Analisis Keamanan Sistem Informasi Dengan ISO 27001 (Studi Kasus: Sistem Informasi Akademik Universitas Muhammadiyah Purwokerto)

Siti Alvi Sholikhatin[1], Dr. Arief Setyanto, S.Si.,M.T.[2], Emha Taufiq Luthfi, S.T.,M.Kom.[3]
[1]STMIK Amikom Purwokerto , [2,3]Universitas Amikom Yogyakarta
Email : [1]alvi.sholikhatin@gmail.com,
[2]arief_s@amikom.ac.id,[3]emhataufiqluthfi@amikom.ac.id

Abstract

Business process can not be done properly without appropriate information management, where information is an important asset that needs to be protected with utmost care and concern. Information security is a way to protect information from large scale threats, thus to ensure the sustainability of organization's operational, to reduce business risks and to increase business opportunity and return of investment. The need of information security is highly developed and urgent, ISO 27001 as a recommended framework and implementation of Information Security Governance (ISG) to maintain the information security. Information security is about confidentiality, integrity and availability. This research is conducted to measure the accountability of ISO 27001 in assisting the organization to document the information security policy. The object of this research is University of Muhammadiyah Purwokerto, in which after a deep observation, it is needed to have one additional variable to maximaze Information Security Management System: Server Security.

Keywords:*ISO 27001, security, information, server security*

Abstraksi

Proses bisnis organisasi tidak bisa lepas dari pengelolaan informasi, dimana informasi adalah aset penting yang sama seperti aset bisnis lainnya, informasi perlu mendapatkan perlindungan yang baik dan konsekuen. Keamanan informasi yaitu melindungi informasi dari ancaman yang berskala luas untuk menjamin kelangsungan operasional organisasi, meminimalisasi resiko bisnis, dan memaksimalkan kesempatan bisnis dan return of investment. Keamanan sistem informasi yang dimaksud yaitu menyangkut confidentiality (kerahasiaan), integrity (integritas) dan availability (ketersediaan). Penelitian ini dilakukan untuk mengukur akuntabilitas ISO 27001 dalam membantu organisasi dalam penyusunan kebijakan keamanan informasi, dimana objek yang digunakan yaitu Universitas Muhammadiyah Purwokerto. Berdasarkan klausul dalam ISO 27001 dan dengan hasil penelitian pada objek, penambahan variabel Server Security menjadi penting dalam memaksimalkan sistem manajemen keamanan informasi.

Kata Kunci*:ISO 27001, keamanan, informasi, server security*

1. PENDAHULUAN

Informasi adalah aset penting bagi sebuah organisasi, sama seperti aset bisnis lainnya, informasi perlu mendapatkan perlindungan yang baik dan konsekuen. Keamanan informasi yaitu melindungi informasi dari ancaman yang berskala luas untuk menjamin kelangsungan operasional organisasi, meminimalisasi resiko bisnis, memaksimalkan kesempatan bisnis dan *return of investments*.Pentingnya menjaga keamanan teknologi informasi dalam suatu organisasi terkait dengan berbagai alasan, antara lain: 1) mempertahankan keunggulan kompetitif, 2) menjaga nama baik/reputasi, dan 3) memastikan organisasi tegak pada aturan dan hukum yang berlaku (Hohan et al., 2015).

Keamanan sistem informasi yang dimaksud yaitu menyangkut *confidentiality* (kerahasiaan), *integrity* (integritas) dan *availability* (ketersediaan). Penilaian dalam mengukur seberapa aman informasi yang tersedia dan dikelola dalam suatu organisasi, dapat dilakukan dengan menggunakan serangkaian proses, alat dan teknik standar yang disebut *Information Security Management System* (ISMS) atau Sistem Manajemen Keamanan Informasi (SMKI). Itradat et al. (2014) mengungkapkan pelanggaran akses aset informasi bisa berasal dari permasalahan internal organisasi, yang sebetulnya bisa dicegah dengan mengeliminasi penyebab masalah sedini mungkin. Oleh sebab itu, ISMS diperlukan oleh organisasi sebagai kontrol untuk mencegah kemungkinan pelanggaran terhadap aset informasi dari lingkungan internal.

