IDENTIFIKASI RISIKO KEAMANAN INFORMASI MENGGUNAKAN ISO 27005 PADA SEBUAH PERGURUAN TINGGI SWASTA DI SURABAYA

Syukron Salahuddin [1], Awalludiyah Ambarwati [2], Mohammad Noor Al Azam [3]

[1] Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Narotama
Email : syukronsalahuddin@gmail.com
[2] Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Narotama
Email: ambarwati1578@yahoo.com
[3] Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Narotama
Email: noor@rad.net.id

Abstrak

Penerapan Teknologi Informasi/Sistem Informasi (TI/SI) yang selaras dengan visi dan misi suatu perguruan tinggi dapat memberikan nilai tambah dan keunggulan skompetitif. Informasi dalam bentuk digital yang dihasilkan dari penerapan TI/SI tersebut merupakan aset yang sangat berharga. Aset yang dimiliki harus dijaga dan dilindungi dari risiko. Penelitian ini bertujuan untuk melakukan identifikasi risiko keamanan informasi menggunakan ISO 27005 pada sebuah perguruan tinggi swasta (PTS) di Surabaya. Hal ini dilakukan karena adanya beberapa kejadian yang dialami PTS tersebut, salah satunya berupa peretasan website yang digunakan untuk layanan akademik, sehingga mengakibatkan terganggunya layanan bagi civitas akademik. Identifikasi risiko dilakukan untuk mengetahui potensi kerugian dan penyebab terjadinya kerugian sehingga dapat dilakukan tindakan pengamanan yang bersifat pencegahan, deteksi maupun koreksi. Hasil penelitian berupa dokumentasi identifikasi risiko keamanan informasi dan rekomendasi kontrol yang sesuai kebutuhan.
Kata kunci: identifikasi risiko, ISO 27005, keamanan informasi

Abstract

Information Technology/Information Technology (IT/SI) implementation which aligned with the vision and mission of a university can provide added value and competitive advantage. Digital information resulting from the IT/SI implementation is a very valuable asset. Those assets must be safeguarded and protected against risk. This study aims to identify information security risks using ISO 27005 at a private university in Surabaya. This research conducted because of several incidents happened in this private university, one of the incident is hacking of academic services website, thus resulting in disruption of services for the academic community. Risk identification is performed to determine the potential loss and cause of loss so that security measures can be prevented, detected or corrected. The result of the research is documentation of risk identification of information security and recommendation of control as needed.
Keyword: *information security, ISO 27005, risk identification*

I. PENDAHULUAN

Penerapan Teknologi Informasi/Sistem Informasi (TI/SI) yang selaras dengan visi dan misi suatu perguruan tinggi dapat memberikan nilai tambah dan keunggulan kompetitif. Informasi dalam bentuk digital yang dihasilkan dari penerapan TI/SI tersebut merupakan aset yang sangat berharga. Aset yang dimiliki harus dijaga dan dilindungi dari risiko. Sedangkan

risiko dapat diartikan sebagai kemungkinan terjadinya insiden yang merusak (bila ada ancaman karena adanya kerentanan), serta kemungkinan kerusakan jika insiden tersebut terjadi (Jones and Ashenden, 2005; Dewi, Ambarwati and Darujati, 2018).

Salah satu perguruan tinggi swasta (PTS) di Surabaya telah menerapkan dan mengembangkan TI/SI untuk mendukung kegiatan operasional. PTS ini mengimplementasikan SIM-PTS yang merupakan suatu sistem informasi manajemen yang mendukung kegiatan operasional dan digunakan oleh mahasiswa, dosen, maupun pegawai. Versi pertama SIM-PTS dibuat oleh vendor yang kemudian dikembangkan secara berkala oleh Departemen Sistem Teknologi Informasi (DSTI), departemen yang bertanggung jawab atas pengembangan dan operasional TI/SI dilingkungan PTS. Kehadiran SIM-PTS ini dinilai sangat penting dalam mendukung kegiatan operasional dan penyampaian informasi ke seluruh civitas akademika. Layanan SIM-PTS harus dijaga untuk tersedia selama kegiatan akademik berlangsung.

