AUDIT KEAMANAN SISTEM INFORMASI DIGITAL LIBRARY UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA MENGGUNAKAN STANDAR SNI-ISO 27001

Skripsi

Untuk Memenuhi Sebagian Persyaratan

Mencapai Derajat Sarjana S-1

Program Studi Teknik Informatika

Disusun Oleh

Juhdan

12651095

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.01.1/2277/2016

Skripsi/Tugas Akhir dengan judul : Audit Keamanan Sistem Informasi Digital Library Universitas Islam Negeri Sunan Kalijaga Menggunakan Standar SNI – ISO 27001

Yang dipersiapkan dan disusun oleh :
Nama : Juhdan
NIM : 12651095
Telah dimunaqasyahkan pada : Selasa, 21 Juni 2016
Nilai Munaqasyah : A -
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

Sumarsono, M.Kom
NIP.19710209 200501 1 003

Penguji II

M. Didik R Wahyudi, M.T
NIP. 19760812 200901 1 015

Yogyakarta, 27 Juni 2016
UIN Sunan Kalijaga
Fakultas Sains dan Teknologi
Dekan

Dr. Maizer Said Nahdi, M.Si
NIP. 19650427 198403 2 001

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 : Juhdan
NIM : 12651095
Judul Skripsi : Audit Keamanan Sistem Informasi Digital Library Universitas Islam Negeri Sunan Kalijaga Menggunakan Standar SNI-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 dimunaqosyahkan. Atas perhatiannya kami ucapkan terima kasih.

Wassalamu'alaikum wr. wb.

Yogyakarta, 1 Juni 2016
Pembimbing

Agus Mulyanto, S.Si, M.Kom
NIP: 19710823 199903 1 003

PERNYATAAN KEASLIAN SKRIPSI

Yang bertanda tangan dibawah ini :

Nama	: Juhdan
Nim	: 12651095
Program Studi	: Teknik Informatika
Fakultas	: Sains dan Teknologi

Menyatakan bahwa skripsi dengan judul **Audit Keamanan Sistem Informasi Digital Library Universitas Islam Negeri Sunan Kalijaga Menggunakan Standar SNI-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, 1 Juni 2016

Yang menyatakan

Juhdan

Nim : 12651095

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 Keamanan Sistem Informasi Digital Library Universitas Islam Negeri Sunan Kalijaga Menggunakan Standart SNI-ISO 27001". Tak lupa pula penulis haturkan salawat serta salam kepada Nabi junjungan kita Nabi Muhammad SAW yang telah berjuang demi berdiri tegaknya daulah islamiyah 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. Ibu Dr. Maizer Said Nahdi, 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. Ayahanda Murtalib dan Mamaku Kalisom tercinta, serta seluruh anggota keluarga tersayang (kakak-kakak ku) atas doa, perhatian, kasih sayang dan dukungan moril maupun materilnya.
7. Teman-teman Program Studi Teknik Informatika, khususnya angkatan 2012 Mandiri Kelas K (Katak12) yang telah banyak memberi dukungan.
8. Semua Pengelola Sistem Informasi Digital Library dan pegawai yang ada di UPT Perpustakaan
9. 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, 1 juni 2016

Juhdan
12651096

HALAMAN PERSEMBAHAN

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

- Ayahku yang telah berjuang sejauh ini buatku, Mamaku 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 Mama panjang umur dan bisa melihatku menjadi anak yang membanggakan keluarga suatu hari nanti, amin.
- Kakak kakak-ku yang selalu sayang sama aku, Kak Mulyati, Kak Sri, Kak Nia, Kak khairul Rizky dan spesial buat Kak Dina yang selalu peduli dan mengkhawatirkanku, yang telah seperti mama kedua buatku selama di jogja terimakasih buat semuanya, adik bungsu mu ini akan selalu sayang kalian.
- 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, Pak Mustakim, 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, Eri, Indah, Rizky, Nuge, Mursyd, Fajar, Rohman, Choirudin, Deviyanto, Krisna, Bintang, Malika, Maya, Iza, Edis, 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 Kos Inomi tercinta, Mas Wira senior inomi yang selalu baik dan peduli sama anak-anaknya semoga cepat nikah dan ketemu jodohnya supaya tidak jadi jomblo senior, Zakariah, Latif, Faruq, Fauzi, Baini, Bagus, Wak Sifa, Lisma, Mbak Alvi, Mbak Novi, Mas Dika dan Adik-Adik kos Indra, Putra, Yuan, Gede, Rahmat, Wisnu, Zaky semoga semua tujuan dan cita-cita kalian tercapai.
- Keluarga besar Pelajar dan Mahasiswa Bima Yogyakarta, Aminullah, Fajar, Nandar, Mas bukhari, Mas Pipon, Bung Robin, Bung Rizal dan semua teman-teman yang selalu peduli selama di Asrama.
- Pihak-pihak yang selalu memberikan bantuannya, semangat, dan doanya baik secara langsung maupun tidak yang tidak dapat penulis sebutkan namanya satu per satu.

MOTTO

Aku akan berjalan bersama mereka yang berjalan. Karena aku tidak akan berdiri diam sebagai penonton yang menyaksikan perarakan berlalu.

(Kahlil Gibran)

Bekerjalah bagaikan tak butuh uang.

Mencintailah bagaikan tak pernah disakiti.

Menarilah bagaikan tak seorang pun sedang menonton

(Mark Twain)

Kegagalan hadir saat manusia sudah berhenti untuk mencoba

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
HO	:	Head Operation
ITIL	:	Information Technology Infrastructure Library
COBIT	:	Control Objective for Information and Related Technology
FQ	:	Form Question
ADIN	:	Admin Infrastructur
ADSOF	:	Admin Software
GDL	:	Ganesha Digital Library
HDD	:	Hard Disk Drive
ID	:	Identity

AUDIT KEAMANAN SISTEM INFORMASI DIGITAL LIBRARY UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA MENGGUNAKAN STANDAR SNI-ISO 27001

Juhdan
12651095

INTISARI

Perpustakaan adalah salah satu Unit Pelaksana Teknis (UPT) yang ada di UIN Sunan Kalijaga. Perpustakaan menggunakan Sistem Informasi Digital Library (Digilib) sebagai fasilitas pendukung layanan repository untuk mendapatkan bahan pustaka. Dengan adanya Sistem Informasi yang diterapkan maka perlu dilakukan perencanaan audit, melaksanakan audit, mengetahui tingkat keamanan dan membuat rekomendasi berdasarkan hasil keamanan audit. Analisis yang dilakukan adalah menggunakan metode scoring dengan pendekatan yang diambil berdasarkan maturity model. Output yang dihasilkan berupa laporan hasil temuan dan rekomendasi berdasarkan hasil audit yang telah dilakukan.

Penelitian ini menggunakan kerangka kerja tata kelola TI SNI-ISO 27001. Strategi pengumpulan data berdasarkan observasi, wawancara, kertas kerja audit dan audit forensik. SNI-ISO 27001 digunakan sebagai panduan dan pedoman untuk mengukur tingkat kematangan manajemen keamanan Sistem Informasi yang diterapkan oleh sebuah perusahaan atau organisasi. Proses audit menggunakan enam 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*.

Hasil Audit Keamanan Sistem Informasi Digital Library berada pada tingkat keamanan dengan skala kematangan 2.19 (Repeatable but Intuitive). Hal ini menunjukan bahwa pengelolaan keamanan telah diterapkan tetapi prosedur pengelolaan belum didokumentasikan. UPT Perpustakaan 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 Digilib, Unit Pelaksana Teknis, SNI-ISO 27001.

AUDIT INFORMATION SYSTEM SECURITY OF DIGITAL LIBRARY STATE ISLAMIC UNIVERSITY SUNAN KALIJAGA USING SNI-ISO 27001 STANDAR

Juhdan
12651095

ABSTRACT

The library is one of the Technical Implementation Unit (UPT) in UIN Sunan Kalijaga. Libraries use the Digital Library Information System (Digilib) as a repository service support facilities to obtain library materials. With the Information System applied it is necessary to audits planning, performing audits, determine the level of security and make recommendations based on the results of a security audit. Analysis is conducted using the method of scoring with the approach taken by maturity models. The output of the report's findings and recommendations based on the results of audits that have been conducted.

This research uses an IT governance framework SNI ISO 27001. Data collection strategy based on observations, interviews, audit working papers and forensic audits. SNI ISO 27001 is used as a guide and guidelines for measuring the maturity level of security management information system applied by a company or organization. The audit process uses six clauses of the 11 clauses contained in SNI ISO 27001, namely, Clause Security Policy (A5), Clause Asset Management (A7), Clause Physical Security and Environment (A9), Clause Security Operating System (A10), Klasul Control access (A11), and Klasul acquisition of Information Systems Development and Maintenance.

Results of Audit Information System Security Digital Library is located on the security level at maturity scale 2:19 (Repeatable but Intuitive). This shows that the security management has been implemented but not yet documented management procedures. Library Unit does not have any formal training so that the lack of understanding of the importance of management, but the manager has had the initiative to do the treatment and control of changes that affect the system.

Keywords : Digilib Information System, Technical Implementation Unit, SNI ISO 27001.

BAB I

PENDAHULUAN

1.1 Latar Belakang

Salah satu faktor penunjang terselesaikannya tugas akhir atau skripsi mahasiswa disebuah universitas adalah adanya sebuah dokumentasi data dan berkas-berkas dari hasil penelitian atau skripsi alumni supaya bisa dimanfaatkan oleh angkatan berikutnya untuk mengembangkan penelitian tersebut serta menambah informasi dan data yang menjadi referensi dan petunjuk dalam proses penyelesaian penulisan TA (Tugas Akhir) atau skripsi Mahasiswa.

Dalam hal ini UIN sunan kalijaga sebagai salah satu universitas terbaik di yogyakarta yang menerapkan pendokumentasian skripsi alumni dalam bentuk sistem informasi Digilib (Digital Library) melalui pemanfaatan teknologi informasi yang berkembang sehingga mahasiswa tidak selalu harus ke perpustakaan jika membutuhkan referensi ketika ingin menyusun skripsi maka dengan adanya sistem informasi Digital Library mahasiswa dapat mudah mengakses dan mendownloadnya melalui internet tanpa harus langsung ke perpustakaan.

Kemajuan teknologi informasi telah memberikan banyak kontribusi dan dampak yang besar terhadap perkembangan suatu organisasi khususnya UPT (Unit Pelaksana Teknis) perpustakaan UIN Sunan Kalijaga 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.

