PERANCANGAN KEBIJAKAN KEAMANAN SISTEM INFORMASI STUDI KASUS UNIVERSITAS PERTAMINA

LAPORAN TUGAS AKHIR

Oleh:

Adam Marsono Putra

105216001

FAKULTAS SAINS DAN ILMU KOMPUTER

PROGRAM STUDI ILMU KOMPUTER

UNIVERSITAS PERTAMINA

2020

DAFTAR ISI

Contents

BAB I
PENDAHULUAN

1.1 Latar Belakang

Sebagai institusi profesional, Universitas Pertamina yang didirikan pada tahun 2016 memiliki Visi dan Misi untuk dicapai yaitu "Menjadi Universitas Kelas Dunia di bidang Energi paling lambat tahun 2035" (Visi & Misi, 2019). Sebagai langkah konkrit mencapai visi dan misi tersebut, Universitas Pertamina menetapkan indikator-indikator pencapaian di antaranya adalah Penilaian Akreditasi Perguruan Tinggi. Dalam dokumen Penilaian Akreditasi Perguruan Tinggi, terdapat salah satunya indikator yang menyatakan keharusan adanya sistem TIK (Teknologi Informasi dan Komunikasi) untuk mengumpulkan data yang akurat, dapat dipertanggungjawabkan dan terjaga kerahasiaannya (Universitas Pertamina).

Namun pada kenyataannya, berdasarkan wawancara dengan asisten manajer keamanan informasi Universitas Pertamina, pernah terjadi insiden yang menggagalkan beberapa aspek utama keamanan informasi dalam sistem teknologi informasi dan komunikasi Universitas Pertamina (Ardi, 2019), tepatnya aspek kerahasiaan dan ketersediaan. Padahal aspek kerahasiaan merupakan yang disyaratkan pada salah satu indikator yang ada di dokumen Penilaian Akreditasi Perguruan Tinggi yang dijadikan sebagai patokan pencapaian menuju visi dan misinya.

Menurut Amanda (Andress A. , 2003), manusia beserta proses, dan teknologi yang berperan dan terlibat di dalam suatu sistem informasi merupakan pilar keamanan siber dari sistem informasi tersebut dan juga organisasi yang menerapkan sistem informasi tersebut. Hal ini yang kemudian dalam penelusuran masalah utama dalam masalah ini, ketiga aspek ini diperhatikan sebagai sumber penyebab yang mungkin menyebabkan adanya insiden-insiden keamanan informasi di Universitas Pertamina dan mengganggu kerahasiaan data-data yang disimpan di dalam sistem TIK Universitas Pertama.

Pada aspek manusia, kesadaran akan keamanan informasi yang rendah menjadi salah satu penyebab utama terjadinya insiden keamanan informasi (Siponen, Pahnila, & Mahmood, 2010). Namun untuk bisa menciptakan kesadaran terhadap keamanan informasi institusi, dibutuhkan sebuah kebijakan keamanan informasi yang dapat dijadikan patokan oleh para pihak yang terlibat tentang memahami hal-hal yang boleh dan tidak boleh dilakukan dalam menjaga keamanan informasi di sebuah institusi itu sendiri (Siponen, Pahnila, & Mahmood, 2010). Artinya adanya kebijakan keamanan informasi di suatu organisasi menjadi salah satu faktor wajib untuk mensukseskan keamanan informasi dari pilar manusia.

Kemudian pada aspek proses, kebijakan itu sendiri merupakan bentuk lain dari proses. Steven (Schlarman, 2001) menjelaskan bahwa kebijakan dapat disebut sebagai proses yang terdefinisikan oleh prosedur dan arahan yang mendukung suatu sistem keamanan informasi. Artinya kegagalan keamanan informasi dari sisi proses di Universitas Pertamina, dapat diminimalisir apabila Universitas Pertamina memiliki kebijakan yang mengatur proses-proses yang melibatkan sistem informasi Universitas Pertamina.