Beberapa kendala yang sering dialami belakangan ini, adalah sulitnya akses pengguna akibat paket data yang dikirim ke server melebihi kapasitas yang adakalanya membuat *server down*. Selain itu pernah beberapa kali terjadi peretasan *website* yang digunakan untuk layanan akademik, juga beberapa ancaman lain yang melumpuhkan layanan SIM-PTS sehingga mengakibatkan terganggunya beberapa layanan bagi civitas akademika. Untuk menghindarinya kejadian yang sama terulang kembali di masa yang akan datang, perlu dilakukan identifikasi risiko.

Penelitian ini bertujuan untuk melakukan identifikasi risiko keamanan informasi menggunakan ISO 27005/2011 pada sebuah PTS di Surabaya. ISO 27005/2011 merupakan standar internasional yang menyediakan *guidelines* (pedoman) untuk *information security risk management* pada suatu organisasi. Identifikasi risiko bertujuan untuk menentukan apa yang dapat terjadi hingga memiliki potensi menyebabkan kerugian, dan untuk mendapatkan wawasan tentang bagaimana, di mana dan mengapa kerugian tersebut dapat terjadi (International Standard, 2011).

II. KAJIAN LITERATUR

Adanya ancaman yang pernah terjadi di beberapa bank yang telah menerapkan sistem informasi yang berbasis komputer mengakibatkan kerugian cukup besar bagi bank tersebut. Untuk itu perlu dilakukan peningkatan keamaan informasi didalam menjamin kualitas informasi. Perancangan model sistem manajemen sekuritas informasi (SMSI) dilakukan berdasarkan dampak manajemen risiko, yaitu Perancangan atas Dokumen Pengembangan Sistem, Perancangan atas Standar Operasional Prosedur (SOP), Perancangan atas Penanggungjawab Sistem, Perancangan atas Peraturan Penggunaan Sistem Informasi serta Perancangan dalam Sosialisasi Sistem Informasi. Setiap perusahaan hendaknya mengembangkan atau membangun Sistem Manajemen Sekuritas Informasi (SMSI) yang berbasis aplikasi ISO 27001 dan ISO 27005, agar segala risiko yang sering terjadi pada pemanfaatan sistem informasi sudah dapat diantisipasi lebih dini (Taufiq, 2016).

Kerahasiaan, keutuhan, dan ketersediaan merupakan konsep utama keamanan sistem suatu informasi. Untuk mengetahui tingkat risiko dan kondisi keamanan pada Badan Pertanahan Nasional dilakukan *Risk Assessment* menggunakan ISO/IEC 27005. Objek penelitian berupa sebuah infrastruktur aliran data digital data – data pertanahan dan database OLTP serta OLAP pada Badan Pertanahan Nasional. Risiko yang telah teridentifikasi diprioritaskan

berdasarkan penilaian yang ditentukan menurut standar ISO mulai dari prioritas risiko mana yang paling berpengaruh ke tingkat risiko yang paling kecil (Yudha and Gunadhi, 2016).

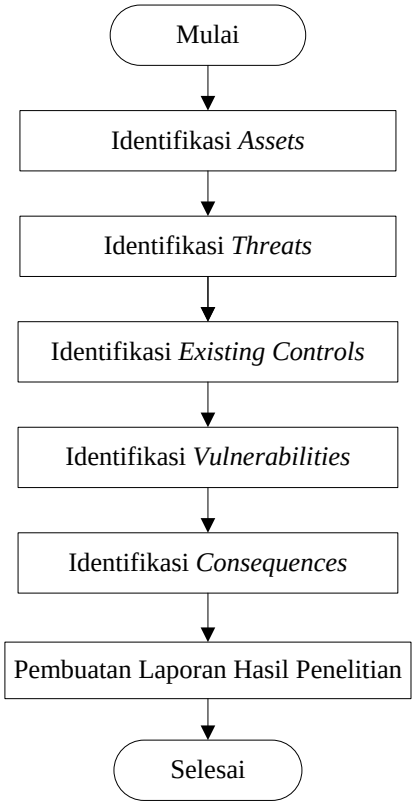
Lembaga Penerbangan dan Antariksa Nasional (LAPAN) telah menerapkan pengelolaan informasi yang terkomputerisasi yang berisiko sehingga dapat mengganggu kinerja organisasi maupun operasional. Risiko dapat disebabkan oleh manusia atau sistem yang digunakan. LAPAN perlu memiliki manajemen risiko yang merupakan suatu pengelolaan yang melihat potensi-potensi atau hal-hal apa saja yang harus dilakukan agar dapat meminimalkan risiko sekecil mungkin yang dapat terjadi sewaktu-waktu. Manajemen risiko dilakukan menggunakan ISO 27005:2011 mencakup proses manajemen risiko yang dilakukan pada klausul *context establishment* (klausul 7) dan *risk assessment* (klausul 8). Penilaian dan analisi risiko dilakukan pada 21 daftar aset yang menunjukan perangkat keras merupakan aset bernilai 3 dan 4 (*high* dan *very high*). Penilaian risiko menunjukkan level risiko cenderung berada pada *risk acceptance level*, namun ada beberapa aset yang memiliki level risiko diantara 6-8 (*high risk*) seperti hilangnya pasokan listrik, kerusakan pada perangkat keras, sehingga harus dilakukan penanganan yang sesuai (Imbar and Ayala, 2018).

