AUDIT SISTEM INFORMASI BARANG SITAAN DI RUMAH PENYIMPANAN BENDA SITAAN MILIK NEGARA (RUPBASAN) BANTUL MENGGUNAKAN STANDAR SNI-ISO 27001

Skripsi

Untuk Memenuhi Sebagian Persyaratan

Mencapai Derajat Sarjana S-1

Program Studi Teknik Informatika

Disusun Oleh :

Eri Kurniawan

12651087

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 : UIN.02/D.ST/PP.01.1/3117/2016

Skripsi/Tugas Akhir dengan judul : Audit Sistem Informasi Barang Sitaan di Rumah Penyimpanan Benda Sitaan Milik Negara (RUPBASAN)) Bantul Menggunakan Standar SNI-ISO 27001

Yang dipersiapkan dan disusun oleh :
Nama : Eri Kurniawan
NIM : 12651087
Telah dimunaqasyahkan pada : Selasa, 30 Agustus 2016
Nilai Munaqasyah : A / B
Dan dinyatakan telah diterima oleh Fakultas Sains dan Teknologi UIN Sunan Kalijaga

TIM MUNAQASYAH :

Ketua Sidang

Agus Mulyanto, M.Kom
NIP. 19710823 199903 1 003

Penguji I

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

Penguji II

Aulia Faqih R, M.Kom
NIP. 19860306 201101 1 009

Yogyakarta, 5 September 2016
UIN Sunan Kalijaga
Fakultas Sains dan Teknologi
Dekan

KEMENTERIAN AGAMA UIN SUNAN KALIJAGA YOGYAKARTA

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

Universitas Islam Negeri Sunan Kalijaga

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 etunjuk dan mengoreksi serta mengadakan perbaikan seperlunya, maka kami selaku pembimbing berpendapat bahwa skripsi Saudara :

Nama : Eri Kurniawan

NIM : 12651087

Judul Skripsi : Audit Sistem Informasi Barang Sitaan di Rumah Penyimpanan Benda Sitaan Milik Negara (Rupbasan) Bantul Menggunakan Standart ISO 27001

sudah dapat diajukan 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 diatas dapat segera dimunaqosahkan. Atas perhatiannya kami ucapkan terimakasih.

Wassalamu'alaikum wr. Wb.

Yogyakarta, 24 Agustus 2016

Pembimbing

Agus Mulyanto, S.Si. M.Kom

NIP. 19710823 199903 1 003

Pernyataan Keaslian Skripsi

Yang bertanda tangan dibawah ini :

Nama	:	Eri Kurniawan
Nim	:	12651087
Program Studi	:	Teknik Informatika
Fakultas	:	Sains dan Teknologi

Menyatakan bahwa skripsi dengan judul Audit Sistem Informasi Barang Sitaan di Rumah Penyimpanan Benda Sitaan Milik Negara (RUPBASAN BANTUL) Menggunakan Standar ISO 27001 tidak terdapat pada karya yang pernah diajukan untuk memperoleh gelar sarjana di suatu perguruan tinggi, dan sepengetahuan saya tidak terdapat pada karya atau pendapat yang pernah ditulis oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Yogyakarta, 24 Agustus 2016

Yang Menyatakan

Eri Kurniawan

NIM : 12651087

KATA PENGANTAR

Segala puji bagi Allah SWT tuhan semesta alam yang selalu memberikan rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan skripsi dengan judul "Audit Sistem Informasi Barang Sitaan di Rumah Penyimpanan Benda Sitaan Milik Negara (RUPBASAN BANTUL) Menggunakan Standar ISO 27001". Tak lupa pula penulis haturkan shalawat serta salam kepada Nabi junjungan kita Nabi akhir zaman Nabi Muhammad SAW beserta seluruh keluarga dan sahabat yang telah berjuang dan mengorbankan jiwa raganya demi berdiri tegak dan kokohnya agama islam di muka 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 Sumarsono, M.Kom, selaku Ketua Program Studi Teknik Informatika UIN Sunan Kalijaga Yogyakarta.
4. Bapak Agus Mulyanto, M.Kom, selaku Dosen Pembimbing akademik sekaligus Dosen Pembimbing skripsi yang telah mengayomi dan mengarahkan dengan segala kesabarannya.

5. Seluruh Dosen Program Studi Teknik Informatika yang telah memberi bekal ilmu pengetahuan kepada penulis, semoga ilmunya menjadi amal jariyah.
6. Kepala Rupbasan Bantul Dra. Mei Kartini dan seluruh pegawai Rupbasan Bantul yang telah memberikan izin tempat utuk penelitian.
7. Bapakku Supangat dan Ibuku Suparmi tercinta, serta seluruh anggota keluarga tersayang atas doa, perhatian dan dukungan moril terhadap saya
8. Teman-teman Program Studi Teknik Informatika, khususnya angkatan 2012 Mandiri Kelas K (Katak12) yang telah banyak memberi dukungan.
9. Teman-teman Garda Depan Angkatan 56 Pt. Aseli Dagadu Djokdja yang telah memberikan semangat dan dukungan.
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.
11. 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. Terimakasih

Yogyakarta, 24 Agustus 2016

Eri Kurniawan

12651087

HALAMAN PERSEMBAHAN

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

- Bapakku Supangat yang telah berjuang sejauh ini buatku, ibuku Suparmi 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 Bapak dan Ibu panjang umur dan bisa melihatku menjadi anak yang membanggakan keluarga suatu hari nanti, amin.
- Dosen dan keluarga besar Teknik Informatika, Pak Sumarsono ketua program studi yang selalu sedia dan terbuka menerima keluh kesah para mahasiswanya, Pak Agus Mulyanto yang selalu mengarahkan dan selalu peduli kepada anak bimbingnya, Ibu Ade yang selalu hadir dengan pertanyaan–pertanyaan kritisnya, Pak Mustakim yang selalu bijak mengkaitkan teori di mata kuliah dengan kehidupan sehari-hari, Pak Agung, Ibu Uyun, Pak Bambang, Pak Rahmat, Pak Didik dan Pak Aulia yang selalu sabar memberikan ilmu-ilmunya, semoga Bapak dan Ibu dosen panjang umur dan selalu bahagia sampai tua kelak, amin.
- Teman–teman seperjuangan dan keluarga besar Teknik Informatika Mandiri/Khusus 2012 (Katak012) Lusi, Juhdan, Indah, Rizky, Nuge, Mursyd, Fajar, Rohman, Choirudin, Deviyanto, Krisna, Bintang, Malika, Maya, Iza, Edi, Bayu, Mandrok, Gumeta, Ripa, Kukuh, Afin, Berlin, Nanang, Deviyanto, Valdi, Kharizma, Erin, Novie, Zuni, Andi, Wiji, Gustav, Taufik,

Edita, Dana, Iwan, Asep, Ainul, Irham, Ulfa, Edigun, Agni, Indra, Kiki, Ikhzan, Surahmat dan Abdul, terimakasih buat kebersamaan kalian.

- Teman-teman Garda Depan Angkatan 56 Pt. Aseli Dagadu Djokdja Agnes, Ahmad, Ama, Andung, Ardan, Ardian, Badar, Bilqis, Citra, danang, Defa, Diana, Diani, Dini, Dita, Dono, Dyno, Fatah, Fendi, Fika, Habib, Hayu, Hegar, Hendra, Ita, Keken, Kezia, Kharis, Krisna, Made, Mala, Nadia, Nanda, Nia, Nisa, Pangger, Pina, Ria, Rika, Risang, Sendy, Setya, Subchan, Susan, Tami, Tria, dan Uswah atas semangat dan dukungan.
- Pihak-pihak yang selalu memberikan bantuannya, semangat, dan doanya baik secara langsung maupun tidak, yang tidak dapat saya sebutkan namanya satu per satu.

MOTTO

“ Tidak bertindak karena menunggu hilangnya rasa malas,adalah bentuk kemalasan yang lebih parah lagi”

“ Bukan kurangnya bakat atau tidak adanya modal yang menghalangi kita dari sukses,tapi tidak cukupnya keberanian ”

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

DAFTAR SINGKATAN

SNI	:	Standar Nasional Indonesia
ISO	:	International Organization for Standardization
IEC	:	International Electrotechnical Commission
UPT	:	Unit Pelaksana Teknis
TI	:	Teknologi Informasi
SI	:	Sistem Informasi
SMKI	:	Sistem Manajemen Keamanan Informasi
CMMI	:	Capability Maturity Model for Integration
CIO	:	Chief Information Officer
FQ	:	Form Question
Basan	:	Barang Rampasan
Baran	:	Barang Sitaan
HDD	:	Hard Disk Drive
ID	:	Identity

AUDIT SISTEM INFORMASI BARANG SITAAN DI RUMAH PENYIMPANAN BENDA SITAAN MILIK NEGARA (RUPBASAN BANTUL) MENGGUNAKANSTANDAR SNI-ISO 27001

Eri Kurniawan
12651087

INTISARI

RUPBASAN atau Rumah Penyimpanan Barang Sitaan Negara adalah tempat dimana benda yang di sita oleh Negara untuk keperluan proses peradilan. Di dalam Rupbasan di tempatkan benda-benda yang harus disimpan untuk keperluan barang bukti dalam pemeriksaan penyidikan, penuntutan dan pemeriksaan di siding pengadilan termasuk barang yang dinyatakan di rampas berdasarkan putusan hakim. Rupbasan bertujuan dilaksanakannya pengelolaan, penyimpanan, pengamanan dan perawatan Basan dan Baran sesuai dengan ketentuan yang berlaku. Rupbasan sebagai sebuah sumber dan pusat layanan informasi dalam pengelolaan, penyimpanan , pengamanan dan perawatan Basan dan Baran, untuk membuktikan tingkat keamanan terhadap pengelolaan Sistem Informasi yang diterapkan maka perlu dilakukan proses audit.

Penelitian ini menggunakan kerangka kerja tata kelola TI SNI-ISO 27001 yang telah distandarkan oleh pemerintah indonesia. Kerangka kerja tata kelola TI SNI-ISO 27001 digunakan sebagai panduan dan pedoman untuk mengukur tingkat manajemen keamanan Sistem Informasi yang diterapkan oleh sebuah perusahaan atau organisasi. Penelitian ini menggunakan enam proses klausul dari 11 klausul yang terdapat pada SNI-ISO 27001 yaitu, Klausul Kebijakan Keamanan (A5), Klausul Pengelolaan Aset (A7), Klausul Keamanan Fisik dan Lingkungan (A9), Klausul Keamanan Sistem Operasi (A10), Klasul Pengendalian akses (A11), dan Klasul Akuisisi Pengembangan dan Pemeliharaan Sistem Informasi. Analisa data pada penelitian ini mengacu pada maturity model.