Steven juga menjelaskan, bahwa kebijakan keamanan informasi harusnya mencakup aspek teknologi juga, seperti contohnya standar teknologi yang diterapkan untuk menjaga informasi, siapa yang boleh menggunakan teknologi tersebut hingga cara mengoperasikan teknologi tersebut (Schlarman, 2001). Ini artinya, jika Universitas Pertamina memiliki kebijakan keamanan informasi yang mencakup hingga aspek teknologi yang digunakan, kegagalan pengamanan informasi di Universitas Pertamina yang disebabkan oleh faktor teknologi dapat diminimalisir.

Dari 3 aspek keamanan informasi yang sudah dikaji, ketiganya kemudian bermuara pada 1 solusi yang sama, yaitu keharusan adanya kebijakan keamanan informasi Universitas Pertamina. Hal tersebut yang kemudian melatarbelakangi penelitian untuk membuat rancangan kebijakan keamanan informasi Universitas Pertamina. Penelitian ini mengusulkan perancangan kebijakan keamanan informasi sebagai upaya untuk meminimalisir insiden-insiden keamanan informasi yang ada di Universitas Pertamina.

Perancangan dalam penelitian ini memerlukan data-data dan informasi terkait bagaimana kondisi keamanan informasi di Universitas Pertamina sebelum diterapkannya kebijakan keamanan informasi Universitas Pertamina. Data-data dan informasi tersebut kemudian diproses dan diolah menjadi pertimbangan dalam menilai aset (informasi dan tempat informasi tersebut bernaung) yang dimiliki Universitas Pertamina, risiko yang mungkin terjadi terhadap aset, dan ancaman yang mungkin menyerang aset.

1.2 Rumusan Masalah

Rancangan kebijakan keamanan sistem informasi seperti apa yang dapat menjamin aspek kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*) dari informasi yang ada di sistem informasi Universitas Pertamina

1.3 Batasan Masalah

Penelitian ini memiliki beberapa batasan 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) Penelitian ini merancang rumusan kebijakan keamanan sistem informasi Universitas Pertamina berdasarkan pada data-data yang diberikan aksesnya
3) 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.

1.4 Tujuan Penelitian

Tujuan yang hendak dicapai yaitu:

1. Terciptanya rancangan/rumusan kebijakan keamanan sistem informasi Universitas Pertamina yang dapat dijadikan tatanan kebijakan keamanan sistem informasi yang disahkan oleh Universitas Pertamina
2. Terciptanya rancangan kebijakan keamanan sistem informasi yang dapat meningkatkan keamanan dari informasi yang dimiliki Universitas Pertamina berdasarkan aspek kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*).

1.5 Manfaat Penelitian

Manfaat yang diperoleh dari penelitian ini yaitu di antaranya

1. Rumusan hasil penelitian ini dapat disahkan sebagai tatanan kebijakan keamanan informasi Universitas Pertamina
2. Meningkatkan kualitas keamanan informasi Universitas Pertamina yang ditandai dengan terjaminnya aspek-aspek penting dalam keamanan informasi, yaitu kerahasiaan (*confidentiality*), keutuhan (*integrity)*, dan ketersediaan (*availability)* apabila disahkannya rancangan/rumusan kebijakan keamanan sistem informasi yang dihasilkan dari penelitian ini.
3. Dalam jangka panjang meningkatkan reputasi dan nama baik Universitas Pertamina dan mendekatkan Universitas Pertamina ke visi dan misi yang akan dicapai
4. Dalam jangka pendek dapat menurunkan dan mengurangi risiko-risiko keamanan informasi yang terjadi di luar kendali.

BAB II
TINJAUAN PUSTAKA

2.1 Keamanan Informasi

Keamanan secara umum didefinisikan sebagai upaya menjaga aset (Andress J., 2014). Ini dapat diartikan bahwa upaya penjagaan bisa berupa penjagaan dari berbagai macam ancaman di antaranya penyerang, virus, bencana alam, kecelakaan, pencurian, dan hal-hal tidak diinginkan lainnya yang mengancam perubahan status pada hal yang dijaga.

