PERANCANGAN KEBIJAKAN KEAMANAN SISTEM INFORMASI STUDI KASUS UNIVERSITAS PERTAMINA

PROPOSAL TUGAS AKHIR

Oleh:

Adam Marsono Putra

105216001

FAKULTAS SAINS DAN ILMU KOMPUTER

PROGRAM STUDI ILMU KOMPUTER

UNIVERSITAS PERTAMINA

2019

BAB I
PENDAHULUAN

1.1 Latar Belakang

Nama baik atau reputasi merupakan salah satu hal paling penting yang perlu dimiliki institusi pendidikan tinggi, hal ini karena reputasi merepresentasikan kualitas dari institusi yang mana menjadi landasan siswa dalam memilih institusi pendidikan tinggi (Munisamy, Jaafar, & Nagaraj, 2014). Hal ini menyebabkan institusi yang mempunyai reputasi yang lebih baik mempunyai kunggulan kompetitif yang lebih dibanding pesaingnya.

Reputasi institusi pendidikan tinggi juga berpengaruh terhadap ranking universitas (Bowman & Bastedo, 2011). Di sisi lain, Universitas Pertamina mempunyai visi "Menjadi Universitas Kelas Duni di bidang Energi paling lambat tahun 2035", hal ini artinya bahwa Universitas Pertamina akan terus berupaya supaya ranking Universitas Pertamina masuk ke jajaran Universitas Kelas Dunia, termasuk salah satunya mempertahankan dan menjaga reputasi yang baik.

Ada banyak hal yang perlu dilakukan untuk bisa mempertahankan reputasi yang baik, salah satunya adalah dengan terus berupaya dalam meningkatkan kualitas keamanan informasi, karena kualitas keamanan informasi suatu institusi mempengaruhi reputasi institusi tersebut (Safa, Solms, & Furnell, 2016). Bagaimana caranya institusi meningkatkan kualitas keamanan informasi salah satunya adalah dengan membuat kebijakan keamanan sistem informasi yang baik.

Namun pada faktanya Universitas Pertamina belum memiliki kebijakan keamanan sistem informasi (Setiawan, 2019). Padahal, selain karena alasan yang dituliskan di atas, kebijakan keamanan sistem informasi merupakan hal yang sangat penting bagi sebuah institusi pendidikan tinggi mengingat betapa pentingnya peran informasi dalam kegiatan-kegiatan utama institusi pendidikan tinggi seperti pengajaran, riset, dan pemberian beasiswa (Doherty, Anastasakis, & Fulford, 2009).

Menyadari hal tersebut, maka melakukan perancangan dan penerapan kebijakan keamanan sistem informasi di Universitas Pertamina menjadi hal yang penting sehingga hal tersebut dapat memicu peningkatan kualitas keamanan informasi di Universitas Pertamina dan meningkatkan reputasi dan nama baik Universitas Pertamina. Pada konteks ini, diusulkan penggunaan ISO/IEC 27001:2013 dan ISO/IEC 27002:2013 sebagai landasan perancangan tata kelola dan kebijakan sistem keamanan informasi di Universitas Pertamina.

ISO 27001 merupakan kerangka kerja standar internasional yang digunakan sebagai standar dalam perancangan sistem manajemen keamanan informasi, sementara ISO 27002 merupakan panduan penerapan sistem manajemen keamanan informasi untuk mencapai standar yang ditetapkan di ISO 27001 (Disterer, 2013). Pengacuan pada ISO 27002 dalam perancangan sistem manajemen

keamanan informasinya membuat Universitas Pertamina dapat mendapatkan sertifikasi ISO 27001 setelah diaudit oleh organisasi pihak ketiga, dengan begitu Universitas Pertamina dapat mendapatkan reputasi dan kepercayaan lebih baik dari siswa sebagai calon pelanggan dan juga pihak luar lain yang akan menjalin kerjasama dengan Universitas Pertamina (Disterer, 2013). Perancangan dan penerapan kebijakan keamanan informasi sebagai bagian dari sistem manajemen keamanan informasi Universitas Pertamina diharapkan dapat meningkatkan kualitas keamanan informasi Universitas Pertamina yang didasarkan pada terjaminnya kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*) informasi yang dimiliki Universitas Pertamina.

1.2 Rumusan Masalah

Belum adanya rumusan dan rancangan kebijakan keamanan sistem informasi sebagai bagian dari sistem manajemen keamana informasi di Universitas Pertamina sehingga masih kurangnya kualitas keamanan informasi di Universitas Pertamina yang menyebabkan adanya celah dan kerentanan akan terjadinya gangguan pada masalah keamanan informasi di Universitas Pertamina.