Disamping itu penerapan tata kelola teknologi 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 Digital Library memiliki prosedur dan tata kelola keamanan informasi dan data yang baik maka sangat mendukung tercapainya pelayanan perpustakaan online yang baik bagi user library secara berkelanjutan. 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 Digital Library, 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 Digital Library Universitas Islam Negeri Sunan Kalijaga perlu dilakukan untuk memastikan apakah proses pengawasan dan pengelolaan keamanan sistem informasi Digital Library 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 digital library menggunakan Standar SNI-ISO 27001 ?
2. Bagaimana melaksanakan audit keamanan sistem informasi Digital Library UIN Sunan Kalijaga menggunakan Standar SNI-ISO 27001 ?
3. Bagaimana mengetahui tingkat keamanan sistem informasi Digital Library UIN Sunan Kalijaga menggunakan Standar SNI-ISO 27001 ?
4. Bagaimana menyusun rekomendasi hasil audit keamanan sistem informasi Digital Library menggunakan Standar SNI-ISO 27001 ?

1.3 Batasan Masalah

1. Penelitian ini dilakukan di UPT (Unit Pelaksana Teknis) Perpustakaan UIN Sunan Kalijaga dan objek yang diteliti adalah sistem informasi Digilib (Digital Library) .

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. Strategi pengumpulan data dilakukan berdasarkan observasi, wawancara kertas kerja audit dan audit forensik.
5. 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.
6. *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 Digital Library adalah sebagai berikut :

1. Membuat perencanaan audit keamanaan sistem informasi Digital Library di UIN Sunan Kalijaga dari dokumen wawancara dan lembar kerja yang merupakan hasil dari pengumpulan data.
2. Melaksanakan audit keamanan sistem informasi Digital Library UIN Sunan Kalijaga dengan menggunakan Standar SNI-ISO 27001.

3. Mengetahui tingkat keamanan sistem informasi Digital Library UIN Sunan Kalijaga menggunakan Standar SNI-ISO 27001.
4. Membuat rekomendasi berdasarkan hasil audit keamanan sistem informasi Digital Library untuk evaluasi sistem.

1.5 Manfaat Penelitian

1. Memberikan masukan terhadap staf maupun pemegang kendali sistem informasi Digital Library agar memperhatikan pentingnya keamanan sistem informasi pada digital library 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 digital library UIN Sunan Kalijaga.
3. Menambah literatur dan memberikan sumbangan berupa pengembangan ilmu yang berkaitan dengan audit keamanan sistem informasi Digital Library 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 Digital Library Universitas Islam Negeri Sunan Kalijaga dengan Menggunakan Standart SNI-ISO 27001 setahu 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 Digital Library adalah :

1). Peneliti berhasil melakukan perencanaan Audit terhadap pengelolaan Sistem Informasi Digital Library di UPT Perpustakaan UIN Sunan Kalijaga dengan menggunakan standart SNI-ISO 27001.

2). Peneliti telah berhasil melaksanakan proses Audit Keamanan Sistem Informasi Digilib yang mengambil studi kasus di UPT Perpustakaan UIN Sunan Kalijaga dengan menggunakan standart SNI-ISO 27001 yang menghasilkan data penelitian berupa hasil interview terhadap bentuk pengelolaan Sistem Informasi Digital Library.

3). Hasil analisa kematangan menggunakan maturity level menunjukan bahwa tingkat keamanan Sistem Informasi Digital Library berada pada level *Repeatable but Intuitive* yaitu sebesar 2,19. 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 acuan dan tanggung

jawab sepenuhnya dilimpahkan kepada masing-masing individu dan kesalahan sangat mungkin terjadi.

4). Rekomendasi audit pada Sistem Informasi Digital Library 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). Hendaknya dilakukan audit internal menggunakan standar SNI-ISO 27001 secara rutin oleh pengelola agar mengetahui berapa tingkat keamanan sistem informasi Digital Library serta dapat memberikan pengaruh yang signifikan atas keberlangsungan pelayanan di UPT Perpustakaan.

2). Perlunya penerapan manajemen keamanan sistem informasi berdasarkan standart SNI-ISO 27001 secara bertahap dan berkala pada UPT Perpustakaan khususnya pada Sistem Informasi Digital Library.

3). Untuk penelitian lebih lanjut tentang Sistem Informasi Digital Library di UPT Perpustakaan sebaiknya menggunakan lebih banyak klausul yang ada pada ISO 27001 karena dapat memperoleh nilai kematangan dalam proses pengelolaan Sistem Informasi Digilib yang semakin akurat.

DAFTAR PUSTAKA

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

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

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

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

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

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

Sarno, Riyanarto. 2009. *Audit Sistem dan Teknologi Informasi*. ITSPRess : Surabaya.

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

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

Hery. 2013. *Auditing*. CAPS (Center of Academic Publishing Service) : Yogyakarta.

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

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

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

LAMPIRAN A Surat Izin Penelitian

KEMENTERIAN AGAMA
UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA
FAKULTAS SAINS DAN TEKNOLOGI

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

Alamat : Jl. Marsda Adisucipto, No. 1 Telp. (0274) 519739 Fax (0274) 540971
Email: *fst@uin-suka.ac.id.*Yogyakarta 55281

Nomor : UIN.02/DST.1/TL.00/388/2016 Yogyakarta,02 Februari 2016
Lamp : 1 bendel Proposal
Perihal : Permohonan Izin Penelitian

Kepada
Yth: Kepala UPT Perpustakaan
UIN Sunan Kalijaga
di
Yogyakarta

Assalamu'alaikum Wr.Wb.

Kami beritahukan bahwa untuk kelengkapan penyusunan skripsi dengan judul :

AUDIT KEAMANAN SISTEM INFORMASI DIGITAL LIBRARY UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA MENGGUNAKAN STANDAR SNI-ISO 27001

diperlukan penelitian. Oleh karena itu, kami mengharap kiranya Bapak/Ibu berkenan memberi izin kepada mahasiswa kami:

Nama	:	Juhdan
NIM	:	12651095
Semester	:	7
Program studi	:	Teknik Informatika
Alamat	:	JL. Bimo Kurdo CT/XI/64F Papringan Depok Sleman Yogyakarta
Untuk mengadakan penelitian di	:	UPT Perpustakaan UIN Sunan Kalijaga
Metode pengumpulan data	:	Observasi dan Wawancara
Adapun waktunya mulai tanggal	:	15 Februari 2016 s.d tanggal 31 April 2016

Kemudian atas perkenan Bapak/Ibu kami sampaikan terima kasih.

Wassalamu'alaikum Wr.Wb.

a.n. Dekan
Wakil Dekan Bidang Akademik

Dr. Khurul Wardati, M.Si
NIP. 19660731 200003 2 001

LAMPIRAN B Project Definition (Audit Charter)

Audit Charter

Project ID : SNI-ISO 27001-Audit-01

Project Name : Information System Management Audit

Auditor : Juhdan

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 : February - Mei

Stakeholder list :

Jabatan	**Respondent**	**Klausul Pengendalian audit**
Kabid Layanan Teknologi Informasi (Chief Information Officer)	Drs. Bambang Heru Nurwoto	Kebijakan keamanan, SNI-ISO 27001 A.5 (A.5.1)
Kaur Sistem Informasi dan Jaringan (Head Operation)	Edi Prasetya, S.Kom	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).
Maintenance server dan back-up data	Miftakhul Yazid Fuadi, SIP	Manajemen Komunikasi dan Operasi, SNI-ISO 27001 A.10 (A.10.1 – A.10.5 - A.10.6)
Pengembangan Sistem	Fatchul Hijrih, S.Kom	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, 30 Maret 2016

Mengetahui Kabid Layanan TI
UPT Perpustaakaan UIN Sunan Kalijaga

Drs. Bambang Heru Nurwoto
NIP :

Auditor

Juhdan
NIM : 12651095

LEMBAR KERTAS KERJA AUDIT

Audit Keamanan Sistem Informasi
Digital Library Universitas Islam Negeri Sunan Kalijaga
Menggunakan Standar SNI-ISO 27001

Document ID	:	INTV-CIO
Project Name	:	Audit Keamanan Sistem Informasi Digital Library Universitas Islam Negeri Sunan Kalijaga Menggunakan Standar SNI-ISO 27001
Auditor	:	Juhdan
Audite	:	Drs. Bambang Heru Nurwoto
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 Digital Library Universitas Islam Negeri Sunan Kalijaga.
Date	:	
Responsible	:	Chief Information Officer (CIO)

Approved by | Auditor

Drs. Bambang Heru Nurwoto | Juhdan

LEMBAR KERTAS KERJA AUDIT

Audit Keamanan Sistem Informasi
Digital Library Universitas Islam Negeri Sunan Kalijaga
Menggunakan Standar SNI-ISO 27001

Document ID	:	INTV-HO
Project Name	:	Audit Keamanan Sistem Informasi Digital Library Universitas Islam Negeri Sunan Kalijaga Menggunakan Standar SNI-ISO 27001
Auditor	:	Juhdan
Audite	:	Edi Prasetya, S.Kom
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 dan Keamanan Fisik & Lingkungan yang di terapkan oleh pengelola Sistem Informasi Digital Library Universitas Islam Negeri Sunan Kalijaga.
Date	:	
Responsible	:	Head Operation (HO)

Approved by | Auditor

Edi Prasetya, S.Kom | Juhdan

LEMBAR KERTAS KERJA AUDIT

Audit Keamanan Sistem Informasi
Digital Library Universitas Islam Negeri Sunan Kalijaga
Menggunakan Standar SNI-ISO 27001

Document ID	:	INTV-ADIN
Project Name	:	Audit Keamanan Sistem Informasi Digital Library Universitas Islam Negeri Sunan Kalijaga Menggunakan Standar SNI-ISO 27001
Auditor	:	Juhdan
Audite	:	Miftakhul Yazid Fuadi, SIP
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 yang di terapkan oleh pengelola Sistem Informasi Digital Library Universitas Islam Negeri Sunan Kalijaga.
Date	:	
Responsible	:	Maintenance server dan back-up data (Admin Infrastructur)

Approved by | Auditor

Miftakhul Yazid Fuadi, SIP | Juhdan

LEMBAR KERTAS KERJA AUDIT

Audit Keamanan Sistem Informasi
Digital Library Universitas Islam Negeri Sunan Kalijaga
Menggunakan Standar SNI-ISO 27001

Document ID	:	INTV-ADSOF
Project Name	:	Audit Keamanan Sistem Informasi Digital Library Universitas Islam Negeri Sunan Kalijaga Menggunakan Standar SNI-ISO 27001
Auditor	:	Juhdan
Audite	:	Fatchul Hijrih, S.Kom
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 Pengendalian Akses serta Akuisisi, Pengembangan, dan Pemeliharaan Sistem Informasi yang di terapkan oleh pengelola Sistem Informasi Digital Library Universitas Islam Negeri Sunan Kalijaga.
Date	:	
Responsible	:	Pengembang sistem (Admin Software)

Approved by Audit

Fatchul Hijrih, S.Kom Juhdan

LAMPIRAN C 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	HO
	A.7.2	Klasifikasi Informasi	HO
3.	A.9	Keamanan Fisik dan Lingkungan	
	A.9.1	Area yang aman	HO
	A.9.2	Keamanan Peralatan	HO
4.	A.10	Manajemen Komunikasi dan Operasi	
	A.10.1	Prosedur Operasional dan Tanggung Jawab	ADIN
	A.10.5	Back-up	ADIN
	A.10.6	Manajemen Keamanan Jaringan	ADIN
5.	A.11	Pengendalian Akses	
	A.11.5	Pengendalian Akses Sistem Operasi	ADSOF
6.	A.12	Akuisisi, Pengembangan, dan Pemeliharaan Sistem Informasi	
	A.12.2	Pengolahan Yang Benar Dalam Aplikasi	ADSOF
	A.12.5	Keamanan Dalam Proses Pengembangan dan pendukung.	ADSOF

LAMPIRAN D 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 digital library?
		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 digital library ?
		Q43	Jika ada perbaikan ruangan dan peralatan informasi lainnya apakah pekerja yang berasal dari luar UPT perpustakaan 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 UPT perpustakaan 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 E 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.

