemen risiko berikutnya diharapkan lebih spesifik terhadap manajemen risiko dibidang keamanan sistem yang berkaitan dengan sistem informasi berbasis online atau berkenaan dengan sistem *cloud computing*.

1. **Penulis:**

Budiarto, R. (2017). MANAJEMEN RISIKO KEAMANAN SISTEM INFORMASI MENGGUNAKAN METODE FMEA DAN ISO 27001 PADA ORGANISASI XYZ. *CESS (Journal Of Computer Engineering System And Science), 2(2),* 105-115. https://www.researchgate.net/publication/318360589

**Area masalah:**

Mengidentifikasi potensi gangguan dan permasalahan yang ada pada sistem teknologi keamanan informasi di organisasi XYZ kemudian memberikan rekomendasi kontrol yang perlu diterapkan untuk manajemen risiko keamanan informasi yang lebih baik.

**Pertanyaan penelitian:**

* Bagaimana kondisi tingkat rawan dan risiko keamanan pada sistem informasi organisasi XYZ saat ini?
* Apa saja yang menjadi akar permasalahan yang potensi menimbulkan kerawanan atau kegagalan sistem informasi organisasi XYZ?
* Bagaimanakah model manajemen risiko keamanan informasi yang seharusnya diterapkan dalam upaya meningkatkan keamanan dan kehandalan sistem informasi di lingkungan organisasi XYZ?

**Metodologi:** Menggunakan metode FMEA dan standar ISO 27001

**Konklusi:**

* FMEA merupakan salah upaya nyata yang dapat dilakukan untuk mengetahui keadaan tingkat kerawanan dari sistem informasi, mengidentifikasi penyebab potensial dari berbagai bentuk kegagalan serta mengurutkan prioritas kegagalan berdasarkan nilai RPN
* Terdapat sisi negatif dari penggunaan metode FMEA yaitu sifatnya yang reaktif terhadap risiko kegagalan ketimbang pencegahan terhadap risiko. Hal ini dikarenakan FMEA menganalisis risiko dari data sejarah kejadian berbagai mode kegagalan kemudian melakukan tindakan reaktif untuk penanggulangan atau pencegahan di kemudian hari

1. **Penulis:**

(Megawati & Kazmaini, 2018). ANALISA MANAJEMEN RESIKO SISTEM INFORMASI PERPUSTAKAAN MENGGUNAKAN COBIT 4.1 PADA DOMAIN PO9. *Jurnal Ilmiah Rekayasa dan Manajemen Sistem Informasi, 4*(1), 73-76. http://ejournal.uin-suska.ac.id/index.php/RMSI/article/download/5573/3262

**Pertanyaan penelitian:**

* Risiko apa saja yang dapat terjadi pada sistem informasi perpustakaan
* Apa saja yang menyebabkan risiko dapat terjadi pada sistem informasi perpustakaan
* Bagaimana mengimplementasikan COBIT 4.1 pada domain PO9 untuk menganalisis risiko sistem informasi perpustakaan

**Area masalah:** Penilaian resiko sistem informasi perpustakaan UIN SUSKA Riau menggunakan metode COBIT 5 pada domain PO9

**Metodologi:** Menggunakan metode COBIT 5 pada domain PO9 untuk melakukan penilaian risiko

**Konklusi:** Dari analisa resiko yang telah dilakukan, sistem informasi perpustakaan UIN SUSKA Riau telah memiliki mekanisme dan prosedur yang jelas mengenai tata cara dan manajemen IT Governance, dan telah terkomunikasikan dengan baik di seluruh jajaran manajemen dan sesuai dengan kondisi sistem yang sedang berjalan saat ini

1. **Penulis:**

Astuti, R. (2018). IMPLEMENTASI MANAJEMEN RESIKO SISTEM INFORMASI MENGGUNAKAN COBIT 5. *Media Informatika, 17*(1), 23-37. http://jurnal.likmi.ac.id/Jurnal/3\_2018/0318\_04\_Rini.pdf

**Pertanyaan penelitian:**

* Ancaman apa saja yang dapat terjadi terkait dengan organisasi
* Faktor apa saja yang dapat mempengaruhi kerentanan baik internal dan eksternal untuk organisasi
* Dampak apa saja yang mungkin terjadi terkait potensi ancaman terhadap organisasi
* Apa solusi untuk mengatasi resiko-resiko tersebut

**Area masalah:**

Menganalisis resiko pada sistem informasi digital library perguruan tinggi di Bandung menggunakan framework COBIT 5

**Metodologi:** Menggunakan framework COBIT 5 untuk melakukan analisis penilaian risiko

**Konklusi:**

Berdasarkan pengumpulan data, temuan resiko yang tinggi pada Digital Library adalah password yang jarang diganti, sedangkan dokumentasi, keamanan sistem, link, pencarian dan kecepatan akses bernilai sedang. Perancangan antarmuka aplikasi dan koneksi jaringan memiliki nilai risiko kecil.

**Rekomendasi:**

Untuk mengoptimalkan proses manajemen risiko, perlu dilakukan penangan atau tanggapan risiko dengan melakukan tindak lanjut terhadap rekomendasi berdasarkan hasil temuan risiko.

1. **Penulis:**

(Jakaria et al, 2013). Manajemen Risiko Sistem Informasi Akademik pada Perguruan Tinggi Menggunakan Metoda Octave Allegro. *Seminar Nasional Aplikasi Teknologi Informasi (SNATI),* E-37 – E-42. <https://media.neliti.com/media/publications/175059-ID-manajemen-risiko-sistem-informasi-akadem.pdf>

**Pertanyaan penelitian:**

* Kesulitan apa yang terjadi dalam menyampaikan pentingnya untuk menjaga sistem informasi beserta aset-asetnya dalam rangka menjaga keberlanjutan proses bisnis.
* Bagaimana cara melakukan penilaian risiko pada sistem informasi yang terdapat pada universitas tersebut.

**Area masalah:**

* Penilaian risiko difokuskan pada Sistem Informasi untuk melindungi aset-aset yang penting.
* Penilaian risiko dilakukan pada bagian Divisi TI yang bertanggungjawab dan mengelola Sistem Informasi Akademik.
* Metoda yang digunakan adalah OCTAVE Allegro.

**Metodologi:** Menggunakan metode OCTAVE Allegro untuk melakukan penilaian risiko

**Konklusi:**

* Penilaian risiko dapat memberikan gambaran mengenai kemungkinan adanya ancaman pada aset kritikal dan mengambil langkah – langkah pencegahan yang tepat untuk meminimalkan kemungkinan ancaman tersebut terjadi.
* Dari hasil penilaian risiko maka pembuat kebijakan dapat membuat perencanaan strategis untuk menjaga aset informasi kritikal secara tepat serta langkah – langkah pemulihan jika skenario ancaman benar – benar terjadi