Hasil Audit Keamanan Sistem Informasi berada pada tingkat keamanan dengan skala kematangan 1.53 (Repeatable but Intuitive). Hal ini menunjukan bahwa pengelolaan keamanan telah diterapkan tetapi prosedur pengelolaan belum didokumentasikan. Rupbasan belum mengadakan pelatihan secara formal sehingga kurangnya pemahaman terhadap pentingnya pengelolaan, namun pengelola sudah memiliki inisiatif untuk melakukan perawatan dan pengendalian terhadap perubahan yang mempengaruhi sistem.

Kata Kunci : Sistem Informasi Barang Sitaan, Audit Sistem Informasi, SNI-ISO 27001.

AUDIT OF CONSFICATED OBJECT INFORMATION SYSTEMSAT STORAGE OF CONSFICATED OBJECT BELONGING TO THE STATE (RUPBASAN BANTUL) USINGSTANDARD IEC-ISO 27001

Eri Kurniawan
12651087

ABSTRACT

RUPBASAN or Storage Confiscated Object Belonging to the State is a place where objects confiscated by the State for the purposes of judicial proceedings. Rupbasan is a place where objects for the purposes of the examination of evidence in an investigation, prosecution and examination before the court including looted goods declared by the judge's decision should be kept. Rupbasan has the purpose of implementation of the management, storage, security and maintenance Bashan and Baran in accordance with applicable regulations. Rupbasan as a resource and information center in the management, storage, security and maintenance Basan and Baran, to prove the security level of the management information system that is applied it is necessary to audit the process.

This study uses an IT governance framework SNI-ISO 27001 that has been standardized by the Indonesian government. IT governance framework SNI-ISO 27001 is used as a guideline and guidance to measure the level of security management of Information Systems applied by a company or organization. This study uses 6 process clauses of 11 clauses contained in SNI ISO 27001, namely, Clause of Security Policy (A5), Clause of Asset Management (A7), Clause of Physical and Environment Security (A9), Clause of Operating System Security (A10), Clause of access control (A11), and Clause of the acquisition of Information Systems Development and Maintenance. Data analysis in this study refers to the maturity models.

The audit results of Information system security are at the level of security with a maturity level of 1:53 (Repeatable but Intuitive). This shows that the security management has been implemented but not yet documented in management procedures. Rupbasan has not held formal training so there is a lack of understanding on the importance of management, but the manager has had the initiative to perform maintenance and control of changes that affect the system.

Keywords: Confiscated Object Information Systems, Information Systems Auditing, SNI ISO 27001.

BAB 1

PENDAHULUAN

1.1 **Latar Belakang**

Pemanfaatann teknologi informasi saat ini sudah tidak asing lagi dalam kehidupan kita. Mulai dari sekolah, universitas bahkan instansi pemerintah dan perusahaan sudah memanfaatkan teknologi informasi untuk membantu mempercepat proses bisnisnya.Salah satu instansi yang memerlukan pemanfaatan system informasi adalah Rupbasan Kelas II Bantul (Rumah Penyimpanan Barang Sitaan Milik Negara). System informasi Rupbasan merupakan salah satu bentuk pemanfaatan teknologi informasi yang berupa layanan perangkat lunak dengan tujuan mempermudah mengelola semua data yang ada pada Rupbasan Kelas II Bantul seperti data barang sitaan yang disita, data penyimpanan barang sitaan dan lain sebagainya. Dengan demikian proses-proses di di dalamnya akan lebih cepat dan lebih mudah dipantau.

Untuk mendapatkan sebuah layanan system informasi yang baik maka perlu adanya tata kelola system informasi yang baik pula, termasuk didalamnya tata kelola keamanan dari system informasi tersebut. Salah satu metode pengelolaan system informasi yang sering digunakan adalah ISO 27001 (International Standart Organisation 27001). ISO 27001 merupakan dokumen standar system manajemen keamanan informasi (SMKI) atau Informtion Security Management System (ISMS) yang memberikan gambaran secara umum mengenai apa saja yang seharusnya dilakukan dalam usaha pengimplementasian konsep-konsep keamanan informasi di dalam sebuah perusahaan

Kemajuan tekhnologi informasi telah memberikan banyak kontribusi dan dampak yang besar terhadap perkembangan suatu organisasi khususnya Rupbasan Bantul yang memiliki tugas untuk melakukan pemeliharaan, pengembangan dan pengelolaan sistem informasi. Dalam hal ini berkaitan langsung dengan fungsi manajemen pemegang kendali tata kelola sistem informasi yang melakukan pengendalian (controlling) untuk mengurangi resiko kerugian, penyimpangan serta kerusakan sebuah sistem informasi terhadap usaha atau tindakan yang merugikan organisasi baik tindakan atau usaha dari luar maupun dari dalam manajemen tata kelola sistem informasi itu sendiri.

Alasam mengapa penulis memilih stadar ISO dibandingkan Coso atau COBIT adalah kareana COBIT memiliki tujuan melakukan riset dan mempunlikasikan suatu standar teknologi informasi yang di terima umun dan selalu *up to date* untuk digunakan dalam kegiatan bisnis sehari-hari. Sedangkan COSO memiliki tujuan sebuah proses yang dipengaruhi oelh dewan komisaris, manajemen dan pegawai perusahaan lainnya yang dibentuk untuk menyediakan keyakinan yang memadai atau wajar berkaitan dengan pencapaian tujuan dalam kategori sebagai berikut : efiktifitas dan efisieni aktivitas operasi, kehamdalan pelaporan keuangan, ketaatan terhadap hokum dan peraturan yang berlaku, dan pengamayan asset entitas. COBIT dan COSO sama sama mendefinisak pengendalian yaitu kebijakan, prosedur, praktik, dan struktur organisasi yang dirancang untuk memberikan hal-hal yang tidak diinginkan dapat dicegah atau dideteksi dan diperbaiki. Sedangkan objek yang diteliti di Rupbasan Bantul bukanlah dari segi organisasi atau struktur organisasinya, jadi penulis lebih memilih menggunakan standar ISO 27001 yang memiliki klausul Kebijakan Keamanan (A.5), Pengelolaan Aset (A.7), Keamanan Fisik dan Lingkungan (A.9),

Manajemen Komunikasi dan Operasi (A.10), Pengendalian Akses (A.11), Akuisisi, Pengembangan, dan Pemeliharaan Sistem Informasi (A.12) yang dirasa penulis lebih cocok.

Disamping itu penerapan tata kelola tekhnologi informasi yang sesuai dengan prosedur sudah menjadi kebutuhan dan tuntutan di setiap instansi penyelenggara pelayanan publik. Hal yang paling mendasar adalah apabila layanan Sistem Informasi Barang Sitaan di Rupbasan memiliki prosedur dan tata kelola keamanan informasi dan data yang baik maka sangat mendukung tercapainya pelayanan online yang baik, untuk menjamin pengelolaan keamanan informasi yang tidak mengandung error karena kesalahan atau penyalahgunaan, maka dapat dicapai melalui pembenahan aspek manajemen yang dilengkapi dengan mekanisme kontrol internal, hal tersebut disebabkan karena secanggih apapun produk teknologi keamanan informasi yang dipakai tanpa dilengkapi dengan mekanisme kontrol internal maka sistem informasi tersebut akan mudah dibobol dan dirusak, maka secara periodik diperlukan adanya pemeriksaan atau audit sistem.

Mengingat kinerja layanan sistem informasi tata kelola TI akan terganggu jika sistem informasi sebagai salah satu objek utama tata kelola TI mengalami masalah keamanan informasi. Sangat penting disini untuk mengetahui bagaimana kebijakan keamanan informasi yang diterapkan oleh pengelola sistem informasi Barang Sitaan, seperti apa bentuk pengelolaan aset, keamanan fisik dan lingkungannya apakah sudah dikendalikan, bagaimana bentuk manajemen jaringan yang diterapkan, bagaimana pengendalian akses sistem operasi dan apakah sudah diterapkan akuisisi, pengembangan dan pemeliharaan sistem informasi.

Oleh karena itu dalam hal ini audit keamanan sistem informasi pada Sistem Informasi Barang Sitaan di Rupbasan Bantul perlu dilakukan untuk memastikan apakah

proses pengawasan dan pengelolaan keamanan sistem informasi sudah diterapkan sesuai prosedur dan standart yang telah ditetapkan.

1.2 **Rumusan Masalah**

Berdasarkan latar belakang yang telah diuraikan diatas, dapat diambil perumusan masalah sebagai berikut :

1. Bagaimana merencanakan audit keamanan pada sistem informasi barang sitaan di Rupbasan Bantul menggunakan Standar SNI-ISO 27001 ?
2. Bagaimana melaksanakan audit keamanan sistem informasi Barang Sitaan di Rupbasan Bantul menggunakan Standar SNI-ISO 27001 ?
3. Bagaimana mengetahui tingkat keamanan sistem informasi Barang Sitaan di Rupbasan menggunakan Standar SNI-ISO 27001 ?
4. Bagaimana memberikan penilaian tata kelola keamanan sistem dan rekomendasi hasil audit keamanan sistem informasi Barang Sitaan di Rupbasan menggunakan Standar SNI-ISO 27001 ?

1.3 **Batasan Masalah**

1. Penelitian ini dilakukan di RUPBASAN Bantul (Rumah Penyimpanan Benda Sitaan Negara) dan objek yang diteliti adalah sistem informasi Barang Sitaan
2. Penelitian ini menggunakan Standar SNI-ISO 27001.
3. Ruang lingkup dari penelitian ini adalah berfokus pada klausul Kebijakan Keamanan (A.5), Pengelolaan Aset (A.7), Keamanan Fisik dan Lingkungan (A.9), Manajemen Komunikasi dan Operasi (A.10), Pengendalian Akses (A.11), Akuisisi pengembangan dan pemeliharaan Sistem Informasi (A.12).

4. Analisis yang digunakan adalah metode penilaian (scoring) dengan pendekatan yang diambil berdasarkan maturity model yang memiliki 6 skala kematangan yakni skala 0- Non-Existent, 1- Initial, 2- Reapetable, 3- Defined, 4- Managed, dan 5- Optimised.
5. Output yang dihasilkan berupa laporan hasil temuan dan rekomendasi berdasarkan hasil audit yang telah dilakukan.

1.4 **Tujuan Penelitian**

Tujuan penelitian yang dilakukan pada sistem informasi adalah sebagai berikut :

1. Membuat perencanaan audit keamanaan sistem informasi di Rupbasan Bantul dari dokumen wawancara dan lembar kerja yang merupakan hasil dari pengumpulan data.
2. Melaksanakan audit keamanan sistem informasi barang sitaan di Rupbasan Bantul dengan menggunakan Standar SNI-ISO 27001.
3. Mengetahui tingkat keamanan sistem informasi di Rupbasan Bantul menggunakan Standar SNI-ISO 27001.
4. Membuat rekomendasi berdasarkan hasil audit keamanan sistem informasi Rupbasan Bantul untuk evaluasi sistem.

