AUDIT KEAMANAN SISTEM INFORMASI PERPUSTAKAAN KOTA YOGYAKARTA BERDASARKAN STANDAR ISO 27001

Skripsi

Untuk Memenuhi Sebagian Persyaratan

Mencapai Derajat Sarjana S-1

Program Studi Teknik Informatika

Disusun Oleh:

Lusi Anggarini

12651076

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA

YOGYAKARTA

2016

Universitas Islam Negeri Sunan Kalijaga FM-UINSK-BM-05-07/R0

PENGESAHAN SKRIPSI/TUGAS AKHIR

Nomor : B-4311 /Un.02/DST/PP.05.3/ 11 /2016

Skripsi/Tugas Akhir dengan judul : Audit Keamanan Sistem Informasi Perpustakaan Kota Yogyakarta Berdasarkan Standar ISO 27001

Yang dipersiapkan dan disusun oleh :
Nama : Lusi Anggarini
NIM : 12651076
Telah dimunaqasyahkan pada : 17 November 2016
Nilai Munaqasyah : A/B

Dan dinyatakan telah diterima oleh Fakultas Sains dan Teknologi UIN Sunan Kalijaga

TIM MUNAQASYAH :

Ketua Sidang

Ade Ratnasari, M.T
NIP. 19801217 200604 2 002

Penguji I

Agung Fatwanto, Ph.D
NIP.19770103 200501 1 003

Penguji II

Sumarsono, M. Kom
NIP.19710209 200501 1 003

Yogyakarta, 2016
UIN Sunan Kalijaga
Fakultas Sains dan Teknologi
Dekan

Dr. Murtono, M.Si
NIP. 19691212 200003 1 001

SURAT PERSETUJUAN SKRIPSI/TUGAS AKHIR

Hal : Permohonan
Lamp : -

Kepada
Yth. Dekan Fakultas Sains dan Teknologi
UIN Sunan Kalijaga Yogyakarta
di Yogyakarta

Assalamu'alaikum wr. wb.

Setelah membaca, meneliti, memberikan petunjuk dan mengoreksi serta mengadakan perbaikan seperlunya, maka kami selaku pembimbing berpendapat bahwa skripsi Saudara:

Nama : Lusi Anggarini
NIM : 12651076
Judul Skripsi : Audit Keamanan Sistem Informasi Perpustakaan Kota Yogyakarta Berdasarkan Standar ISO 27001.

Sudah dapat diajukan kembali kepada Program Studi Teknik Informatika Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta sebagai salah satu syarat untuk memperoleh gelar Sarjana Strata Satu dalam Teknik Informatika

Dengan ini kami mengharap agar skripsi/tugas akhir Saudara tersebut di atas dapat segera dimunaqsyahkan. Atas perhatiannya kami ucapkan terima kasih.

Wassalamu'alaikum wr. wb.

Yogyakarta, 11 November 2016
Pembimbing

Ade Ratnasari, M.T.
NIP: 1980121720060422002

PERNYATAAN KEASLIAN SKRIPSI

Yang bertanda tangan dibawah ini :

Nama	: Lusi Anggarini
NIM	: 12651076
Program Studi	: Teknik Informatika
Fakultas	: Sains dan Teknologi

Menyatakan bahwa skripsi dengan judul **Audit Keamanan Sistem Informasi Perpustakaan Kota Yogyakarta Berdasarkan Standar ISO 27001,** tidak terdapat pada karya yang pernah diajukan untuk memperoleh gelar sarjana di suatu Perguruan Tinggi, dan sepengetahuan saya tidak terdapat karya atau pendapat yang pernah ditulis oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Yogyakarta, 11 November 2016

Yang Menyatakan,

METERAI TEMPEL
TGL. 20
FD9F9AEF089205105
6000
ENAM RIBU RUPIAH

Lusi Anggarini

NIM. 12651076

KATA PENGANTAR

بسم الله الرحمن الرحيم

Segala puji bagi Allah SWT tuhan semesta alam yang selalu memberikan rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan skripsi dengan judul "Audit Keamanan Sistem Informasi Perpustakaan Kota Yogyakarta Berdasarkan Standar ISO 27001". Tak lupa pula penulis haturkan shalawat serta salam kepada Nabi junjungan kita Nabi Muhammad SAW yang telah berjuang demi berdiri tegaknya daulah islamiyah dimuka bumi ini.

Penulis juga mengucapkan terimakasih kepada semua pihak yang telah membantu dalam proses pelaksanaan penelitian tugas akhir ini sehingga laporan tugas akhir ini dapat terselesaikan.

Selanjutnya penulis mengucapkan terimakasih kepada :

1. Bapak Prof. Drs. Yudian Wahyudi, M.A. Ph.D., selaku Rektor UIN Sunan Kalijaga Yogyakarta.
2. Bapak Dr. Murtono, M. Si., selaku Dekan Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta.
3. Bapak Dr. Bambang Sugiantoro, MT., selaku Ketua Program Studi Teknik Informatika UIN Sunan Kalijaga Yogyakarta.
4. Bapak M.Didik Rohmad Wahyudi, S.T. M.T., selaku Sekretaris Program Studi Teknik Informatika UIN Sunan Kalijaga Yogyakarta.
5. Bapak Agus Mulyanto, S.Si., M.Kom., selaku Dosen Pembimbing akademik yang telah mengayomi dan mengarahkan kepada anak didiknya.

6. Ibu Ade Ratnasari, M.T., selaku Dosen Pembimbing Tugas Akhir yang telah mengayomi, membimbing serta mengarahkan dengan sangat baik dan sabar.
7. Seluruh Dosen Program Studi Teknik Informatika yang telah memberi bekal ilmu pengetahuan kepada penulis, semoga ilmunya menjadi amal jariyah.
8. Teman-teman Program Studi Teknik Informatika, khususnya angkatan 2012 Mandiri Kelas K (Katak 012) yang telah banyak memberi dukungan.
9. Pimpinan dan seluruh jajaran staf Pengelola Sistem Informasi Perpustakaan Kota Yogyakarta yang telah bersedia membantu demi kelancaran tugas akhir.
10. Serta semua pihak yang tidak dapat disebutkan satu per satu, yang telah banyak memberikan dukungan, motivasi, inspirasi dan membantu dalam proses penyelesaian skripsi ini.

Penulis menyadari masih banyak sekali kekurangan dalam penelitian ini, oleh karena itu kritik dan saran senantiasa penulis harapkan. Akhir kata semoga penelitian ini dapat menjadi panduan serta referensi yang sangat berguna bagi pembaca dan dapat dimanfaatkan dalam pengembangan ilmu pengetahuan.

Yogyakarta, 11 November 2016

Penulis,

HALAMAN PERSEMBAHAN

Dengan mengucap segala rasa syukur penulis mempersembahkan tugas akhir ini untuk :

- Suamiku tercinta, Sandy Aristiandy. Sepertinya tidak ada kata yang tepat yang dapat menggambarkan bentuk ucapan Terimakasihku kepadamu yang tak terbatas. Atas apa – apa yang telah engkau perjuangkan demi terwujudnya salah satu cita – citaku untuk menyelesaikan pendidikanku ini. Terimakasih sayang atas segala dukungannya. Semoga engkau selalu ada dalam lindungannya Allah SWT. Aamiin
- Ayahanda Didin Sunardin yang telah berjuang sejauh ini buatku, Ibunda Maryati dan yang tetap menjadi motivasi terbesar dalam perjalanan hidupku. Kedua malaikat tanpa sayapku yang tak pernah bosan mendoakan dan menyayangiku, yang terus mendukungku sampai sejauh ini. Semoga Ayah dan Ibu panjang umur dan bisa melihatku menjadi anak yang membanggakan keluarga suatu hari nanti, amin.
- Kakak kakak-ku yang selalu sayang sama aku, A Ayi dan Teh Iyet dan Kakak Iparku Abang Hendra, Adik Ipar ku Teteh Resti, yang selalu peduli dan selalu memberi semangat, terimakasih buat semuanya, adikmu ini akan selalu sayang kalian.
- Dosen dan keluarga besar Teknik Informatika, Bapak Bambang selaku ketua program studi yang selalu sedia dan terbuka menerima keluh

kesah para mahasiswanya. Pak Agus Mulyanto dan Ibu Ade Ratnasari yang selalu mengarahkan dan selalu peduli kepada anak bimbingnya, Pak Sumarsono, Pak Mustakim, Pak Agung, Ibu Uyun, Pak Nurochman, Pak Didik dan Pak Aulia yang selalu sabar memberikan ilmu-ilmunya. semoga Bapak dan Ibu dosen panjang umur dan sehat selalu. Amiin.

- Teman–teman seperjuangan dan keluarga besar Teknik Informatika Mandiri/Khusus 2012 (Katak 2012) Gumeta, Deviyanto, Wiji, Indah, Berlian, Rizky, Hilyas, Mursyid, Fajar, Rohman, Choirudin, Eri, Krisna, Bintang, Malika, Maya, Iza, Edi, Bayu, Andri, Ripa, Kukuh, Afin, Nanang, Valdi, Kharizma, Erin, Novie, Zuni, Andi, Gustav, Taufik, Edita, Dana, Iwan, Asep, Ainul, Irham, Ulfa, Edigun, Indra, Kiki, Ikhzan, Surahmat, Abdul dan Aghni, terimakasih buat kebersamaan kalian.
- Pihak-pihak yang selalu memberikan bantuannya, semangat, dan doanya baik secara langsung maupun tidak yang tidak dapat penulis sebutkan namanya satu per satu. Terimakasih.

MOTTO

"Maka nikmat Tuhanmu yang manakah

yang kamu dustakan?"

(Q.S Ar - Rahman : 55)

Tidakkah kamu memperhatikan,

bahwa sesungguhnya kapal itu berlayar di laut

dengan nikmat Allah, supaya diperlihatkannya kepdamu

sebagian dari tanda – tanda (kekuasaan)-Nya.

Sesungguhnya pada tanda yang demikian itu,

benar – benar terdapat tanda – tanda

bagi semua orang, yang sangat sabar,

lagi banyak bersyukur.

(Q.S Luqman : 31)

Janganlah mengeluh,

sesungguhnya kita telah diberi nikmat oleh Allah SWT.

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

DAFTAR SINGKATAN

SNI	:	Standar Nasional Indonesia
ISO	:	*International Organization for Standardization*
IEC	:	*International Electrotechnical Commission*
TI	:	Teknologi Informasi
SI	:	Sistem Informasi
ARPUSDA	:	Arsip Pustaka Daerah
SISKA	:	Sistem Informasi Perpustakaan
SOP	:	Standar Operasional Pustaka
OSL	:	*Operational Standard Library*
SarPras	:	Sarana dan Prasarana
TIK	:	Teknologi Informasi dan Komunikasi
SMKI	:	Sistem Manajemen Keamanan Informasi
ISMS	:	*Information Security Management System*
CMMI	:	*Capability Maturity Model for Integration*
COBIT	:	*Control Objective for Information and Related Technology*
FQ	:	*Form Question*
HDD	:	*Hard Disk Drive*
ID	:	*Identity*

AUDIT KEAMANAN SISTEM INFORMASI

PERPUSTAKAAN KOTA YOGYAKARTA BERDASARKAN

STANDAR ISO 27001

Lusi Anggarini
12651076

INTISARI

Mengingat pentingnya keamanan informasi, maka kebijakan tentang keamanan informasi harus baik dan harus mencakup beberapa prosedur seperti prosedur kebijakan keamanan, prosedur pengelolaan aset, prosedur keamanan fisik dan lingkungan, prosedur manajemen komunikasi dan operasi, prosedur pengendalian akses, prosedur akuisisi, pengembangan, dan pemeliharaan sistem informasi serta prosedur manajemen kejadian keamanan informasi.

Untuk mendapatkan keamanan sebuah layanan Sistem Informasi yang baik, maka perlu dilakukan Audit Sistem Informasi untuk memastikan keamanan informasi diterapkan sesuai prosedur. ISO/IEC 27001 merupakan dokumen standar Sistem Manajemen Keamanan Informasi (SMKI) secara umum membahas mengenai apa saja yang seharusnya dilakukan dalam usaha mengimplementasikan konsep – konsep keamanan informasi pada Perpustakaan Kota Yogyakarta dari aspek keamanan sistem informasi berdasarkan standar ISO 27001 dengan mengukur keamanan sistem informasi dan mengaudit berdasarkan SMKI.

Penelitian ini menghasilkan temuan Sistem Informasi Perpustakaan Kota Yogyakarta berada pada tingkat keamanan dengan skala kematangan 2,6 (*Defined Process*). Hal ini menunjukan bahwa pengelolaan Keamanan Teknologi Informasi telah didokumentasi dan dikomunikasikan serta aktivitas yang ada berjalan sesuai prosedur yang mengacu pada Standar Operasional Pustaka (SOP). Setelah mengukur keamanan sistem informasi dan melakukan audit terhadap keamanan sistem informasi Perpustakaan Kota Yogyakarta diharapkan dapat memberikan solusi terhadap keamanan sistem informasi yang diterapkan di Perpustakaan Kota Yoyakarta.

Kata Kunci : Audit keamanan sistem informasi, ISO/IEC 27001, SMKI

SECURITY AUDIT OF INFORMATION SYSTEM

YOGYAKARTA CITY LIBRARY BASED

STANDARD ISO 27001

Lusi Anggarini
12651076

ABSTRACT

Given the importance of information security, the policy on information security must be good and should include several procedures such as procedures of security policies, procedures of asset management, procedures of physical and environmental security, procedures of communications management and operations, procedures of access control, procedures of aquisition, development and maintenance of information systems, as well as procedures of incident management of information security.

To get the security of a good information system services, it is necessary to Audit the Information Systems to ensure information security that is applied is in accordance with procedures. ISO / IEC 27001 is a standard document for Information Security Management System (ISMS) is generally discussed about what should be done in an attempt to implement the concept - the concept of information security at the Library of Yogyakarta City on the security aspects of information systems based on standard ISO 27001 by measuring the security of information systems and auditing by ISMS based.

This research has resulted in findings of Yogyakarta City Library Information System at the level of security with a maturity scale of 2.6 (Defined Process). This shows that the management of Information System Security has been documented and communicated as well as the activity is running according to procedure referring to the Operational Standard Library (OSL). After measuring the security of information systems and audit the security of Yogyakarta City Library Information System is expected to provide solutions to the security of information systems applied in Yogyakarta City Library.

Keywords: Security audit of information systems, ISO / IEC 27001 , ISMS

BAB I

PENDAHULUAN

1.1 Latar Belakang

Pengelolaan Teknologi Informasi dan Komunikasi yang baik akan mendorong hadir dan terwujudnya *good governance*. Metodologi dan tata kelola yang baik merupakan suatu prasyarat yang menjadi kewajiban dalam pengelolaan sebuah sistem yang baik. Dengan tata kelola yang baik, maka sistem informasi yang *accountable* serta *sustainable* dapat tercapai bagi suatu badan atau lembaga dan dapat memberikan manfaat kepada publik seluas-luasnya.(Audit Kemenpora, 2012)

Dalam penyelenggaraan tata kelola TIK, faktor keamanan informasi merupakan aspek yang sangat penting diperhatikan mengingat kinerja tata kelola akan terganggu jika informasi sebagai salah satu objek utama tata kelola mengalami masalah keamanan informasi yang menyangkut kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*).