Form Questions 2 (FQ 2) : HD

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 3 (FQ 3) : Admin Infrastructur

Q51, Q52, Q53, Q54, Q55, Q56, Q57, Q58, Q59, Q60, Q61, Q62, Q63, Q64, Q65, Q66, Q67, Q68, Q69.

Form Questions 4 (FQ 4) : Admin Software

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 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 Wawancara Audit

LEMBAR KERTAS KERJA AUDIT

Audit Keamanan Sistem Informasi
Digital Library Universitas Islam Negeri Sunan Kalijaga
Menggunakan Standar SNI-ISO 27001

Document ID	:	INTV-CIO
Project Name	:	Audit Keamanan Sistem Informasi Digital Library Universitas Islam Negeri Sunan Kalijaga Menggunakan Standar SNI-ISO 27001
Auditor	:	Juhdan
Audite	:	Drs. Bambang Heru Nurwoto
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 Digital Library Universitas Islam Negeri Sunan Kalijaga.
Date	:	15 April 2016
Responsible	:	Chief Information Officer (CIO)

Approved by

Drs. Bambang Heru Nurwoto

Auditor

Juhdan

QUESTIONS OF INTERVIEW

Document ID : INTV-CIO

No	Code	Questions	Answer	Score
1	Q1	Sudah adakah kebijakan keamanan informasi ?	Masih dalam taraf penyusunan	2
2	Q2	Apakah sudah terdokumentasi kebijakan tersebut ?	Belum	1
3	Q3	Apakah dokumen kebijakan tersebut sudah di publikasikan kepada semua pihak terkait ?	Belum	1
4	Q4	Apakah kebijakan tersebut sudah disosialisasikan dalam bentuk yang relevan, mudah di akses dan dimengerti oleh pembaca ?	Belum	1
5	Q5	Jika terjadi perubahan kebijakan, apakah kebijakan tersebut tetap disesuaikan dengan keefektifan yang berkelanjutan ?	Ya.	2
6	Q6	Kebijakan tersebut apakah akan dikomunikasikan kepada semua pihak ?	Ya.	2

7	Q7	Apakah ada pernyataan komitmen manajemen serta dukungannya terhadap tujuan dan prinsip keamanan informasi ?	Ada	2
8	Q8	Apakah semua pegawai atau karyawan telah benar-benar memahami keamanan informasi ?	Belum sepenuhnya	2
9	Q9	Apakah kebijakan keamanan informasi sudah dilakukan tinjauan ulang guna mengantisipasi setiap perubahan yang mempengaruhi analisa resiko, seperti kerawanan ?	Belum	1
10	Q10	Apakah tinjauan ulang kebijakan dilakukan secara berkala dan terjadwal ?	Belum	1

LEMBAR KERTAS KERJA AUDIT

Audit Keamanan Sistem Informasi
Digital Library Universitas Islam Negeri Sunan Kalijaga
Menggunakan Standar SNI-ISO 27001

Document ID	:	INTV-HO
Project Name	:	Audit Keamanan Sistem Informasi Digital Library Universitas Islam Negeri Sunan Kalijaga Menggunakan Standar SNI-ISO 27001
Auditor	:	Juhdan
Audite	:	Edi Prasetya, S.Kom
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 dan Keamanan Fisik & Lingkungan yang di terapkan oleh pengelola Sistem Informasi Digital Library Universitas Islam Negeri Sunan Kalijaga.
Date	:	15 April 2016
Responsible	:	Head Operation (HO)

Approved by

Edi Prasetya, S.Kom

Auditor

Juhdan

QUESTIONS OF INTERVIEW

Document ID : INTV-HO

No	Code	Questions	Answer	Score
1	Q11	Apakah semua inventaris aset (aset informasi, aset piranti lunak, aset fisik dan layanan) sudah di identifikasi dan di catat ?	sudah	3
2	Q12	Masing-masing inventaris aset apakah sudah disusun dan dipelihara ?	sudah	3
3	Q13	Bagaimanakah kebijakan pengelolaan inventaris aset ?	kebijakan inventaris Aset fisik sepenuhnya pada petugas UAKPB	3
4	Q14	Apakah klasifikasi lokasi keamanan aset sudah di dokumentasikan (sebagai catatan jika terjadi kehilangan atau kerugian) ?	sudah	2
5	Q15	Apakah sudah ditentukan pegawai atau sub bagian yang menjaga (mengontrol dan memelihara) keamanan informasi inventaris aset ?	sudah	3
6	Q16	Siapa yang bertanggung jawab mengontrol dan memelihara semua informasi dan kepemilikan aset ?	semua pegawai di bawah koordinasi bagian Repositori digital	3

7	Q17	Berapa jangka waktu pengecekan inventaris aset secara berkala ?	i-hardware pertahun, sistem setiap saat minim 1 minggu	3
8	Q18	Apakah sudah di identifikasi nilai dan tingkat kepentingan aset ?	sudah	3
9	Q19	Apakah ada aturan ketika pihak–pihak tertentu menggunakan informasi aset ?	ada	2
10	Q20	Apakah informasi pengolahan aset sudah di dokumentasikan ?	sebagian	2
11	Q21	Yang sudah di dokumentasikan sudah mencakup keseluruhan informasi pengolahan aset ?	belum	2
12	Q22	Apakah informasi aset di klasifikasikan dengan tingkat perlindungan yang tepat ?	sebagian	2
13	Q23	Bagaimanakah prosedur pengklasifikasian informasi pengolahan aset tersebut ?	ada	3
14	Q24	Apakah ada satu set prosedur yang baik untuk menentukan pemberian tanda pelabelan dan penanganan informasi yang bersifat rahasia atau penting ?	ada	3
15	Q25	Apakah prosedur tersebut sudah mencakup informasi baik secara fisik maupun dalam format elektronik ?	sebagian	2

16	Q26	Apakah penanganan informasi sudah di kembangkan dan diterapkan ?	sudah	2
17	Q27	Apakah pintu masuk sudah dikendalikan dengan kartu gesek dan PIN guna meminimalisir resiko pencurian atau kesalahan dalam penggunaan fasilitas ?	belum	1
18	Q28	Apakah penting pintu masuk ruang sistem informasi dibatasi dengan sistem pengamanan dan karrtu kontrol ?	belum penting, karena lokasi kerja dan sistem berbeda ?	1
19	Q29	Apakah ada kontrol akses fisik atau ruang /wilayah sebagai tempat menerima tamu?	ada	3
20	Q30	Pernahkah meninggalkan komputer dalam keadaan menyala dan ada pegawai lain di dalamnya ?	pernah	1
21	Q31	Perlukah ruangan khusus atau pembatas seperti dinding untuk seorang pemegang kendali sistem informasi digital library?	perlu	2
22	Q32	Apakah tembok terluar bangunan sudah terbuat dari konstruksi kuat dan terlindungi dari akses tanpa izin ?	sudah	3

23	Q33	Apakah pengunjung yang datang diawasi dan tanggal datang dan perginya dicatat ?	iya	2
24	Q34	Akses ke informasi sensitif dan fasilitas pemrosesan informasi apakah harus di kontrol dan dibatasi ?	iya	2
25	Q35	Semua pegawai dan karyawan apakah sudah diwajibkan memakai tanda pengenal ?	sudah, tapi tidak terlaksana	2
26	Q36	Apakah hak akses ke wilayah aman harus dikaji ulang dan diperbaharui secara berkala ?	iya	3
27	Q37	Apakah sudah ada perlindungan fisik terhadap kerusakan akibat dari ledakan, banjir dan bencana alam lainnya ?	sudah	2
28	Q38	Apakah bahan berhaya dan mudah meledak sudah disimpan diwilayah aman ?	sudah	2
29	Q39	Apakah penempatan ruang sistem informasi sudah termasuk dalam area yang aman ?	sudah	3
30	Q40	Apakah sudah mempertimbangkan kebijakan tentang makan, minum dan merokok disekitar fasilitas pemrosesan informasi ?	sudah	3

31	Q41	Apakah kabel listrik sudah dipisahkan dari kabel komunikasi untuk mencegah gangguan (interferensi) ?	Belum semua ...	2
32	Q42	Dari segi wilayah keamanan pakah penempatan posisi sistem informasi digilib sudah membuat nyaman pengelola sistem informasi digital library ?	Kami Kira sudah	3
33	Q43	Jika ada perbaikan ruangan dan peralatan informasi lainnya apakah pekerja yang berasal dari luar UPT perpustakaan akan dilakukan pengawasan dan di pantau ?	iya	3
34	Q44	Apakah penting mendampingi pekerja yang melakukan perbaikan dan bagaimana prosedur pengawasan-nya?	penting, dengan cara memproteksi fungsi transfer data (USB)	2
35	Q45	Apakah komputer dan peralatan informasi lainnya seperti server, sudah di tempatkan pada tempat yang dirasa cukup aman ?	sudah	2
36	Q46	Apakah keamanan peralatan sudah dilindungi dari peluang akses oleh pihak yang tidak berwenang ?	sudah	2

37	Q47	Apakah peralatannya sudah dilindungi dari kegagalan catu daya listrik ?	Sudah sebagian	2
38	Q48	Apakah sudah tersedia peralatan pendukung seperti UPS dan pembangkit listrik cadangan ?	Sudah	2
39	Q49	Apakah kabel daya dan telekomunikasi yang membawa data atau jasa sudah dilindungi dari penyadapan dan kerusakan, seperti menggunakan pipa pengaman ?	Sudah	3
40	Q50	Apakah sudah dihindari melakukan routing melalui tempat umum ?	Sudah.	2