Ketiga penelitian tersebut menjadi rujukan dalam melakukan penelitian identifikasi risiko keamanan informasi menggunakan ISO 27005/2011 pada sebuah PTS di Surabaya. Identifikasi risiko dilakukan untuk mengetahui potensi kerugian dan penyebab terjadinya kerugian sehingga dapat dilakukan tindakan pengamanan yang bersifat pencegahan, deteksi maupun koreksi.

III. METODE PENELITIAN

Identifikasi risiko berdasarkan ISO 27005/2011 terdiri dari lima tahapan, yaitu identifikasi *assets*, *threats*, *existing controls*, *vulnerabilities* dan *consequences* (International Standard, 2011). Aset merupakan sesuatu yang bernilai bagi organisasi sehingga perlu perlindungan. Aset sistem informasi lebih dari sekedar *hardware* dan *software* melainkan juga *information, processes and systems*.

Tahapan penelitian dapat dilihat pada Gambar 1. Pengumpulan data dilakukan melalui observasi dan wawancara kepada pimpinan dan staf DSTI.



Gambar 1. Tahapan penelitian

Tahap pertama adalah identifikasi aset yang harus dilakukan pada level rincian yang sesuai sehingga memberikan cukup informasi untuk penilaian risiko. Level rincian yang digunakan pada identifikasi aset akan mempengaruhi jumlah

keseluruhan informasi yang dikumpulkan selama penilaian risiko. Level tersebut dapat disempurnakan dalam iterasi lebih lanjut dari penilaian risiko. Pemilik aset perlu diidentifikasi untuk setiap aset yang dimiliki sehingga dapat diketahui *responsibility* and *accountability*. Pemilik aset bisa jadi tidak memiliki *property rights* pada aset tersebut, tetapi memiliki tanggung jawab dalam *production, development, maintenance, use and security*.

Tahap kedua adalah identifikasi *threats*. Ancaman memiliki potensi yang dapat membahayakan aset yang dimiliki organisasi seperti *information, processes and systems.* Ancaman bisa berasal dari alam atau manusia, dan bisa disengaja atau tidak disengaja. Ancaman dapat ditimbul dari dalam maupun luar organisasi. Sumber ancaman tersebut dapat diidentifikasi secara umum ataupun berdasarkan jenis ancaman, seperti *unauthorized actions, physical damage, technical failures*. Setiap ancaman dapat diidentifikasi termasuk ancaman yang tidak diharapkan. Beberapa ancaman dapat memengaruhi lebih dari satu aset. Suatu ancaman dapat menyebabkan dampak yang berbeda pada suatu aset.

Ketiga, identifikasi *existing controls* harus dilakukan untuk menghindari pekerjaan berulang atau biaya yang tidak perlu, misalnya dalam duplikasi kontrol. Selain itu, sementara mengidentifikasi kontrol yang ada, pemeriksaan harus dilakukan untuk memastikan bahwa kontrol bekerja dengan benar.

Keempat, identifikasi *vulnerabilities* dilakukan pada bidang Organisasi, Proses dan prosedur, Rutinitas manajemen, Personel, Lingkungan fisik, Konfigurasi sistem Informasi, Perangkat keras, perangkat lunak atau peralatan komunikasi serta Ketergantungan pada pihak luar. Keberadaan dari suatu kerentanan tidak menyebabkan bahaya, karena perlu ada ancaman yang hadir untuk memanfaatkannya.