Pentingnya menjaga keamanan sistem informasi di Universitas Muhammadiyah Purwokerto adalah upaya untuk menjaga integritas, kerahasiaan dan ketersediaan informasi yang akurat dan berkualitas dalam mendukung kegiatan akademis. ISO 27001 sebagai standar internasional membantu organisasi menyusun kebijakan keamanan informasi dengan klausul *assessment* yang telah ditetapkan. Akan tetapi, berdasarkan objek penelitian yaitu di Universitas Muhammadiyah Purwokerto, diperlukan variabel ukur tambahan yang sesuai dengan keadaan dan kebutuhan: *server security*.

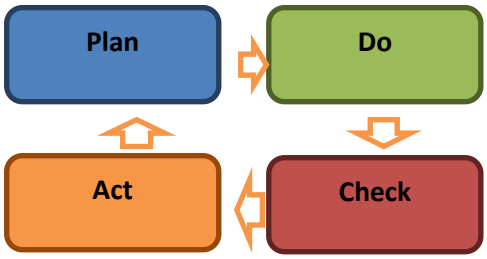
Tujuan penelitian ini yaitu:

a. Mengetahui posisi keamanan informasi yang berjalan pada sistem informasi akademik di Universitas Muhammadiyah Purwokerto.
b. Membantu menyusun kebijakan keamanan informasi dan saran untuk

meningkatkan keamanan informasi sesuai dengan standar ISO 27001 dan variabel pendukung.

2. METODE PENELITIAN

Metode penelitian dilakukan dengan merujuk pada siklus PDCA (*Plan-Do-Check-Act*). Siklus terdiri dari aktivitas: membangun, mengimplementasi, mengoperasikan, memonitor, me-*review*, merawat dan meningkatkan SMKI secara terdokumentasi dalam konteks aktifitas bisnis organisasi dan risiko yang dihadapi.



Gambar 1. Diagram siklus PDCA

Metode pengumpulan data yang dilakukan pada penelitian ini yaitu menggunakan observasi langsung. Kemudian dari hasil observasi akan dilakukan *self-assessment* menggunakan klausul standar ISO 27001 dan parameter tambahan yaitu *Sever Security* untuk kemudian ditentukan dimana posisi keamanan informasi yang telah berjalan serta mencegah resiko terjadinya potensi ketidakamanan informasi. Standar ISO 27001 menggunakan *project check list* untuk mengukur tingkat keamanan informasi sebuah organisasi dengan klausul-klausul yang berbeda di setiap tahapan siklus PDCA.

Tabel 1. Siklus Plan-Do-Check-Act (PDCA)

Plan (membangun SMKI)	Menyusun kebijakan SMKI, objektif, proses dan prosedur yang sesuai untuk pengelolaan risiko dan meningkatkan keamanan informasi untuk memberikan hasil yang sesuai dengan kebijakan organisasi secara keseluruhan.
Do (implementasi dan operasi SMKI)	Implementasi dan menjalankan kebijakan, kontrol, proses dan prosedur SMKI.
Check (memonitor dan me-*review* SMKI)	Mengukur kinerja proses yang tidak sesuai dengan kebijakan, objek dan laporan praktis SMKI untuk menghasilkan *review* manajemen.