LEMBAR KERTAS KERJA AUDIT

Audit Keamanan Sistem Informasi
Digital Library Universitas Islam Negeri Sunan Kalijaga
Menggunakan Standar SNI-ISO 27001

Document ID	:	INTV-ADIN
Project Name	:	Audit Keamanan Sistem Informasi Digital Library Universitas Islam Negeri Sunan Kalijaga Menggunakan Standar SNI-ISO 27001
Auditor	:	Juhdan
Audite	:	Miftakhul Yazid Fuadi, SIP
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 yang di terapkan oleh pengelola Sistem Informasi Digital Library Universitas Islam Negeri Sunan Kalijaga.
Date	:	15 April 2016
Responsible	:	Maintenance server dan back-up data (Admin Infrastructur)

Approved by

Miftakhul Yazid Fuadi, SIP

Auditor

Juhdan

QUESTIONS OF INTERVIEW

Document ID : INTV-ADIN

No	Code	Questions	Answer	Score
1	Q51	Apakah pengoperasian fasilitas pengolahan informasi (Maintenance Server) sudah dilakukan secara benar dan aman ?	iya sudah dilakukan. Salah satunya melakukan kegiatan back-up secara rutin, selain itu dilakukan dengan cara membersihkan hardware	2
2	Q52	Jika ada kesalahan operasi dan kesulitan teknis, apakah akan meminta bantuan pengelola/pegawai lain-nya ?	iya tentunya terus membangun komunikasi dan kerjasama yang baik dengan intern bag. TI Perpus dan PTIPD (PKSI).	2
3	Q53	Apakah (Back-up data) sudah di dipelihara serta sudah dilakukan sesuai prosedur ?	Back-up data kita lakukan min 1 bulan sekali kita simpan di penyimpanan internal (HDD Server) dan HDD external.	2
4	Q54	Jika ada perubahan terhadap fasilitas dan sistem pengolahan informasi apakah sudah di kontrol dan dikendalikan ?	kita selalu melakukan kontrol terhadap sistem dan memastikan berjalan dengan baik dan bisa diakses dengan mudah oleh user / pemustaka.	2

5	Q55	Apakah sudah dilakukan pencatatan perubahan dan perubahan tersebut sudah disosialisasikan ke semua pihak ?	ya Tentunya Ketika ada Perubahan menu /Tampilan misalnya, Kita ~~Akan~~ Sosialisasi kan ke Staf Perpustakaan yang berkaitan dengan Repository / Digilib uin-suka.	2
6	Q56	Apakah pegawai di ruang sistem informasi UPT perpustakaan sudah dipisahkan menurut tugas dan tanggung jawabnya masing-masing ?	Iya betul, Kami Bekerja menurut Tugas dan Tanggung jawab. di bag. TI Perpus dipisah menjadi 2 : 1. Urusan Repository 2. Sistem Informasi dan jaringan.	3
7	Q57	Untuk mengurangi resiko insiden memodifikasi tanpa ijin atau penyalahgunaan sistem, apakah ada pengawasan?	Jadi di bag. TI sudah dibagi menurut Kompetensi masing2 : 1orang di bag. Programmer, 1 orang menangani Hardware dan 1orang dibag. Gravis. Jadi Sistem Terus Kita Pantau dan awasi.	3
8	Q58	Apakah salinan back-up dan piranti lunak yang penting sudah dilakukan secara berkala ?	Iya sudah. Untuk digilib minimal 1bulan Sekali Kita back up database dan File PDF dan juga Back-up aplikasi eprints.	2
9	Q59	apakah fasilitas back up sudah memadai guna memulihkan seluruh sisitem informasi jika terjadi bencana atau kegagalan ?	Fasilitas back-up biasa kita menggunakan PC dan juga HDD external. ya Sejauh ini masih bisa mengcover dan masih memadai.	3
10	Q60	Salinan back-up dan prosedur pemulihan apakah tersimpan terpisah ?	Salinan ada dua jenis/macam lokasi, yang Pertama di Internal Server dan yg ke-2 HDD external.	2

11	Q61	Apakah media back-up sudah di uji secara berkala untuk memastikan bisa digunakan di situasi darurat ?	media backup yo kita gunakan Perangkat Komputer dan HDD eksternal. Sudah pernah kita gunakan untuk migrasi dari Server lama ke Server baru, jadi bisa dignakan	2
12	Q62	Apakah sudah menerapkan kontrol jaringan untuk memastikan keamanan data dalam jaringan ?	Untuk kontrol jaringan kalau di perpustakaan Hanya sebatas memastikan Akses berjalan lancar, Koneksi Internet Lancar, Selebihnya wewenang PTIPD.	3
13	Q63	Untuk melindungi hak akses tanpa ijin pada jaringan, apakah tanggung jawab operasi jaringan harus dipisahkan dari operasi komputer ?	mengenai Hal ini yang mempunyai wewenang adalah bag. PTIPD (mana jemen, Hak akses dan juga keamanan jaringan global di UIN). ya tentunya Tanggung jawab ~~di~~ masing2 ~~ma~~bagian.	2
14	Q64	Apakah fitur-fitur dan level layanan diseluruh jaringan harus di identifikasi ?	iya betul, setiap masuk jaringan Internet Harus Identifikasi dulu, dan berkaitan juga Pada Server eprints	2
15	Q65	Apakah ada petugas atau pegawai yang khusus menangani keamanan jaringan ?	iya ada, di bagian PTIPD (Karena disana Sebagai Central jaringan Kampus.	3
16	Q66	Apakah sudah terdapat mekanisme pengamanan jaringan sebagai upaya pencegahan serangan ?	Secara teknis di bag. Perpustakaan belum ada.	3
17	Q67	Apakah manajemen sudah mengidentifikasi titik jaringan yang rawan terhadap serangan ?	wah kalau masalah itu kurang tau, soalnya kembali ke bag. PTIPD lagi. (yang berwewenang.	3

18	Q68	Apabila serangan telah terjadi, adakah mekanisme recovery jaringan yang diterapkan ?	ini bukan wewenagg bag. TI di perpustakaan. Karena ini level nya lebih Tinggi (bag. PTIPD).	3
19	Q69	Seberapa sering fitur keamanan dan tingkat layanan jaringan di identifikasi ?	bag. ini juga wewenng PTIPd, bisa Cross cek di PTIPD.	2

LEMBAR KERTAS KERJA AUDIT

Audit Keamanan Sistem Informasi
Digital Library Universitas Islam Negeri Sunan Kalijaga
Menggunakan Standar SNI-ISO 27001

Document ID	:	INTV-ADSOF
Project Name	:	Audit Keamanan Sistem Informasi Digital Library Universitas Islam Negeri Sunan Kalijaga Menggunakan Standar SNI-ISO 27001
Auditor	:	Juhdan
Audite	:	Fatchul Hijrih, S.Kom
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 Pengendalian Akses serta Akuisisi, Pengembangan, dan Pemeliharaan Sistem Informasi yang di terapkan oleh pengelola Sistem Informasi Digital Library Universitas Islam Negeri Sunan Kalijaga.
Date	:	15 April 2016
Responsible	:	Pengembang sistem (Admin Software)

Approved by

Fatchul Hijrih, S.Kom

Auditor

Juhdan

QUESTIONS OF INTERVIEW

Document ID : INTV-ADSOF

No	Code	Questions	Answer	Score
1	Q70	Apakah sudah di terapkan prosedur log-on yang aman ?	Belum karena menggunakan port 80	2
2	Q71	Bagaimana contoh prosedur log-on yang aman ?	menggunakan port 443 (SSL) dan capcha.	2
3	Q72	Apakah seluruh pengguna (termasuk staf pendukung teknis) memiliki user ID yang berbeda ?	Iya setiap staf mempunyai akun masing-masing	3
4	Q73	Apakah user ID tersebut sudah di batasi untuk penggunaan pribadi ?	Benar	3
5	Q74	Apakah sudah ada sistem manajemen password dan untuk memastikan kualitas password ?	Belum Ada. secara sistem, tetapi petugas SI selalu mengedukasi pegawai tentang password yg Aman.	1
6	Q75	Apakah sudah ada prosedur batasan jangka waktu pemakaian akun user ?	Sudah.	3
7	Q76	Sudah adakah prosedur penonaktifan akun user guna memastikan tidak adanya pemakaian ulang ?	Sudah.	3

8	Q77	Apakah sudah menggunakan program utility sehingga mampu meminimalisir overriding ?	Belum.	1
9	Q78	Apakah sudah menggunakan sesi time-out ?	Sudah.	2
10	Q79	Bagaimana prosedur sesi time-out ?	user log in set timeout 600	3
11	Q80	Apakah sudah ada prosedur validasi data ketika memasukan data ke sistem informasi digilib ?	Sudah ada	3
12	Q81	Apakah ada prosedur untuk merespon kesalahan validasi ?	Sudah ada.	3
13	Q82	Apakah pengecekan validasi harus digabungkan kedalam aplikasi untuk mendeteksi setiap kerusakan ?	tidak	2
14	Q83	Ketika ada kerusakan karena ada kesalahan pengolahan apakah bisa dideteksi oleh sistem ?	Bisa.	2
15	Q84	Apakah sudah ada perlindungan integritas pesan dalam aplikasi ?	~~Sudah~~ tidak Aktif	1
16	Q85	Bagaimana mekanisme penerapan dan pengendalian integritas pesan ?	Pesan hanya bisa dilihat oleh user sebenarnya di halaman digilib	2

17	Q86	Untuk memastikan bahwa pengolahan informasi yang disimpan adalah benar, apakah validasi data keluaran begitu penting ?	Iya.	2
18	Q87	Apakah keluaran data dari aplikasi sudah divalidasi ?	Iya.	2
19	Q88	Apakah sudah ada prosedur pengendalian perubahan yang formal ?	Tidak	1
20	Q89	Apakah pengendalian perubahan harus diterapkan ?	IYA.	2
21	Q90	Bila sistem operasi di ubah, apakah sistem informasi digilib ditinjau dan di uji untuk memastikan tidak ada dampak yang merugikan ?	IYA sudah teruji.	3
22	Q91	Apakah penting menjaga keamanan sistem informasi digilib ketika dilakukan perubahan sistem operasi ?	IYA	2
23	Q92	Apakah sering melakukan modifikasi perangkat lunak ?	IYA	2
24	Q93	Apakah modifikasi perangkat lunak sudah dibatasi ?	Tidak	1
25	Q94	Apakah seluruh perubahan sudah di kendalikan dengan ketat ?	IYA	2

26	Q95	Apakah sudah dilakukan pencegahan terhadap peluang kebocoran informasi ?	Selama ini belum ditemukan.	3
27	Q96	Bagaimana prosedur pencegahannya ?	~~menutup celah~~ mencari celah kemunculan melalui log server kemudian menutup celah~~nya~~ tersebut.	3
28	Q97	Apakah sudah dilakukan supervisi dan dipantau pengembangan terhadap perangkat lunak yang dialihdayakan ?	Iya.	2