Perpustakaan adalah salah satu lembaga yang memanfaatkan teknologi informasi dalam mengelola dan menyebarkan informasi kepada penggunanya, serta menjadikan teknologi informasi sebagai salah satu akses perpustakaan dalam memberikan pelayanan terhadap penggunanya. Dengan didukung oleh material aset perpustakaan seperti, koleksi bahan pustaka (konten), dokumen (arsip), data, inventaris, infrastruktur, sumber daya manusia dan pengguna perpustakaan.

Salah satu lembaga yang menerapkan teknologi informasi tersebut adalah Perpustakaan Kota Yogyakarta, Perpustakaan Kota Yogyakarta merupakan perpustakaan umum yang dimiliki oleh Pemerintah Kota Yogyakarta. Tidak dipungkiri bahwa dengan adanya teknologi informasi perpustakaan sangatlah memudahkan terutama bagi pemustaka yang akan meminjam buku. Kemajuan teknologi informasi telah memberikan banyak kontribusi dan dampak yang besar terhadap perkembangan Perpustakaan Kota Yogyakarta yang mempunyai Visi yaitu "Menjadikan perpustakaan sebagai wahana Pendidikan, Penelitian, Pelestarian, Informasi, dan Rekreasi (P3IR)" dan Misi "Meningkatkan pelayanan kepada masyarakat melalui pelayanan prima". Dalam memberikan pelayanan yang baik salah satunya ialah memudahkan pemustaka dengan adanya pengelolaan sistem informasi. Hal ini berkaitan langsung dengan fungsi manajemen tata kelola Informasi yang melakukan pengendalian untuk mengurangi resiko suatu tindakan dalam manajemen tata kelola sistem informasi tersebut.

Keamanan Informasi di perpustakaan kota yogyakarta sangat diperlukan karena menyangkut tentang keamanan informasi sebuah kelembagaan perpustakaan umum. Keamanan sistem informasi sangat penting untuk melindungi data dan sistem yang ada, apapun bentuk informasi yang disajikan, informasi tersebut harus selalu aman. Mengingat pentingnya keamanan informasi, untuk itu perlu dilakukan audit untuk mengetahui bagaimana kebijakan keamanan informasi yang diterapkan oleh pengelola sistem informasi Perpustakaan Kota Yogyakarta, seperti apa bentuk pengelolaan aset, keamanan fisik dan

lingkungannya, apakah sudah dikendalikan, bagaimana bentuk manajemen komunikasi dan operasi, pengendalian akses, akuisisi pengembangan dan pemeliharaan sistem informasi serta manajemen kejadian keamanan informasinya. Sasaran pengendalian - pengendalian tersebut terdapat dalam standar manajemen keamanan informasi yaitu SNI/ISO 27001. SNI/ISO 27001 dipilih karena standar ini sangat fleksibel dikembangkan karena sangat tergantung dari kebutuhan suatu lembaga atau organisasi, tujuan organisasi, persyaratan keamanan, proses bisnis dan jumlah pegawai serta ukuran struktur organisasi.

Berdasarkan uraian-uraian diatas maka penulis bermaksud untuk mengangkat permasalahan tersebut sebagai bahan penelitian ini. Dan penulis berharap dapat menghasilkan dokumen (temuan dan rekomendasi) yang merupakan hasil audit keamanan sistem informasi. Perpustakaan Kota Yogyakarta belum pernah melakukan audit terhadap keamanan sistem informasi, Adapun judul yang diangkat untuk penilitian ini yaitu “Audit Keamanan Sistem Informasi Perpustakaan Kota Yogyakarta Berdasarkan Standar ISO 27001”.

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas, penulis dapat merumusan masalah sebagai berikut:

a. Bagaimana merencanakan audit keamanan sistem informasi Perpustakaan Kota Yogyakarta?
b. Bagaimana melaksanakan audit keamanan informasi Perpustakaan Kota Yogyakarta terhadap faktor keamanan informasi?

c. Bagaimana mengetahui tingkat keamanan sistem informasi Perpustakaan Kota Yogyakarta?

d. Bagaimana merumuskan dan merekomendasikan hasil audit keamanan sistem informasi pada sistem informasi Perpustakaan Kota Yogyakarta?

1.3 Batasan Masalah

Batasan masalah pada penelitian ini adalah:

a. Penelitian ini mengacu pada standar SNI/ISO 27001.

b. Objek yang diteliti adalah sistem informasi Perpustakaan Kota Yogyakarta.

c. Data-data yang akan dianalisis adalah data yang diperoleh dari hasil *observasi*, wawancara menggunakan kertas kerja audit dan audit foreksik.

d. Ruang lingkup penelitian berfokus pada 7 klausul yaitu: Kebijakan Keamanan, Pengelolaan Aset, Keamanan Fisik dan Lingkungan, Manajemen Komunikasi dan Operasi, Pengendalian Akses, Akuisisi Pengembangan dan Pemeliharaan Sistem Informasi serta Manajemen Kejadian Keamanan Informasi.

e. Metode penilaian dalam penelitian ini ialah menggunakan pendekatan berdasarkan *maturity* model dengan 6 tahapan skala kematangan.

f. *Output* yang dihasilkan dalam penelitian ini adalah temuan yang didapatkan dari bukti (*evidence)* pada tahap akhir yaitu audit forensik berupa bukti dokumentasi yang terdapat pada halaman lampiran, untuk selanjutnya disusun rekomendasi tentang keamanan sistem informasi Perpustakaan Kota Yogyakarta.

1.4 Tujuan Penelitian

Tujuan penelitian ini adalah :

a. Merencanakan audit keamanan sistem informasi dengan membuat kesepakatan dengan pimpinan Perpustakaan Kota Yogyakarta.
b. Melaksanakan audit keamanan Sistem Informasi Perpustakaan Kota Yogyakarta menggunakan dokumen wawancara (*interview*) yaitu lembar kerja audit.
c. Menganalisis tingkat keamanan sistem informasi Perpustakaan Kota Yogyakarta
d. Membuat evaluasi hasil dari audit terhadap sistem yang diterapkan sehingga dapat memberikan rekomendasi yang baik terhadap sistem tersebut.

1.5 Manfaat Penelitian

Manfaat yang didapat dari penelitian ini adalah:

a. Memahami audit keamanan sistem informasi dengan menggunakan standar SNI/ISO 27001 yang diterapkan pada sistem informasi Perpustakaan Kota Yogyakarta.
b. Mengoptimalisasi keamanan sistem informasi Perpustakaan Kota Yogyakarta untuk meningkatkan efektifitas sistem dan kinerja pelayanan.
c. Memberikan masukan atau rekomendasi pengembangan sistem Perpustakaan Kota Yogyakarta untuk kedepannya.

1.6 Keaslian Penelitian

Penelitian audit keamanan sistem informasi sebelumnya sudah banyak dilakukan, tetapi dengan objek dan metode penelitian yang berbeda. Adapun penelitian mengenai Audit Keamanan Sistem Informasi Perpustakaan Kota Yogyakarta Berdasarkan Standar ISO 27001 belum pernah dilakukan sebelumnya.

BAB VI

KESIMPULAN DAN SARAN

6.1 Kesimpulan

Berdasarkan hasil penelitian yang dilakukan dari mulai perencanaan hingga didapatkannya hasil penelitian, maka kesimpulan yang peneliti hasilkan dari proses audit Sistem Informasi Perpustakaan Kota Yogyakarta ialah sebagai berikut :

a. Perencanaan audit untuk kegiatan penelitian audit keamanan sistem informasi dengan standar ISO 27001 pada Sistem Informasi yang dikelola oleh Perpustakaan Kota Yogyakarta telah berhasil dilaksanakan.
b. Peneliti telah berhasil melaksanakan proses Audit Keamanan Sistem Informasi dengan mengambil kasus di Perpustakaan Kota Yogyakarta dengan menggunakan standar SNI–ISO 27001 yang mengasilkan data-data penelitian berupa hasil wawancara menggunakan kertas kerja audit terhadap bentuk pengelolaan Sistem Perpustakaan Kota Yogyakarta.
c. Peneliti juga berhasil memberikan penilaian terhadap Keamanan Sistem Informasi Perpustakaan Kota Yogyakarta. Hasil analisa menunjukan tingkat kematangan keamanan Sistem Informasi berada pada level *Defined Process* yaitu sebesar 2,6 (Baik). Dengan berdasarkan nilai maturity yang didapat kan artinya proses pengelolaan

keamanan sistem informasi pada setiap klausul sebagian besar proses telah didokumentasikan dan dikomunikasikan, prosedur telah distandarisasi, didokumentasikan dan dikomunikasikan melalui pelatihan. Proses berada pada keadaan diamanatkan, namun kecil kemungkinan penyimpangan dapat terdeteksi. Prosedur yang ada hanya formalitas praktek yang ada.

d. Rekomendasi audit pada Sistem Informasi Perpustakaan Kota Yogyakarta telah berhasil disusun untuk setiap klausul berdasarkan analisa hasil audit, yang diharapkan dapat menjadi masukan untuk perbaikan dalam meningkatkan pengelolaan keamanan sistem yang sudah diterapkan.

6.2 Saran

Dari semua proses yang telah dilakukan oleh peneliti, tentunya masih terdapat beberapa yang harus diperbaiki dan ditingkatkan. Oleh karena itu untuk penelitian lebih lanjut, peneliti memberikan saran berupa masukan sebagai berikut.

a. Hendaknya dilakukan audit internal menggunakan standar SNI-ISO 27001 secara rutin oleh pengelola agar mengetahui berapa tingkat kematangan keamanan sistem informasi Perpustakaan Kota Yogyakarta serta dapat memberikan pengaruh yang signifikan atas keberlangsungan pelayanan yang ada di Perpustakaan Kota Yogyakarta.

b. Perlu adanya penerapan manaejemen keamanan sistem informasi berdasarkan standar SNI - ISO 27001 secara bertahap dan berkala pada Sistem Informasi Perpustakaan Kota Yogykarta.

c. Diharapkan untuk penelitian lebih lanjut mengenai Sistem Informasi Perpustakaan Kota Yogyakarta dapat menggunakan klausul secara keseluruhan yang ada pada ISO 27001 karena dapat memperoleh nilai kematangan yang menyeluruh dalam proses pengelolaan Sistem Informasi Perpustakaan Kota Yogyakarta yang semakin akurat.

DAFTAR PUSTAKA

Sarno, Riyanarto & Iffano, Irsyat. 2009. *Sistem Manajemen Keamanan Sistem Informasi Berbasis ISO 27001*. ITS Press : Surabaya.

Kemenpora. 2012. *Bakuan Audit Keamanan Informasi*. Kementrian Pemuda dan Olahraga Republik Indonesia : Jakarta.

Kusuma, Riawan Arbi. 2014. *Audit Keamanan Sistem Informasi Berdasarkan Standar SNI-ISO 27001 Pada Sistem Informasi Akademik Universitas Islam Negeri Sunan Kalijaga*. Yogyakarta.

Juhdan. 2016. *Audit Keamanan Sistem Informasi Digital Library Universitas Islam Negeri Sunan Kalijaga Menggunakan Standar SNI-ISO 27001*. Yogyakarta.

Permatasari, Dwi Indah. 2016. *Audit Keamanan Sistem Informasi Berdasarkan Standar SNI-ISO 27001 Pada Sistem Admisi Universitas Islam Negeri Sunan Kalijaga Yogyakarta*. Yogyakarta.

Puspitasari Devi. 2015. *Audit Sistem Manajemen Keamanan Informasi Menggunakan ISO/SNI 27001 Pada Sistem Informasi Apotek Sanata Darma*. Yogyakarta.

Setiawan Heri. 2015. *Audit Sistem Informasi Rumah Sakit Menggunakan Standart ISO 27001 (Studi Kasus Di RSU PKU Muhammadiyah Bantul)*. Yogyakarta.

Badan Standardisasi Nasional. 2009. *Information technology–Security techniques–Information Security Management Systems–Requirements*. Senayan Jakarta

Kominfo. 2011. *Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik Edisi 20*. Tim Direktorat Keamanan Informasi : Jakarta.

http://www.aptika.kominfo.go.id/index.php/profile/direktorat-e-government. Diakses pada hari 07 Agustus 2016

http://diklat.jogjaprov.go.id/v2/kegiatan/item/21-sertifikasi-manajemen-mutu-iso-9001-2008. Diakses pada hari 14 Agustus 2016

http://software.endy.muhardin.com/manajemen/apa-itu-cmmi/. Diakses 29 November 2016.

http://karto-iskandar.blogspot.co.id/2010_07_01_archive.html. Diakses 29 November 2016

DAFTAR LAMPIRAN

LAMPIRAN A

Surat Izin Penelitian

PEMERINTAHAN KOTA YOGYAKARTA
DINAS PERIZINAN
Jl. Kenari No. 56 Yogyakarta 55165 Telepon 514448, 515865, 515865, 515866, 562682
Fax (0274) 555241
E-MAIL : perizinan@jogjakota.go.id
HOTLINE SMS : 081227625000 HOT LINE EMAIL : upik@jogjakota.go.id
WEBSITE : www.perizinan.jogjakota.go.id

SURAT IZIN

NOMOR : 070/2152
3994/34

Membaca Surat : Dari Surat izin/ Rekomendasi dari Gubernur Kepala Daerah Istimewa Yogyakarta
Nomor : 070/REG/V/607/5/2016 Tanggal : 26 Mei 2016

Mengingat :
1. Peraturan Gubernur Daerah istimewa Yogyakarta Nomor : 18 Tahun 2009 tentang Pedoman Pelayanan Perizinan, Rekomendasi Pelaksanaan Survei, Penelitian, Pendataan, Pengembangan, Pengkajian dan Studi Lapangan di Daerah Istimewa Yogyakarta.
2. Peraturan Daerah Kota Yogyakarta Nomor 10 Tahun 2008 tentang Pembentukan, Susunan, Kedudukan dan Tugas Pokok Dinas Daerah;
3. Peraturan Walikota Yogyakarta Nomor 29 Tahun 2007 tentang Pemberian Izin Penelitian, Praktek Kerja Lapangan dan Kuliah Kerja Nyata di Wilayah Kota Yogyakarta;
4. Peraturan Walikota Yogyakarta Nomor 85 Tahun 2008 tentang Fungsi, Rincian Tugas Dinas Perizinan Kota Yogyakarta;
5. Peraturan Walikota Yogyakarta Nomor 20 tahun 2014 tentang Penyelenggaraan Perizinan pada Pemerintah Kota Yogyakarta;

Diijinkan Kepada :
Nama : LUSI ANGGARINI
No. Mhs/ NIM : 12651076
Pekerjaan : Mahasiswa Fak. Sains dan Teknologi - UIN SUKA Yk
Alamat : Jl. Marsda Adisucipto, Yogyakarta
Penanggungjawab : Ade Ratnasari, M.T.
Keperluan : Melakukan Penelitian dengan judul Proposal : AUDIT KEAMANAN SISTEM INFORMASI BERDASARKAN STANDAR ISO 27001 PADA SISTEM INFORMASI PERPUSTAKAAN KOTA YOGYAKARTA

Lokasi/Responden : Kota Yogyakarta
Waktu : 26 Mei 2016 s/d 26 Agustus 2016
Lampiran : Proposal dan Daftar Pertanyaan
Dengan Ketentuan :
1. Wajib Memberikan Laporan hasil Penelitian berupa CD kepada Walikota Yogyakarta (Cq. Dinas Perizinan Kota Yogyakarta)
2. Wajib Menjaga Tata tertib dan menaati ketentuan-ketentuan yang berlaku setempat
3. Izin ini tidak disalahgunakan untuk tujuan tertentu yang dapat mengganggu kesetabilan pemerintahan dan hanya diperlukan untuk keperluan ilmiah
4. Surat izin ini sewaktu-waktu dapat dibatalkan apabila tidak dipenuhinya ketentuan-ketentuan tersebut diatas

Kemudian diharap para Pejabat Pemerintahan setempat dapat memberikan bantuan seperlunya

Tanda Tangan
Pemegang Izin

LUSI ANGGARINI

Dikeluarkan di : Yogyakarta
Pada Tanggal : 27 Mei 2016

Plt. Sekretaris

PEMERINTAH KOTA YOGYAKARTA DINAS PERIZINAN

Drs. SAHLAN SUMANTRI
NIP. 196610041993031008

Tembusan Kepada :
Yth 1.Walikota Yogyakarta (sebagai laporan)
2.Ka. Biro Administrasi Pembangunan Setda DIY
3.Ka. Kantor Arsip & Perpustakaan Daerah Kota Yk
4.Ybs.