Act (menjaga dan meningkatkan SMKI)	Mengambil langkah preventif dan korektif berdasarkan hasil audit internal SMKI dan review manajemen atau informasi lain yang relevan, untuk meningkatkan SMKI yang terus berkelanjutan

3. HASIL DAN PEMBAHASAN

Assessment dan observasi dilakukan menggunakan *project list* sesuai standar ISO 27001 dan fase pada model PDCA (*Plan-Do-Check-Act*), Pada fase *Plan* (membangun SMKI), kegiatan yang dilakukan antara lain:

a. Menentukan *scope* dan batasan SMKI dalam sebuah karakteristik bisnis, organisasi, lokasi, aset dan teknologi.
b. Menentukan kebijakan SMKI.
c. Menentukan pendekatan penilaian risiko organisasi.
d. Mengidentifikasi risiko.
e. Menganalisis dan mengevaluasi risiko.
f. Mengidentifikasi dan mengevaluasi opsi untuk menangani risiko.
g. Menyeleksi objek kontrol dan kontrol penanganan risiko.
h. Mendapatkan persetujuan manajemen terhadap risiko residual yang diajukan.
i. Mendapatkan otorisasi manajemen untuk mengimplementasikan dan mengoperasikan SMKI.
j. Menyiapkan *Statement of Applicability* (pernyataan untuk dapat diaplikasikan).

Selanjutnya, pada fase kedua yaitu *Do* (implementasi dan operasi SMKI), aktivitas-aktivitas yang dilakukan:

a. Memformulasikan rencana penanganan risiko yang mengidentifikasi langkah manajemen yang sesuai, sumber daya, tanggung jawab dan prioritas untuk mengelola risiko keamanan informasi.
b. Mengimplementasi rencana penanganan risiko untuk mendapatkan objek kontrol yang teridentifikasi, termasuk rencana anggaran dan alokasi peran serta tanggung jawab.
c. Mengimplementasi kontrol yang telah ditentukan di tahap Plan untuk bisa sejalan dengan objek kontrol.
d. Menentukan bagaimana mengukur efektifitas kontrol yang telah ada dan

menspesifikasi bagaimana pengukuran bisa digunakan untuk menilai efektifitas untuk mendapatkan hasil yang bisa dikomparasi.

e. Mengimplementasikan program *training* dan *awareness.*
f. Mengelola operasi SMKI.
g. Mengelola sumber daya SMKI.
h. Mengimplementasikan prosedur dan kontrol lain yang bisa mendeteksi keamanan dan merespon ancaman terhadap keamanan.

Fase ketiga yaitu *Check* (memonitor dan me-*review* SMKI) meliputi:

a. Memonitor dan mengecek ulang prosedur dan kontrol lain.
b. Melakukan review secara berkala tentang efektifitas SMKI.
c. Mengukur efektifitas kontrol untuk memverifikasi persyaratan keamanan.
d. Mengecek ulang penilaian risiko pada interval yang telah direncanakan.
e. Mengadakan audit internal SMKI.
f. Melakukan *review* manajemen SMKI secara berkala untuk memastikan *scope* tetap memadai dan meningkatkan identifikasi proses SMKI.
g. Memperbarui rencana keamanan.
h. Merekam aksi dan kegiatan yang dimungkinkan berimbas pada efektifitas kinerja SMKI.

Langkah terakhir pada siklus PDCA yaitu *Act* (merawat dan meningkatkan SMKI) yaitu organisasi secara berkala harus:

a. Mengimplementasikan peningkatan SMKI.
b. Melakukan tindakan korektif dan preventif yang sesuai.
c. Mengkomunikasikan setiap tindakan dan *improvements* kepada seluruh departemen yang terkait.
d. Memastikan bahwa peningkatan telah sesai dengan objek yang teridentifikasi.

Tabel 2. Prinsip-prinsip OECD (*Organization for Economic Coorporation and Development*)dan model PDCA