Sebuah kerentanan yang tidak memiliki ancaman terkait bisa jadi tidak memerlukan pelaksanaan kontrol, tetapi harus dikenali dan dipantau untuk perubahan. Penerapan kontrol yang tidak tepat atau tidak berfungsinya pengendalian atau pengendalian yang digunakan secara tidak benar bisa menjadi kerentanan. Kontrol dapat efektif atau tidak efektif tergantung pada lingkungan tempat beroperasi. Sebaliknya, ancaman yang tidak memiliki kerentanan yang sesuai bisa jadi tidak menimbulkan risiko.

Tahap terakhir adalah identifikasi *consequences* yang dilakukan untuk mengetahui kerusakan atau konsekuensi kepada organisasi yang dapat disebabkan oleh skenario insiden. Sebuah skenario insiden adalah deskripsi ancaman yang mengeksploitasi kerentanan tertentu atau serangkaian kerentanan dalam insiden keamanan informasi. Konsekuensi dapat berupa kehilangan efektivitas, kondisi operasi yang merugikan, kerugian bisnis, reputasi, kerusakan dan lain sebagainya. Konsekuensi bisa jadi bersifat sementara atau mungkin permanen seperti dalam kasus perusakan aset.

Suatu organisasi dapat melakukan identifikasi konsekuensi operasional dari skenario insiden dalam hal (namun tidak terbatas pada):

a. Investigasi dan waktu perbaikan.
b. Waktu (kerja) yang hilang.
c. Peluang yang hilang.
d. Kesehatan dan keselamatan.
e. Biaya keuangan akan keterampilan khusus untuk memperbaiki kerusakan.
f. Kesan nama baik dan iktikad baik.

IV. HASIL DAN PEMBAHASAN

PTS ini memiliki aset yang tersebar di beberapa lokasi, yaitu lokasi dalam lingkungan kampus dan lokasi mitra. Tabel

1 menyajikan aset yang dimiliki PTS yang diklasifikasikan menjadi aset utama dan aset pendukung. Sedangkan Tabel 2 menyajikan identifikasi *threats* terhadap aset yang dimiliki PTS, beserta penyebab dan sumber ancaman.

Tabel 1. Identifikasi Aset yang dimiliki PTS

No	Aset	Jenis Aset	Lokasi Aset
1.	Aplikasi Pelayanan Online SIM-PTS	Aset Utama	1. Ruangan Server 2. DSTI
2.	*Windows Server* (Proxmox, FreeBSD, VMWareESXI)	Aset Pendukung	1. Ruangan Server 2. RadNet (Plaza BRI lt8)
3.	*Firewall*	Aset Pendukung	Ruangan Server
4.	PC (4 Unit)	Aset Pendukung	1. Ruangan Server (3 Unit) 2. RadNet (Plaza BRI lt8)
5.	*Storage Server*	Aset Pendukung	Ruangan Server
6.	*Database Server*	Aset Pendukung	Ruangan Server
7.	UPS *(Uninterruptible Power Supply)*	Aset pendukung	Ruangan Server
8.	HP Compaq 8100 Elte CMT	Aset Utama	Ruangan Server
9.	IBM DS3924 SAN Storage	Aset Pendukung	Ruangan Server
10.	IBM X3950 M2	Aset Pendukung	Ruangan Server
11.	IBM x3400 M3	Aset Pendukung	RadNet (Plaza BRI lt 8)
12.	*Rack Network*	Aset Pendukung	1. DSTI 2. Keuangan 3. Perpustakaan 4. Gedung E 5. Gedung A lt 7 6. Ruangan Server
13.	*Routers*	Aset Utama	DSTI
14.	Dell Power EDGE T320	Aset Pendukung	Ruangan Server
15.	*Mikrotik Switch*	Aset Pendukung	1. Perpustakaan (3 Unit) 2. Gedung E1.03 (2 Unit) 3. Gedung A7.01 4. Gedung A4.01 5. Ruang DPM 6. DSTI 7. Biro Rektor (2 Unit) 8. Ruang LPPM