LAMPIRAN B

Project Definition (Audit Charter)

Audit Charter

Project ID : SNI-ISO 27001- Audit

Project Name : Audit Keamanan Sistem Informasi

Auditor : Lusi

Project Description :

Penelitian yang berkaitan dengan keamanan informasi ini menggunakan parameter SNI-ISO 27001. Penelitian ini berfokus pada klausul kebijakan keamanan, pengelolaan aset, keamanan fisik dan lingkungan, manajemen komunikasi dan operasi, pengendalian akses, akuisisi pengembangan dan pemeliharaan sistem informasi, dan manajemen kejadian keamanan informasi.

Project Schedule : Agustus - Oktober 2016

Stakeholder list :

Jabatan	Responden	Klausul Pengendalian
Unit Pengembangan	Triyanta, S.Pd., M.IP	Kebijakan keamanan, SNI-ISO 27001 A.5 (A.5.1)
Unit Sarana dan Prasarana (Unit Sar-Pras)	Nurhadi	Pengelolaan Aset, SNI-ISO 27001 A.7 (A.7.1 - A.7.2). Keamanan Fisik dan Lingkungan, SNI-ISO 27001 A.9 (A.9.1 -A.9.2).
Unit Teknologi Informasi dan Komunikasi (Unit	Budi Isti Wijayanti, A. Md	Manajemen Komunikasi dan Operasi, SNI-ISO 27001

TIK 1)		A.10 (A.10.1 – A.10.5 - A.10.6) Pengendalian Akses, SNI-ISO 27001 A.11 (A.11.5).
Unit Teknologi Informasi dan Komunikasi (Unit TIK 2)	Lailiyatul Anisah	Akuisisi, Pengembangan, dan Pemeliharaan Sistem Informasi, SNI-ISO 27001 A.12 (A.12.2- A.12.5)
Unit Layanan	Nurlia Rahmawati, A. Md.	Manajemen Kejadian Keamanan Informasi, SNI-ISO 27001 A.13 (A.13.1 – A.13.2)

Yogyakarta, 31 Agustus 2016

Mengetahui
Perpustakaan Kota Yogyakarta

Auditor

Triyanta, S.Pd., M.IP
NIP : 196901111990031004

Lusi Anggarini
NIM : 12651076

LEMBAR KERTAS KERJA AUDIT

Audit Keamanan Sistem Informasi
Perpustakaan Kota Yogyakarta Berdasarkan
Standar ISO 27001

Document ID	:	INTERVIEW - 01
Project Name	:	Audit Keamanan Sistem Informasi Perpustakaan Kota Yogyakarta Berdasarkan Standar ISO 27001.
Auditor	:	Lusi
Audite	:	Bapak Triyanta
Description	:	Lembar kertas kerja audit ini merupakan bagian dari Penelitian tugas akhir mahasiswa Program Studi Teknik Informatika, Universitas Islam Negeri Sunan Kalijaga Yogyakarta. Lembar kertas kerja audit ini digunakan untuk mengevaluasi Kebijakan Keamanan yang diterapkan oleh pengelola Sistem Informasi Perpustakaan Kota Yogyakarta
Date	:	
Responsible	:	Unit Pengembangan

Approved by Auditor

Triyanta, S.Pd., M.IP Lusi

LEMBAR KERTAS KERJA AUDIT

Audit Keamanan Sistem Informasi
Perpustakaan Kota Yogyakarta Berdasarkan
Standar ISO 27001

Document ID	:	INTERVIEW – 02 , 03
Project Name	:	Audit Keamanan Sistem Informasi Perpustakaan Kota Yogyakarta Berdasarkan Standar ISO 27001.
Auditor	:	Lusi
Audite	:	Bapak Nurhadi
Description	:	Lembar kertas kerja audit ini merupakan bagian dari Penelitian tugas akhir mahasiswa Program Studi Teknik Informatika, Universitas Islam Negeri Sunan Kalijaga Yogyakarta. Lembar kertas kerja audit ini digunakan untuk mengevaluasi Pengelolaan Aset serta Keamanan Fisik dan Lingkungan yang diterapkan oleh pengelola Sistem Informasi Perpustakaan Kota Yogyakarta.
Date	:	
Responsible	:	Unit Sarana dan Prasarana (Unit Sar-pras)

Approved by Auditor

Nurhadi Lusi

LEMBAR KERTAS KERJA AUDIT

Audit Keamanan Sistem Informasi
Perpustakaan Kota Yogyakarta Berdasarkan
Standar ISO 27001

Document ID	:	INTERVIEW – 04, 05
Project Name	:	Audit Keamanan Sistem Informasi Perpustakaan Kota Yogyakarta Berdasarkan Standar ISO 27001.
Auditor	:	Lusi
Audite	:	Ibu Isti
Description	:	Lembar kertas kerja audit ini merupakan bagian dari Penelitian tugas akhir mahasiswa Program Studi Teknik Informatika, Universitas Islam Negeri Sunan Kalijaga Yogyakarta. Lembar kertas kerja audit ini digunakan untuk mengevaluasi Manajemen Komunikasi dan Operasi serta Pengendalian Akses yang diterapkan oleh pengelola Sistem Informasi Perpustakaan Kota Yogyakarta.
Date	:	
Responsible	:	Unit TIK 1

Approved by Auditor

Budi Isti Wijayanti, A. Md. Lusi

LEMBAR KERTAS KERJA AUDIT

Audit Keamanan Sistem Informasi
Perpustakaan Kota Yogyakarta Berdasarkan
Standar ISO 27001

Document ID	:	INTERVIEW - 06
Project Name	:	Audit Keamanan Sistem Informasi Perpustakaan Kota Yogyakarta Berdasarkan Standar ISO 27001.
Auditor	:	Lusi
Audite	:	Ibu Laili
Description	:	Lembar kertas kerja audit ini merupakan bagian dari Penelitian tugas akhir mahasiswa Program Studi Teknik Informatika, Universitas Islam Negeri Sunan Kalijaga Yogyakarta. Lembar kertas kerja audit ini digunakan untuk mengevaluasi Akuisisi, Pengembangan dan Pemeliharaan Sistem Informasi yang diterapkan oleh pengelola Sistem Informasi Perpustakaan Kota Yogyakarta.
Date	:	
Responsible	:	Unit TIK 2

Approved by Auditor

Lailiyatul Anisah Lusi

LEMBAR KERTAS KERJA AUDIT

Audit Keamanan Sistem Informasi
Perpustakaan Kota Yogyakarta Berdasarkan
Standar ISO 27001

Document ID	:	INTERVIEW - 07
Project Name	:	Audit Keamanan Sistem Informasi Perpustakaan Kota Yogyakarta Berdasarkan Standar ISO 27001.
Auditor	:	Lusi
Audite	:	Ibu Nurlia
Description	:	Lembar kertas kerja audit ini merupakan bagian dari Penelitian tugas akhir mahasiswa Program Studi Teknik Informatika, Universitas Islam Negeri Sunan Kalijaga Yogyakarta. Lembar kertas kerja audit ini digunakan untuk mengevaluasi Manajemen Kejadian Keamanan Informasi yang diterapkan oleh pengelola Sistem Informasi Perpustakaan Kota Yogyakarta.
Date	:	
Responsible	:	Unit Layanan

Approved by Auditor

Nurlia Rahmawati, A. Md. Lusi

LAMPIRAN C

Control Objective

Acuan Kontrol Saat Melakukan Audit

NO	KLAUSUL	DESKRIPSI	AUDITE
1.	A.5	Kebijakan Keamanan	Bpk Triyanta
	A.5.1	Kebijakan Keamanan Informasi	
2.	A.7	Pengelolaan Aset	Bpk Nurhadi
	A.7.1	Tanggung Jawab terhadap Aset	
	A.7.2	Klasifikasi Informasi	
3.	A.9	Keamanan Fisik dan Lingkungan	Bpk Nurhadi
	A.9.1	Area yang aman	
	A.9.2	Keamanan Peralatan	
4.	A.10	Manajemen Komunikasi dan Operasi	Ibu Isti
	A.10.1	Prosedur Operasional dan Tanggung Jawab	
	A.10.5	Back-up	
	A.10.6	Manajemen Keamanan Jaringan	
5.	A.11	Pengendalian Akses	Ibu Isti
	A.11.5	Pengendalian Akses Sistem Operasi	
6.	A.12	Akuisisi, Pengembangan, dan Pemeliharaan Sistem Informasi	Ibu Laili
	A.12.2	Pengolahan Yang Benar Dalam Aplikasi	
	A.12.5	Keamanan Dalam Proses Pengembangan dan pendukung.	
7.	A.13	Manajemen Kejadian Keamanan Informasi	Ibu Nurlia
	A.13.1	Pelaporan Kejadian dan Kelemahan Keamanan Informasi	
	A.13.2	Manajemen Kejadian Keamanan Informasi dan Pengembangannya	

LAMPIRAN D

Question of Control Objective

Kontrol Acuan Pertanyaan Saat Melakukan Proses Audit

NO	KLAUSUL	CODE	QUESTIONS
1	A.5		
	A.5.1		
	A.5.1.1	Q1	Sudah adakah kebijakan keamanan informasi?
		Q2	Apakah kebijakan keamanan tersebut sudah didokumentasikan?
		Q3	Apabila sudah, apakah dokumen kebijakan keamanan informasi itu sudah disetujui oleh pihak manajemen?
		Q4	Apakah dokumen kebijakan tersebut sudah di publikasikan kepada semua pihak terkait?
		Q5	Apakah kebijakan tersebut sudah dikomunikasikan?
	A.5.1.2	Q6	Apakah sudah dilakukan tinjauan ulang terehadap kebijakan keamanan informasi (untuk antisipasi perubahan yang mempengaruhi analisa resiko)?
		Q7	Apakah tinjauan ulang kebijakan dilakukan secara berkala dan terjadwal ?
		Q8	Apabila terjadi perubahan mengenai kebijakan, apakah kebijakan tersebut merupakan pengembangan dari sebelumnya (guna memenuhi kebutuhan dan efektif dalam pelaksanaan)?
		Q9	Apakah kebijakan yang diterapkan sudah sesuai dengan aturan yang berlaku?
		Q10	Siapakah yang bertanggung jawab terhadap kebijakan keamanan informasi?
2	A.7		
	A.7.1		
	A.7.1.1	Q11	Apakah semua inventaris aset (informasi, perangkat lunak, fisik dan layanan) sudah diidentifikasi dan dicatat?
		Q12	Apakah inventaris aset tersebut dijaga dan dipelihara?
		Q13	Apakah sudah diterapkan kebijakan pengelolaan aset?
		Q14	Apakah kebijakan pengelolaan inventaris aset tersebut sudah didokumentasikan?
	A.7.1.2	Q15	Apakah ada pegawai / petugas yang menjaga (mengontrol dan memelihara) keamanan informasi inventaris aset?
		Q16	Siapa yang bertanggung jawab mengontrol dan memelihara terhadap pemrosesan informasi tersebut?
		Q17	Apakah ada jangka waktu pengecekan inventaris aset secara berkala?
		Q18	Apakah sudah diidentifikasi nilai dan tingkat kepentingan aset?
	A.7.1.3	Q19	Apakah terdapat aturan dalam menggunakan informasi yang berhubungan dengan fasilitas pemrosesan informasi (misal hardware server)?

		Q20	Apakah aturan dalam menggunakan aset informasi tersebut sudah diimplementasikan?
		Q21	Adakah dokumentasi mengenai informasi pengelolaan aset?
	A.7.2		
	A.7.2.1	Q22	Apakah informasi aset sudah diklasifikasikan dengan tingkat perlindungan yang tepat?
		Q23	Apakah ada prosedur yang baik berupa pemberian tanda pelabelan dan penanganan informasi?
	A.7.2.2	Q24	Apakah prosedur pelabelan dan penanganan informasi harus sesuai dengan skema klasifikasi informasi?
3	A.9		
	A.9.1		
	A.9.1.1	Q25	Apakah terdapat petugas yang berjaga dipintu masuk perpustakaan, guna meminimalisir resiko pencurian atau kesalahan dalam penggunaan fasilitas?
		Q26	Apakah terdapat aturan tertentu ketika memasuki ruang pemrosesan informasi?
		Q27	Apakah ada kontrol akses fisik atau ruang /wilayah sebagai tempat menerima tamu?
		Q28	Pernahkah meninggalkan komputer dalam keadaan menyala dan ada pegawai lain di dalamnya?
		Q29	Adakah ruangan khusus atau pembatas seperti dinding bagi pemegang kendali sistem informasi perpustakaan kota?
		Q30	Apakah tembok terluar bangunan sudah terbuat dari konstruksi kuat dan terlindungi dari akses tanpa izin?
	A.9.1.2	Q31	Apakah pengunjung / pemustaka yang datang diawasi dan menulis tanggal datang dibuku tamu?
		Q32	Apakah hak akses ke ruang informasi dan fasilitas pemrosesan informasi selalu dikontrol dan dibatasi?
	A.9.1.3	Q33	Apakah semua pegawai dan karyawan diwajibkan memakai tanda pengenal?
		Q34	Apakah sudah diidentifikasi siapa saja yang berhak masuk ruangan kantor, guna memastikan keamanan kantor tetap terjaga?
	A.9.1.4	Q35	Apakah sudah ada perlindungan fisik terhadap kerusakan akibat dari ledakan, banjir dan bencana alam lainnya?
		Q36	Apakah bahan yang berbahaya dan mudah meledak sudah disimpan diwilayah aman?
	A.9.1.5	Q37	Apakah penempatan ruang sistem informasi / server sudah termasuk dalam area yang aman?
		Q38	Apakah terdapat kebijakan mengenai makan, minum dan merokok disekitar fasilitas pemrosesan informasi?
		Q39	Apakah kabel listrik sudah dipisahkan dari kabel komunikasi untuk mencegah gangguan (interferensi)?
	A.9.2		
	A.9.2.1	Q40	Apakah komputer server dan peralatan informasi sudah dicek dan ditempatkan pada tempat yang aman?