Keamanan informasi didefinisikan sebagai perlindungan terhadap informasi dan sistem informasi dari akses, penggunaan, penutupan, gangguan, perubahan, dan penghancuran yang tidak terotorisasi (Andress J., 2014). Secara esensi, keamanan informasi dapat diartikan sebagai upaya perlindungan data dan informasi dari mereka yang ingin menyalahgunakannya. Namun karena keamanan secara umum mencakup hampir semua hal seperti bencana alam dan kecelakaan, maka keamanan informasi lebih tepat apabila disimpulkan sebagai upaya perlindungan data dan informasi dari segala hal yang membuat informasi dan data tersebut tidak aman.

2.1.1 Elemen dalam Keamanan Informasi

Tiga elemen/konsep utama yang ada dalam keamanan informasi di antaranya adalah kerahasiaan (confidentiality), keutuhan (integrity), dan ketersediaan (availability), yang pada umumnya disebut sebagai tritunggal CIA (Andress J., 2014). Tritunggal CIA ini yang kemudian mendefinisikan konsep aman dalam keamanan informasi yang harus dicapai (Andress J., 2014). Sehingga, untuk suatu sistem keamanan informasi dapat dikatakan aman, maka sistem tersebut harus bisa menjaga kerahasiaan, keutuhan dan ketersediaan dari informasi yang dijaga/disimpan.

Dalam definisi yang lebih mendalamnya, kerahasiaan didefinisikan sebagai ukuran seberapa mampu suatu sistem melindungi informasi dari orang-orang yang tidak berwenang atas data dan informasi tersebut. Kemudian keutuhan didefinisikan sebagai ukuran suatu sistem melindungi informasi dari pengubahan, baik parsial maupun total, yang tidak terotorisasi ataupun yang terotorisasi namun dengan cara yang tidak diharapkan. Sedangkan ketersediaan didefinisikan sebagai kemampuan atau kesiapan suatu sistem dalam menyediakan data dan informasi ketika data atau informasi tersebut dibutuhkan (Andress J., 2014).

2.1.2 Protection-Usability-Cost

Dalam bukunya (Andress J., 2014), Andress menyebutkan sebuah kutipan terkenal yang berbunyi “Satu-satunya sistem keamanan yang benar-benar aman adalah sistem yang menerapkan balok semen sebagai pelindung, di dalam ruangan yang terbuat dari baja, dan dijaga oleh penjaga bersenjata”. Meskipun sistem keamanan yang demikian bisa dianggap aman, namun sistem tersebut membuat hal yang dijaganya menjadi produktif atau bisa digunakan. Dengan sistem yang dijelaskan

dalam kutipan, tingkat keamanannya sangat tinggi namun tingkat kebermanfaatannya atau produktifitasnya jadi sangat rendah.

Selain itu, ketika melindungi aset, organisasi harus juga mempertimbangkan seberapa berharga nilai aset tersebut terhadap tingkat keamanan yang akan kita terapkan (Andress J., 2014). Sebuah organisasi bisa saja, jika ia bersedia menurunkan produktifitas aset, menerapkan pengamanan tingkat tinggi terhadap semua aset yang ia kelola, namun hal tersebut menjadi tidak masuk akal apabila ternyata biaya penerapan sistem keamanan tersebut malah lebih mahal dari nilai aset yang dilindungi.

Penyeimbangan atas keamanan, kebermanfaatan, dan biaya yang perlu dikeluarkan untuk menerapkan suatu sistem keamanan informasi ini yang kemudian menjadi tujuan diterapkannya keamanan informasi. Sehingga dapat disimpulkan bahwa keamanan informasi bertujuan untuk memastikan keberlanjutan bisnis (produktifitas akan aset yang dilindungi), meminimalkan risiko yang mungkin terjadi (aman), dan memaksimalkan keuntungan yang didapat dari investasi dan kesempatan bisnis (biaya) (Utomo, Noor, & Affandi, 2012).