Sumber: hasil penelitian, diolah kembali

Tabel 2. Identifikasi Threats

No	Aset	Ancaman	Penyebab Ancaman	Sumber Ancaman
1	Aplikasi Pelayanan Online SIM-PTS	Layanaan Tidak Jalan	Aplikasi erorr/tidak bisa diakses karena proses *troubleshooting* membutuhkan waktu lebih lama	1. Teknisi 2. Pengembang Aplikasi
		Modifikasi	1. *Defacing* 2. DDoS *(Dsitributed Denial of Service)*	*Hacker*
2	*Windows Server* (Proxmox, FreeBSD, VMWare ESXI)	Windows tidak berjalan dengan semestinya	Terdapat banyak virus di PC	Virus
3	*Firewall*	Layanan tidak jalan	Adanya kebijakan yang membatasi aplikasi. Power listik mati.	1. Teknisi 2. *Source Power*
		Password Lemah atau menggunakan *default password*	Mengubah konfigurasi yang tidak sesuai degan standar oleh pihak yang tidak berwenang	*Hacker*
4	PC	PC error	Banyaknya virus yang terdapat di PC. Terdapat kendala didalam *hardware* atau *software*.	Virus
5	*Storage Server*	*Password* Lemah atau menggunakan *default password*	Akses yang dilakukan oleh pihak yang tidak berwenang	1. Teknisi 2. Pengembang Aplikasi 3. *Hacker*
6	*Database Server*	Server aplikasi dan database tidak ada konfigurasi standar keamanan.	Akses yang dilakukan oleh pihak yang tidak berwenang untuk mengubah konfigurasi pada *database* server.	1. Teknisi 2. Pengembang Aplikasi 3. *Hacker*
7	UPS	Baterai pada ups tidak dapat menyimpan daya	UPS terlalu banyak beban untuk melakukan *cover* dari perangkat lunak yang melebihi dari ketentuan	Teknisi

Sumber: hasil penelitian, diolah kembali

Identifikasi *existing controls* dilakukan untuk mengetahui kontrol yang telah diterapkan pada aset yang dimiliki PTS, sebagai berikut:

a. Aplikasi Pelayanan *Online* SIM-PTS
    1. Menerapkan DRP (*Disaster Recovery Plan*)
    2. Melakukan pembekalan terhadap help desk terkait *problem solving*
b. Windows Server (Proxmox, FreeBSD, VMWareESXI)
    1. *Install* Antivirus
    2. *Update* Antivirus
    3. Membuat *privileges user*
    4. Hanya beberapa personel saja yang mempunyai hak akses terhadap server dan *data center*
    5. Menerapkan DRP
c. PC (*Personal Computer*)
    1. *Install* Antivirus
    2. *Update* Antivirus
    3. Akses ke internet tidak diperkenankan, hanya dapat akses server aplikasi pelayanan *online*
    4. Tidak bisa install program illegal
    5. Menerapkan DRP
d. *Storage Server*
    1. Menerapkan SMKI (Sistem Manajemen Keamanan Informasi)
    2. Ditempatkan di *data center* yang sudah memenuhi standar keamanan
e. *Database Server*
    1. Menyusun konfigurasi standar keamanan informasi
    2. Menerapkan standar konfigurasi kemanan diatas standar yang ada
    3. Ditempatkan di data center yang sudah memenuhi standar
    4. Menerapkan DRP
f. UPS (*Uninterruptible Power Supply*)
    Melakukan pengecekan berkala terhadap baterai dan tegangan listrik.
g. *Firewall*
    1. Melakukan *review* konfigurasi dan kebijakan
    2. Menerapkan DRP
h. *Routers*
    1. Mengimplementasikan IPS (*Intrusion Prevention System*)
    2. Menerapkan DRP
    3. Membuat *privileges per user*

Identifikasi *vulnerabilities* dilakukan untuk mengetahui kerentanan yang dapat terjadi pada aset yang dimiliki, sebagai berikut:

a. Aplikasi Pelayanan *Online* SIM-PTS
    1. Pengendalian dokumen belum diterapkan dengan baik
    2. Proses rekruitmen kurang memadai
b. Windows Server (Proxmox, FreeBSD, VMWareESXI)
    1. OS Bajakan
    2. Tidak ada antivirus
    3. *Database* antivirus tidak *update*
    4. Sistem otomatis logout otomatis, tidak jalan
c. PC (*Personal Computer*)
    1. OS Bajakan
    2. Tidak ada antivirus
    3. *Database* antivirus tidak update
d. *Storage Server* dan *Database Server*
    Sharing *password* dengan pengguna yang tidak diotorisasi
e. *UPS* (*Uninterruptible Power Supply*)
    Perangkat keras yang terhubung pada satu UPS melebihi kapasitas yang dimiliki UPS tersebut.
f. Routers
    Konfigurasi *network* belum sepenuhnya diterapkan
g. Firewall
    1. Konfigurasi *firewall default* tidak disesuaikan
    2. Konfigurasi *network* belum sepenuhnya disesuaikan