		Q41	Apakah tata letak hardware sudah ditempatkan dengan tepat guna memastikan tidak ada peluang akses oleh pihak yang tidak berwenang?
	A.9.2.2	Q42	Apakah peralatan sudah dilindungi dari kegagalan daya listrik?
		Q43	Apakah sudah tersedia peralatan pendukung cadangan seperti genset atau UPS?
	A.9.2.3	Q44	apakah utilitas pendukung seperti sumber daya listrik, UPS, genset selalu dicek keamanannya?
		Q45	Apakah kabel daya dan telekomunikasi kebutuhan data sudah dilindungi dari ancaman kerusakan atau penyadapan misal pencurian listrik / menggunakan pipa pengaman ?
	A.9.2.4	Q46	Apakah peralatan hardware selalu dijaga dan dipelihara dengan baik?
		Q47	Apakah ada prosedur dalam menggunakan peralatan / hardware?
		Q48	Apakah waktu pengecekan peralatan / hardware sudah sesuai dengan prosedur yang ada?
4	A.10		
	A.10.1		
	A.10.1.1	Q49	Apakah terdapat prosedur pengoprasian dalam pemrosesan informasi (guna memastikan keamanan operasi)?
		Q50	Jika ada, apakah prosedur tersebut sudah di dokumentasikan dan tersedia bagi pengguna?
		Q51	Apakah pengoperasian fasilitas pengolahan informasi (Maintenance Server) sudah dilakukan secara benar dan aman?
		Q52	Apakah setiap data penting dilakukan back-up?
	A.10.1.2	Q53	Jika ada perubahan terhadap fasilitas dan sistem pengolahan informasi, apakah akan dikomunikasikan kepada pihak terkait?
	A.10.1.3	Q54	Apakah pegawai di ruang sistem informasi Perpustakaan Kota sudah dipisahkan menurut tugas dan tanggung jawabnya masing-masing?
		Q55	Apakah ada pengawasan dan pemantauan terhadap sistem untuk mengurangi resiko / insiden penyalahgunaan atau modifikasi tanpa ijin?
	A.10.5		
	A.10.5.1	Q56	Apakah perangkat lunak / software dilakukan uji secara berkala?
		Q57	Apakah setiap data berupa informasi dilakukan back-up guna mencegah terjadinya kehilangan atau kegagalan?
		Q58	Apakah salinan back-up dan prosedur pemulihan yang terdokumentasi disimpan di lokasi terpisah?
		Q59	Apakah media back-up tersebut sudah diuji secara berkala untuk memastikan bisa digunakan pada situasi darurat?

	A.10.6		
	A.10.6.1	Q60	Apakah sudah menerapkan kontrol jaringan untuk memastikan keamanan sistem dan data dalam jaringan?
		Q61	Apakah kontrol tersebut dilakukan secara berkala, guna melindungi hak akses tanpa ijin pada jaringan / serangan?
		Q62	Sejauh ini, apakah terdapat titik jaringan yang rawan terhadap serangan?
		Q63	Apakah ada petugas atau pegawai yang khusus menangani keamanan jaringan?
		Q64	Apakah sudah terdapat mekanisme pengamanan jaringan sebagai upaya pencegahan serangan ?
		Q65	Apabila serangan telah terjadi, adakah mekanisme recovery jaringan yang diterapkan ?
5	A.11		
	A.11.5		
	A.11.5.1	Q66	Apakah sudah di terapkan prosedur log-on pada sistem informasi?
		Q67	Apakah sistem sudah membatasi kegagalan percobaan log-on?
	A.11.5.2	Q68	Apakah seluruh pengguna (termasuk staf pendukung teknis) memiliki user ID yang berbeda ?
		Q69	Apakah user ID tersebut disyaratkan agar mempunyai ID yang unik seperti menggabungkan huruf dan angka?
	A.11.5.3	Q70	Apakah sudah ada sistem manajemen password dan sistem pengelola password untuk memastikan kualitas password?
		Q71	Apakah terdapat prosedur batasan jangka waktu pemakaian akun user?
	A.11.5.4	Q72	Sudah adakah prosedur penonaktifan akun user (seperti password) guna memastikan tidak adanya pemakaian ulang?
	A.11.5.5	Q73	Apakah sudah menggunakan sesi time-out?
	A.12		
	A.12.2		
	A.12.2.1	Q74	Apakah sudah ada prosedur validasi data ketika akan memasukan data ke sistem informasi Perpustakaan Kota Yogyakarta?
		Q75	Apakah terdapat prosedur untuk merespon kesalahan validasi?
6	A.12.2.2	Q76	Apakah cek validasi harus disediakan kedalam aplikasi / sistem guna mendeteksi adanya kerusakan (corrupt) informasi dalam kesalahan atau proses pengiriman?
		Q77	Ketika ada kerusakan informasi karena ada kesalahan pengolahan apakah dapat terdeteksi oleh sistem?

	A.12.2.4	Q78	Untuk memastikan bahwa pemroresan informasi yang disimpan adalah benar, apakah validasi data keluaran penting?
	A.12.5		
	A.12.5.1	Q79	Apakah sudah ada prosedur mengenai pengendalian perubahan kontrol?
		Q80	Apakah pengendalian perubahan kontrol tersebut sudah diimplementasikan?
	A.12.5.2	Q81	Bila sistem operasi di ubah, apakah sistem informasi perpustakaan ditinjau dan diuji ulang untuk memastikan tidak ada dampak yang merugikan?
		Q82	Apakah penting menjaga keamanan sistem informasi perpustakaan ketika dilakukan perubahan sistem operasi?
	A.12.5.3	Q83	Apakah perangkat lunak / software selalu diperbaharui / update?
		Q84	Apakah ada jangka waktu perbaharuan terhadap perangkat lunak tersebut?
		Q85	Apakah setiap kali melakukan perubahan sudah di kendalikan (untuk memastikan supaya tidak terjadi hal yang tidak diinginkan)?
	A.12.5.4	Q86	Apakah sudah dilakukan pencegahan terhadap peluang kebocoran informasi?
		Q87	Apakah ada prosedur pencegahannya?
		Q88	Apakah sudah dilakukan pantauan terhadap pengembangan perangkat lunak?
	A.13		
	A.13.1		
	A.13.1.1	Q89	Apakah setiap kejadian keamanan sistem / layanan sudah dilaporkan dengan cepat?
		Q90	Apakah pelaporan kejadian tersebut sudah sesuai dengan mekasnisme yang ditentukan?
		Q91	Apakah staf / petugas selalu melaporkan apabila menemukan kelemahan keamanan sistem?
		Q92	Apakah setiap pelaporan mengenai temuan / dugaan kelemahan keamanan tersebut dicatat?
	A.13.2		
	A.13.2.1	Q93	Apakah sudah dibentuk manjemen penanggung jawab dalam penanganan keamanan informasi?
		Q94	Apakah sudah ada prosedur untuk penanganan kejadian kemanan informasi tersebut (guna memastikan kecepatan dan keefektivitasan penanganan) ?
		Q95	Apakah pihak manajemen memberikan respon yang cepat terhadap laporan keamanan sistem informasi?

		Q96	Apakah ada petugas yang memonitor terhadap penanganan keamanan informasi (untuk memastikan pennganan tersebut sesuai prosedur) ?
		Q97	Apakah sudah dilakukan pembaharuan terhadap tata cara (mekanisme) penanganan keamanan informasi?
	A.13.2.3	Q98	Apakah perlu adanya tindak lanjut setelah penanganan insiden?
		Q99	Apabila terjadi insiden, apakah perlu dikumpulkan bukti - bukti tersebut?
		Q100	Apakah bukti- bukti tersebut didokumentasikan dan dilaporkan kepada pihak yang berwajib (untuk dilakukannya tindak lanjut)?

LAMPIRAN E

Form Question (FQ)

Pemetaan Pertanyaan yang Akan Digunakan Saat Proses Audit

Form Questions 1 (FQ 1) : Unit Pengembangan

Q1, Q2, Q3, Q4, Q5, Q6, Q7, Q8, Q9, Q10.

Form Questions 2 (FQ 2) : Unit Sarana dan Prasarana

Q11, Q12, Q13, Q14, Q15, Q16, Q17, Q18, Q19, Q20, Q21, Q22, Q23, Q24, Q25, Q26, Q27, Q28, Q29, Q30, Q31, Q32, Q33, Q34, Q35, Q36, Q37, Q38, Q39, Q40, Q41, Q42, Q43, Q44, Q45, Q46, Q47, Q48.

Form Questions 3 (FQ 3) : Unit TIK 1

Q49, Q50,Q51, Q52, Q53, Q54, Q55, Q56, Q57, Q58, Q59, Q60, Q61, Q62, Q63, Q64, Q65, Q66, Q67, Q68, Q69, Q70, Q71, Q72, Q73.

Form Questions 4 (FQ 4) : Unit TIK 2

Q74, Q75, Q76, Q77, Q78, Q79, Q80, Q81, Q82, Q83, Q84, Q85, Q86, Q87, Q88.

Form Questions 5 (FQ 5) : Unit Layanan

Q89, Q90, Q91, Q92, Q93, Q94, Q95, Q96, Q97, 98, 99, 100.

LAMPIRAN F

Maturity Model

Tingkatan Kematangan	Definisi
0 - (Non- Existent)	Proses manajemen tidak diterapkan sama sekali. Semua proses tidak dapat diidentifikasi dan dikenali. Status kesiapan keamanan informasi tidak diketahui.
1 - (Initial/Ad Hoc)	Mulai adanya pemahaman mengenai perlunya pengelolaan keamanan informasi. Penerapan langkah pengamanan masih bersifat reaktif, tidak teratur, tidak mengacu kepada keseluruhan risiko yang ada, tanpa alur komunikasi dan kewenangan yang jelas dan tanpa pengawasan, Kelemahan teknis dan non-teknis tidak teridentifikasi dengan baik, pihak yang terlibat tidak menyadari tanggung jawab mereka.
2 - (Repeatable but Intuitive)	Proses mengikuti pola yang teratur dimana prosedur serupa diikuti pegawai/karyawan lainya tetapi tidak ada pelatihan formal sebelumnya dan tidak ada standar prosedur yang digunakan sebagai acuan. Tanggung jawab sepenuhnya dilimpahkan kepada individu masing – masing dan kesalahan sangat mungkin terjadi.
3 - (Defined process)	Proses telah didokumentasikan dan dikomunikasikan, prosedur telah distandarisasi, didokumentasikan dan dikomunikasikan melalui pelatihan. Proses berada pada keadaan diamanatkan namun, kecil kemungkinan penyimpangan dapat terdeteksi. Prosedur yang ada hanya formalisasi praktek yang ada.

4 - (Managed and Measurable)	Monitor dari manajemen dan mengukur kepatuhan prosedur dan mengambil tindakan apabila diperlukan. Selalu ada proses pembaharuan yang konstan dan berkala dan memberikan pelaksanaan yang baik. Otomasi dan alat – alat yang digunakan diakses secara terbatas dan sudah terfragmentasi
5 - (Optimized)	Praktek yang baik diikuti dan secara otomatis. Proses telah disempurnakan ke tingkat pelaksanaan yang baik, berdasarkan hasil dari peningkatan berkelanjutan dan maturity pemodelan dengan informasi lainnya tentang perusahaan. TI digunakan secara terpadu untuk mengotomatisasi alur kerja, menyediakan alat untuk meningkatkan kualitas dan efektivitas.

LAMPIRAN G

Hasil Audit *Interview*

LEMBAR KERTAS KERJA AUDIT

Audit Keamanan Sistem Informasi
Berdasarkan Standar SNI-ISO 27001 Pada Sistem Informasi
Perpustakaan Kota Yogyakarta

Document ID	:	INTERVIEW - 01
Project Name	:	Audit Keamanan Sistem Informasi Berdasarkan Standar SNI-ISO 27001 Pada Sistem Informasi Perpustakaan Kota Yogyakarta.
Auditor	:	Lusi
Audite	:	Bapak Triyanta
Description	:	Lembar kertas kerja audit ini merupakan bagian dari Penelitian tugas akhir mahasiswa Program Studi Teknik Informatika, Universitas Islam Negeri Sunan Kalijaga Yogyakarta. Lembar kertas kerja audit ini digunakan untuk mengevaluasi Kebijakan Keamanan yang diterapkan oleh pengelola Sistem Informasi Perpustakaan Kota Yogyakarta
Date	:	
Responsible	:	Unit Pengembangan

Approved by

Triyanta, S.Pd., M.IP

Auditor

Lusi

QUESTIONS OF INTERVIEW

Document ID : INTERVIEW – 01

Klausul : Kebijakan Keamanan (A.5)

No	Code	Question	Answer	Score
1	Q1	Sudah adakah kebijakan keamanan informasi?	'Idah	3
2	Q2	Apakah kebijakan keamanan tersebut sudah didokumentasikan?	Sudah	3
3	Q3	Apabila sudah, apakah dokumen kebijakan keamanan informasi itu sudah disetujui oleh pihak manajemen?	Sudah	3
4	Q4	Apakah dokumen kebijakan tersebut sudah di publikasikan kepada semua pihak terkait?	Sebagian sudah	2
5	Q5	Apakah kebijakan tersebut sudah dikomunikasikan?	Sudah	3
6	Q6	Apakah sudah dilakukan tinjauan ulang terehadap kebijakan keamanan informasi (untuk antisipasi	Sudah	3

		perubahan yang mempengaruhi analisa resiko)?		
7	Q7	Apakah tinjauan ulang kebijakan dilakukan secara berkala dan terjadwal ?	Tidak, Temporary.	2
8	Q8	Apabila terjadi perubahan mengenai kebijakan, apakah kebijakan tersebut merupakan pengembangan dari sebelumnya (guna memenuhi kebutuhan dan efektif dalam pelaksanaan)?	Ya.	3
9	Q9	Apakah kebijakan yang diterapkan sudah sesuai dengan aturan yang berlaku?	Ya.	3
10	Q10	Siapakah yang bertanggung jawab terhadap kebijakan keamanan informasi?	Sebagian teknis ada unit TIK, secara strategis ada pada ka kantor / Pimp.	3