2.1.3 Kebijakan Keamanan Informasi

Kebijakan keamanan informasi didefinisikan sebagai tata kelola yang terdiri dari standar keamanan yang perlu diterapkan, pembatasan kontrol, dan regulasi yang perlu diterapkan pada informasi yang dijaga (Schlarman, 2001). Secara dasar, kebijakan keamanan informasi bisa dikatakan sebagai bentuk tertulis yang menggambarkan lingkungan keamanan yang perlu diciptakan dalam rangka melindungi informasi yang ada di organisasi.

Adapun tahapan yang perlu dilakukan dalam perancangan kebijakan keamanan informasi adalah sebagai berikut (Utomo, Noor, & Affandi, 2012)

1. Mengidentifikasi dan memahami proses bisnis yang berjalan di perusahaan/organisasi
2. Menentukan standar dan kerangka kerja kebijakan keamanan informasi yang disesuaikan dengan profil perusahaan dan hasil tahap 1
3. Mengidentifikasi dan menghitung nilai aset perusahaan yang berada dalam lingkup tata kelola informasi yang ditentukan
4. Mengidentifikasi dan menilai ancaman yang mungkin mengintai aset
5. Menganalisis risiko dan mengukur dampaknya terhadap bisnis perusahaan berdasarkan standar toleransi yang ditetapkan perusahaan
6. Merancang kebijakan keamanan informasi berdasarkan standar, kerangka kerja, dan kontrol yang telah ditetapkan

2.1.4 Kerangka Kerja Keamanan Informasi

Frank Kim (Kim, 2019) menjelaskan ada beberapa kerangka kerja keamanan informasi yang pada umumnya digunakan di banyak perusahaan. Kerangka-kerangka kerja tersebut kemudian dikelompokkan menjadi 3 kelompok besar sebagai berikut

1. Kerangka Kerja Kontrol
   Kerangka kerja jenis ini biasa digunakan oleh para profesional untuk membangun sistem keamanan informasi dari awal, khususnya di perusahaan yang masih belum sadar akan keamanan informasi sama sekali. Kerangka kerja kontrol digunakan untuk cakupan kerja sebagai berikut

- Identifikasi kontrol yang akan diterapkan
- Menilai kemampuan teknis perusahaan saat ini
- Memprioritaskan implementasi kontrol
- Mengembangkan *roadmap* untuk tim keamanan informasi

Beberapa kerangka kerja yang masuk jenis ini adalah NIST 800-53 dan CIS Controls. NIST 800-53 merupakan katalog kontrol keamanan dan privasi yang isinya adalah kontrol-kontrol yang dapat diterapkan berdasarkan prioritas dan *baseline*. Sedangkan CIS Controls berisi 20 kontrol keamanan kritis teratas (Kim, 2019).

2. Kerangka Kerja Program
   Kerangka kerja program digunakan untuk cakupan kerja sebagai berikut
   - Menilai keadaan keseluruhan dari organisasi
   - Membangun program keamanan yang komprehensif
   - Menyederhanakan komunikasi dengan para pimpinan bisnis
   - Mengukur kesiapan perusahaan dan riset perbandingan industri

   Dalam jenis ini, 2 di antaranya adalah ISO 27001 dan NIST CSF. Seri ISO 27000 merupakan kumpulan standar yang semuanya berkaitan dengan keamanan informasi. ISO 27001 mencakup tata kelola keamanan informasi dan mendefinisikan area-area yang akan difokuskan dalam membangun sistem keamanan informasi di antaranya kepemimpinan, perencanaan, dukungan, operasi, hingga evaluasi (Kim, 2019).

   Sementara NIST CSF adalah framework yang lebih jelas pembagian komponennya namun lebih condong ke pengelolaan risiko. NIST CSF terdiri dari 3 komponen utama : Core, Implementation Tiers, dan Profile. Pembedaan yang jelas ini membantu perusahaan mempertanyakan “Apa yang kita lakukan sekarang? Bagaimana kita melakukannya? Ke arah mana kita akan menuju? Kapan kita akan sampai di sana?” (Kim, 2019).

