AUDIT KEAMANAN DATA USER PADA APLIKASI TANDA TANGAN DIGITAL PRIVYID DENGAN MENGGUNAKAN STANDAR SNI-ISO 27001

Untuk Memenuhi Sebagai Persyaratan Mencapai Darajat Sarjana S-1

Teknik Informatika

Disusun oleh:

Harry Mustika Hadi

13650006

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI YOGYAKARTA

2018

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

PENGESAHAN SKRIPSI/TUGAS AKHIR

Nomor :B-3270 UIN.02/D.ST/PP.01.1/12/2018

Skripsi/Tugas Akhir dengan judul : Audit Keamanan Data User pada Aplikasi Tanda Tangan Digital PrivyID dengan Menggunakan Standar SNI-ISO 27001

Yang dipersiapkan dan disusun oleh :
Nama : Harry Mustika Hadi
NIM : 13650006
Telah dimunaqasyahkan pada : 6 Desember 2018
Nilai Munaqasyah : B+

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

TIM MUNAQASYAH :

Ketua Sidang

Rahmat Hidayat.S.Kom.M.CS
NIP. 19850514 201503 1 002

Penguji I

Dr. Shofwatul 'Uyun, M.Kom
NIP.19820511 200604 2 002

Penguji II

Sumarsono, M. Kom
NIP.19710209 200501 1 003

Yogyakarta, 28 Desember 2018
UIN Sunan Kalijaga
Fakultas Sains dan Teknologi
Dekan

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

SURAT PERSETUJUAN SKRIPSI/TUGAS AKHIR

Hal : Permohonan
Lamp : -

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

Assalamu'alaikum wr. wb.

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

Nama	: Harry Mustika Hadi
NIM	: 13650006
Judul Skripsi	: Audit Keamanan Data User Pada Aplikasi Tanda Tangan Digital PrivyID dengan 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 Program Studi Teknik Informatika

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

Wassalamu'alaikum wr. wb.

Yogyakarta, 22 Mei 2018
Pembimbing

Rahmat Hidayat, S.Kom., M.Cs
NIP. 19850514 201503 1 002

PERNYATAAN KEASLIAN SKRIPSI

Yang bertanda tangan dibawah ini :

Nama : Harry Mustika Hadi

NIM : 13650006

Program Studi : Teknik Informatika

Fakultas : Sains dan Teknologi

Menyatakan bahwa skripsi dengan judul **"Audit Keamanan Data User Pada Aplikasi Tanda Tangan Digital PrivyiD dengan Menggunakan Standar SNI-ISO 27001"** tidak terdapat karya yang pernah diajukan untuk memperoleh gelar sarjana di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Yogyakarta, 22 Mei 2018

Yang Menyatakan

Harry Mustika Hadi

NIM. 13650006

KATA PENGANTAR

Alhamdulillahirabbil'alamin. Segala puji syukur penulis panjatkan kepada Allah SWT Tuhan seluruh alam semesta yang selalu memberikan rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan skripsi dengan **judul "Audit Keamanan Data User Pada Aplikasi Tanda Tangan Digital Privyid Dengan Menggunakan Standar SNI-ISO 27001"** Tak lupa pula penulis haturkan shalawat serta salam kita curahkan kepada Nabi junjungan kita Nabi Muhammad Shallallahu 'Alaihi wa Sallam.

Skripsi ini diselesaikan untuk memenuhi salah satu syarat guna mencapai gelar sarjana pada program studi Teknik Informatika UIN Sunan Kalijaga Yogyakarta. Penulis juga mengucapkan terimakasih kepada semua pihak yang telah membantu dalam proses pelaksanaan penelitian tugas akhir ini sehingga laporan tugas akhir ini dapat terselesaikan. Oleh karena itu, penulis mengucapkan terima kasih sebesar-besarnya kepada:

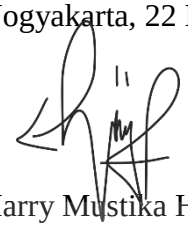
1. Allah SWT, Tuhan Semesta Alam yang telah memberikan kelancaran dan ridho dalam penyusunan skripsi ini, tanpa kehendak-Nya penyusunan skripsi ini tidak akan terlaksana dengan baik.
2. Ayah – Ibu dan seluruh anggota keluarga yang tak henti-hentinya memberikan doa, semangat, nasihat, motivasi dan dukungannya.
3. Bapak Prof Drs. KH Yudian Wahyudi, Ph.D selaku Rektor UIN Sunan Kalijaga Yogyakarta.