Sampe ke P. Nurjadi

LEMBAR KERTAS KERJA AUDIT

Audit Keamanan Sistem Informasi
Berdasarkan Standar SNI-ISO 27001 Pada Sistem Informasi
Perpustakaan Kota Yogyakarta

Document ID	:	INTERVIEW – 02 , 03
Project Name	:	Audit Keamanan Sistem Informasi Berdasarkan Standar SNI-ISO 27001 Pada Sistem Informasi Perpustakaan Kota Yogyakarta.
Auditor	:	Lusi
Audite	:	Bapak Nurhadi
Description	:	Lembar kertas kerja audit ini merupakan bagian dari Penelitian tugas akhir mahasiswa Program Studi Teknik Informatika, Universitas Islam Negeri Sunan Kalijaga Yogyakarta. Lembar kertas kerja audit ini digunakan untuk mengevaluasi Pengelolaan Aset serta Keamanan Fisik dan Lingkungan yang diterapkan oleh pengelola Sistem Informasi Perpustakaan Kota Yogyakarta.
Date	:	
Responsible	:	Unit Sarana dan Prasarana (Unit Sar-pras)

Approved by

Nurhadi

Auditor

Lusi

QUESTIONS OF INTERVIEW

Document ID : INTERVIEW – 02

Klausul : Pengelolaan Aset (A.7)

No	Code	Questions	Answer	Score
1	Q11	Apakah semua inventaris aset (informasi, perangkat lunak, fisik dan layanan) sudah diidentifikasi dan dicatat?	SUDAH	3
2	Q12	Apakah inventaris aset tersebut dijaga dan dipelihara?	DIJAGA & DIPELIHARA	3
3	Q13	Apakah sudah diterapkan kebijakan pengelolaan aset?	SUDAH	3
4	Q14	Apakah kebijakan pengelolaan inventaris aset tersebut sudah didokumentasikan?	SUDAH	3
5	Q15	Apakah ada pegawai / petugas yang menjaga (mengontrol dan memelihara) keamanan informasi inventaris aset?	ADA PETUGAS YG BERTANGGUNG JWB RUANGAN	3
6	Q16	Siapa yang bertanggung jawab mengontrol dan memelihara terhadap pemrosesan informasi tersebut?	PETUGAS DIBATU PETUGAS RUANGAN	3
7	Q17	Apakah ada jangka waktu pengecekan inventaris aset	ADA	3

		secara berkala?		
8	Q18	Apakah sudah diidentifikasi nilai dan tingkat kepentingan aset?	SUDAH & BELUM.	2
9	Q19	Apakah terdapat aturan dalam menggunakan informasi yang berhubungan dengan fasilitas pemrosesan informasi (misal hardware server)?	ADA	3
10	Q20	Apakah aturan dalam menggunakan aset informasi tersebut sudah di implementasikan?	SUDAH	3
11	Q21	Adakah dokumentasi mengenai informasi pengelolaan aset?	ADA	3
12	Q22	Apakah informasi aset sudah diklasifikasikan dengan tingkat perlindungan yang tepat?	YA & TIDAK	2
13	Q23	Apakah ada prosedur yang baik berupa pemberian tanda pelabelan dan penanganan informasi?	ADA	3
14	Q24	Apakah prosedur pelabelan dan penanganan informasi harus sesuai dengan skema klasifikasi informasi?	IYA	3

QUESTIONS OF INTERVIEW

Document ID : INTERVIEW – 03

Klausul : Keamanan Fisik dan Lingkungan (A.9)

No	Code	Questions	Answer	Score
1	Q25	Apakah terdapat petugas yang berjaga dipintu masuk perpustakaan, guna meminimalisir resiko pencurian atau kesalahan dalam penggunaan fasilitas?	ADA	3
2	Q26	Apakah terdapat aturan tertentu ketika memasuki ruang pemrosesan informasi?	ADA	3
3	Q27	Apakah ada kontrol akses fisik atau ruang /wilayah sebagai tempat menerima tamu?	ADA	3
4	Q28	Pernahkah meninggalkan komputer dalam keadaan menyala dan ada pegawai lain di dalamnya?	PERNAH	1
5	Q29	Adakah ruangan khusus atau pembatas seperti dinding bagi pemegang kendali sistem	ADA	3

		informasi perpustakaan kota?		
6	Q30	Apakah tembok terluar bangunan sudah terbuat dari konstruksi kuat dan terlindungi dari akses tanpa izin?	ADA	3
7	Q31	Apakah pengunjung / pemustaka yang datang diawasi dan menulis tanggal datang dibuku tamu?	ADA	3
8	Q32	Apakah hak akses ke ruang informasi dan fasilitas pemrosesan informasi selalu dikontrol dan dibatasi?	IYA & TIDAK	1
9	Q33	Apakah semua pegawai dan karyawan diwajibkan memakai tanda pengenal?	IYA	3
10	Q34	Apakah sudah diidentifikasi siapa saja yang berhak masuk ruangan kantor, guna memastikan keamanan kantor tetap terjaga?	SUDAH	3
11	Q35	Apakah sudah ada perlindungan fisik terhadap kerusakan akibat dari ledakan, banjir dan bencana alam lainnya?	SUDAH	3
12	Q36	Apakah bahan yang berbahaya dan mudah		

		meledak sudah disimpan diwilayah aman?	SUDAH	3
13	Q37	Apakah penempatan ruang sistem informasi / server sudah termasuk dalam area yang aman?	SUDAH	3
14	Q38	Apakah terdapat kebijakan mengenai makan, minum dan merokok disekitar fasilitas pemrosesan informasi?	TIDAK BOLEH ROKOK & MKN MNM	3
15	Q39	Apakah kabel listrik sudah dipisahkan dari kabel komunikasi untuk mencegah gangguan (interferensi)?	SUDAH	3
16	Q40	Apakah komputer server dan peralatan informasi sudah dicek dan ditempatkan pada tempat yang aman?	SUDAH	3
17	Q41	Apakah tata letak hardware sudah ditempatkan dengan tepat guna memastikan tidak ada peluang akses oleh pihak yang tidak berwenang?	SUDAH	3
18	Q42	Apakah peralatan sudah dilindungi dari kegagalan daya listrik?	SUDAH	3
19	Q43	Apakah sudah tersedia peralatan pendukung cadangan seperti genset atau	SUDAH	3

		UPS?		
20	Q44	apakah utilitas pendukung seperti sumber daya listrik, UPS, genset selalu dicek keamanannya?	SUDAH	3
21	Q45	Apakah kabel daya dan telekomunikasi kebutuhan data sudah dilindungi dari ancaman kerusakan atau penyadapan misal pencurian listrik / menggunakan pipa pengaman?	SUDAH	3
22	Q46	Apakah peralatan hardware selalu dijaga dan dipelihara dengan baik?	SELALU	3
23	Q47	Apakah ada prosedur dalam menggunakan peralatan / hardware?	ADA	3
24	Q48	Apakah waktu pengecekan peralatan / hardware sudah sesuai dengan prosedur yang ada?	SESUAI PROSEDUR	3

LEMBAR KERTAS KERJA AUDIT

Audit Keamanan Sistem Informasi
Berdasarkan Standar SNI-ISO 27001 Pada Sistem Informasi
Perpustakaan Kota Yogyakarta

Document ID	:	INTERVIEW – 04, 05
Project Name	:	Audit Keamanan Sistem Informasi Berdasarkan Standar SNI-ISO 27001 Pada Sistem Informasi Perpustakaan Kota Yogyakarta.
Auditor	:	Lusi
Audite	:	Ibu Isti
Description	:	Lembar kertas kerja audit ini merupakan bagian dari Penelitian tugas akhir mahasiswa Program Studi Teknik Informatika, Universitas Islam Negeri Sunan Kalijaga Yogyakarta. Lembar kertas kerja audit ini digunakan untuk mengevaluasi Manajemen Komunikasi dan Operasi serta Pengendalian Akses yang diterapkan oleh pengelola Sistem Informasi Perpustakaan Kota Yogyakarta.
Date	:	
Responsible	:	Unit TIK

Approved by	Auditor
Budi Isti Wijayanti, A. Md.	Lusi

QUESTIONS OF INTERVIEW

Document ID : INTERVIEW – 04

Klausul : Manajemen Komunikasi dan Operasi (A.10)

No	Code	Questions	Answer	Score
1	Q49	Apakah terdapat prosedur pengoprasian dalam pemrosesan informasi (guna memastikan keamanan operasi)?	Ada	3
2	Q50	Jika ada, apakah prosedur tersebut sudah di dokumentasikan dan tersedia bagi pengguna?	Sudah didokumentasikan dalam bentuk SOP dan tersedia bagi pengguna dalam bentuk cetak	3
3	Q51	Apakah pengoperasian fasilitas pengolahan informasi (Maintenance Server) sudah dilakukan secara benar dan aman?	Sudah, dilakukan maintenance server dan back-up data 1 bulan sekali	3
4	Q52	Apakah setiap data penting dilakukan back-up?	Ya, back-up data dilakukan rutin setiap bulan	3
5	Q53	Jika ada perubahan terhadap fasilitas dan sistem pengolahan informasi, apakah akan dikomunikasikan	Ya	3

		kepada pihak terkait?		
6	Q54	Apakah pegawai di ruang sistem informasi Perpustakaan Kota sudah dipisahkan menurut tugas dan tanggung jawabnya masing-masing?	Ya	3
7	Q55	Apakah ada pengawasan dan pemantauan terhadap sistem untuk mengurangi resiko / insiden penyalahgunaan atau modifikasi tanpa ijin?	Ada	3
8	Q56	Apakah perangkat lunak / software dilakukan uji secara berkala?	Tidak	1
9	Q57	Apakah setiap data berupa informasi dilakukan back-up guna mencegah terjadinya kehilangan atau kegagalan?	Ya	3
10	Q58	Apakah salinan back-up dan prosedur pemulihan yang terdokumentasi disimpan di lokasi terpisah?	Ya	3
11	Q59	Apakah media back-up tersebut sudah diuji secara berkala untuk memastikan bisa digunakan pada situasi darurat?	Sudah	3
12	Q60	Apakah sudah menerapkan		

		kontrol jaringan untuk memastikan keamanan sistem dan data dalam jaringan?	Sudah	3
13	Q61	Apakah kontrol tersebut dilakukan secara berkala, guna melindungi hak akses tanpa ijin pada jaringan / serangan?	Ya	3
14	Q62	Sejauh ini, apakah terdapat titik jaringan yang rawan terhadap serangan?	Tidak	3
15	Q63	Apakah ada petugas atau pegawai yang khusus menangani keamanan jaringan?	Ada	3
16	Q64	Apakah sudah terdapat mekanisme pengamanan jaringan sebagai upaya pencegahan serangan?	Sudah	3
17	Q65	Apabila serangan telah terjadi, adakah mekanisme recovery jaringan yang diterapkan?	Ada	3

QUESTIONS OF INTERVIEW

Document ID : INTERVIEW – 05

Klausul : Pengendalian Akses (A.11)

No	Code	Questions	Answer	Score
1	Q66	Apakah sudah di terapkan prosedur log-on pada sistem informasi?	Sudah	3
2	Q67	Apakah sistem sudah membatasi kegagalan percobaan log-on?	Belum	1
3	Q68	Apakah seluruh pengguna (termasuk staf pendukung teknis) memiliki user ID yang berbeda?	Ya	3
4	Q69	Apakah user ID tersebut disyaratkan agar mempunyai ID yang unik seperti menggabungkan huruf dan angka?	Tidak	1
5	Q70	Apakah sudah ada sistem manajemen password dan sistem pengelola password untuk memastikan kualitas password?	Belum	1

6	Q71	Apakah terdapat prosedur batasan jangka waktu pemakaian akun user?	Tidak	1
7	Q72	Sudah adakah prosedur penonaktifan akun user (seperti password) guna memastikan tidak adanya pemakaian ulang?	Tidak	1
8	Q73	Apakah sudah menggunakan sesi time-out?	Belum	1

LEMBAR KERTAS KERJA AUDIT

Audit Keamanan Sistem Informasi
Berdasarkan Standar SNI-ISO 27001 Pada Sistem Informasi
Perpustakaan Kota Yogyakarta

Document ID	:	INTERVIEW - 06
Project Name	:	Audit Keamanan Sistem Informasi Berdasarkan Standar SNI-ISO 27001 Pada Sistem Informasi Perpustakaan Kota Yogyakarta.
Auditor	:	Lusi
Audite	:	Ibu Laili
Description	:	Lembar kertas kerja audit ini merupakan bagian dari Penelitian tugas akhir mahasiswa Program Studi Teknik Informatika, Universitas Islam Negeri Sunan Kalijaga Yogyakarta. Lembar kertas kerja audit ini digunakan untuk mengevaluasi Akuisisi, Pengembangan dan Pemeliharaan Sistem Informasi yang diterapkan oleh pengelola Sistem Informasi Perpustakaan Kota Yogyakarta.
Date	:	
Responsible	:	Unit TIK

Approved by

Lailiyatul Anisah

Auditor

Lusi

QUESTIONS OF INTERVIEW

Document ID : INTERVIEW – 06

Klausul : Akuisisi, Pengembangan, dan Pemeliharaan Sistem Informasi (A.12)

No	Code	Questions	Answer	Score
1	Q74	Apakah sudah ada prosedur validasi data ketika akan memasukan data ke sistem informasi Perpustakaan Kota Yogyakarta?	Sudah ada SOP.	3
2	Q75	Apakah terdapat prosedur untuk merespon kesalahan validasi?	Iya. kalau ada keselahan validasi harus segera di cek dan dilakukan pembetulan.	3
3	Q76	Apakah cek validasi harus disediakan kedalam aplikasi / sistem guna mendeteksi adanya kerusakan (corrupt) informasi dalam kesalahan atau proses pengiriman?	Iya harus disediakan. supaya kita tahu apakah data yang kita inputkan sesuai dengan data /buku.	3
4	Q77	Ketika ada kerusakan informasi karena ada kesalahan pengolahan apakah dapat terdeteksi oleh sistem?	~~Iya ada~~. Bisa. dengan dilakukan pengecekan.	3
5	Q78	Untuk memastikan bahwa pemroresan informasi yang		

		disimpan adalah benar, apakah validasi data keluaran penting?	Iya. Penting.	3
6	Q79	Apakah sudah ada prosedur mengenai pengendalian perubahan kontrol?	~~Belum~~ Sudah ada.	3
7	Q80	Apakah pengendalian perubahan kontrol tersebut sudah diimplementasikan?	Sudah diimplementasikan.	3
8	Q81	Bila sistem operasi di ubah, apakah sistem informasi perpustakaan ditinjau dan diuji ulang untuk memastikan tidak ada dampak yang merugikan?	Iya harus diuji ulang. dan ditinjau.	3
9	Q82	Apakah penting menjaga keamanan sistem informasi perpustakaan ketika dilakukan perubahan sistem operasi?	Iya penting. supaya sistem yang sudah ada tidak ada kerusakan.	3
10	Q83	Apakah perangkat lunak / software selalu diperbaharui / update?	Tidak.	1
11	Q84	Apakah ada jangka waktu perbaharuan terhadap perangkat lunak tersebut?	Tidak.	1
12	Q85	Apakah setiap kali melakukan perubahan sudah di kendalikan (untuk	Iya, apabila ada penambahan fitur harus dipastikan bahwa tidak mengganggu data (sistem yang sudah ada.	3

		memastikan supaya tidak terjadi hal yang tidak diinginkan)?		
13	Q86	Apakah sudah dilakukan pencegahan terhadap peluang kebocoran informasi?	sudah ada sistem keamanan untuk sistem.	3
14	Q87	Apakah ada prosedur pencegahannya?	Ada. salah satunya dengan mainterance dan backup data secara berkala.	3
15	Q88	Apakah sudah dilakukan pantauan terhadap pengembangan perangkat lunak?	Sudah ada rencana untuk pengembangan sistem.	3