LAMPIRAN H Hasil Evaluasi Audit

Hasil Evaluasi Akhir Perhitungan Nilai Maturity Proses Audit

NO	KLAUSUL	KODE	QUESTIONS	FORM QUESTIONS				SCORE	MATURITY	SCORE MATURITY
				FQ1	FQ2	FQ3	FQ4			
1	A.5									
	A.5.1									
	A.5.1.1	Q1	Sudah adakah kebijakan keamanan informasi ?	2				2	Repeatable But Intuitive	1.5
		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 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 pihak ?	2				2	Repeatable But Intuitive	

		Q7	Apakah ada pernyataan komitmen manajemen terhadap tujuan dan prinsip keamanan informasi ?	2				2	Repeatable But Intuitive	
		Q8	Apakah semua pegawai atau karyawan telah benar-benar memahami keamanan informasi ?	2				2	Repeatable But Intuitive	
		Q9	Apakah kebijakan keamanan informasi sudah dilakukan tinjauan ulang guna mengantisipasi terjadinya resiko seperti kerawanan ?	1				1	Initial/Ad hoc	
		Q10	Apakah tinjauan ulang kebijakan dilakukan secara berkala dan terjadwal?	1				1	Initial/Ad hoc	
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	2.5625
		Q12	Masing-masing inventaris aset apakah sudah disusun dan dipelihara ?		3			3	Defined process	
		Q13	Bagaimanakah kebijakan pengelolaan 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 ?		2			2	Repeatable But Intuitive	
		Q20	Apakah informasi pengolahan aset sudah didokumentasikan ?		2			2	Repeatable But Intuitive	
		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 ?		2			2	Repeatable But Intuitive	
		Q23	Bagaimanakah prosedur pengklasifikasian informasi pengolahan aset tersebut ?		3			3	Defined process	
	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 ?		3			3	Defined process	

		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	2.208333333
		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 ?		1			1	Initial/Ad hoc	
		Q31	Perlukah ruangan khusus atau pembatas seperti dinding untuk seorang pemegang kendali sistem informasi digital library?		2			2	Repeatable But Intuitive	
		Q32	Apakah tembok terluar bangunan sudah terbuat dari konstruksi kuat dan terlindungi dari akses tanpa izin ?		3			3	Defined process	

	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 ?		3			3	Defined process	
	A.9.1.4	Q37	Apakah sudah ada perlindungan fisik terhadap kerusakan akibat dari ledakan, banjir dan bencana alam lainnya ?		2			2	Repeatable But Intuitive	
		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 digilib sudah membuat nyaman pengelola sistem informasi digital library ?		3			3	Defined process	
		Q43	Jika ada perbaikan ruangan dan peralatan informasi lainnya apakah pekerja yang berasal dari luar UPT perpustakaan 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 ?		2			2	Repeatable But Intuitive	
	A.9.2.2	Q47	Apakah peralatannya sudah dilindungi dari kegagalan catu daya listrik ?		2			2	Repeatable But Intuitive	

		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 ?		2			2	Repeatable But Intuitive	
4	A.10									
	A.10.1									
	A.10.1.1	Q51	Apakah pengoperasian fasilitas pengolahan informasi (maintenance server) sudah dilakukan secara benar dan aman ?			2		2	Repeatable But Intuitive	2.421052631
		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 ?			2		2	Repeatable But Intuitive	
	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 UPT perpustakaan sudah dipisahkan menurut tugas dan tanggung jawabnya masing-masing ?			3		3	Defined process	
		Q57	Untuk mengurangi resiko insiden memodifikasi tanpa ijin atau penyalahgunaan sistem, apakah ada pengawasan dan pemantauan ?			3		3	Defined process	
	A.10.5									
	A.10.5.1	Q58	Apakah salinan back-up dan piranti lunak yang penting sudah dilakukan secara berkala ?			2		2	Repeatable But Intuitive	
		Q59	Apakah fasilitas back up sudah memadai guna memulihkan seluruh sistem informasi jika terjadi bencana atau kegagalan ?			3		3	Defined process	
		60	Catatan yang akurat dari salinan back-up dan prosedur pemulihan yang terdokumentasi apakah sudah di simpan di lokasi terpisah ?			2		2	Repeatable But Intuitive	
		61	Apakah media back-up sudah di uji secara berkala untuk memastikan bisa digunakan disituasi darurat ?			2		2	Repeatable But Intuitive	
	A.10.6									

	A.10.6.1	Q62	Apakah sudah menerapkan kontrol jaringan untuk memastikan keamanan data dalam jaringan ?			3		3	Defined process	
		Q63	Untuk melindungi hak akses tanpa ijin pada jaringan, apakah tanggung jawab operasi jaringan harus dipisahkan dari operasi komputer ?			2		2	Repeatable But Intuitive	
		Q64	Apakah fitur-fitur dan level layanan diseluruh jaringan harus diidentifikasi ?			2		2	Repeatable But Intuitive	
		Q65	Apakah ada petugas atau pegawai yang khusus menangani keamanan jaringan ?			3		3	Defined process	
	A.10.6.2	Q66	Apakah sudah terdapat mekanisme pengamanan jaringan sebagai upaya pencegahan serangan ?			3		3	Defined process	
		Q67	Apakah manajemen sudah mengidentifikasi titik jaringan yang rawan terhadap serangan ?			3		3	Defined process	
		Q68	Apabila serangan telah terjadi, adakah mekanisme recovery jaringan yang diterapkan ?			3		3	Defined process	
		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 ?				2	2	Repeatable But Intuitive	2.3
		Q71	Apakah sudah membatasi kegagalan percobaan log-on ?				2	2	Repeatable But Intuitive	

	A.11.5.2	Q72	Apakah seluruh pengguna (termasuk staf pendukung teknis) memiliki user ID yang berbeda ?				3	3	Defined process	
		Q73	Apakah user ID tersebut sudah di batasi untuk penggunaan pribadi ?				3	3	Defined process	
	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 ?				3	3	Defined process	
	A.11.5.4	Q76	Sudah adakah prosedur penonaktifan akun user guna memastikan tidak adanya pemakaian ulang ?				3	3	Defined process	
		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 ?				2	2	Repeatable But Intuitive	
		Q79	Bagaimana prosedurnya ?				2	3	Defined process	
6	A.12									
	A.12.2									
	A.12.2.1	Q80	Apakah sudah ada prosedur validasi data ketika memasukan data ke sistem informasi digilib ?				3	3	Defined process	2.111111111

		Q81	Apakah ada prosedur untuk merespon kesalahan validasi ?				3	3	Defined process	
	A.12.2.2	Q82	Apakah pengecekan validasi harus digabungkan kedalam aplikasi untuk mendeteksi setiap kerusakan ?				2	2	Repeatable But Intuitive	
		Q83	Ketika ada kerusakan informasi karena ada kesalahan pengolahan apakah bisa dideteksi oleh sistem ?				2	2	Repeatable But Intuitive	
	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 ?				2	2	Repeatable But Intuitive	
	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 ?				2	2	Repeatable But Intuitive	
	A.12.5									
	A.12.5.1	Q88	Apakah sudah ada prosedur pengendalian perubahan yang formal ?				1	1	Initial/Ad hoc	
		Q89	Apakah pengendalian perubahan harus diterapkan ?				2	2	Repeatable But Intuitive	

	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 ?				3	3	Defined process	
		Q91	Apakah penting menjaga keamanan sistem informasi digilib 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 ?				2	2	Repeatable But Intuitive	
	A.12.5.4	Q95	Apakah sudah dilakukan pencegahan terhadap peluang kebocoran informasi ?				3	3	Defined process	
		Q96	Bagaimana prosedur pencegahannya ?				3	3	Defined process	
	A.12.5.5	Q97	Apakah sudah dilakukan supervisi dan dipantau pengembangan terhadap perangkat lunak yang dialihdayakan ?				2	2	Repeatable But Intuitive	
Maturity Level										2.183832845