1.5 **Manfaat Penelitian**

1. Memberikan masukan terhadap staf maupun pemegang kendali sistem informasi di Rupbasan terhadap pentingnya keamanan sistem informasi serta dapat membantu manajemen tata kelola keamanan informasi untuk melakukan pengelolaan sesuai standart tata kelola TI.

2. Sebagai dasar acuan pengembangan sistem informasi dan pelayanan apa yang perlu dilakukan untuk meningkatkan kinerja dari sistem informasi di Rupbasan Bantul.

3. Menambah literatur dan memberikan sumbangan berupa pengembangan ilmu yang berkaitan dengan audit keamanan sistem informasi menggunakan Standar SNI-ISO 27001.

1.6 **Keaslian Penelitian**

Penelitian tentang audit sudah banyak dilakukan sebelumnya, namun pada objek yang berbeda, dan menggunakan standar atau metode yang berbeda. Sedangkan penelitian yang membahas tentang Audit Keamanan Sistem Informasi studi kasus pada Sitem Informasi Baran di Rupbasan Bantul Menggunakan Standart SNI-ISO 27001 sepengetahuan peneliti belum pernah dilakukan sebelumnya.

BAB VI

KESIMPULAN DAN SARAN

6.1 **Kesimpulan**

Berdasarkan penelitian yang telah dilakukan dari perencanaan hingga didapatkannya hasil penelitian, maka kesimpulan yang dapat peneliti hasilkan dari proses audit Sistem Informasi adalah :

1. Peneliti berhasil melakukan perencanaan Audit terhadap pengelolaan Sistem Informasi Barang Sitaan di Rupbasan Bantul dengan menggunakan standar SNI-ISO 27001.
2. Peneliti telah berhasil melaksanakan proses Audit Keamanan Sistem Informasi Barang Sitaan yang mengambil studi kasus di Rupbasan Bantul dengan menggunakan standart SNI-ISO 27001 yang menghasilkan data penelitian berupa hasil interview terhadap bentuk pengelolaan Sistem Informasi Barang Sitaan Rupbasan Bantul.
3. Hasil analisa kematangan menggunakan maturity level menunjukan bahwa tingkat keamanan Sistem Informasi berada pada level Repeatable but Intuitive yaitu sebesar 1.53 berarti belum mencapai dari batas minimal dari Peraturan Menteri BUMN Nomor:PER-02/MBU/2013 yang menyatakan target maturity level dari tata kelola TI BUMN menyatakan target minimum adalah level 3. Kemudian berdasarkan hasil rata-rata kematangan dari setiap klausul dengan nilai maturity yang didapatkan artinya proses pengelolaan sistem informasi masih sebatas mengikuti pola yang teratur dimana prosedur serupa diikuti oleh pegawai/pengelola lainnya tanpa ada pelatihan formal sebelumnya dan tidak ada standart prosedur yang digunakan sebagai

4. acuan dan tanggung jawab sepenuhnya dilimpahkan kepada masing-masing individu dan kesalahan sangat mungkin terjadi.
5. Rekomendasi audit pada Sistem Informasi berhasil disusun dan diberikan pada setiap klausul berdasarkan analisa hasil audit untuk memperbaiki sistem pengelolaan yang diterapkan.

6.2 **Saran**

Dari keseluruhan penelitian yang telah dilakukan tentunya tidak terlepas dari kekurangan dan kelemahan yang harus diperbaiki dan ditingkatkan. Oleh karena itu untuk penelitian lebih lanjut peneliti menyarankan beberapa hal sebagai berikut :

1. Organisasi perlu memperbaiki dan mengevalasi tata kelola TI baik dari segi kebijakan keamanan, pengelolaan asset, keamanan fisik dan lingkungan, manajemen komunikasi dan operasi, pengendalian akses, akuisisi pengembangan dan pemeliharaan sistem informasi serta melengkapi dokumen SOP terkait dengan keamanan informasi.
2. Hendaknya dilakukan audit internal menggunakan standar SNI-ISO 27001 secara rutin oleh pengelola agar mengetahui berapa tingkat keamanan sistem informasi serta dapat memberikan pengaruh yang signifikan atas keberlangsungan pelayanan.
3. Perlunya penerapan manajemen keamanan sistem informasi berdasarkan standart SNI-ISO 27001 secara bertahap dan berkala pada Rupbasan khususnya pada Sistem Informasi Barang sitaan karena keamanan infromasi yang baik hanya dapat dicapai melalui pembenahan pada aspek manajemennya.
4. Untuk penelitian lebih lanjut tentang Sistem Informasi Barang Sitaan di Rupbasan Bantul sebaiknya menggunakan lebih banyak klausul yang ada pada ISO 27001

karena dapat memperoleh nilai kematangan dalam proses pengelolaan Sistem Informasi yang semakin akurat.

DAFTAR PUSTAKA

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

Herry. 2013. Auditing. CAPS (Center of Academic Publising Service) : Yogyakarta.

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

Komalasari, Rizky dan Perdana, Ilham. 2014. "Audit Keamanan Informasi Bagian Teknologi Informasi PT PLN (Persero) DJBB Menggunakan SNI ISO/IEC 27001: 2009. Bandung

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

Kusuma, Riawan Abi. 2014. "Audit Keamanan Sistem Informasi Berdasarkan Standar SNI-ISO 27001 Pada Sistem Informasi Akademik UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA". Yogyakarta.

Laudon, Kenneth C. & Laudon, Jane P. 2008. Management Information System. Salemba Empat : Yogyakarta

Rahayu, Siti Kurnia dan Suhayati, Ely. 2010. Auditing : Konsep Dasar dan Pedoman Pemeriksaan Akuntan Publik. Graha Ilmu : Yogyakarta

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

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

Sudrajat, Handoyo. (2013). Pedoman Mutasi Basan dan Baran. Jakarta

Sudrajat, Handoyo. (2014). Standart Pengeluaran dan Pengembalian Basan dan Baran di Rupbasan. Jakarta

Winaro, Wing Wahyu. 2004. Sistem Informasi Manajemen. UPP (Unit penerbit dan percetakan) STIM YKPN : Yogyakarta

Lampiran 1 : Sasaran pengendalian SNI-ISO 27001

KLAUSUL	SASARAN PENGENDALIAN DALAM SNI ISO 27001
SNI – ISO 27001 A.5.1 Kebijakan Keamanan Informasi	Memberikan arahan dan dukungan untuk keamanan informasi menurut persyaratan bisnis dan hukum beserta regulasi yang relevan.
SNI – ISO 27001 A.6.1 Organisasi Keamanan Informasi (Internal)	Mengelola keamanan informasi dalam organisasi
SNI – ISO 27001 A.6.2 Organisasi Keamanan Informasi (Pihak Eksternal)	Memelihara keamanan informasi organisasi dan fasilitas pengolahan informasi yang di akses, diolah dikomunikasikan kepada atau dikelola pihak eksternal
SNI – ISO 27001 A.7.1 Pengelolaan Aset (Tanggung Jawab Ter hadap Aset)	Mencapai dan memelihara perlindungan yang sesuai terhadap aset organisasi.
SNI – ISO 27001 A.7.2 Pengelolaan Aset (Klasifikasi Informasi)	Memastikan bahwa informasi menerima tingkat perlindungan yang tepat.
SNI – ISO 27001 A.8.1 Keamanan Sumber Daya Manusia (Sebelum Dipekerjakan)	Memastikan bahwa pegawai, kontraktor dan pengguna pihak ketiga memahami tanggung jawab sesuai dengan perannya, dan untuk mengurangi resiko pencurian, kecurangan atau penyalahgunaan fasilitas
SNI – ISO 27001 A.8.2 Keamanan Sumber Daya Manusia (Selama bekerja)	Memastikan bahwa semua pegawai, kontraktor dan pengguna pihak ketiga telah peduli terhadap ancaman dan masalah keamanan informasi, tanggung jawab dan pertanggungan-gugatan mereka dan disediakan perlengkapan yang memadai untuk mendukung kebijakan keamanan organisasi selama bekerja dan untuk mengurangi resiko kesalahan manusia.

SNI – ISO 27001 A.8.3 Keamanan Sumber Daya Manusia (Pengakhiran atau Perubahan Pekerjaan)	Memastikan bahwa pegawai kontraktor dan pengguna pihak ketiga keluar dari organisasi atau adanya perubahan pekerjaan dengan cara yang sesuai
SNI – ISO 27001 A.9.1 Keamanan Fisik Dan Lingkungan (Area yang aman)	Mencegah akses fisik oleh pihak yang tidak berwenang, kerusakan dan interfensi terhadap lokasi dan informasi organisasi
SNI – ISO 27001 A.9.2 Keamanan Fisik Dan Lingkungan (Keamanan Peralatan)	Mencegah kehilangan, kerusakan, pencurian atau gangguan aset dan interupsi terhadap kegiatan organisasi
SNI – ISO 27001 A.10.1 Manajemen Komunikasi dan Operasi (Prosedur Operasional dan Tanggung Jawab)	Memastikan pengoperasian fasilitas pengolahan informasi secara benar dan aman
SNI – ISO 27001 A.10.2 Manajemen Komunikasi dan Operasi (Manajemen Pelayanan Jasa Pihak Ketiga)	Menerapkan dan memelihara tingkat keamanan informasi dan pelayanan jasa yang sesuai dengan perjanjian pelayanan jasa pihak ketiga
SNI – ISO 27001 A.10.3 Manajemen Komunikasi dan Operasi (Perencanaan dan Ketertiban Sistem)	Mengurangi resiko kegagalan sistem
SNI – ISO 27001 A.10.4 Manajemen Komunikasi dan Operasi (Perlindungan Terhadap Malicious dan Mobile Code)	Melindungi integritas perangkat lunak dan informasi.
SNI – ISO 27001 A.10.5 Manajemen Komunikasi dan Operasi (Back Up)	Memelihara integritas dan ketersediaan informasi dan fasilitas pengolahan informasi