LEMBAR KERTAS KERJA AUDIT

Audit Keamanan Sistem Informasi
Berdasarkan Standar SNI-ISO 27001 Pada Sistem Informasi
Perpustakaan Kota Yogyakarta

Document ID	:	INTERVIEW - 07
Project Name	:	Audit Keamanan Sistem Informasi Berdasarkan Standar SNI-ISO 27001 Pada Sistem Informasi Perpustakaan Kota Yogyakarta.
Auditor	:	Lusi
Audite	:	Ibu Nurlia
Description	:	Lembar kertas kerja audit ini merupakan bagian dari Penelitian tugas akhir mahasiswa Program Studi Teknik Informatika, Universitas Islam Negeri Sunan Kalijaga Yogyakarta. Lembar kertas kerja audit ini digunakan untuk mengevaluasi Manajemen Kejadian Keamanan Informasi yang diterapkan oleh pengelola Sistem Informasi Perpustakaan Kota Yogyakarta.
Date	:	
Responsible	:	Unit Layanan

Approved by | Auditor

Nurlia Rahmawati, A. Md. | Lusi

QUESTIONS OF INTERVIEW

Document ID : INTERVIEW – 07

Klausul : Manajemen Kejadian Keamanan Informasi (A.13)

No	Code	Questions	Answer	Score
1	Q89	Apakah setiap kejadian keamanan sistem / layanan sudah dilaporkan dengan cepat?	SUDAH. SETIAP ADA KEJADIAN SELALU DILAPORKAN DENGAN CEPAT.	3
2	Q90	Apakah pelaporan kejadian tersebut sudah sesuai dengan mekasnisme yang ditentukan?	SUDAH. ADA SOP YANG MENGATUR MEKANISME PELAPORAN.	3
3	Q91	Apakah staf / petugas selalu melaporkan apabila menemukan kelemahan keamanan sistem?	IYA. SELALU DILAPORKAN.	3
4	Q92	Apakah setiap pelaporan mengenai temuan / dugaan kelemahan keamanan tersebut dicatat?	IYA, SELALU DICATAT DALAM BUKU CATATAN LAYANAN SISKA.	3
5	Q93	Apakah sudah dibentuk manjemen penanggung jawab dalam penanganan keamanan informasi?	SUDAH ADA TIM PENANGANAN PENGADUAN/INFORMASI SISKA.	3
6	Q94	Apakah sudah ada prosedur untuk penanganan kejadian kemanan informasi tersebut	SUDAH ADA SOP TERKAIT LAYANAN SISKA	3

		(guna memastikan kecepatan dan keefektivitasan penanganan)?		
7	Q95	Apakah pihak manajemen memberikan respon yang cepat terhadap laporan keamanan sistem informasi?	IYA, SELALU MERESPON DENGAN CEPAT DENGAN TINDAK LANJUT TERHADAP LAPORAN.	3
8	Q96	Apakah ada petugas yang memonitor terhadap penanganan keamanan informasi (untuk memastikan pennganan tersebut sesuai prosedur)?	ADA	3
9	Q97	Apakah sudah dilakukan pembaharuan terhadap tata cara (mekanisme) penanganan keamanan informasi?	BELUM DILAKUKAN	1
10	Q98	Apakah perlu adanya tindak lanjut setelah penanganan insiden?	IYA SELALU ADA TINDAK LANJUT	3
11	Q99	Apabila terjadi insiden, apakah perlu dikumpulkan bukti - bukti tersebut?	IYA PERLU DIKUMPULKAN	3
12	Q100	Apakah bukti- bukti tersebut didokumentasikan dan dilaporkan kepada pihak yang berwajib (untuk dilakukannya tindak lanjut)?	TIDAK DILAPORKAN /BELUM DILAPORKAN	1

LAMPIRAN H

Hasil Evaluasi Audit

HASIL EVALUASI AUDIT PROSES PERHITUNGAN AKHIR NILAI MATURITY

NO	KLAUSUL	KODE	QUESTIONS	FORM QUESTIONS					SCORE	MATURITY	SCORE MATURITY
				FQ1	FQ2	FQ3	FQ4	FQ5			
1.	A.5										2,8
	A.5.1										
	A.5.1.1	Q1	Sudah adakah kebijakan keamanan informasi?	3					3	Defined Process	
		Q2	Apakah kebijakan keamanan tersebut sudah didokumentasikan?	3					3	Defined Process	
		Q3	Apabila sudah, apakah dokumen kebijakan keamanan informasi itu sudah disetujui oleh pihak manajemen?	3					3	Defined Process	
		Q4	Apakah dokumen kebijakan tersebut sudah di publikasikan kepada semua pihak terkait?	2					2	Repeatable But Intuitive	
		Q5	Apakah kebijakan tersebut sudah dikomunikasikan?	3					3	Defined Process	
		Q6	Apakah sudah dilakukan tinjauan ulang terehadap kebijakan keamanan informasi (untuk antisipasi perubahan yang mempengaruhi analisa resiko)?	3					3	Defined Process	
		Q7	Apakah tinjauan ulang kebijakan dilakukan secara berkala dan terjadwal ?	2					2	Repeatable But Intuitive	
		Q8	Apabila terjadi perubahan mengenai kebijakan, apakah kebijakan tersebut	3					3	Defined Process	

	A.5.1.2		merupakan pengembangan dari sebelumnya (guna memenuhi kebutuhan dan efektif dalam pelaksanaan)?								
		Q9	Apakah kebijakan yang diterapkan sudah sesuai dengan aturan yang berlaku?	3					3	Defined Process	
		Q10	Siapakah yang bertanggung jawab terhadap kebijakan keamanan informasi?	3					3	Defined Process	
2.	A.7										
	A.7.1										
	A.7.1.1	Q11	Apakah semua inventaris aset (informasi, perangkat lunak, fisik dan layanan) sudah diidentifikasi dan dicatat?		3				3	Defined process	2,85714286
		Q12	Apakah inventaris aset tersebut dijaga dan dipelihara?		3				3	Defined process	
		Q13	Apakah sudah diterapkan kebijakan pengelolaan aset?		3				3	Defined process	
		Q14	Apakah kebijakan pengelolaan inventaris aset tersebut sudah didokumentasikan?		3				3	Repeatable But Intuitive	
	A.7.1.2	Q15	Apakah ada pegawai / petugas yang menjaga (mengontrol dan memelihara) keamanan informasi inventaris aset?		3				3	Defined process	
		Q16	Siapa yang bertanggung jawab mengontrol dan memelihara terhadap pemrosesan informasi tersebut?		3				3	Defined process	
		Q17	Apakah ada jangka waktu pengecekan inventaris aset secara berkala?		3				3	Defined process	
		Q18	Apakah sudah diidentifikasi nilai dan		2				2	Repeatable But	

			tingkat kepentingan aset?							Intuitive	
	A.7.1.3	Q19	Apakah terdapat aturan dalam menggunakan informasi yang berhubungan dengan fasilitas pemrosesan informasi (misal hardware server)?		3				3	Defined Process	
		Q20	Apakah aturan dalam menggunakan aset informasi tersebut sudah di implementasikan?		3				3	Defined Process	
		Q21	Adakah dokumentasi mengenai informasi pengelolaan aset?		3				3	Defined Process	
	A.7.2										
	A.7.2.1	Q22	Apakah informasi aset sudah diklasifikasikan dengan tingkat perlindungan yang tepat?		2				2	Repeatable But Intuitive	
		Q23	Apakah ada prosedur yang baik berupa pemberian tanda pelabelan dan penanganan informasi?		3				3	Defined Process	
	A.7.2.2	Q24	Apakah prosedur pelabelan dan penanganan informasi harus sesuai dengan skema klasifikasi informasi?		3				3	Defined Process	
3.	A.9										
	A.9.1										
	A.9.1.1	Q25	Apakah terdapat petugas yang berjaga dipintu masuk perpustakaan, guna meminimalisir resiko pencurian atau kesalahan dalam penggunaan fasilitas?		3				3	Defined Process	2,83333333

		Q26	Apakah terdapat aturan tertentu ketika memasuki ruang pemrosesan informasi?		3				3	Defined Process	
		Q27	Apakah ada kontrol akses fisik atau ruang /wilayah sebagai tempat menerima tamu?		3				3	Defined process	
		Q38	Pernahkah meninggalkan komputer dalam keadaan menyala dan ada pegawai lain di dalamnya?		1				1	Initial/Ad Hoc	
		Q29	Adakah ruangan khusus atau pembatas seperti dinding bagi pemegang kendali sistem informasi perpustakaan kota?		3				3	Defined Process	
		Q30	Apakah tembok terluar bangunan sudah terbuat dari konstruksi kuat dan terlindungi dari akses tanpa izin?		3				3	Defined process	
	A.9.1.2	Q31	Apakah pengunjung / pemustaka yang datang diawasi dan menulis tanggal datang dibuku tamu?		3				3	Repeatable But Intuitive	
		Q32	Apakah hak akses ke ruang informasi dan fasilitas pemrosesan informasi selalu dikontrol dan dibatasi?		1				1	Initial/Ad Hoc	
	A.9.1.3	Q33	Apakah semua pegawai dan karyawan diwajibkan memakai tanda pengenal?		3				3	Defined Process	
		Q34	Apakah sudah diidentifikasi siapa saja yang berhak masuk ruangan kantor, guna memastikan keamanan kantor tetap terjaga?		3				3	Defined process	
	A.9.14	Q35	Apakah sudah ada perlindungan fisik terhadap kerusakan akibat dari ledakan, banjir dan bencana alam lainnya?		3				3	Defined Process	
		Q36	Apakah bahan yang berbahaya dan mudah meledak sudah disimpan diwilayah aman?		3				3	Defined Process	

	A.9.1.5	Q37	Apakah penempatan ruang sistem informasi / server sudah termasuk dalam area yang aman?		3				3	Defined process	
		Q38	Apakah terdapat kebijakan mengenai makan, minum dan merokok disekitar fasilitas pemrosesan informasi?		3				3	Defined process	
		Q39	Apakah kabel listrik sudah dipisahkan dari kabel komunikasi untuk mencegah gangguan (interferensi)?		3				3	Defined Process	
	A.9.2										
	A.9.2.1	Q40	Apakah komputer server dan peralatan informasi sudah dicek dan ditempatkan pada tempat yang aman?		3				3	Defined process	
		Q41	Apakah tata letak hardware sudah ditempatkan dengan tepat guna memastikan tidak ada peluang akses oleh pihak yang tidak berwenang?		3				3	Defined process	
	A.9.2.2	Q42	Apakah peralatan sudah dilindungi dari kegagalan daya listrik?		3				3	Defined Process	
		Q43	Apakah sudah tersedia peralatan pendukung cadangan seperti genset atau UPS?		3				3	Defined Process	
	A.9.2.3	Q44	apakah utilitas pendukung seperti sumber daya listrik, UPS, genset selalu dicek keamanannya?		3				3	Defined Process	
		Q45	Apakah kabel daya dan telekomunikasi kebutuhan data sudah dilindungi dari ancaman kerusakan atau penyadapan misal pencurian listrik / menggunakan pipa pengaman?		3				3	Defined Process	

	A.9.2.4	Q46	Apakah peralatan hardware selalu dijaga dan dipelihara dengan baik?		3				3	Defined Process	
		Q47	Apakah ada prosedur dalam menggunakan peralatan / hardware?		3				3	Defined process	
		Q48	Apakah waktu pengecekan peralatan / hardware sudah sesuai dengan prosedur yang ada?		3				3	Defined Process	
4.	A.10										
	A.10.1										
	A.10.1.1	Q49	Apakah terdapat prosedur pengoprasian dalam pemrosesan informasi (guna memastikan keamanan operasi)?			3			3	Defined Process	2,88235294
		Q50	Jika ada, apakah prosedur tersebut sudah di dokumentasikan dan tersedia bagi pengguna?			3			3	Defined Process	
		Q51	Apakah pengoperasian fasilitas pengolahan informasi (Maintenance Server) sudah dilakukan secara benar dan aman?			3			3	Defined Process	
		Q52	Apakah setiap data penting dilakukan back-up?			3			3	Defined Process	
	A.10.1.2	Q53	Jika ada perubahan terhadap fasilitas dan sistem pengolahan informasi, apakah akan dikomunikasikan kepada pihak terkait?			3			3	Defined Process	
	A.10.1.3	Q54	Apakah pegawai di ruang sistem informasi Perpustakaan Kota sudah dipisahkan menurut tugas dan tanggung jawabnya masing-masing?			3			3	Defined process	

		Q55	Apakah ada pengawasan dan pemantauan terhadap sistem untuk mengurangi resiko / insiden penyalahgunaan atau modifikasi tanpa ijin?			3			3	Defined process	
	A.10.5										
	A.10.5.1	Q56	Apakah perangkat lunak / software dilakukan uji secara berkala?			1			1	Initial/Ad Hoc	
		Q57	Apakah setiap data berupa informasi dilakukan back-up guna mencegah terjadinya kehilangan atau kegagalan?			3			3	Defined process	
		Q58	Apakah salinan back-up dan prosedur pemulihan yang terdokumentasi disimpan di lokasi terpisah?			3			3	Defined Process	
		Q59	Apakah media back-up tersebut sudah diuji secara berkala untuk memastikan bisa digunakan pada situasi darurat?			3			3	Defined Process	
	A.10.6										
	A.10.6.1	Q60	Apakah sudah menerapkan kontrol jaringan untuk memastikan keamanan sistem dan data dalam jaringan?			3			3	Defined process	
		Q61	Apakah kontrol tersebut dilakukan secara berkala, guna melindungi hak akses tanpa ijin pada jaringan / serangan?			3			3	Defined Process	
		Q62	Sejauh ini, apakah terdapat titik jaringan yang rawan terhadap serangan?			3			3	Defined Process	
		Q63	Apakah ada petugas atau pegawai yang khusus menangani keamanan jaringan?			3			3	Defined process	