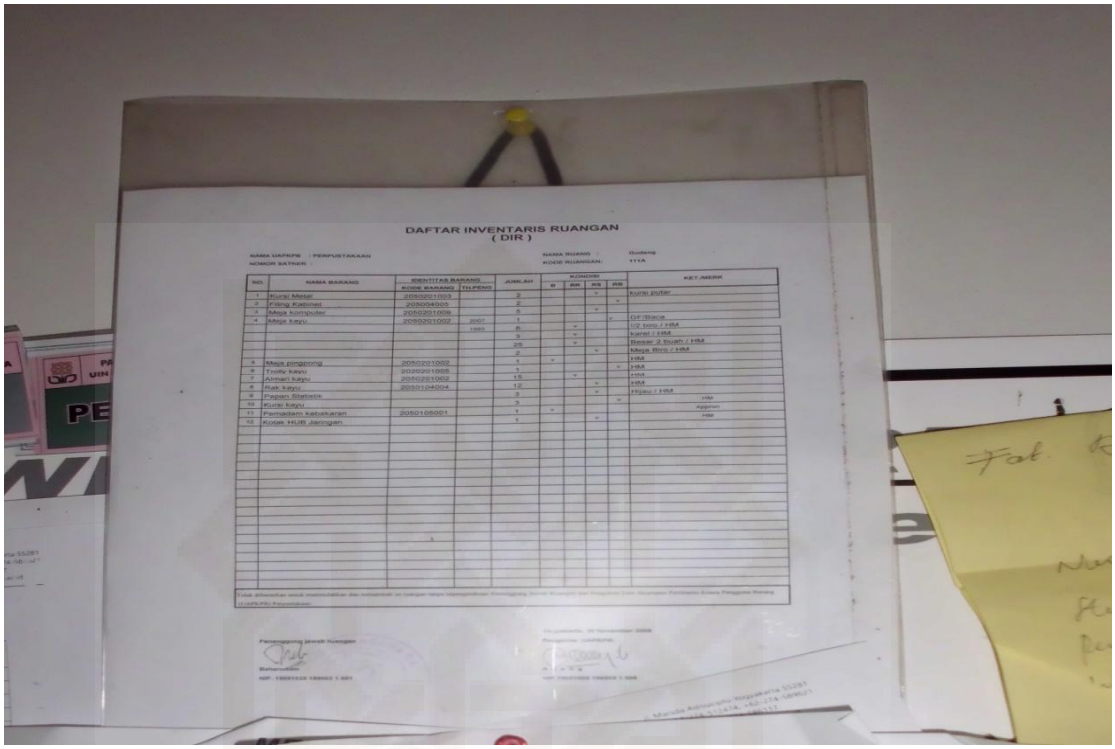
LAMPIRAN I Audit Forensik

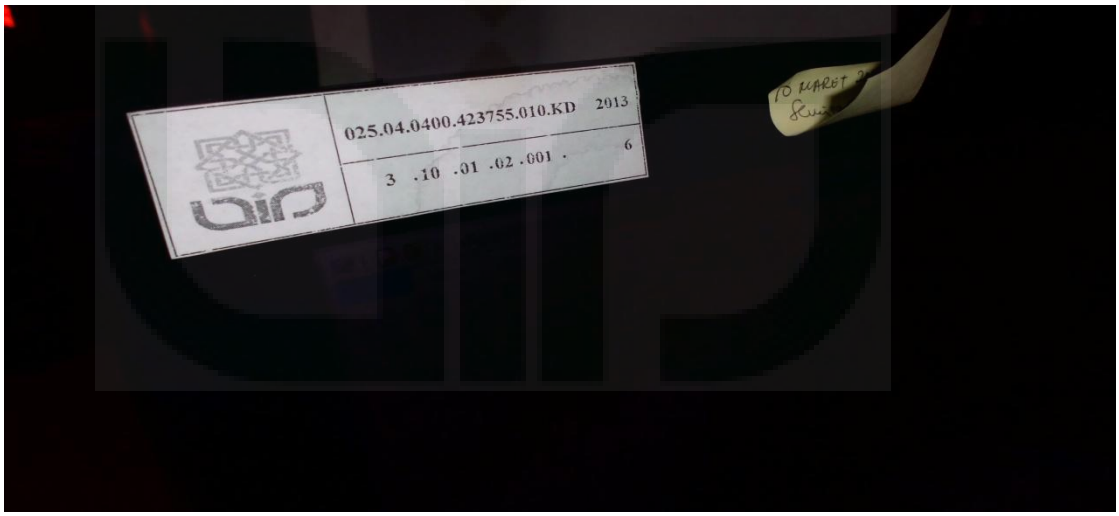
Audit Forensik Klausul Kebijakan Keamanan

Keterangan :

- Kebijakan Keamanan belum didokumentasikan sehingga tidak dapat diketahui, dimengerti dan tidak dapat diakses oleh semua pihak
- Kebijakan keamanan belum diterapkan dan didalam ruangan hanya berisi kalender, jadwal kerja dan inventaris aset

Audit Forensik Klausul Pengelolaan Aset





Keterangan :

- Pengelolaan Aset seperti inventaris aset sudah diterapkan
- Pelabelan dan pemberian tanda terhadap aset sudah diterapkan

Audit Forensik Klausul Keamanan Fisik dan Lingkungan

Keterangan :

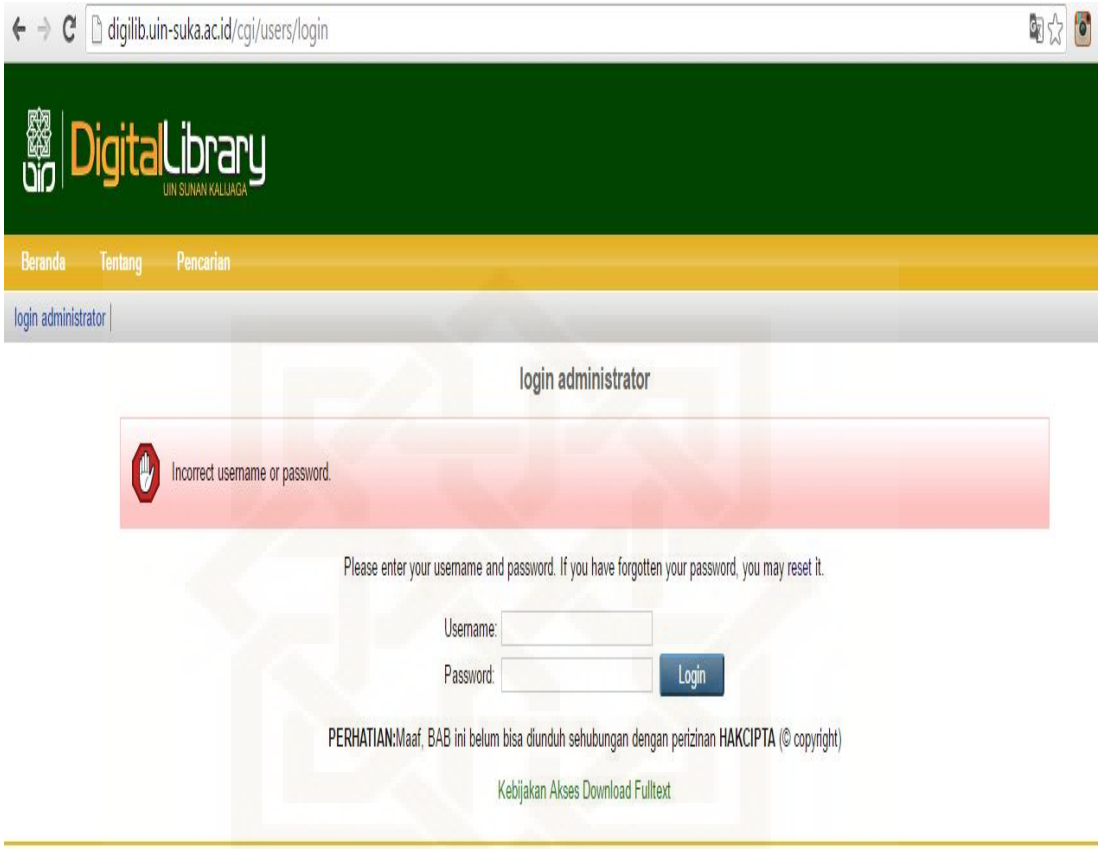
- Pintu masuk Sistem Informasi belum dilakukan pengamanan melalui kartu kontrol atau Pin dan seringkali pintu masuk dibiarkan terbuka
- Alat pemadam api ringan tidak ditempatkan pada semestinya malah digunakan untuk mengganjal pintu masuk ruangan

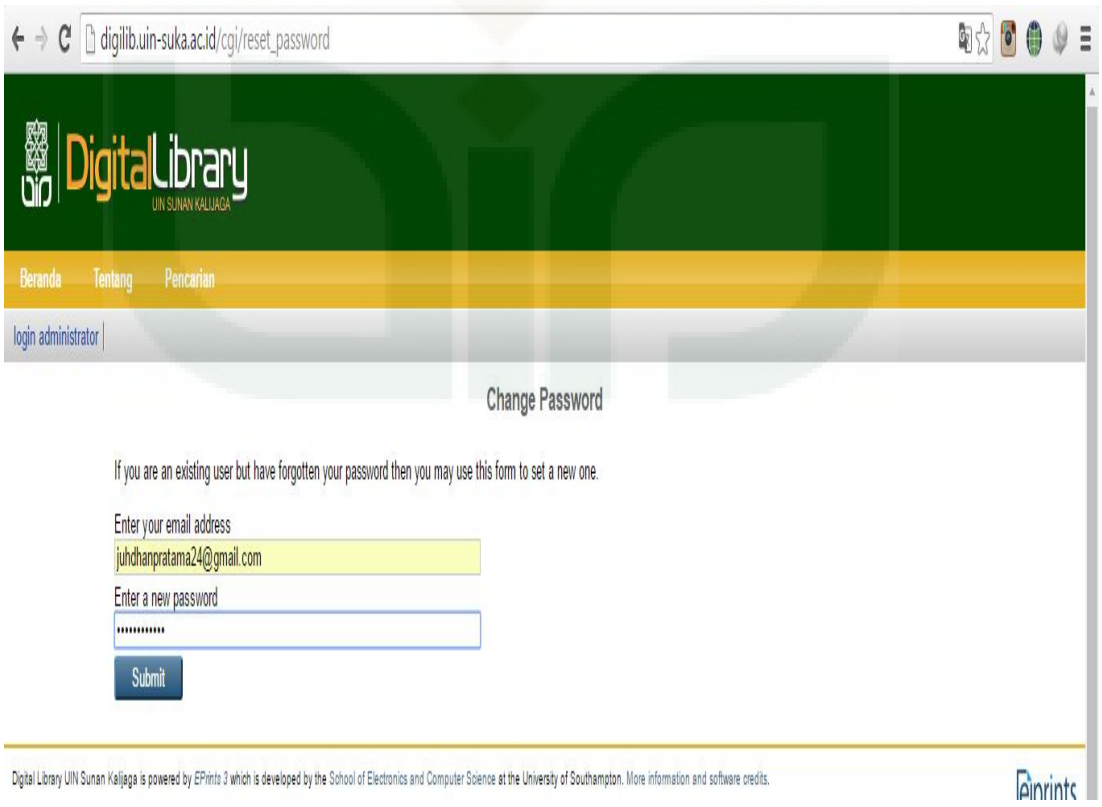
Audit Forensik Klausul Manajemen Komunikasi dan Operasi

Keterangan :

- Sudah dilakukan proses manajemen komunikasi dan operasi seperti back-up file tugas akhir, manajemen jaringan dan server namun belum sesuai prosedur dan standarisasi.

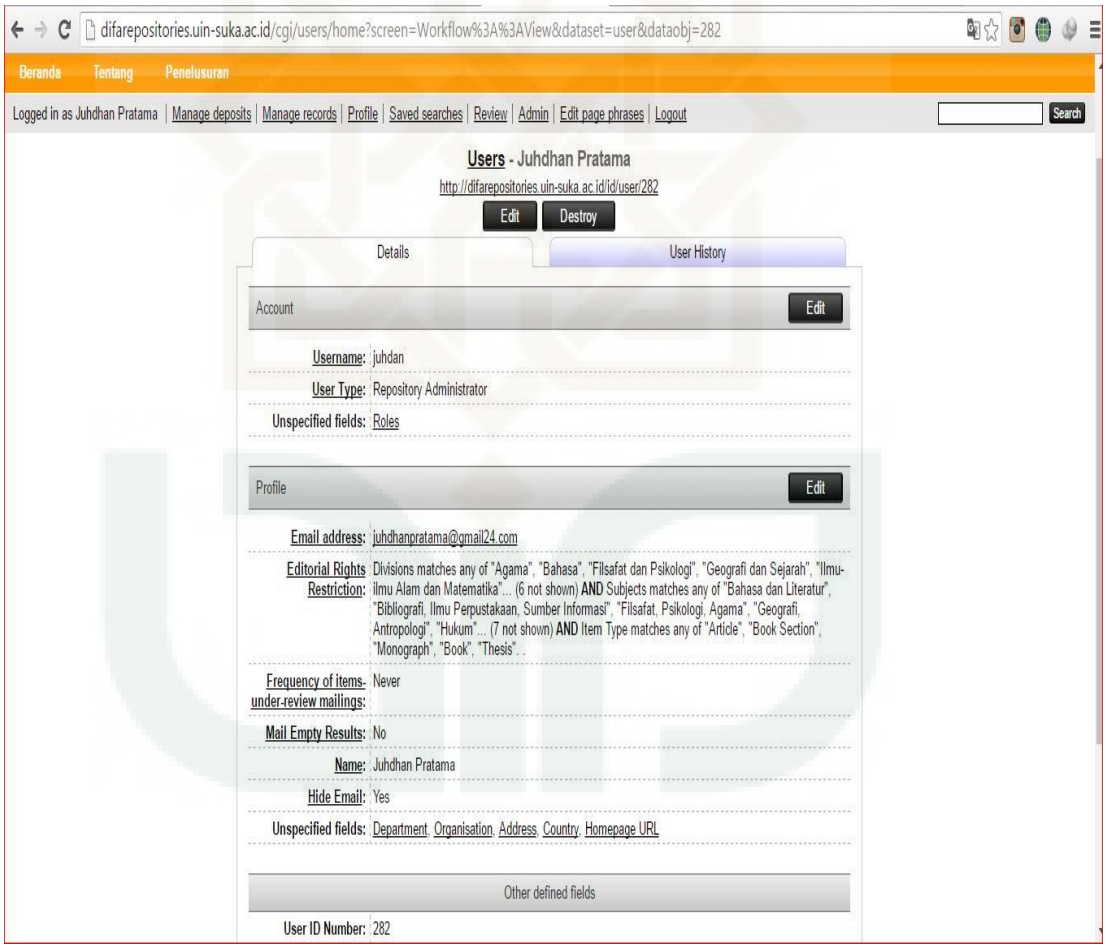
Audit Forensik Klausul Pengendalian Akses