3. Kerangka Kerja Risiko
   Sebagaimana namanya, kerangka kerja ini digunakan khususnya untuk pengelolaan risiko, di antaranya :
   - Mendefinisikan proses-proses penting dalam menilai dan mengelola risiko
   - Menstrukturisasi program pengelolaan risiko
   - Mengidentifikasi, mengukur, dan mengkuantifikasi risiko
   - Memprioritaskan aktivitas-aktivitas keamanan informasi

BAB III
METODE PENELITIAN

3.1 Metodologi Penelitian

Penelitian yang dilakukan merupakan *applied research* (penelitian terapan). Penelitian dilakukan dengan cara mengumpulkan dan menganalisis data-data dan informasi terkait karakteristik, identitas dan proses bisnis yang dimiliki Universitas Pertamina. Hasil analisis berupa pemahaman terhadap proses bisnis di Universitas Pertamina beserta gambaran tentang keadaan keamanan informasi di Universitas Pertamina. Penelitian kemudian dilanjutkan dengan mengidentifikasi aset yang dicakup oleh sistem informasi Universitas Pertamina, beserta ancaman yang mengintai aset serta risiko yang terjadi apabila ancaman terlanjur terjadi. Hasil tahapan tersebut kemudian dijadikan landasan dalam memilih kontrol apa saja yang akan diterapkan di kebijakan keamanan informasi yang akan dirancang.

3.2 Metode Pengumpulan Data

Penelitian ini menggunakan data kualitatif dan data kuantitatif sebagai landasannya. Data kualitatif di antaranya berupa kondisi dan permasalahan organisasi saat ini dan data kuantitatif di antaranya berupa frekuensi dari permasalahan muncul serta jumlah aset yang dimiliki perusahaan. Kedua data tersebut didapatkan melalui berbagai cara di antaranya pengajuan akses terhadap informasi perusahaan, wawancara, dan pengamatan.

3.3 Pemahaman Terhadap Proses Bisnis dan Profil Perusahaan

Tahap pertama dari penelitian ini adalah memahami proses bisnis yang saat ini dijalankan oleh perusahaan dan profil. Tahap ini dilakukan dengan cara mendapatkan akses terhadap informasi-informasi operasional perusahaan tentang bagaimana informasi dikelola di perusahaan. Selain informasi operasional, proses ini juga mencakup tahapan mendapatkan informasi profil perusahaan di antaranya rencana strategis perusahaan, roadmap visi-misi, serta parameter yang digunakan perusahaan dalam menilai capaian khususnya kinerja sistem informasi perusahaan. Hal ini dibutuhkan untuk mengukur seberapa darurat dan siap perusahaan dalam mengadaptasi penerapan kebijakan keamanan informasi serta menentukan kerangka kerja kebijakan informasi yang tepat bagi perusahaan.

3.4 Identifikasi Aset, Ancaman, dan Risiko

Tahap selanjutnya adalah proses pengumpulan data utama. Tahapan ini mencakup proses mendapatkan data dan informasi terkait aset-aset yang tercakup dan berkaitan dengan sistem informasi perusahaan. Data aset tersebut kemudian digunakan untuk mengidentifikasi ancaman pada tiap aset. Kemudian ancaman-ancaman yang sudah diidentifikasi dikuantifikasi berdasarkan seberapa sering kemungkinan ancaman tersebut datang. Dari tiap-tiap ancaman, risiko-risikonya