SNI – ISO 27001 A.10.6 Manajemen Keamanan Jaringan	Memastikan perlindungan informasi dalam jaringan dan perlindungan infrastruktur pendukung.
SNI – ISO 27001 A.10.7 Penanganan Media	Mencegah pengungkapan, modifikasi, pemindahan atau pemusnahan aset yang tidak sah, dan gangguan kegiatan bisnis
SNI – ISO 27001 A.10.8 Pertukaran informasi	Memelihara keamanan informasi dan perangkat lunak yang dipertukarkan dalam suatu organisasi dan dengan setiap entitas eksternal
SNI – ISO 27001 A.10.9 Layanan Electronic Commers	Memastikan keamanan layanan elektronik commerce dan keamanan penggunanya
SNI – ISO 27001 A10.10 Pemantauan	Mendeteksi kegiatan pengolahan informasi yang tidak sah
SNI – ISO 27001 A.11.1 Pengendalian Akses (Persyaratan Bisnis Untuk Pengendalian Akses)	Mengendalikan akses kepada informasi
SNI – ISO 27001 A.11.2 Manajemen Akses Pengguna	Memastikan akses oleh pengguna yang sah dan untuk mencegah pihak yang tidak sah pada sistem informasi
SNI – ISO 27001 A.11.3 Tanggung Jawab Pengguna	Mencegah akses pengguna yang tidak sah dan gangguan atau pencurian atas informasi dan fasilitas pengolahan informasi.
SNI – ISO 27001 A.11.4 Pengendalian Akses Jaringan	Mencegah akses yang tidak sah ke dalam layanan jaringan
SNI – ISO 27001 A.11.5 Pengendalian Akses Sistem Operasi	Mencegah akses tidak sah ke dalam sistem operasi
SNI – ISO 27001 A.11.6 Pengendalian Akses	Mencegah akses yang tidak sah terhadap informasi pada sistem aplikasi

Aplikasi Dan Informasi	
SNI – ISO 27001 A.11.7 Mobile Computing Dan Kerja Jarak Jauh (teleworking)	Memastikan keamanan informasi ketika menggunakan fasilitas mobile computing dan kerja jarak jauh (teleworking).
SNI – ISO 27001 A.12.1 Akuisisi, Pengembangan dan Pemeliharaan Sistem Informasi (Persyaratan Keamanan dari Sistem Informasi)	Memastikan bahwa keamanan merupakan bagian yang utuh dari sistem informasi.
SNI – ISO 27001 A.12.2 Pengolahan yang Benar Dalam Aplikasi	Mencegah kesalahan, kehilangan, modifikasi yang tidak sah atau penyalahgunaan informasi dalam aplikasi.
SNI – ISO 27001 A.12.3 Pengendalian dengan cara Kriptografi	Melindungi kerahasiaan, keaslian atau integritas informasi dengan cara kriptografi.
SNI – ISO 27001 A.12.4 Kemanan System File	Memastikan keamanan system files
SNI – ISO 27001 A.12.5 Keamanan Dalam Proses Pengembangan dan Pendukung	Memelihara keamanan perangkat lunak sistem aplikasi dan informasi
SNI – ISO 27001 A.12.6 Manajemen Kerawanan Teknis	Mengurangi resiko terhadap eksploitasi kerawanan teknis yang dipublikasikan
SNI – ISO 27001 A.13.1 Manajemen Insiden Keamanan Informasi (Pelaporan Kejadian dan Kelemahan Keamanan Informasi)	Memastikan kejadian dan kelemahan keamanan informasi terkait dengan sistem informasi dikomunikasikan sedemikian rupa sehingga memungkinkan tindakan koreksi dilakukan tepat waktu.

SNI – ISO 27001 A.13.2 Manajemen Insiden Keamanan Informasi dan Perbaikan	Memastikan pendekatan yang konsisten dan efektif diterapkan untuk manajemen insiden keamanan informasi.
SNI – ISO 27001 A.14.1 Manajemen Keberlanjutan Bisnis (Business Continuity Management) Aspek Keamanan Informasi dari manajemen Keberlanjutan Bisnis	Menghadapi gangguan kegiatan bisnis dan untuk melindungi proses bisnis kritis dari efek kegagalan utama system
SNI – ISO 27001 A.15.1 Kesesuaian (Kesesuaian Dengan Persyaratan Hukum	Mencegah pelanggaran terhadap undang-undang , peraturan perundangundangan atau kewajiban kontrak dan setiap persyaratan keamanan
SNI – ISO 27001 A.15.2 Pemenuhan Terhadap Kebijakan Keamanan Standart, Pemenuhan Teknis	Memastikan pemenuhan sistem terhadap kebijakan dan standar keamanan organisasi
SNI – ISO 27001 A.15.3 Pertimbangan Audit Sistem Informasi	Memaksimalkan keefektifan dari dan untuk meminimalkan interfensi kepada / dari proses audit sistem informasi

LAMPIRAN 2 Surat Izin Penelitian

LAMPIRAN 3 Project Definition (Audit Charter)

Audit Charter

Project ID : SNI-ISO 27001-Audit-01

Project Name : Information System Management Audit

Auditor : Eri Kurniawan

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, dan akuisisi pengembangan dan pemeliharaan.

Project Schedule : April - Juli

Stakeholder list :

Jabatan	Respondent	Klausul Pengendalian audit
Chief Information Officer	Fajar Gutomo	Kebijakan keamanan, SNI-ISO 27001 A.5 (A.5.1)
Chief Information Officer	Fajar Gutomo	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).

		A.10.6)
Admin	Fajar Gutomo	Pengendalian Akses, SNI-ISO 27001 A.11 (A.11.5). Akuisisi, Pengembangan, dan Pemeliharaan Sistem Informasi, SNI-ISO 27001 A.12 (A.12.2- A.12.5)

Yogyakarta, 29 Juli 2016

Mengetahui Kabid Layanan TI

Kepala Rupbasan Bantul

Dra. Mei Kartini

NIP : 19650501 199603 2 001

Auditor

Eri Kurniawan

NIM : 12651087

Audit Keamanan Sistem Informasi
Barang Sitaan Rumah Penyumpanan Benda Sitaan Negara (RUPBASAN BANTUL)
Menggunakan Standar ISO 27001

Document ID	:	INTV-ADMIN
Project Name	:	Audit Keamanan Sistem Informasi Barang Sitaan di Rumah Penyimpanan Benda Sitaan Milik Negara (Rupbasan Bantul) Menggunakan Standar ISO 27001
Auditor	:	Eri Kurniawan
Audite	:	Fajar Gutomo
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 di terapkan oleh pengelola Sistem Informasi Barang Sitaan di Rupbasan Bantul
Date	:	
Responsible	:	Admin

Approved by

Fajar Gutomo

Auditor

Eri Kurniawan

LEMBAR KERTAS KERJA AUDIT

Audit Keamanan Sistem Informasi
Barang Sitaan Rumah Penyumpanan Benda Sitaan Negara (RUPBASAN BANTUL)
Menggunakan Standar ISO 27001

Document ID	:	INTV-CIO
Project Name	:	Audit Sistem Informasi Barang Sitaan di Rumah Penyimpanan Benda SItaan Milik Negara (RUPBASAN BANTUL) Menggunakan Standar ISO 27001
Auditor	:	Eri Kurniawan
Audite	:	Fajar Gutomo
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 di terapkan oleh pengelola Sistem Informasi Barang Sitaan di Rupbasan Bantul
Date	:	
Responsible	:	Chief Information Officer (CIO)

Approved by

Fajar Gutomo

Auditor

Eri Kurniawan

LAMPIRAN 4 Control Objective

Sebagai Acuan Kontrol Saat Melakukan Audit :

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

LAMPIRAN 5 Question of Detail 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 sudah terdokumentasi kebijakan tersebut ?
		Q3	Apakah dokumen kebijakan tersebut sudah di publikasikan kepada semua pihak terkait ?
		Q4	Apakah kebijakan tersebut sudah disosialisasikan dalam bentuk yang relevan, mudah di akses dan dimengerti oleh pembaca ?
	A.5.1.2	Q5	Jika terjadi perubahan kebijakan, apakah kebijakan tersebut tetap disesuaikan dengan keefektifan yang berkelanjutan ?
		Q6	Perubahan kebijakan tersebut apakah akan di komunikasikan kepada semua pihak ?
		Q7	Apakah ada pernyataan komitmen manajemen serta dukungannya terhadap tujuan dan prinsip keamanan informasi ?
		Q8	Apakah semua pegawai atau karyawan telah benar-benar memahami keamanan informasi ?
		Q9	Apakah kebijakan keamanan informasi sudah dilakukan tinjauan ulang guna mengantisipasi setiap perubahan yang mempengaruhi analisa resiko, seperti kerawanan ?
		Q10	Apakah tinjauan ulang kebijakan dilakukan secara berkala dan terjadwal ?
2	A.7		
	A.7.1		
	A.7.1.1	Q11	Apakah semua inventaris aset (aset informasi, aset piranti lunak, aset fisik dan layanan) sudah di identifikasi dan di catat?
		Q12	Masing-masing inventaris aset apakah sudah disusun dan

			dipelihara ?
		Q13	Bagaimanakah kebijakan pengelolaan inventaris aset ?
		Q14	Apakah klasifikasi lokasi keamanan aset sudah di dokumentasikan (sebagai catatan jika terjadi kehilangan atau kerugian) ?
	A.7.1.2	Q15	Apakah sudah ditentukan pegawai atau sub bagian yang menjaga (mengontrol dan memelihara) keamanan informasi inventaris aset ?
		Q16	Siapa yang bertanggung jawab mengontrol dan memelihara terhadap semua informasi aset ?
		Q17	Berapa jangka waktu pengecekan inventaris aset secara berkala ?
		Q18	Apakah sudah di identifikasi nilai dan tingkat kepentingan aset ?
	A.7.1.3	Q19	Apakah ada aturan ketika pihak–pihak tertentu menggunakan informasi aset ?
		Q20	Apakah informasi pengolahan aset sudah didokumentasikan ?
		Q21	Seberapa perlukah informasi pengolahan aset di dokumentasikan ?
	A.7.2		
	A.7.2.1	Q22	Apakah informasi aset di klasifikasikan dengan tingkat perlindungan yang tepat ?
		Q23	Bagaimanakah prosedur pengklasifikasian informasi pengolahan aset tersebut ?
	A.7.2.2	Q24	Apakah ada satu set prosedur yang baik untuk menetukan pemberian tanda pelabelan dan penanganan informasi yang bersifat rahasia atau penting ?
		Q25	Apakah prosedur tersebut sudah mencakup informasi baik secara fisik maupun dalam format elektronik ?
		Q26	Apakah penanganan informasi di kembangkan dan diterapkan ?
3	A.9		
	A.9.1		
	A.9.1.1	Q27	Apakah pintu masuk sudah dikendalikan dengan kartu gesek dan PIN guna meminimalisir resiko pencurian atau kesalahan