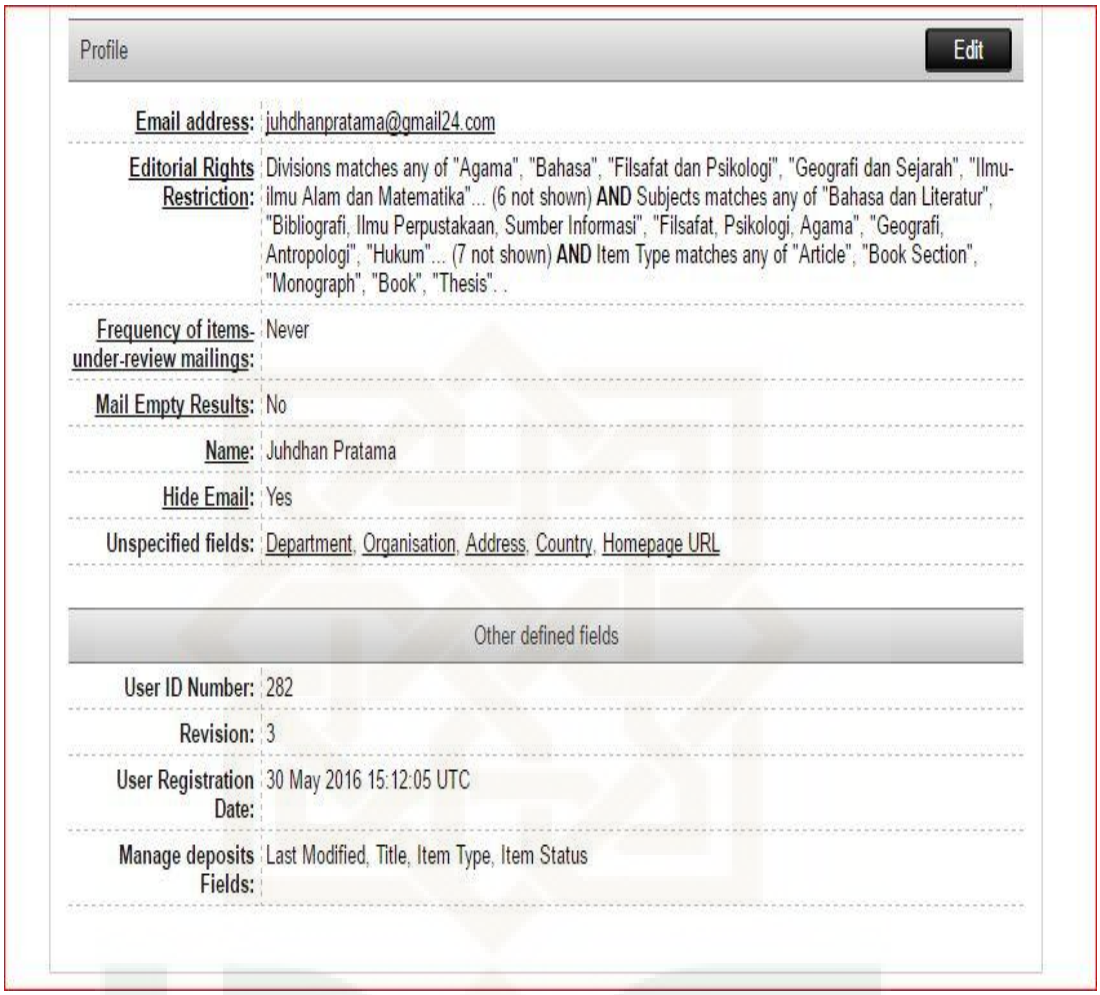
Keterangan :

- 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.
- Sudah diterapkan sistem manajemen password untuk mengganti password yang lama atau karena lupa password.



Keterangan :

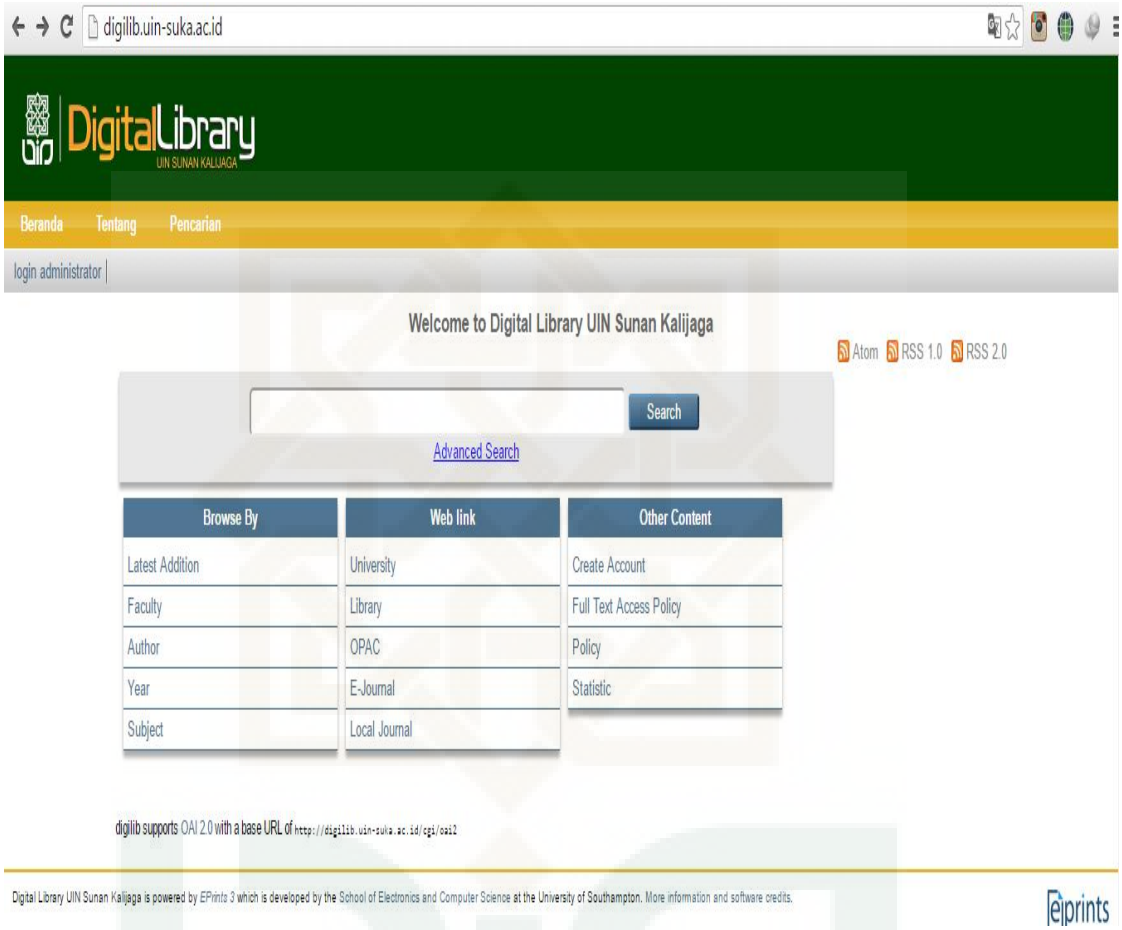
- Seluruh pengguna termasuk pegawai memiliki user yang berbeda dan dibatasi untuk pengunaan pribadi



Keterangan :

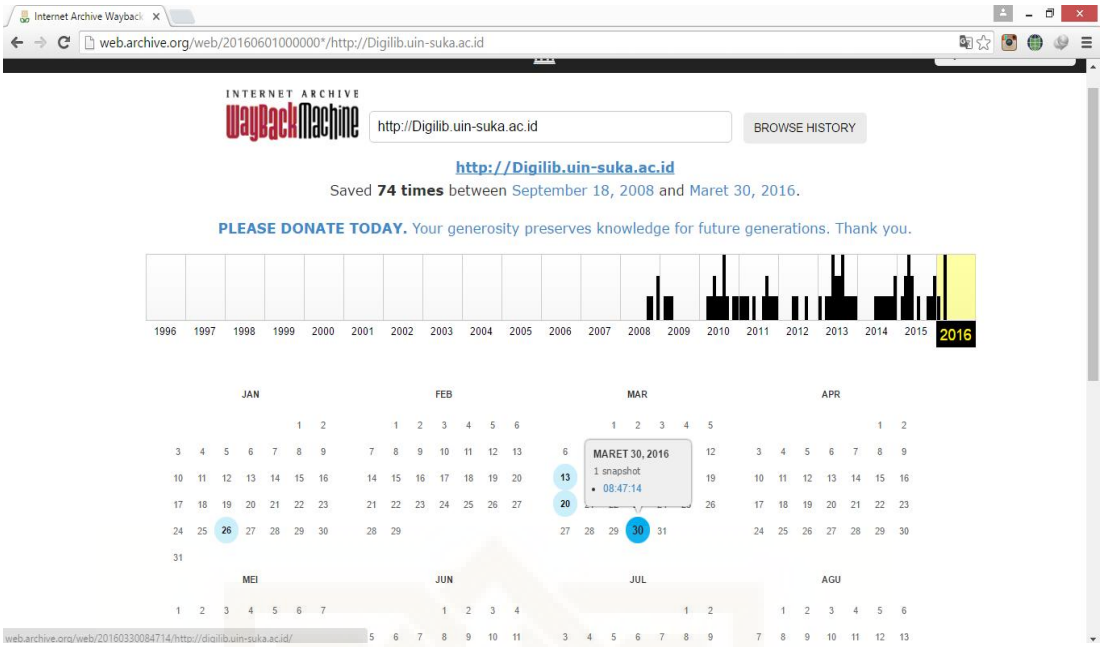
- Belum diterapkan penonaktifan akun user. Tanggal registration user yaitu pada tanggal 30 mei 2016 sedangkan masa berlaku akun selama 3 hari. Kemudian user mencoba masuk kedalam akun pada tanggal 24 juni 2016 akan tetapi akun masih bisa digunakan.