1.3 Batasan Masalah

Penelitian ini memiliki beberapa masalah yang diuraikan sebagai berikut :

1) Dalam penelitian ini membahas tentang tata kelola dan kebijakan keamanan informasi yang berfokus pada pengelolaan sistem informasi di Universitas Pertamina sehingga akan diperoleh rekomendasi-rekomendasi yang tepat untuk diterapkan dalam kebijakan pengelolaan keamanan sistem informasi di Universitas Pertamina
2) ISO/IEC 27001:2013 dan ISO/IEC 27002:2013 yang digunakan sebagai kerangka kerja perancangan dan perumusan kebijakan keamanan sistem informasi mencakup tentang kebijakan keamanan informasi secara umum, penggunaan aset TIK, penyimpanan informasi, pengendalian akses, manajemen hak akses pengguna, dan pengendalian akses terhadap aplikasi dan informasi
3) Penelitian ini merancang rumusan kebijakan keamanan sistem informasi Universitas Pertamina yang akan diterapkan berdasarkan data-data yang diperoleh dari para karyawan yang mengelola sistem informasi Universitas Pertamina dan pihak-pihak yang punya wewenang untuk mengaksesnya
4) Penelitian ini dilakukan sebatas perancangan kebijakan keamanan sistem informasi Universitas Pertamina dan pengusulan penerapan atas rancangan kebijakan keamanan sistem informasi dari hasil penelitian ini. Diterapkan atau tidaknya rancangan yang dihasilkan nantinya dikembalikan wewenang keputusannya ke pihak Universitas Pertamina.

1.5 Tujuan Penelitian

Tujuan yang hendak dicapai yaitu:

1. Terciptanya rancangan/rumusan kebijakan keamanan sistem informasi Universitas Pertamina yang memenuhi standar ISO/IEC 27001:2013 dan ISO/IEC 27002:2013
2. Terciptanya rancangan kebijakan keamanan sistem informasi yang menjamin aspek kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*) dari informasi yang dimiliki Universitas Pertamina.

1.6 Manfaat Penelitian

Manfaat yang diperoleh dari penelitian ini yaitu rumusan hasil penelitian ini dapat dijadikan sebagai tatanan kebijakan keamanan informasi Universitas Pertamina sehingga dapat meningkatkan kualitas keamanan informasi Universitas Pertamina yang ditandai dengan terjaminnya aspek-aspek penting dalam keamanan informasi, yaitu kerahasiaan (*confidentiality*), keutuhan (*integrity)*, dan ketersediaan (*availability)* melalui penerapan rancangan/rumusan kebijakan keamanan sistem informasi yang dihasilkan dari penelitian ini. Keterjaminan terhadap aspek-aspek keamanan informasi yang dihasilkan penelitian ini dapat memberikan manfaat jangka panjang berupa reputasi baik untuk institusi, dan juga manfaat jangka pendek berupa menurunnya risiko-risiko keamanan informasi yang terjadi di luar kendali.

1.7 Waktu Pelaksanaan Penelitian

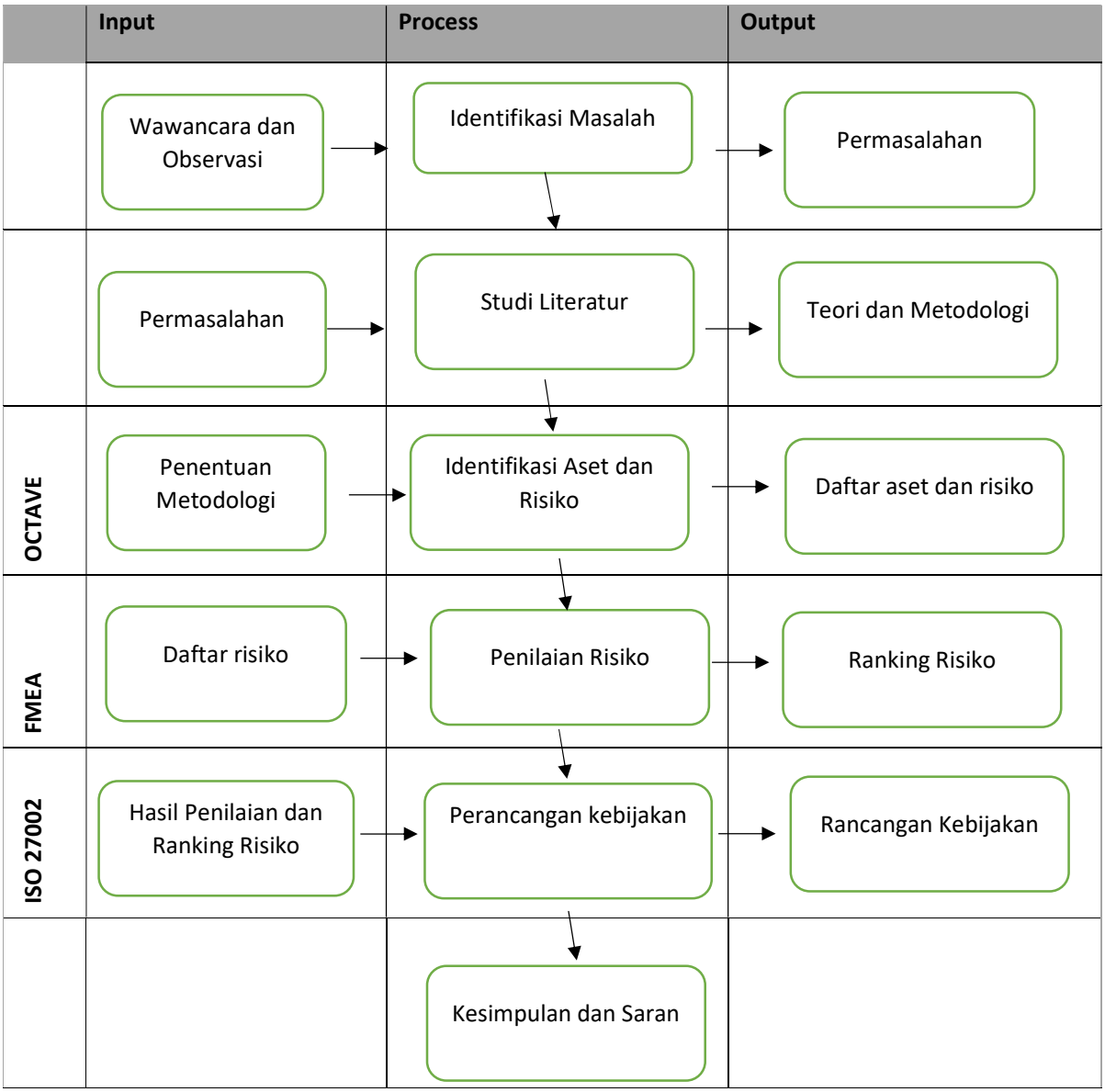
Penelitian dilakukan dari 1 Januari hingga 30 April 2019.