			dalam penggunaan fasilitas ?
		Q28	Apakah penting pintu masuk ruang sistem informasi dibatasi dengan sistem pengamanan dan karrtu control?
		Q29	Apakah ada kontrol akses fisik atau ruang /wilayah sebagai tempat menerima tamu?
		Q30	Pernahkah meninggalkan komputer dalam keadaan menyala dan ada pegawai lain di dalamnya ?
		Q31	Perlukah ruangan khusus atau pembatas seperti dinding untuk seorang pemegang kendali sistem informasi ?
		Q32	Apakah tembok terluar bangunan sudah terbuat dari konstruksi kuat dan terlindungi dari akses tanpa izin ?
	A.9.1.2	Q33	Apakah pengunjung yang datang diawasi dan tanggal datang dan perginya dicatat ?
		Q34	Akses ke informasi sensitif dan fasilitas pemrosesan informasi apakah harus di kontrol dan dibatasi ?
	A.9.1.3	Q35	Semua pegawai dan karyawan apakah sudah diwajibkan memakai tanda pengenal ?
		Q36	Apakah hak akses ke wilayah aman harus dikaji ulang dan diperbaharui secara berkala ?
	A.9.1.4	Q37	Apakah sudah ada perlindungan fisik terhadap kerusakan akibat dari ledakan, banjir dan bencana alam lainnya ?
		Q38	Apakah bahan berbahaya dan mudah meledak sudah disimpan diwilayah aman ?
	A.9.1.5	Q39	Apakah penempatan ruang sistem informasi sudah termasuk dalam area yang aman ?
		Q40	Apakah sudah mempertimbangkan kebijakan tentang makan, minum dan merokok disekitar fasilitas pemrosesan informasi ?
		Q41	Apakah kabel listrik sudah dipisahkan dari kabel komunikasi untuk mencegah gangguan (interferensi) ?
	A.9.1.6	Q42	Dari segi wilayah keamanan apakah penempatan posisi sistem informasi digilib sudah membuat nyaman pengelola sistem informasi ?
		Q43	Jika ada perbaikan ruangan dan peralatan informasi lainnya apakah pekerja yang berasal dari luar akan dilakukan pengawasan dan di pantau ?
		Q44	Apakah penting mendampingi pekerja yang melakukan

			perbaikan dan bagaimana prosedur pengawasan-nya ?
	A.9.2		
	A.9.2.1	Q45	Apakah komputer dan peralatan informasi lainnya seperti server, sudah di tempatkan pada tempat yang dirasa cukup aman ?
		Q46	apakah keamanan peralatannya sudah tidak ada peluang akses oleh pihak yang tidak berwenang ?
	A.9.2.2	Q47	Apakah peralatannya sudah dilindungi dari kegagalan catu daya listrik ?
		Q48	Apakah sudah tersedia peralatan pendukung seperti UPS dan pembangkit listrik cadangan ?
	A.9.2.3	Q49	Apakah kabel daya dan telekomunikasi yang membawa data atau jasa sudah dilindungi dari penyadapan dan kerusakan, seperti menggunakan pipa pengaman ?
		Q50	Apakah sudah dihindari melakukan routing melalui tempat umum ?
4	A.10		
	A.10.1		
	A.10.1.1	Q51	Apakah pengoperasian fasilitas pengolahan informasi (Maintenance Server) sudah dilakukan secara benar dan aman ?
		Q52	Jika ada kesalahan operasi dan kesulitan teknis, apakah akan meminta bantuan pengelola/pegawai lain-nya ?
		Q53	Apakah (back-up data) sudah di dipelihara serta sudah dilakukan sesuai prosedur ?
	A.10.1.2	Q54	Jika ada perubahan terhadap fasilitas dan sistem pengolahan informasi apakah sudah di kontrol dan dikendalikan ?
		Q55	Apakah sudah dilakukan pencatatan perubahan dan perubahan tersebut sudah disosialisasikan ke semua pihak?
	A.10.1.3	Q56	Apakah pegawai di ruang sistem informasi sudah dipisahkan menurut tugas dan tanggung jawabnya masing-masing ?
		Q57	Untuk mengurangi resiko insiden memodifikasi tanpa ijin atau penyalahgunaan sistem, apakah ada pengawasan dan pemantauan ?
	A.10.5		

	A.10.5.1	Q58	Apakah salinan back-up dan piranti lunak yang penting sudah dilakukan secara berkala ?
		Q59	Apakah fasilitas back up sudah memadai guna memulihkan seluruh sisitem informasi jika terjadi bencana atau kegagalan ?
		Q60	Catatan yang akurat dari salinan back-up dan prosedur pemulihan yang terdokumentasi apakah sudah disimpan di lokasi terpisah ?
		Q61	Apakah media back-up sudah di uji secara berkala untuk memastikan bisa digunakan di situasi darurat ?
	A.10.6		
	A.10.6.1	Q62	Apakah sudah menerapkan kontrol jaringan untuk memastikan keamanan data dalam jaringan ?
		Q63	Untuk melindungi hak akses tanpa ijin pada jaringan, apakah tanggung jawab operasi jaringan harus dipisahkan dari operasi komputer ?
		Q64	Apakah fitur-fitur dan level layanan diseluruh jaringan harus diidentifikasi ?
		Q65	Apakah ada petugas atau pegawai yang khusus menangani keamanan jaringan ?
	A.10.6.2	Q66	Apakah sudah terdapat mekanisme pengamanan jaringan sebagai upaya pencegahan serangan ?
		Q67	Apakah manajemen sudah mengidentifikasi titik jaringan yang rawan terhadap serangan ?
		Q68	Apabila serangan telah terjadi, adakah mekanisme recovery jaringan yang diterapkan ?
		Q69	Seberapa sering fitur keamanan dan tingkat layanan jaringan di identifikasi ?
	A.11.		
	A.11.5		
	A.11.5.1	Q70	Apakah sudah di terapkan prosedur log-on yang aman ?
		Q71	Apakah sudah membatasi kegagalan percobaan log-on ?
	A.11.5.2	Q72	Apakah seluruh pengguna (termasuk staf pendukung teknis) memiliki user ID yang berbeda ?
		Q73	Apakah user ID tersebut sudah di batasi untuk penggunaan pribadi ?

	A.11.5.3	Q74	Apakah sudah ada sistem manajemen password dan sistem pengelola password untuk memastikan kualitas password ?
		Q75	Apakah sudah ada prosedur batasan jangka waktu pemakaian akun user ?
	A.11.5.4	Q76	Sudah adakah prosedur penonaktifan akun user (seperti password) guna memastikan tidak adanya pemakaian ulang ?
		Q77	Apakah sudah menggunakan program utility sehingga mampu meminimalisir overriding ?
	A.11.5.5	Q78	Apakah sudah menggunakan sesi time-out ?
		Q79	Bagaimana prosedurnya ?
	A.12		
	A.12.2		
	A.12.2.1	Q80	Apakah sudah ada prosedur validasi data ketika memasukan data ke sistem informasi digilib ?
		Q81	Apakah ada prosedur untuk merespon kesalahan validasi?
	A.12.2.2	Q82	Apakah pengecekan validasi harus digabungkan kedalam aplikasi untuk mendeteksi setiap kerusakan ?
		Q83	Ketika ada kerusakan informasi karena ada kesalahan pengolahan apakah bisa dideteksi oleh sistem ?
	A.12.2.3	Q84	Apakah sudah ada perlindungan integritas pesan dalam aplikasi ?
		Q85	Bagaimana mekanisme penerapan dan pengendalian integritas pesan ?
	A.12.2.4	Q86	Untuk memastikan bahwa pengolahan informasi yang disimpan adalah benar, apakah validasi data keluaran begitu penting ?
		Q87	Apakah keluaran data dari aplikasi sudah divalidasi ?
	A.12.5		
	A.12.5.1	Q88	Apakah sudah ada prosedur pengendalian perubahan yang formal ?
		Q89	Apakah pengendalian perubahan harus diterapkan ?
	A.12.5.2	Q90	Bila sistem operasi di ubah, apakah sistem informasi digilib ditinjau dan di uji untuk memastikan tidak ada dampak yang merugikan ?

		Q91	Apakah penting menjaga keamana sistem informasi digilib ketika dilakukan perubahan sistem operasi ?
	A.12.5.3	Q92	Apakah sering melakukan modifikasi perangkat lunak ?
		Q93	Apakah modifikasi perangkat lunak sudah dibatasi ?
		Q94	Apakah seluruh perubahan sudah di kendalikan?
	A.12.5.4	Q95	Apakah sudah dilakukan pencegahan terhadap peluang kebocoran informasi ?
		Q96	Bagaimana prosedur pencegahannya ?
	A.12.5.5	Q97	Apakah sudah dilakukan supervisi dan dipantau pengembangan terhadap perangkat lunak yang dialihdayakan ?

LAMPIRAN 6 Form Question (FQ)

Pemetaan Pertanyaan yang Akan Digunakan Saat Proses Audit

Form Questions 1 (FQ 1) : CIO

Q1, Q2, Q3, Q4, Q5, Q6, Q7, Q8, Q9, Q10, 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, Q49, Q50.

Form Questions 2 (FQ 2) : Admin

Q51, Q52, Q53, Q54, Q55, Q56, Q57, Q58, Q59, Q60, Q61, Q62, Q63, Q64, Q65, Q66, Q67, Q68, Q69, Q70, Q71, Q72, Q73, Q74, Q75, Q76, Q77, Q78, Q79, Q80, Q81, Q82, Q83, Q84, Q85, Q86, Q87, Q88, Q89, Q90, Q91, Q92, Q93, Q94, Q95, Q96, Q97.

LAMPIRAN 7 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, membuat badan cepat beradaptasi.