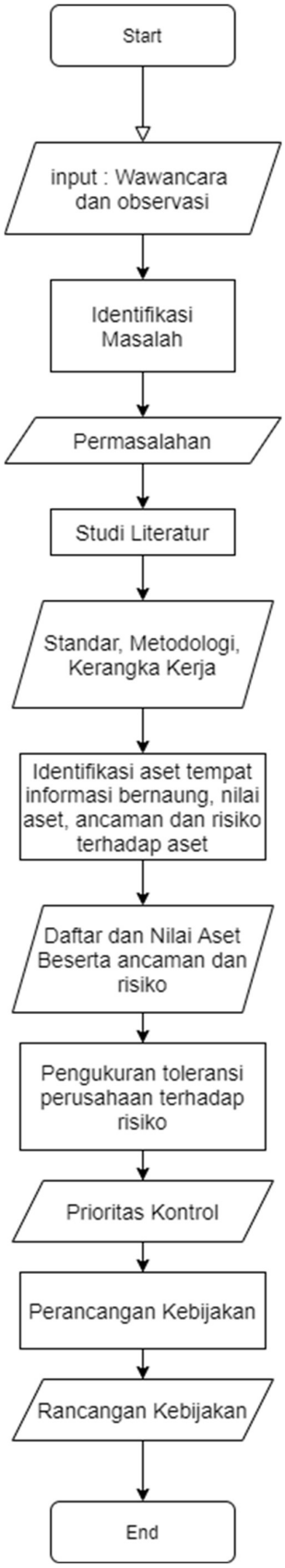

Diagram 1. Diagram Metodologi Penelitian

kemudian diukur berdasarkan seberapa besar dampak terhadap perusahaan. Ukuran besar-kecil dampaknya terhadap perusahaan mengacu pada standar toleransi perusahaan terhadap risiko dan kerugian. Hasil dari tahap ini adalah didapatkannya daftar aset perusahaan beserta kuantifikasi seberapa besar risikonya apabila aset tersebut mengalami gangguan akibat ancaman yang sudah diidentifikasi.

3.5 Penentuan Kontrol dan Perancangan Kebijakan

Hasil identifikasi risiko yang sudah terukur relatif terhadap standar perusahaan kemudian dijadikan acuan dalam memilih kontrol yang ada dalam kerangka kerja tata kelola keamanan informasi yang sebelumnya sudah ditetapkan. Kontrol-kontrol ini yang kemudian dijadikan acuan dalam menilai dan mengubah proses dan standar operasional yang saat ini berjalan di perusahaan. Proses-proses yang kemudian sudah sesuai dengan standar dan kontrol yang ditetapkan kemudian dijadikan satu menjadi dokumen kebijakan keamanan informasi yang dapat dijadikan acuan oleh perusahaan dalam mengambil keputusan-keputusan di masa depan.

DAFTAR PUSTAKA

Andress, A. (2003). *Surviving Security : How to Integrate People, Process, and Technology.* New York: Auerbach Publications.

Andress, J. (2014). *The Basics of Information Security.* Elsevier.

Ardi. (2019, November 29). Manager Assistant in Information Security, Pertamina University. (A. M. Putra, Interviewer)

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 university policies. *International Journal of Information Management*, 449-457.

Kim, F. (2019, Maret 4). How to Make Sense of Cybersecurity Frameworks. RSA Conference. Retrieved Maret 3, 2020, from https://www.youtube.com/watch?v=dt2IqidgpS4

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.

Schlarman, S. (2001). The People, Policy, Technology (PPT) Model: Core Elements of the Security Process. *Information Systems Security*, 1-6.

Setiawan, E. (2019, November 27). Director of Assets and IT, Pertamina University. (A. M. Putra, Interviewer)

Siponen, M., Pahnila, S., & Mahmood, A. (2010). Compliance with Information Security Policies: An Empirical Investigation. *Computer*, 64-71.

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

Universitas Pertamina. (n.d.). *Penilaian Akreditasi Perguruan Tinggi (APT 3.0).* Jakarta: Satuan Penjaminan Mutu Universitas Pertamina.

Utomo, M., Noor, A. H., & Affandi, I. (2012). Pembuatan Tata Kelola Keamanan Informasi Kontrol Akses Berbasis ISO/IEC 27001:2005 Pada Kantor Pelayanan Perbendaharaan Surabaya I. *Jurnal Teknik ITS*, 288-293.

Visi & Misi. (2019, December 12). Retrieved from Universitas Pertamina: https://universitaspertamina.ac.id/visi-misi/