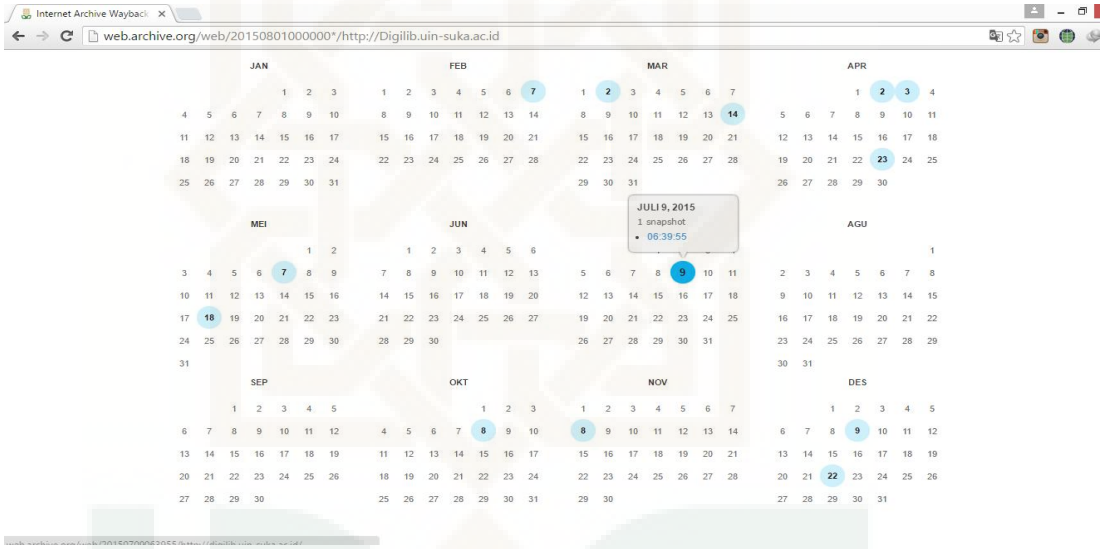
Audit Forensik Klausul Akuisisi, Pengembangan dan Pemeliharaan Sistem Informasi

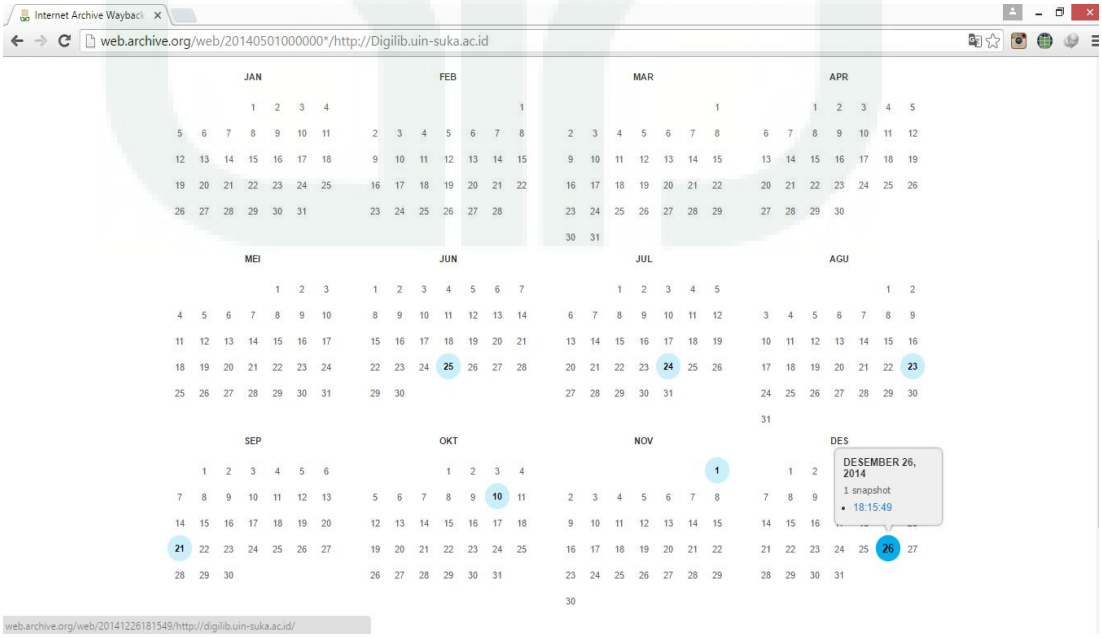


Keterangan :

- Telah dilakukan akuisisi pada sistem dimana sistem langsung menyediakan link dari web lain yang terhubung ke sistem
- Akuisisi data juga tersedia pada sistem, yaitu terdapat data dan berkas penelitian atau skripsi terbaru yang di input ke sistem berdasarkan fakultas, penulis, tahun dan subject.

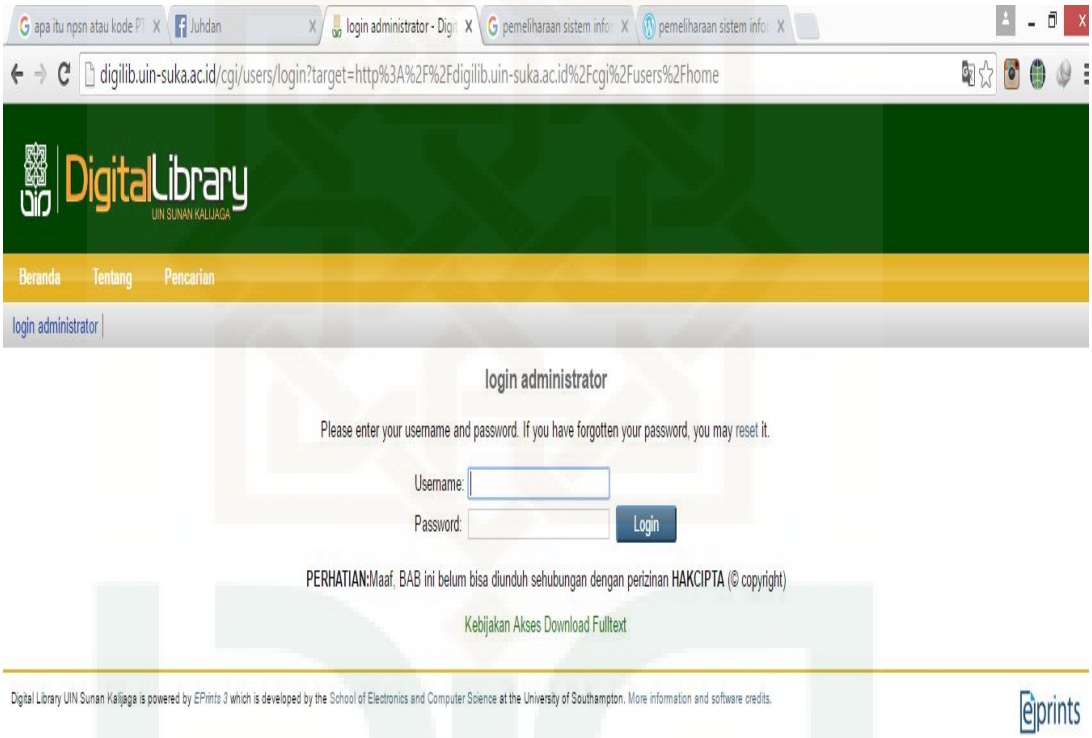

Internet Archive Wayback
web.archive.org/web/20160601000000*/http://Digilib.uin-suka.ac.id
INTERNET ARCHIVE
WayBackMachine
http://Digilib.uin-suka.ac.id
BROWSE HISTORY
http://Digilib.uin-suka.ac.id
Saved 74 times between September 18, 2008 and Maret 30, 2016.
PLEASE DONATE TODAY. Your generosity preserves knowledge for future generations. Thank you.
1996 1997 1998 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016
JAN FEB MAR APR
MARET 30, 2016
1 snapshot
08:47:14
MEI JUN JUL AGU


Internet Archive Wayback
web.archive.org/web/20150801000000*/http://Digilib.uin-suka.ac.id
JAN FEB MAR APR
JULI 9, 2015
1 snapshot
06:39:55
MEI JUN JUL AGU
SEP OKT NOV DES


Internet Archive Wayback
web.archive.org/web/20140501000000*/http://Digilib.uin-suka.ac.id
JAN FEB MAR APR
MEI JUN JUL AGU
SEP OKT NOV DES
DESEMBER 26, 2014
1 snapshot
18:15:49
web.archive.org/web/20141226181549/http://digilib.uin-suka.ac.id/

Keterangan :

- Telah dilakukan pengembangan terhadap sistem, yaitu modifikasi dan perbaikan serta penanganan terhadap kerusakan sistem. Pengembangan pada sistem yang terbanyak dilakukan pada tahun 2014, 2015 dan terakhir dilakukan pada 30 maret 2016



Keterangan :

- Pemeliharaan sistem dilakukan dengan memberikan penyandian pada sistem sehingga membatasi penggunaan oleh banyak pihak yang tidak berwenang.

CURRICULUM VITAE

Nama : Juhdan

Tempat, tanggal lahir : Doro o'o 24 February 1994

Jenis Kelamin : Laki-laki

Alamat : Jln. Tente Karumbu RT 13 RW 003
Desa Doro,o'o Kec. Langgudu Kab. Bima NTB

No. Handphone : 0823-2470-2419

Email/Facebook/Ig : Juhdhanpratama24@gmail.com/Juhdan/J_Dhan24

Riwayat Pendidikan formal :

- 2001-2006 : SD Inpres Doro,o'o
- 2006-2009 : MTS Muhammadiyah Kota Bima
- 2009-2012 : SMA Muhammadiyah Kota Bima
- 2012-2016 : S1 Teknik Informatika UIN Suka Yogyakarta

Riwayat Pendidikan Non Formal :

- 2007-2008 : Pelatihan Bahasa Inggris
- 2009-2010 : Pelatihan Dakwah dan Kepribadian
- 2010-2011 : Pelatihan Bahasa Arab
- 2006-2012 : Pondok Pesantren Al-Ikhlas Muhammadiyah.