Identifikasi *consequences* dilakukan untuk mengetahui kerusakan atau konsekuensi kepada organisasi yang dapat disebabkan oleh skenario insiden. Bila aset TI yang dimiliki PTS baik berupa *hardware*

maupun *software* mengalami kerusakan, *error*, tidak dapat digunakan, akan sangat mengganggu layanan kegiatan operasional dan penyampaian informasi ke seluruh civitas akademik. Bila hal tersebut berlangsung dalam waktu cukup lama dapat mempengaruhi reputasi PTS.

Hasil identifikasi risiko terdiri dari identifikasi *assets, threats, existing controls, vulnerabilities* dan *consequences* pada PTS di Surabaya, menunjukkan bahwa DSTI telah berupaya melakukan perlindungan terhadap aset yang dimiliki. Akan tetapi, ada sebagian yang belum diterapkan. Aset yang diidentifikasi masih terbatas pada *hardware* dan yang *software* yang dimiliki. Beberapa kontrol yang ada belum didokumentasikan dan belum disosialisasikan kepada seluruh civitas akademika, masih terbatas pada personel DSTI.

V. KESIMPULAN DAN SARAN

Hasil penelitian berupa dokumentasi identifikasi risiko keamanan informasi berdasarkan ISO 27005/2011. Identifikasi risiko dilakukan untuk mengetahui potensi kerugian dan penyebab terjadinya kerugian sehingga dapat dilakukan tindakan pengamanan yang bersifat pencegahan, deteksi maupun koreksi. Penelitian ini merupakan tahap awal dalam melakukan *risk assessment* menggunakan ISO 27005/2011, selanjutnya dapat dilakukan *risk analysis* dan *risk evaluation* menggunakan ISO 27005/2011.

REFERENSI

Dewi, M. A., Ambarwati, A. and Darujati, C. (2018) 'ANALISIS RISIKO KUANTITATIF ASET TI PADA BLC E-GOV DINKOMINFO SURABAYA', in *Seminar Nasional Inovasi Teknologi (SEMNAS INOTEK) 2018*. Kediri: UN PGRI Kediri, pp. 7–12. Available at: http://semnasinotek.ft.unpkediri.ac.id/ojs/index.php/semnasinotek/index.php/semnasinotek/article/view/89.

Imbar, R. V. and Ayala, A. E. (2018) 'Penerapan Standar Keamanan Informasi Menggunakan Framework ISO/IEC 27005:2011 di Lapan Bandung', *Jurnal Teknik Informatika dan Sistem Informasi (JUTISI)*. Fakultas Teknologi Informasi, Universitas Kristen Maranatha, 4(April), pp. 195–206. doi: http://dx.doi.org/10.28932/jutisi.v4i1.770.

International Standard (2011) *INTERNATIONAL STANDARD ISO/IEC 27005 Information technology - Security techniques - Information security risk management*. Second edi. International Organization for Standardization.

Jones, A. and Ashenden, D. (2005) *Risk management for computer security : Protecting your network and information assets*. 1st Editio. Elsevier Butterworth–Heinemann.

Taufiq, M. (2016) 'MANAJEMEN RESIKO DIDALAM PEMODELAN SISTEM MANAJEMEN SEKURITAS INFORMASI BERBASIS APLIKASI ISO 27001 dan ISO 27005', in *Seminar Nasional Telekomunikasi dan Informatika (SELISIK 2016)*. Bandung: Universitas Pasundan Bandung, pp. 103–108. Available at: http://jitter.widyatama.ac.id/index.php/Selisik2016/article/download/115/93.

Yudha, F. I. S. and Gunadhi, R. E. (2016) 'RISK ASSESSMENT PADA MANAJEMEN RESIKO KEAMANAN INFORMASI MENGACU PADA BRITISH STANDARD ISO/IEC 27005 RISK MANAGEMENT', *Jurnal Algoritma*. Jurusan Teknik Informatika STT Garut, 13(1), pp. 333–340. Available at: http://jurnal.sttgarut.ac.id/index.php/algoritma/article/viewFile/372/331.