Prinsip OECD	**Fase PDCA dan proses SMKI**
Kewaspadaan Menyadari kebutuhan keamanan dalam sistem informasi dan jaringan, serta	Fase *DO*: • Implementasi dan operasi SMKI Departemen BTIK (Biro Teknologi Informasi dan Komunikasi) belum

mengetahui apa yang bisa dilakukan untuk meningkatkan keamanan.	menyusun dokumen kebijakan keamanan informasi. • Pelatihan, kewaspadaan dan kompetensi. Pelatihan-pelatihan rutin dilakukan dan bergilir, di dalam maupun di luar negeri dengan berbagai topik dan skill yang diusung.
Tanggung jawab Mengetahui tanggung jawab terhadap keamanan sistem informasi dan jaringan.	Fase *DO*: • Implementasi dan operasi SMKI Meski belum memiliki kebijakan tentang keamanan informasi yang terdokumentasi standar, manajemen melakukan berbagai tindakan pengamanan dengan maksimal agar sistem dan informasi terjaga dengan baik. • Komitmen manajemen Manajemen berkoordinasi dengan berbagai pihak dalam penyediaan teknologi dan jaringan dan memastikan keamanan dan tanggung jawab sesuai perjanjian.
Respon Mampu bertindak tepat waktu, cepat dan kooperatif dalam mencegah, mendeteksi dan merespon insiden yang mengancam keamanan informasi.	Face *CHECK*: aktifitas memonitor • Memonitor dan review SMKI Dalam prakteknya, penanganan dan perhatian dilakukan setelah terjadinya insiden. • Audit internal SMKI, manajemen *review* SMKI (*review input* dan *output*) Belum terlaksana dengan maksimal, *review* dan *recheck* dilakukan tidak secara reguler. Fase *ACT*: respon • Menjaga dan meningkatkan SMKI Meningkatkan kesadaran semua staff dan jajaran manajemen perlu digiatkan. • Peningkatan secara berkelanjutan, tindakan koreksi, tindakan pencegahan.
***Assessment* risiko** *Assessment* risiko perlu dilakukan	Fase *PLAN*: *assessment* • Membangun dan mengelola SMKI PTIK perlu membuat jadwal untuk *assessment* dan audit internal secara

	berkala untuk mengetahui potensi risiko yang mengancam sistem dan keamanan informasi Fase *CHECK*: *re-assessment* • Memonitor dan review SMKI Setelah *assessment* dilakukan, penting untuk mendokumentasikan hasil dan kesimpulannya sehingga bisa menentukan tindakan selanjutnya apakah *re-assessment* mendesak untuk dilakukan • Re-audit internal SMKI, manajemen *review* SMKI (*review input* dan *output*)
Desain keamanan dan implementasi Menggabungkan keamanan kedalam elemen esensial jaringan dan sistem informasi.	Fase *PLAN*: setelah *assessment* selesai • Membangun dan mengelola SMKI Kebijakan keamanan informasi sebaiknya menjadi elemen penting dalam pengelolaan sistem informasi. Fase *DO*: sebagai implementasi dan kontrol operasional Implementasi dan operasi SMKI *Resource management (provision of resources, training, awareness and competence).*
Manajemen kamanan Mengadopsi pendekatan yang komprehensif untuk mengelola keamanan	Semua aktifitas pencegahan, pendeteksian dan respon terhadap insiden, *maintenance*, *review* dan audit termasuk ke dalam fase PLAN DO CHECK ACT
Re-assessment Me-*review* dan re-*assess* terhadap keamanan jaringan dan sistem informasi, memodifikasi kebijakan keamanan, praktis dan prosedur	Fase CHECK: re-*assess* dimana review dilakukan secara berkala Memonitor dan review SMKI Audit internal SMKI, manejemen *review* SMKI (*review input* dan *output*) Fase ACT: meningkatkan keamanan Menjaga dan meningkatkan SMKI Peningkatan secara berkelanjutan, tindakan koreksi, tindakan pencegahan

Proses audit dan observasi yang dilakukan yaitu menyangkut seluruh entitas yang berhubungan secara langung maupun tidak langsung dengan sistem informasi dan keamanannya di Universitas Muhammadiyah Purwokerto: teknologi jaringan, staff,

pengelolaan sistem informasi dan integrasinya dengan departemen lain di lingkungan kampus, serta kerjasama pihak ketiga sebagai penyedia teknologi lainnya. Semua klausul dan siklus PDCA pada ISO 27001 telah mampu mengidentifikasi posisi keamanan informasi di UMP, namun dari kondisi riil dan hasil observasi diperlukan satu parameter audit tambahan yaitu *Server Security*. Server menjadi salah satu aset penting dimana semua data dan informasi krusial tersimpan didalamnya dan memerlukan perhatian dan pengelolaan maksimal untuk menjamin keamanannya. Berikut adalah klausul Server Security:

Tabel 3. Server Security

A.16 Keamanan Server		
A.16.1 Kebijakan keamanan fisik Objektif: mendokumentasikan kebijakan untuk melindungi server dari berbagai gangguan dan ancaman fisik.		
A.16.1.1	Dokumen kebijakan keamanan server.	Kontrol: Belum teridentifikasi
A.16.1.2	Kontrol akses terhadap server dan otorisasi pengguna.	Kontrol: Ada
A.16.2 *Back-up*, *maintenance* dan *incidents handling* Objektif: memastikan server melakukan *back-up* secara berkala, mengelola dan memonitor serta menindaklanjuti kejadian-kejadian tak terduga yang mengancam keamanan server secara cepat dan tepat.		
A.16.2.1	Prosedur *back-up* berkala	Kontrol: *Back-up* setiap hari
A.16.2.2	Kebijakan pengelolaan *maintenance* server	Kontrol: *Maintenance* dilakukan namun tidak terdokumentasi
A.16.2.3	*Incidents handling*	Kontrol: Jika terjadi kejadian tak terduga, tanggung jawab ditanggung bersama
A.16.2.4	Tanggung jawab dan standar pengamanan server	Kontrol: Tanggung jawab tim

4. KESIMPULAN

Kesimpulan yang dapat disusun dari penelitian ini antara lain:

1. Universitas Muhammadiyah Purwokerto belum mendokumentasikan kebijakan-kebijakan keamanan informasi, prosedur operasional standar dalam menangani *incident* dan pengelolaan risiko.

2. Penanganan *information breaches* atau kejadian-kejadian tak terduga yang mengancam sistem dan keamanan informasi dilakukan setelah kejadian tersebut terjadi.
3. Bekerjasama dengan pihak ketiga dalam penyediaan teknologi-teknologi penunjang dan disiplin dalam melakukan *review* dan *re-check* kinerja.
4. Jaringan dan sistem informasi dikelola oleh tim BTIK dengan pembagian tugas yang jelas namun dalam penanganan *incident* dilakukan secara praktikal.
5. Server sebagai aset penting perlu mendapat penanganan dan perhatian ekstra baik secara fisik maupun nonfisik.

5. SARAN

Saran-saran yang dapat diberikan antara lain:

1. Menyusun semua risiko yang berpotensi mengancam sistem dan keamanan informasi lengkap dengan bagaimana tindakan pencegahannya.
2. Melakukan audit internal dan *assessment* secara berkala untuk mengetahui bagaimana sistem sedang berjalan dan mendeteksi kemungkinan munculnya *breaches* sehingga bisa ditangani sedini mungkin.
3. Mendokumentasikan semua tindakan yang dilakukan terhadap sistem dan teknologi sehingga memiliki *log* yang lengkap.
4. Menyusun kebijakan pengamanan server dan keamanan informasi.

DAFTAR PUSTAKA

Itradat et all., 2014, *Developing an ISO27001 Information Security Management System for an Educational Institute: Hashemite University as a Case Study*, Jordan Journal of Mechanical and Industrial Engineering, ISSN 1995-6665, Volume 8 Number 2, April. 2014

Hohan et all., 2015, *Assessment and Continous Improvement of Information Security based on TQM and Business Excellence Principles*, Procedia Economics and Finance 32 (2015) 352 – 359, ISSN 1995-6665, 2015

British Standard, 2005, *Information technology – security techniques – Information security management systems – Requirements*, First edition, British Standard, UK

Badan Standardisasi Nasional, 2016, *Teknologi informasi – teknik keamanan – Sistem manajemen keamanan informasi – Persyaratan*, BSN, Jakarta.