BAB II

METODE PENELITIAN

2.1 Metodologi Penelitian

Penelitian yang dilakukan merupakan *applied research* (penelitian terapan). Penelitian dilakukan dengan cara mengumpulkan dan menganalisis data-data terkait kondisi keamanan informasi di Universitas Pertamina saat ini dan data-data terkait karakteristik dan identitas Universitas Pertamina. Hasil analisis berupa identifikasi aset dan risiko beserta ranking risiko yang kemudian dijadikan acuan dalam merumuskan rancangan kebijakan keamanan sistem informasi Universitas Pertamina



1.2.1 Metode Pengumpulan Data

Penelitian ini menggunakan data kualitatif dan data kuantitatif sebagai landasannya. Data kualitatif berupa kondisi dan permasalahan organisasi saat ini dan data kuantitatif berupa frekuensi dari permasalahan muncul. Kedua data tersebut didapatkan melalui wawancara dan observasi terhadap objek yang terkait penelitian ini yaitu Universitas Pertamina.

1.2.2 Identifikasi Aset dan Risiko

Pemahaman terhadap hasil wawancara dan hasil observasi kemudian dijadikan landasan mengidentifikasi aset dan risiko menggunakan *Operationally Critical Threat, Asset, and Vulnerability Evaluation* (OCTAVE). Kemudian setelah risiko teridentifikasi, risiko kemudian diukur dampaknya menggunakan *Failure Mode and Effect Analysis* (FMEA)

1.2.3 Perancangan Kebijakan

Hasil identifikasi risiko yang sudah terukur kemudian dijadikan acuan bersama ISO 27002 dalam menentukan tindakan-tindakan dan aturan apa saja yang harus dicantumkan dalam rancangan kebijakan supaya kebijakan mengantisipasi risiko-risiko yang sudah teridentifikasi dan kebijakan yang dibuat memenuhi standar ISO 27001 dan ISO 27002.

1.3 Jadwal Penelitian

Berikut adalah rencana kegiatan penelitian

Kegiatan	Januari				Februari			
	M1	M2	M3	M4	M1	M2	M3	M4
Merancang metode penelitian dan metode pengumpulan data								
Melakukan pengumpulan data								
Identifikasi permasalahan, aset, risiko, dan pengukuran risiko								
Perancangan Kebijakan								

	Maret				April			
	M1	M2	M3	M4	M1	M2	M3	M4
Perancangan Kebijakan								

DAFTAR PUSTAKA

Bowman, N., & Bastedo, M. (2011). Anchoring effects in world university rankings: exploring biases in reputation scores. *Higher Education*, 431-444.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information. *Journal of Information Security*, 92-100.

Doherty, N. F., Anastasakis, L., & Fulford, H. (2009). The information security policy unpacked: A critical study of the content of. *International Journal of Information Management*, 449-457.

Munisamy, S., Jaafar, N. I., & Nagaraj, S. (2014). Does Reputation Matter? Case Study of Undergraduate Choice at a Premier University. *Asia-Pacific Education Researcher*, 451-462.

Safa, N. S., Solms, R. V., & Furnell, S. (2016). Information security policy compliance. *Computers & Security*, 70-82.

Setiawan, E. (2019, November 27). Personal Communication. (A. M. Putra, Interviewer)

SNI ISO/IEC 27001:2013. (2016). Retrieved from Sistem Informasi Standar Nasional Indonesia: http://sispk.bsn.go.id/SNI/DetailSNI/11003