LAMPIRAN 8 : Hasil Evaluasi Audit

Hasil Evaluasi Akhir Perhitungan Nilai Maturity Proses Audit

NO	KLAUSUL	KODE	QUESTIONS	FORM QUESTIONS		SCORE	MATURITY	SCORE MATURITY
				FQ1 (CIO)	FQ2 (admin)			
1	A.5							
	A.5.1							
	A.5.1.1	Q1	Sudah adakah kebijakan keamanan informasi ?	2		2	Repeatable But Intuitive	1.2
		Q2	Apakah sudah terdokumentasi kebijakan tersebut ?	1		1	Initial/Ad hoc	
		Q3	Apakah dokumen kebijakan tersebut sudah di publikasikan kepada semua pihak terkait ?	1		1	Initial/Ad hoc	
		Q4	Apakah kebijakan tersebut sudah disosialisasikan dalam bentuk yang relevan, mudah di akses dan dimengerti oleh pembaca ?	1		1	Initial/Ad hoc	
	A.5.1.2	Q5	Jika terjadi perubahan kebijakan, apakah kebijakan tersebut tetap disesuaikan dengan keefektifan yang berkelanjutan ?	2		2	Repeatable But Intuitive	
		Q6	Perubahan kebijakan tersebut apakah akan di komunikasikan kepada semua	2		2	Repeatable	

			pihak ?				But Intuitive	
		Q7	Apakah ada pernyataan komitmen manajemen serta dukungannya terhadap tujuan dan prinsip keamanan informasi ?	1		1	Initial/Ad hoc	
		Q8	Apakah semua pegawai atau karyawan telah benar-benar memahami keamanan informasi ?	1		1	Initial/Ad hoc	
		Q9	Apakah kebijakan keamanan informasi sudah dilakukan tinjauan ulang guna mengantisipasi setiap perubahan yang mempengaruhi analisa resiko, seperti kerawanan ?	1		1	Initial/Ad hoc	
		Q10	Apakah tinjauan ulang kebijakan dilakukan secara berkala dan terjadwal ?	2		2	Repeatable But Intuitive	
2	A.7							
	A.7.1							
	A.7.1.1	Q11	Apakah semua inventaris aset (aset informasi, aset piranti lunak, aset fisik dan layanan) sudah di identifikasi dan di catat?	3		3	Defined process	2.565
		Q12	Masing-masing inventaris aset apakah sudah disusun dan dipelihara ?	3		3	Defined process	

		Q13	Bagaimanakah kebijakan pengelolaan inventaris aset ?	3		3	Defined process	
		Q14	Apakah klasifikasi lokasi keamanan aset sudah di dokumentasikan (sebagai catatan jika terjadi kehilangan atau kerugian) ?	2		2	Repeatable But Intuitive	
	A.7.1.2	Q15	Apakah sudah ditentukan pegawai atau sub bagian yang menjaga (mengontrol dan memelihara) keamanan informasi inventaris aset ?	3		3	Defined process	
		Q16	Siapa yang bertanggung jawab mengontrol dan memelihara terhadap semua informasi dan kepemilikan asset?	3		3	Defined process	
		Q17	Berapa jangka waktu pengecekan inventaris aset secara berkala ?	3		3	Defined process	
		Q18	Apakah sudah di identifikasi nilai dan tingkat kepentingan aset ?	3		3	Defined process	
	A.7.1.3	Q19	Apakah ada aturan ketika pihak–pihak tertentu menggunakan informasi aset ?	3		3	Defined process	
		Q20	Apakah informasi pengolahan aset sudah didokumentasikan ?	3		3	Defined process	
		Q21	Seberapa perlukah informasi pengolahan aset di dokumentasikan ?	2		2	Repeatable But Intuitive	
	A.7.2							

	A.7.2.1	Q22	Apakah informasi aset diklasifikasikan dengan tingkat perlindungan yang tepat ?	3		3	Repeatable But Intuitive	
		Q23	Bagaimanakah prosedur pengklasifikasian informasi pengolahan aset tersebut ?	2		2	Repeatable But Intuitive	
	A.7.2.2	Q24	Apakah ada satu set prosedur yang baik untuk menetukan pemberian tanda pelabelan dan penanganan informasi yang bersifat rahasia atau penting ?	2		2	Repeatable But Intuitive	
		Q25	Apakah prosedur tersebut sudah mencakup informasi baik secara fisik maupun dalam format elektronik ?	2		2	Repeatable But Intuitive	
		Q26	Apakah penanganan informasi di kembangkan dan diterapkan ?	2		2	Repeatable But Intuitive	
3	A.9							
	A.9.1							
	A.9.1.1	Q27	Apakah pintu masuk sudah dikendalikan dengan kartu gesek dan PIN guna meminimalisir resiko pencurian atau kesalahan dalam penggunaan fasilitas ?	1		1	Initial/Ad hoc	1.66666667
		Q28	Apakah penting pintu masuk ruang sistem informasi dibatasi dengan sistem pengamanan dan karrtu kontrol ?	1		1	Initial/Ad hoc	

		Q29	Apakah ada kontrol akses fisik atau ruang /wilayah sebagai tempat menerima tamu?	3		3	Defined process	
		Q30	Pernahkah meninggalkan komputer dalam keadaan menyala dan ada pegawai lain di dalamnya ?	3		3	Defined process	
		Q31	Perlukah ruangan khusus atau pembatas seperti dinding untuk seorang pemegang kendali sistem informasi barang sitaan di Rupbasan ?	3		3	Defined process	
		Q32	Apakah tembok terluar bangunan sudah terbuat dari konstruksi kuat dan terlindungi dari akses tanpa izin ?	2		2	Repeatable But Intuitive	
	A.9.1.2	Q33	Apakah pengunjung yang datang diawasi dan tanggal datang dan perginya dicatat ?	2		2	Repeatable But Intuitive	
		Q34	Akses ke informasi sensitif dan fasilitas pemrosesan informasi apakah harus di kontrol dan dibatasi ?	2		2	Repeatable But Intuitive	
	A.9.1.3	Q35	Semua pegawai dan karyawan apakah sudah diwajibkan memakai tanda pengenal ?	2		2	Repeatable But Intuitive	
		Q36	Apakah hak akses ke wilayah aman harus dikaji ulang dan diperbaharui secara berkala ?	2		2	Repeatable But Intuitive	

	A.9.1.4	Q37	Apakah sudah ada perlindungan fisik terhadap kerusakan akibat dari ledakan, banjir dan bencana alam lainnya ?	1		1	Initial/Ad hoc	
		Q38	Apakah bahan berbahaya dan mudah meledak sudah disimpan diwilayah aman ?	2		2	Repeatable But Intuitive	
	A.9.1.5	Q39	Apakah penempatan ruang sistem informasi sudah termasuk dalam area yang aman ?	3		3	Defined process	
		Q40	Apakah sudah mempertimbangkan kebijakan tentang makan, minum dan merokok disekitar fasilitas pemrosesan informasi ?	3		3	Defined process	
	A.9.1.6	Q41	Apakah kabel listrik sudah dipisahkan dari kabel komunikasi untuk mencegah gangguan (interferensi) ?	2		2	Repeatable But Intuitive	
		Q42	Dari segi wilayah keamanan apakah penempatan posisi sistem informasi sudah membuat nyaman pengelola sistem informasi barang sitaan di Rupbasan Bantul?	3		3	Defined process	
		Q43	Jika ada perbaikan ruangan dan peralatan informasi lainnya apakah pekerja yang berasal dari luar akan dilakukan pengawasan dan di pantau ?	3		3	Defined process	

		Q44	Apakah penting mendampingi pekerja yang melakukan perbaikan dan bagaimana prosedur pengawasan-nya ?	2		2	Repeatable But Intuitive	
	A.9.2							
	A.9.2.1	Q45	Apakah komputer dan peralatan informasi lainnya seperti server, sudah di tempatkan pada tempat yang dirasa cukup aman ?	2		2	Repeatable But Intuitive	
		Q46	Apakah keamanan peralatannya sudah tidak ada peluang akses oleh pihak yang tidak berwenang ?	1		1	Initial/Ad hoc	
	A.9.2.2	Q47	Apakah peralatannya sudah dilindungi dari kegagalan catu daya listrik ?	1		1	Initial/Ad hoc	
		Q48	Apakah sudah tersedia peralatan pendukung seperti UPS dan pembangkit listrik cadangan ?	2		2	Repeatable But Intuitive	
	A.9.2.3	Q49	Apakah kabel daya dan telekomunikasi yang membawa data atau jasa sudah dilindungi dari penyadapan dan kerusakan, seperti menggunakan pipa pengaman ?	3		3	Defined process	
		Q50	Apakah sudah dihindari melakukan routing melalui tempat umum ?	1		1	Initial/Ad hoc	
4	A.10							

	A.10.1							
	A.10.1.1	Q51	Apakah pengoperasian fasilitas pengolahan informasi (maintenance server) sudah dilakukan secara benar dan aman ?		1	1	Initial/Ad hoc	1.263157895
		Q52	Jika ada kesalahan operasi dan kesulitan teknis, apakah akan meminta bantuan pengelola/pegawai lain-nya ?		2	2	Repeatable But Intuitive	
		Q53	Apakah (back-up data) sudah di dipelihara serta sudah dilakukan sesuai prosedur ?		1	1	Initial/Ad hoc	
	A.10.1.2	Q54	Jika ada perubahan terhadap fasilitas dan sistem pengolahan informasi apakah sudah di kontrol dan dikendalikan ?		2	2	Repeatable But Intuitive	
		Q55	Apakah sudah dilakukan pencatatan perubahan dan perubahan tersebut sudah disosialisasikan ke semua pihak ?		2	2	Repeatable But Intuitive	
	A.10.1.3	Q56	Apakah pegawai di ruang sistem informasi sudah dipisahkan menurut tugas dan tanggung jawabnya masing-masing ?		1	1	Initial/Ad hoc	
		Q57	Untuk mengurangi resiko insiden memodifikasi tanpa ijin atau penyalahgunaan sistem, apakah ada		2	2	Repeatable But Intuitive	

			pengawasan dan pemantauan ?					
	A.10.5							
	A.10.5.1	Q58	Apakah salinan back-up dan piranti lunak yang penting sudah dilakukan secara berkala ?		1	1	Initial/Ad hoc	
		Q59	Apakah fasilitas back up sudah memadai guna memulihkan seluruh sistem informasi jika terjadi bencana atau kegagalan ?		1	1	Initial/Ad hoc	
		60	Catatan yang akurat dari salinan back-up dan prosedur pemulihan yang terdokumentasi apakah sudah di simpan di lokasi terpisah ?		1	1	Initial/Ad hoc	
		61	Apakah media back-up sudah di uji secara berkala untuk memastikan bisa digunakan disituasi darurat ?		1	1	Initial/Ad hoc	
	A.10.6							
	A.10.6.1	Q62	Apakah sudah menerapkan kontrol jaringan untuk memastikan keamanan data dalam jaringan ?		1	1	Initial/Ad hoc	
		Q63	Untuk melindungi hak akses tanpa ijin pada jaringan, apakah tanggung jawab operasi jaringan harus dipisahkan dari operasi komputer ?		1	1	Initial/Ad hoc	

		Q64	Apakah fitur-fitur dan level layanan diseluruh jaringan harus diidentifikasi ?		1	1	Initial/Ad hoc	
		Q65	Apakah ada petugas atau pegawai yang khusus menangani keamanan jaringan ?		1	1	Initial/Ad hoc	
	A.10.6.2	Q66	Apakah sudah terdapat mekanisme pengamanan jaringan sebagai upaya pencegahan serangan ?		1	1	Initial/Ad hoc	
		Q67	Apakah manajemen sudah mengidentifikasi titik jaringan yang rawan terhadap serangan ?		1	1	Initial/Ad hoc	
		Q68	Apabila serangan telah terjadi, adakah mekanisme recovery jaringan yang diterapkan ?		1	1	Initial/Ad hoc	
		Q69	Seberapa sering fitur keamanan dan tingkat layanan jaringan diidentifikasi ?		2	2	Repeatable But Intuitive	
5	A.11							
	A.11.5							
	A.11.5.1	Q70	Apakah sudah di terapkan prosedur log-on yang aman ?		1	1	Initial/Ad hoc	1
		Q71	Apakah sudah membatasi kegagalan percobaan log-on ?		1	1	Initial/Ad hoc	