4. Bapak Dr. Murtono, M.Si selaku Dekan Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta.
5. Bapak Dr. Bambang Sugiantoro, M.T selaku Ketua Program Studi Teknik Informatika Universitas Islam Negeri Yogyakarta.
6. Bapak Nurochman, S.Kom., M.Kom. selaku dosen pembimbing akademik yang telah senantiasa meluangkan waktu untuk memberikan arahan dalam bidang akademik.
7. Rahmat Hidayat, S.Kom., M.Cs. selaku dosen pembimbing tugas akhir yang telah banyak memberikan arahan, masukan, dukungan, dan motivasi demi kelancaran pelaksanaan penulisan skripsi.
8. Seluruh Dosen Program Studi Teknik Informatika UIN Sunan Kalijaga Yogyakarta. Seluruh staf dan karyawan Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta.
9. Teman-teman Program Studi Teknik Informatika 2013 yang telah banyak memberi arahan dan semangat untuk penyusunan dan penelitian ini.
10. Seluruh pegawai dan pengelola PT. Privy Identitas Digital yang telah bersedia meluangkan waktunya menjadi responden untuk pengambilan data penelitian.
11. Semua pihak yang tidak dapat penulis sebutkan satu persatu yang telah memberikan dukungan dan semangat kepada penulis.

Penulis menyadari masih banyak sekali kekurangan dalam penelitian ini, oleh karena itu kritik dan saran senantiasa penulis harapkan. Semoga skripsi ini

dapat memberikan wawasan dan hal yang bermanfaat bagi pembaca sebagaimana mestinya. Terima kasih.

Yogyakarta, 22 Mei 2018



Harry Mustika Hadi

13650006

HALAMAN PERSEMBAHAN

Alhamdulillahirrabbil'alamin. Dengan mengucap segala rasa syukur sehingga dapat menyelesaikan tugas akhir atau skripsi ini. Penulis mempersembahkan tugas akhir ini untuk:

1. Kedua Orang tuaku tercinta, Bapak Suharno dan Ibu Umi Maryani, S.Pd , yang tak henti-hentinya memanjatkan doa, perhatian, dukungan moril maupun materil, serta kasih sayang yang tak ternilai harganya sampai sejauh ini. Serta Adekku Enggar Jati Wahyu Nurhadi yang sangat baik dan selalu memberi semangat. Semoga panjang umur dan selalu diberkahi oleh Allah SWT kepada kalian.
2. Teruntuk semua jajaran keluarga besar prodi Teknik Informatika UIN Sunan Kalijaga, teman-teman, bapak dan ibu dosen, seluruh staff dan karyawannya. Khususnya Bapak Rahmat Hidayat, S.Kom., M.Cs selaku Dosen Pembimbing Skripsi yang selalu sabar, menerima, dan mengarahkan yang benar tentang penyusunan dan sistematika dalam skripsi ini.
3. Teman–teman seperjuangan dan keluarga besar TFORGAS (Tif 2013) semuanya yang tidak bisa disebutkan satu persatu. Terimakasih atas kebersamaan kalian.
4. Semua keluarga KKN-93 di Turgo Bawah yang bisa memberikan pengalaman baru. semoga semua tujuan dan cita-cita kalian tercapai
5. Pihak-pihak yang memberikan doa, bantuan, semangat, dan motivasi baik secara langsung maupun tidak langsung yang tidak dapat penulis sebutkan namanya satu-persatu.

MOTTO

"Banyak kegagalan dalam hidup ini dikarenakan orang-orang tidak menyadari betapa dekatnya mereka dengan keberhasilan saat mereka menyerah."

(Thomas Alva Edison)

“Saat anda gagal mencapai impian anda, jangan pernah berhenti untuk terus mencoba sampai akhirnya tak ada lagi kekuatan untuk mencobanya.”

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

AUDIT KEAMANAN DATA USER PADA APLIKASI TANDA TANGAN DIGITAL PRIVYID DENGAN MENGGUNAKAN STANDAR SNI-ISO 27001

Harry Mustika Hadi

13650006

INTISARI

PT. Privy Identitas Digital merupakan perusahaan yang sedang mengembangkan bisnis di dunia teknologi informasi yaitu tanda tangan digital. Aplikasi tanda tangan digital digunakan untuk mengelola data data surat yg harus ditanda tangani dan dikirim langsung secara online. Oleh karena itu, untuk mendapatkan data tentang keamanan data user yang tersimpan, perlu adanya audit dengan menggunakan Standar SNI ISO 27001 sebagai panduan dan pedoman untuk mengukur tingkat kesesuaian manajemen keamanan data user pada perusahaan atau organisasi. Maturity Model digunakan untuk mengukur tingkat kematangan sistem dari kondisi saat ini.