		Q64	Apakah sudah terdapat mekanisme pengamanan jaringan sebagai upaya pencegahan serangan?			3			3	Defined process	
		Q65	Apabila serangan telah terjadi, adakah mekanisme recovery jaringan yang diterapkan?			3			3	Defined process	
5.	A.11										
	A.11.5										
	A.11.5.1	Q66	Apakah sudah di terapkan prosedur log-on pada sistem informasi?			3			3	Defined Process	1,5
		Q67	Apakah sistem sudah membatasi kegagalan percobaan log-on?			1			1	Initial/Ad Hoc	
	A.11.5.2	Q68	Apakah seluruh pengguna (termasuk staf pendukung teknis) memiliki user ID yang berbeda?			3			3	Defined process	
		Q69	Apakah user ID tersebut disyaratkan agar mempunyai ID yang unik seperti menggabungkan huruf dan angka?			1			1	Initial/Ad Hoc	
	A.11.5.3	Q70	Apakah sudah ada sistem manajemen password dan sistem pengelola password untuk memastikan kualitas password?			1			1	Initial/Ad Hoc	
		Q71	Apakah terdapat prosedur batasan jangka waktu pemakaian akun user?			1			1	Initial/Ad Hoc	
	A.11.5.4	Q72	Sudah adakah prosedur penonaktifan akun user (seperti password) guna memastikan tidak adanya pemakaian ulang?			1			1	Initial/Ad Hoc	
	A.11.5.5	Q73	Apakah sudah menggunakan sesi time-out?			1			1	Initial/Ad hoc	

	A.12										
	A.12.2										
	A.12.2.1	Q74	Apakah sudah ada prosedur validasi data ketika akan memasukan data ke sistem informasi Perpustakaan Kota Yogyakarta?				3		3	Defined process	
		Q75	Apakah terdapat prosedur untuk merespon kesalahan validasi?				3		3	Defined process	
	A.12.2.2	Q76	Apakah cek validasi harus disediakan kedalam aplikasi / sistem guna mendeteksi adanya kerusakan (corrupt) informasi dalam kesalahan atau proses pengiriman?				3		3	Defined Process	
		Q77	Ketika ada kerusakan informasi karena ada kesalahan pengolahan apakah dapat terdeteksi oleh sistem?				3		3	Defined Process	
	A.12.2.4	Q78	Untuk memastikan bahwa pemroresan informasi yang disimpan adalah benar, apakah validasi data keluaran penting?				3		3	Defined Process	2,66666667
	A.12.5										
	A.12.5.1	Q79	Apakah sudah ada prosedur mengenai pengendalian perubahan kontrol?				3		3	Defined Process	
		Q80	Apakah pengendalian perubahan kontrol tersebut sudah diimplementasikan?				3		3	Defined Process	
	A.12.5.2	Q81	Bila sistem operasi di ubah, apakah sistem informasi perpustakaan ditinjau dan diuji ulang untuk memastikan tidak ada dampak yang merugikan?				3		3	Defined Process	
6.		Q82	Apakah penting menjaga keamanan sistem informasi perpustakaan ketika				3		3	Defined Process	

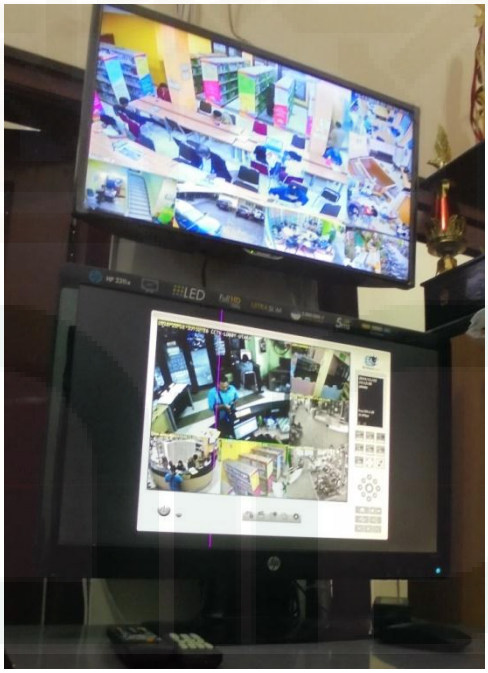
			dilakukan perubahan sistem operasi?								
	A.12.5.3	Q83	Apakah perangkat lunak / software selalu diperbaharui / update?				1		1	Initial/Ad Hoc	
		Q84	Apakah ada jangka waktu perbaharuan terhadap perangkat lunak tersebut?				1		1	Initial/Ad Hoc	
		Q85	Apakah setiap kali melakukan perubahan sudah di kendalikan (untuk memastikan supaya tidak terjadi hal yang tidak diinginkan)?				3		3	Defined Process	
	A.12.5.4	Q86	Apakah sudah dilakukan pencegahan terhadap peluang kebocoran informasi?				3		3	Defined Process	
		Q87	Apakah ada prosedur pencegahannya?				3		3	Defined Process	
		Q88	Apakah sudah dilakukan pantauan terhadap pengembangan perangkat lunak?				2		2	Repeatable But Intuitive	
7.	A.13										
	A.13.1										
	A.13.1.1	Q89	Apakah setiap kejadian keamanan sistem / layanan sudah dilaporkan dengan cepat?					3	3	Defined Process	2,66666667
		Q90	Apakah pelaporan kejadian tersebut sudah sesuai dengan mekasnisme yang ditentukan?					3	3	Defined process	
		Q91	Apakah staf / petugas selalu melaporkan apabila menemukan kelemahan keamanan sistem?					3	3	Defined process	

		Q92	Apakah setiap pelaporan mengenai temuan / dugaan kelemahan keamanan tersebut dicatat?					3	3	Defined Process	
	A.13.2										
	A.13.2.1	Q93	Apakah sudah dibentuk manjemen penanggung jawab dalam penanganan keamanan informasi?					3	3	Defined Process	
		Q94	Apakah sudah ada prosedur untuk penanganan kejadian kemanan informasi tersebut (guna memastikan kecepatan dan keefektivitasan penanganan)?					3	3	Defined Process	
		Q95	Apakah pihak manajemen memberikan respon yang cepat terhadap laporan keamanan sistem informasi?					3	3	Defined Process	
		Q96	Apakah ada petugas yang memonitor terhadap penanganan keamanan informasi (untuk memastikan pennganan tersebut sesuai prosedur)?					3	3	Defined Process	
		Q97	Apakah sudah dilakukan pembaharuan terhadap tata cara (mekanisme) penanganan keamanan informasi?					1	1	Initial/Ad Hoc	
	A.13.2.3	Q98	Apakah perlu adanya tindak lanjut setelah penanganan insiden?					3	3	Defined Process	
		Q99	Apabila terjadi insiden, apakah perlu dikumpulkan bukti - bukti tersebut?					3	3	Defined Process	
		Q100	Apakah bukti- bukti tersebut didokumentasikan dan dilaporkan kepada pihak yang berwajib (untuk dilakukannya tindak lanjut)?					1	1	Initial/Ad Hoc	
Maturity Level											**2,60088036**

LAMPIRAN I

Audit Forensik

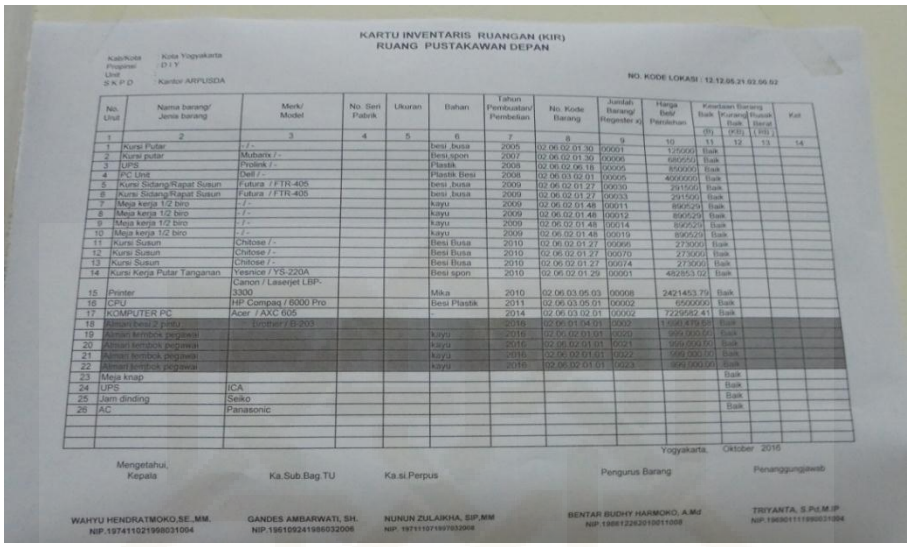
Audit Forensik Klasul Kebijakan Keamanan



Keterangan :

- Kebijakan Keamanan telah didokumentasikan dan dipublikasikan hanya saja belum dikomunikasikan kepada semua pihak terkait.
- Kebijakan Keamanan tersebut telah diterapkan diset di Perpustakaan Kota Yogyakarta.

Audit Forensik Klausul Keamanan Pengelolaan Aset



KARTU INVENTARIS RUANGAN (KIR)
RUANG PUSTAKAWAN DEPAN

Kab/Kota : Kota Yogyakarta
Propinsi : D I Y
Unit : Kantor ARPUSDA
S K P D

NO. KODE LOKASI : 12.12.05.21.02.06.02

No. Urut	Nama barang/ Jenis barang	Merk/ Model	No. Seri Pabrik	Ukuran	Bahan	Tahun Pembuatan/ Pembelian	No. Kode Barang	Jumlah Barang/ Register	Harga Beli/ Perolehan	Keadaan Barang Baik	Kurang Baik (KB)	Rusak Berat (RB)	Ket
1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	Kursi Putar	- / -			besi busa	2005	02.06.02.01.30	00001	125000	Baik			
2	Kursi putar	Mubarix / -			Besi,spon	2007	02.06.02.01.30	00006	585550	Baik			
3	UPS	Prolink / -			Plastik	2008	02.06.02.06.18	00005	850000	Baik			
4	PC Unit	Dell / -			Plastik,Besi	2008	02.06.03.02.01	00005	4000000	Baik			
5	Kursi Sidang/Rapat Susun	Futura / FTR-405			besi busa	2009	02.06.02.01.27	00030	291500	Baik			
6	Kursi Sidang/Rapat Susun	Futura / FTR-405			besi busa	2009	02.06.02.01.27	00033	291500	Baik			
7	Meja kerja 1/2 biro	- / -			kayu	2009	02.06.02.01.48	00011	890529	Baik			
8	Meja kerja 1/2 biro	- / -			kayu	2009	02.06.02.01.48	00012	890529	Baik			
9	Meja kerja 1/2 biro	- / -			kayu	2009	02.06.02.01.48	00014	890529	Baik			
10	Meja kerja 1/2 biro	- / -			kayu	2009	02.06.02.01.48	00019	890529	Baik			
11	Kursi Susun	Chitose / -			Besi Busa	2010	02.06.02.01.27	00066	273000	Baik			
12	Kursi Susun	Chitose / -			Besi Busa	2010	02.06.02.01.27	00070	273000	Baik			
13	Kursi Susun	Chitose / -			Besi Busa	2010	02.06.02.01.27	00074	273000	Baik			
14	Kursi Kerja Putar Tanganan	Yesnice / YS-220A			Besi spon	2010	02.06.02.01.29	00001	482853.02	Baik			
15	Printer	Canon / Laserjet LBP-3300			Mika	2010	02.06.03.05.03	00008	2421453.79	Baik			
16	CPU	HP Compaq / 6000 Pro			Besi Plastik	2011	02.06.03.05.01	00002	6500000	Baik			
17	KOMPUTER PC	Acer / AXC 605				2014	02.06.03.02.01	00002	7229582.41	Baik			
18	Almari besi 2 pintu	brother / B-203				2016	02.06.01.04.01	0002	1.690.479.68	Baik			
19	Almari lembok pegawai				kayu	2016	02.06.02.01.01	0020	999.000.00	Baik			
20	Almari lembok pegawai				kayu	2016	02.06.02.01.01	0021	999.000.00	Baik			
21	Almari lembok pegawai				kayu	2016	02.06.02.01.01	0022	999.000.00	Baik			
22	Almari lembok pegawai				kayu	2016	02.06.02.01.01	0023	999.000.00	Baik			
23	Meja knap									Baik			
24	UPS	ICA								Baik			
25	Jam dinding	Seiko								Baik			
26	AC	Panasonic								Baik			

Yogyakarta, Oktober 2016

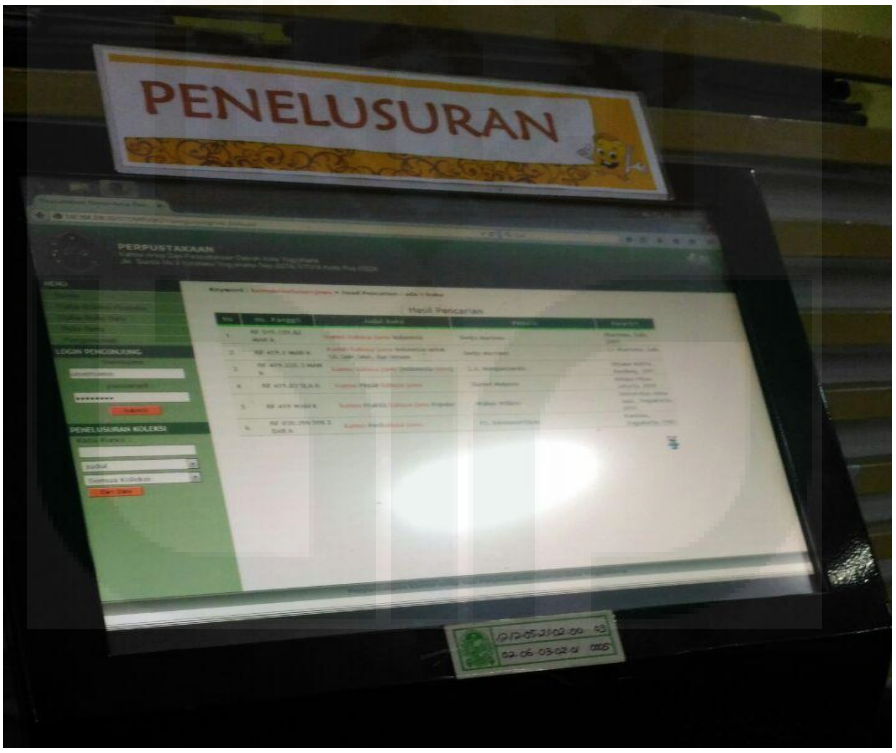
Mengetahui, Kepala — WAHYU HENDRATMOKO,SE.,MM. NIP.197411021998031004