	A.11.5.2	Q72	Apakah seluruh pengguna (termasuk staf pendukung teknis) memiliki user ID yang berbeda ?		1	1	Initial/Ad hoc	
		Q73	Apakah user ID tersebut sudah di batasi untuk penggunaan pribadi ?		1	1	Initial/Ad hoc	
	A.11.5.3	Q74	Apakah sudah ada sistem manajemen password untuk memastikan kualitas password ?		1	1	Initial/Ad hoc	
		Q75	Apakah sudah ada prosedur batasan jangka waktu pemakaian akun user ?		1	1	Initial/Ad hoc	
	A.11.5.4	Q76	Sudah adakah prosedur penonaktifan akun user guna memastikan tidak adanya pemakaian ulang ?		1	1	Initial/Ad hoc	
		Q77	Apakah sudah menggunakan program utility supaya mampu meminimalisir overriding ?		1	1	Initial/Ad hoc	
	A.11.5.5	Q78	Apakah sudah menggunakan sesi time-out ?		1	1	Initial/Ad hoc	
		Q79	Bagaimana prosedurnya ?		1	1	Initial/Ad hoc	
6	A.12							
	A.12.2							
	A.12.2.1	Q80	Apakah sudah ada prosedur validasi data ketika memasukan data ke sistem informasi ?		1	1	Initial/Ad hoc	1.444444

		Q81	Apakah ada prosedur untuk merespon kesalahan validasi ?		1	1	Initial/Ad hoc	
	A.12.2.2	Q82	Apakah pengecekan validasi harus digabungkan kedalam aplikasi untuk mendeteksi setiap kerusakan ?		1	1	Initial/Ad hoc	
		Q83	Ketika ada kerusakan informasi karena ada kesalahan pengolahan apakah bisa dideteksi oleh sistem ?		1	1	Initial/Ad hoc	
	A.12.2.3	Q84	Apakah sudah ada perlindungan integritas pesan dalam aplikasi ?		1	1	Initial/Ad hoc	
		Q85	Bagaimana mekanisme penerapan dan pengendalian integritas pesan ?		1	1	Initial/Ad hoc	
	A.12.2.4	Q86	Untuk memastikan bahwa pengolahan informasi yang disimpan adalah benar, apakah validasi data keluaran penting ?		2	2	Repeatable But Intuitive	
		Q87	Apakah keluaran data dari aplikasi sudah divalidasi ?		1	1	Initial/Ad hoc	
	A.12.5							
	A.12.5.1	Q88	Apakah sudah ada prosedur pengendalian perubahan yang formal ?		2	2	Repeatable But Intuitive	
		Q89	Apakah pengendalian perubahan harus diterapkan ?		2	2	Repeatable But Intuitive	

	A.12.5.2	Q90	Bila sistem operasi di ubah, apakah sistem informasi ditinjau dan di uji untuk memastikan tidak ada dampak yang merugikan ?		3	3	Defined process	
		Q91	Apakah penting menjaga keamana sistem informasi ketika dilakukan perubahan sistem operasi ?		2	2	Repeatable But Intuitive	
	A.12.5.3	Q92	Apakah sering melakukan modifikasi perangkat lunak ?		2	2	Repeatable But Intuitive	
		Q93	Apakah modifikasi perangkat lunak sudah dibatasi ?		1	1	Initial/Ad hoc	
		Q94	Apakah seluruh perubahan sudah dikendalikan dengan ketat ?		1	1	Initial/Ad hoc	
	A.12.5.4	Q95	Apakah sudah dilakukan pencegahan terhadap peluang kebocoran informasi ?		1	1	Initial/Ad hoc	
		Q96	Bagaimana prosedur pencegahannya ?		1	1	Initial/Ad hoc	
	A.12.5.5	Q97	Apakah sudah dilakukan supervisi dan dipantau pengembangan terhadap perangkat lunak yang dialihdayakan ?		2	2	Repeatable But Intuitive	
Maturity Level								1.533211501

Lampiran 9 : Hasil Wawancara Audit

LEMBAR KERTAS KERJA AUDIT

Audit Keamanan Sistem Informasi
Barang Sitaan Rumah Penyumpanan Benda Sitaan Negara (RUPBASAN BANTUL)
Menggunakan Standar ISO 27001

Docuent ID	: INTV-CIO
Project Name	: Audit Sistem Informasi Barang Sitaan di Rumah Penyimpanan Benda Sitaan Milik Negara (RUPBASAN BANTUL) Menggunakan Standar ISO 27001
Auditor	: Eri Kurniawan
Audite	: Fajar Gutomo
Description	: Lembar kerja ini merupakan bagian dari Penelitian tugas akhir mahasiswa Program Studi Teknik Informatika Universitas Islam Negeri Sunan Kalijaga Yogyakarta. Lembar kerja audit ini digunakan untuk mengevaluasi Kebijakan Keamanan yang di terapkan oleh pengelola Sistem Informasi Barang Sitaan di Rupbasan Bantul.
Date	: 29 Juli 2016
Responsible	: Chief Information Officer (CIO)

Approved by :

Fajar Gutomo

Auditor

Eri Kurniawan

NO	CODE	QUESTION	ANSWER
1	Q1	Sudah adakah kebijakan keamanan informasi ?	Ya
2	Q2	Apakah sudah terdokumentasi kebijakan tersebut ?	Belum
3	Q3	Apakah dokumen kebijakan tersebut sudah di publikasikan kepada semua pihak terkait ?	Belum
4	Q4	Apakah kebijakan tersebut sudah disosialisasikan dalam bentuk yang relevan, mudah di akses dan dimengerti oleh pembaca ?	Belum
5	Q5	Jika terjadi perubahan kebijakan, apakah kebijakan tersebut tetap disesuaikan dengan keefektifan yang berkelanjutan ?	Ya
6	Q6	Perubahan kebijakan tersebut apakah akan di komunikasikan kepada semua pihak ?	Ya
7	Q7	Apakah ada pernyataan komitmen manajemen serta dukungannya terhadap tujuan dan prinsip keamanan informasi ?	Belum
8	Q8	Apakah semua pegawai atau karyawan telah benar-benar memahami keamanan informasi ?	Belum
9	Q9	Apakah kebijakan keamanan informasi sudah dilakukan tinjauan ulang guna mengantisipasi setiap perubahan yang mempengaruhi analisa resiko, seperti kerawanan ?	Belum
10	Q10	Apakah tinjauan ulang kebijakan	Dalam Proses

		dilakukan secara berkala dan terjadwal ?	
11	Q11	Apakah semua inventaris aset (aset informasi, aset piranti lunak, aset fisik dan layanan) sudah di identifikasi dan di catat?	Ya
12	Q12	Masing-masing inventaris aset apakah sudah disusun dan dipelihara ?	Ya
13	Q13	Bagaimanakah kebijakan pengelolaan inventaris aset ?	Mengikuti SOP BMN (Barang Milik Negara)
14	Q14	Apakah klasifikasi lokasi keamanan aset sudah di dokumentasikan (sebagai catatan jika terjadi kehilangan atau kerugian) ?	Ya (Bagian BMN)
15	Q15	Apakah sudah ditentukan pegawai atau sub bagian yang menjaga (mengontrol dan memelihara) keamanan informasi inventaris aset ?	Ya
16	Q16	Siapa yang bertanggung jawab mengontrol dan memelihara terhadap semua informasi dan kepemilikan aset ?	Kepala UPT → Petugas BMN & bagian Informasi Publik → Regu Pengamanan (menjaga aset secara langsung)
17	Q17	Berapa jangka waktu pengecekan inventaris aset secara berkala ?	Setiap bulan minimal 1 (satu) kali
18	Q18	Apakah sudah di identifikasi nilai dan tingkat kepentingan aset ?	Sudah,
19	Q19	Apakah ada aturan ketika pihak–	

		pihak tertentu menggunakan informasi aset ?	Ada, sesuai dengan kewenangan / kepentingan pihak tertentu tsb. Namun terkait informasi umum dapat diakses secara terbuka.
20	Q20	Apakah informasi pengolahan aset sudah didokumentasikan ?	Ya, sudah terdokumentasikan
21	Q21	Seberapa perlukah informasi pengolahan aset di dokumentasikan ?	Sangat perlu terkait dengan akuntabilitas dan transparansi
22	Q22	Apakah informasi aset di klasifikasikan dengan tingkat perlindungan yang tepat ?	Ya, terdapat SOP berhubungan dengan hal tsb.
23	Q23	Bagaimanakah prosedur pengklasifikasian informasi pengolahan aset tersebut ?	Sebagai contoh dalam hal basan baran secara umum dapat diakses, namun terdapat syarat2 tertentu untuk melihat secara langsung maupun mengambil bagan baran.
24	Q24	Apakah ada satu set prosedur yang baik untuk menetukan pemberian tanda pelabelan dan penanganan informasi yang bersifat rahasia atau penting ?	Belum ada yg secara khusus mengatur. terkait informasi publik.
25	Q25	Apakah prosedur tersebut sudah mencakup informasi baik secara fisik maupun dalam format elektronik ?	Belum
26	Q26	Apakah penanganan informasi di kembangkan dan diterapkan ?	Dalam proses
27	Q27	Apakah pintu masuk sudah dikendalikan dengan kartu gesek dan PIN guna meminimalisir resiko pencurian atau kesalahan dalam penggunaan fasilitas ?	Belum, masih kunci konvensional
28	Q28	Apakah penting pintu masuk ruang sistem informasi dibatasi dengan	Belum

		sistem pengamanan dan karrtu kontrol ?	
29	Q29	Apakah ada kontrol akses fisik atau ruang /wilayah sebagai tempat menerima tamu?	Ya
30	Q30	Pernahkah meninggalkan komputer dalam keadaan menyala dan ada pegawai lain di dalamnya ?	Ya
31	Q31	Perlukah ruangan khusus atau pembatas seperti dinding untuk seorang pemegang kendali sistem informasi barang sitaan di Rupbasan ?	Ya
32	Q32	Apakah tembok terluar bangunan sudah terbuat dari konstruksi kuat dan terlindungi dari akses tanpa izin ?	Belum optimal
33	Q33	Apakah pengunjung yang datang diawasi dan tanggal datang dan perginya dicatat ?	Ya
34	Q34	Akses ke informasi sensitif dan fasilitas pemrosesan informasi apakah harus di kontrol dan dibatasi ?	Ya
35	Q35	Semua pegawai dan karyawan apakah sudah diwajibkan memakai tanda pengenal ?	Ya
36	Q36	Apakah hak akses ke wilayah aman harus dikaji ulang dan diperbaharui secara berkala ?	Ya
37	Q37	Apakah sudah ada perlindungan fisik terhadap kerusakan akibat	Belum optimal, masih dalam tahap minimal