Ka.Sub.Bag.TU — GANDES AMBARWATI, SH. NIP.196109241986032006

Ka.si.Perpus — NUNUN ZULAIKHA, SIP,MM NIP. 197111071997032008

Pengurus Barang — BENTAR BUDHY HARMOKO, A.Md NIP.198612202010011008

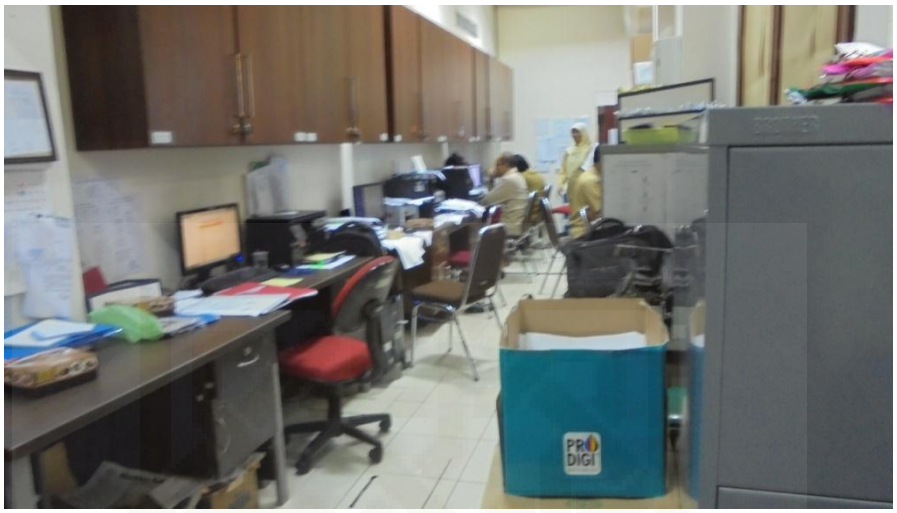
Penanggungjawab — TRIYANTA, S.Pd.M.IP NIP.196901111990031004

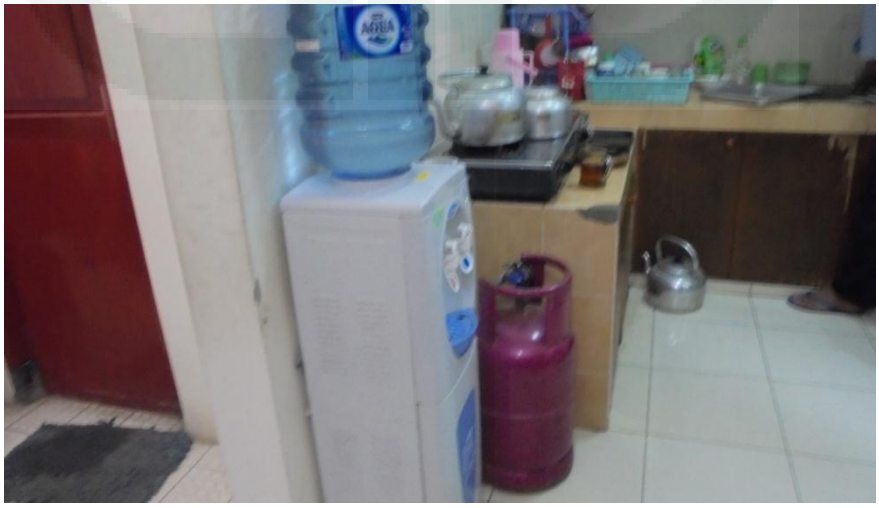


Keterangan :

- Pengelolaan Aset seperti inventaris aset sudah diterapkan di Perpustakaan Kota Yogyakarta.
- Pelabelan dan pemberian tanda terhadap aset sudah diterapkan.

Audit Forensik Klausul Keamanan Fisik dan Lingkungan

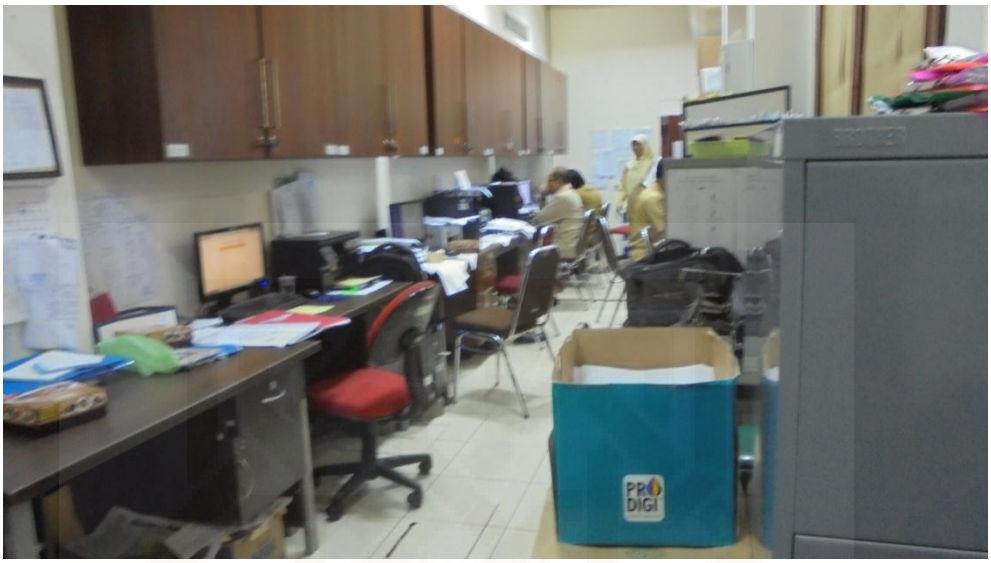




Keterangan :

- Pintu masuk ruang Sistem Informasi belum dilengkapi dengan pengamanan menggunakan Kartu Kontrol maupun PIN, hanya saja terdapat lebel peringatan pada pintu masuk ruang kontrol sistem yang berisi himbauan hanya pegawai perpustakaan yang dapat memasuki ruang Sistem Informasi.
- Gas / Bahan lainnya yang bersifat mudah meledak telah ditempatkan didapur, akan tetapi masih terlalu dekat dengan ruang kontrol yang ada.
- Tata letak alat pemadam api ringan (APAR) telah ditempatkan pada posisi semestinya dan tidak jauh dari switch kontrol pelistrikan.

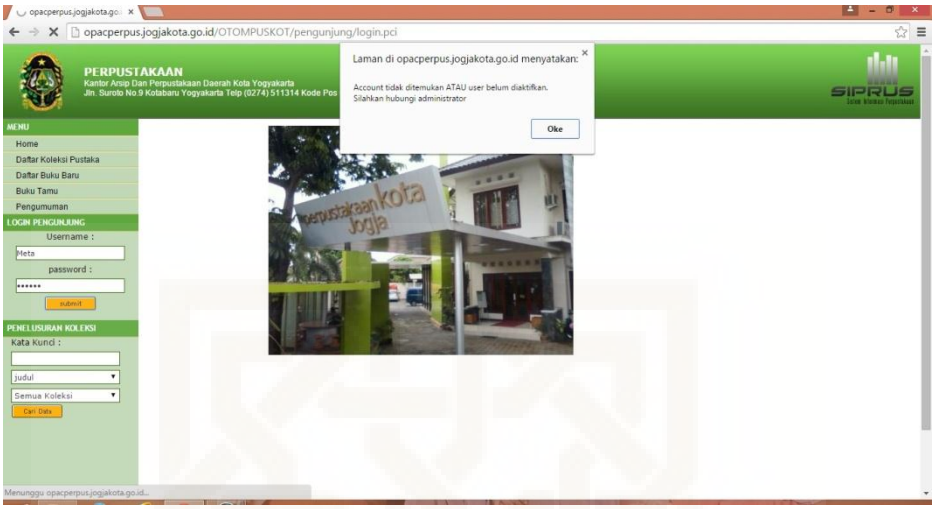
Audit Forensik Klausul Manajemen Komunikasi dan Operasi



Keterangan :

- Proses Manajemen Komunikasi dan Operasi telah dilakukan oleh pihak Perpustakaan Kota Yogykarta secara rutin dan berkala sesuai prosedur dan standarisasi, salah satunya adalah back-up data, manajemen jaringan dan server.

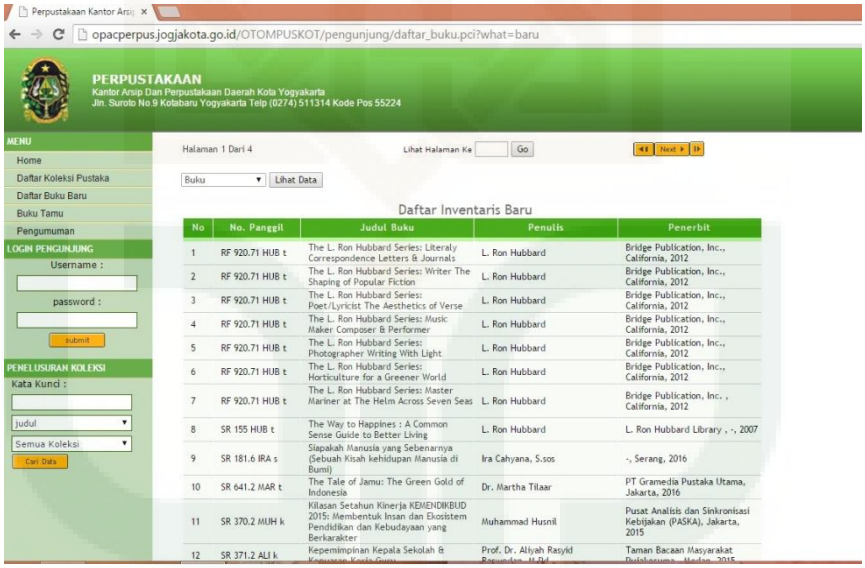
Audit Forensik Klausul Pengendalian Akses



Keterangan :

- Perpustakaan Kota Yogyakarta telah menerapkan pesan error jika ada kesalahan saat memasukkan password dan username.
- Belum membatasi jumlah kegagalan percobaan log-on. Jika terjadi kesalahan dalam memasukkan password sebanyak 3 kali akun tetap aktif.
- Sistem belum dilengkapi dengan manajemen password untuk mengganti password yang lama atau karena lupa password.

Audit Forensik Klausul Akuisisi, Pengembangan, dan Pemeliharaan Sistem Informasi

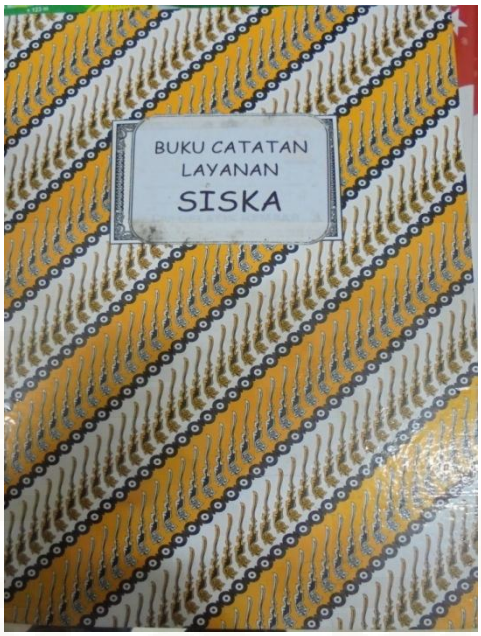


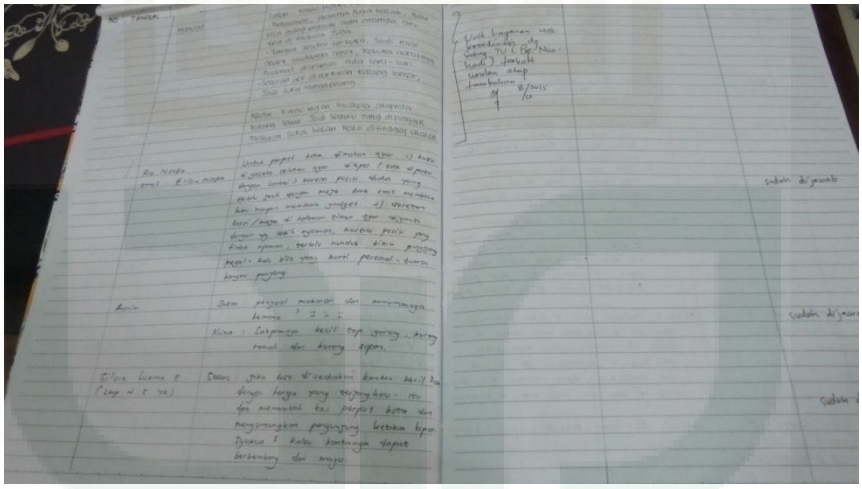
Keterangan :

- Perpustakaan Kota Yogyakarta telah melakukan akuisisi, salah satunya ialah dimana sistem telah menyediakan link yang langsung terhubung ke web yang lain yaitu opacperpus.jogjakota.go.id

- Akuisisi data juga terdapat pada sistem perpustakaan, yaitu data inventaris buku, jurnal / artikel terbaru yang diinputkan ke dalam sistem berdasarkan Judul, Penulis dan Penerbit.
- Pemeliharaan sistem dilakukan oleh Perpustakaan Kota Yogyakarta dilihat dari adanya Login Pengunjung bagi pemustaka untuk membatasi penggunaan hak akses bagi pihak yang tidak berwenang.
- Adanya pemberikan kode verifikasi bagi pemustaka yang akan memberikan saran maupun kritik.

Audit Forensik Klausul Manajemen Kejadian Keamanan Informasi





Keterangan :

- Setiap ada kejadian mengenai keamanan sistem selalu di laporkan dengan cepat dan dicatat dalam buku Sistem Informasi Perpustakaan (SISKA) untuk selanjutnya ditindak lanjuti.

- Setiap hari senin, Perpustakaan Kota Yogyakarta selalu merapatkan mengenai kejadian – kejadian yang tercatat dalam buku Sistem Informasi Perpustakaan (SISKA). Perpustakaan Kota Yogyakarta selalu mengedepankan dan mengutamakan Pelayanan demi kepuasan para pengunjung / pemustaka.

CURRICULUM VITAE

Nama	:	Lusi Anggarini
Tempat, tanggal lahir	:	Bantul, 29 September 1992
Jenis Kelamin	:	Perempuan
Alamat	:	Jl Delima Utara IV / 26 , RT 002 /RW 001, Kramat Utara, Magelang Utara, Magelang
No. Handphone	:	0857-9937-0133
Email/Facebook	:	lusiananda347@gmail.com /Lusi Anggarini

Riwayat Pendidikan formal :

- 1998-2004 : SD Negeri Wanajaya III, Garut
- 2004-2007 : SMP Negeri 1 Wanaraja, Garut
- 2008-2011 : SMK Negeri 4 Garut
- 2012-2016 : S1 Teknik Informatika UIN Suka Yogyakarta

Riwayat Pendidikan Non Formal :

- Oracle