		dari ledakan, banjir dan bencana alam lainnya ?	
38	Q38	Apakah bahan berbahaya dan mudah meledak sudah disimpan diwilayah aman ?	Ya
39	Q39	Apakah penempatan ruang sistem informasi sudah termasuk dalam area yang aman ?	Ya
40	Q40	Apakah sudah mempertimbangkan kebijakan tentang makan, minum dan merokok disekitar fasilitas pemrosesan informasi ?	Ya
41	Q41	Apakah kabel listrik sudah dipisahkan dari kabel komunikasi untuk mencegah gangguan (interferensi) ?	Belum
42	Q42	Dari segi wilayah keamanan apakah penempatan posisi sistem informasi sudah membuat nyaman pengelola sistem informasi barang sitaan di Rupbasan Bantul?	Ya
43	Q43	Jika ada perbaikan ruangan dan peralatan informasi lainnya apakah pekerja yang berasal dari luar akan dilakukan pengawasan dan di pantau ?	Ya
44	Q44	Apakah penting mendampingi pekerja yang melakukan perbaikan dan bagaimana prosedur pengawasan-nya ?	Ya, sangat penting
45	Q45	Apakah komputer dan peralatan informasi lainnya seperti server, sudah di tempatkan pada tempat	Ya

		yang dirasa cukup aman ?	
46	Q46	apakah keamanan peralatannya sudah tidak ada peluang akses oleh pihak yang tidak berwenang ?	Masih ada peluang
47	Q47	Apakah peralatannya sudah dilindungi dari kegagalan catu daya listrik ?	Ya namun belum optimal (UPS masih berdaya kecil)
48	Q48	Apakah sudah tersedia peralatan pendukung seperti UPS dan pembangkit listrik cadangan ?	Ya, UPS dan Genset sudah ada
49	Q49	Apakah kabel daya dan telekomunikasi yang membawa data atau jasa sudah dilindungi dari penyadapan dan kerusakan, seperti menggunakan pipa pengaman ?	Belum
50	Q50	Apakah sudah dihindari melakukan routing melalui tempat umum ?	Belum

LEMBAR KERTAS KERJA AUDIT

Audit Keamanan Sistem Informasi

Barang Sitaan Rumah Penyumpanan Benda Sitaan Negara (RUPBASAN BANTUL)

Menggunakan Standar ISO 27001

Docuent ID	: INTV-ADMIN
Project Name	: Audit Sistem Informasi Barang Sitaan di Rumah Penyimpanan Benda Sitaan Milik Negara (RUPBASAN BANTUL) Menggunakan Standar ISO 27001
Auditor	: Eri Kurniawan
Audite	: Fajar Gutomo
Description	: Lembar kerja ini merupakan bagian dari Penelitian tugas akhir mahasiswa Program Studi Teknik Informatika Universitas Islam Negeri Sunan Kalijaga Yogyakarta. Lembar kerja audit ini digunakan untuk mengevaluasi Kebijakan Keamanan yang di terapkan oleh pengelola Sistem Informasi Barang Sitaan di Rupbasan Bantul.
Date	: 13 Juni 2016
Responsible	: Admin

Approved by :

Fajar Gutomo

Auditor

Eri Kurniawan

1	Q51	Apakah pengoperasian fasilitas pengolahan informasi (Maintenance Server) sudah dilakukan secara benar dan aman ?	Belum
2	Q52	Jika ada kesalahan operasi dan kesulitan teknis, apakah akan meminta bantuan pengelola/pegawai lain-nya ?	Ya
3	Q53	Apakah (Back-up data) sudah di dipelihara serta sudah dilakukan sesuai prosedur ?	Belum
4	Q54	Jika ada perubahan terhadap fasilitas dan sistem pengolahan informasi apakah sudah di kontrol dan dikendalikan ?	Ya
5	Q55	Apakah sudah dilakukan pencatatan perubahan dan perubahan tersebut sudah disosialisasikan ke semua pihak ?	Ya
6	Q56	Apakah pegawai di ruang sistem informasi sudah dipisahkan menurut tugas dan tanggung jawabnya masing-masing ?	Belum
7	Q57	Untuk mengurangi resiko insiden memodifikasi tanpa ijin atau penyalahgunaan sistem, apakah ada pengawasan dan pemantauan ?	Belum optimal
8	Q58	Apakah salinan back-up dan piranti lunak yang penting sudah dilakukan secara berkala ?	Belum , terkendala media back up
9	Q59	apakah fasilitas back up sudah memadai guna memulihkan seluruh sisitem informasi jika	Belum

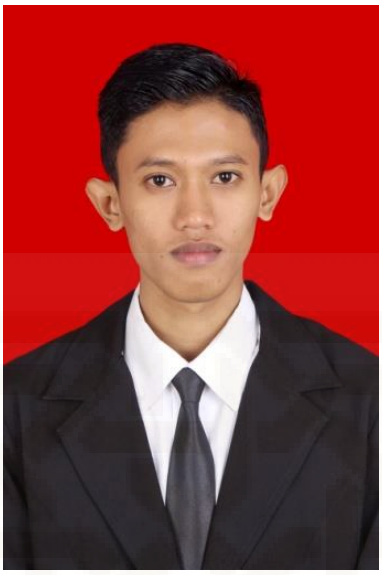
		terjadi bencana atau kegagalan ?	
10	Q60	catatan yang akurat dari salinan back-up dan prosedur pemulihan yang terdokumentasi apakah sudah disimpan di lokasi terpisah ?	Belum
11	Q61	Apakah media back-up sudah di uji secara berkala untuk memastikan bisa digunakan di situasi darurat ?	Belum
12	Q62	Apakah sudah menerapkan kontrol jaringan untuk memastikan keamanan data dalam jaringan ?	Belum
13	Q63	Untuk melindungi hak akses tanpa ijin pada jaringan, apakah tanggung jawab operasi jaringan harus dipisahkan dari operasi komputer ?	Belum, terkendala SDM
14	Q62	Apakah fitur-fitur dan level layanan diseluruh jaringan harus diidentifikasi ?	Belum dilakukan
15	Q65	Apakah ada petugas atau pegawai yang khusus menangani keamanan jaringan ?	Tidak ada
16	Q66	Apakah sudah terdapat mekanisme pengamanan jaringan sebagai upaya pencegahan serangan ?	Tidak ada, masih mengandalkan piranti lunak konvensional
17	Q67	Apakah manajemen sudah mengidentifikasi titik jaringan yang rawan terhadap serangan ?	Belum
18	Q68	Apabila serangan telah terjadi, adakah mekanisme recovery jaringan yang diterapkan ?	Belum

19	Q69	Seberapa sering fitur keamanan dan tingkat layanan jaringan di identifikasi ?	Sangat penting
20	Q70	Apakah sudah di terapkan prosedur log-on yang aman ?	Belum
21	Q71	Apakah sudah membatasi kegagalan percobaan log-on ?	Belum
22	Q72	Apakah seluruh pengguna (termasuk staf pendukung teknis) memiliki user ID yang berbeda ?	Belum
23	Q73	Apakah user ID tersebut sudah di batasi untuk penggunaan pribadi ?	Belum,
24	Q74	Apakah sudah ada sistem manajemen password dan sistem pengelola password untuk memastikan kualitas password ?	Belum, komputer pda informasi publik tidak dipassword
25	Q75	Apakah sudah ada prosedur batasan jangka waktu pemakaian akun user ?	Belum
26	Q76	Sudah adakah prosedur penonaktifan akun user (seperti password) guna memastikan tidak adanya pemakaian ulang ?	Tidak
27	Q77	Apakah sudah menggunakan program utility sehingga mampu meminimalisir overriding ?	Belum
28	Q78	Apakah sudah menggunakan sesi time-out ?	Belum
29	Q79	Bagaimana prosedurnya ?	-

30	Q80	Apakah sudah ada prosedur validasi data ketika memasukan data ke sistem informasi ?	Belum ada
31	Q81	Apakah ada prosedur untuk merespon kesalahan validasi ?	Belum
32	Q82	Apakah pengecekan validasi harus digabungkan kedalam aplikasi untuk mendeteksi setiap kerusakan ?	Belum
33	Q83	Ketika ada kerusakan informasi karena ada kesalahan pengolahan apakah bisa dideteksi oleh sistem ?	Tidak, masih menggunakan penilaian personal
34	Q84	Apakah sudah ada perlindungan integritas pesan dalam aplikasi	Belum
35	Q85	Bagaimana mekanisme penerapan dan pengendalian integritas pesan ?	—
36	Q86	Untuk memastikan bahwa pengolahan informasi yang disimpan adalah benar, apakah validasi data keluaran begitu penting ?	Ya sangat penting
37	Q87	Apakah keluaran data dari aplikasi sudah divalidasi ?	Belum, kekurangan SDM dan dukungan sarana
38	Q88	Apakah sudah ada prosedur pengendalian perubahan yang formal ?	Belum optimal
39	Q89	Apakah pengendalian perubahan harus diterapkan ?	Perlu terkait informasi yg sensitif

40	Q90	Bila sistem operasi di ubah, apakah sistem informasi ditinjau dan di uji untuk memastikan tidak ada dampak yang merugikan ?	Ya, terlebih dalam hal kompatibilitas
41	Q91	Apakah penting menjaga keamana sistem informasi digilib ketika dilakukan perubahan sistem operasi ?	Ya
42	Q92	Apakah sering melakukan modifikasi perangkat lunak ?	Ya
43	Q93	Apakah modifikasi perangkat lunak sudah dibatasi ?	Belum, Penggunaan komputer untuk task yg spesifik blm optimal karena kurang fasilitas
44	Q94	Apakah seluruh perubahan sudah di kendalikan dengan ketat ?	Belum
45	Q95	Apakah sudah dilakukan pencegahan terhadap peluang kebocoran informasi ?	Belum optimal
46	Q96	Bagaimana prosedur pencegahannya ?	Masih secara random, belum terkoordinir dan tersasar SOP
47	Q97	Apakah sudah dilakukan supervisi dan dipantau pengembangan terhadap perangkat lunak yang dialihdayakan ?	Masih sebatas personal, belum menyeluruh.

CURRICULUM VITAE



Nama : Eri Kurniawan

Tempat, tanggal lahir : Bantul, 2 Oktober 1993

Jenis Kelamin : Laki-laki

Alamat : Perumnas Bumi Trimulyo Permai Blok II NO 29, Jetis,Bantul

No. Handphone : 085780444446

Email : eri021093@gmail.com

Riwayat Pendidikan formal :

- 2001-2006 : SDN Jurug
- 2006-2009 : SMP N 2 Sewon
- 2009-2012 : SMA N 1 Pleret
- 2012-2016 : S1 Teknik Informatika UIN Suka Yogyakarta