Dari hasil penelitian ini, disimpulkan bahwa tingkat kematangan keamanan data user pada aplikasi tanda tangan digital Privy ID pada skala 2.8 (Defined Process). Menunjukan bahwa pengelolaan keamanan data yang diterapkan oleh PrivyID telah mempunyai perencanaan keamanan data, standar operasional kerja, dan recovery data yang sudah mulai didokumentasikan dan dikomunikasikan sesuai prosedur.

Kata Kunci: Audit Keamanan Data User, SNI-ISO 27001, Maturity Level

AUDIT USER DATA SECURITY ON DIGITAL SIGNATURE APPLICATION PRIVY ID USING SNI-ISO 27001 STANDARD

Harry Mustika Hadi

13650006

ABSTRACT

PT. Privy Digital Identity is a company that is developing business in the world of information technology, specifically digital signatures. The digital signature application is used to manage mail data that must be signed and sent directly online. Therefore, to obtain data about the security of user data, it is necessary to have an audit using the Standard ISO 27001 as a guideline and guideline for measuring the level of conformity of user data security management in companies or organizations. Maturity Model is used to measure the maturity level of the system from the current condition.

From the results of this study, it was concluded that the level of maturity of user data security on digital Privy ID signature applications on a scale 2.8 (Defined Process). Showing that data security management implemented by PrivyID has data security planning, work operational standards, and data recovery that have begin to be documented and communicated according to procedures.

Keywords: Audit User Data Security, SNI-ISO 27001, Maturity Level

BAB I

PENDAHULUAN

1.1. Latar Belakang

Di era modern ini perkembangan laju teknologi sangatlah pesat. Kemampuan dari teknologi tersebut untuk menyediakan informasi yang akurat dan cepat menjadi suatu hal yang penting dari perkembangan tersebut. Bahkan bisa dikatakan bahwa teknologi sudah menjadi bagian dari kehidupan sehari - hari. Perkembangan teknologi yang pesat ini juga turut berimbas kepada berbagai bidang pekerjaan, pendidikan, kedokteran, pemerintahan, maupun kegunaan individual. Yang mana disetiap bidang tersebut menerapkan teknologi sebagai sistem informasi. Bahkan ada perusahaan yang memanfaatkan teknologi tersebut untuk membuat suatu sistem yang memepermudah pekerjaan manusia dengan membuat suatu aplikasi. Tetapi faktor keamanan juga harus selalu diperhatikan dalam setiap sistem. Manajemen data dalam suatu informasi saat ini menjadi hal yang sangat penting, terutama terhadap individu maupun organisasi yang menggunakan teknologi Informasi sebagai pendukung proses bisnisnya. Dukungan keamanan informasi bertujuan agar informasi data yang dimiliki terjamin kerahasiaannya (*confidentiality*), keutuhannya (*integrity*) dan ketersediaannya (*availability*). Salah satu bentuk dukungan keamanan dari data informasi adalah dengan

adanya tata kelola keamanan data dari user yang menggunakan sistem tersebut agar risiko keamanan dapat dikurangi atau dihindari.

Salah satu perusahaan yang memanfaatkan dan mengembangkan teknologi tersebut adalah PrivyID. PrivyID sendiri adalah perusahaan yang bergerak di bidang tanda tangan digital. Perusahaan tersebut membuat suatu sistem dan aplikasi yang mengelola berbagai data tanda tangan yang informasi yang dilekatkan, terasosiasi, atau terkait dengan informasi elektronik lainnya. Aplikasi tersebut dapat digunakan dengan mudah oleh pengguna dimanapun dan kapanpun. Dan semua data dari user yang akan tersimpan dalam database perusahaan PrivyID. Di PrivyID sendiri ditemukan beberapa kekurangan dalam pengamanan data seperti belum dilakukan dekumentasi secara tersusun yang dilakukan secara berkala, proses maintance system juga tidak dilakukan secara berkala dan hanya dilakukan jika ada laporan kerusakan saja.

Mengingat pentingnya informasi data tanda tangan yang ada pada aplikasi PrivyID, maka diperlukan kebijakan tentang keamanan pengelolaan manajemen data yang ada. Kebijakan keamanan terhadap manajemen data yang baik dalam suatu sistem setidaknya mencakup beberapa prosedur seperti prosedur pengendalian dokumen, prosedur pengendalian rekaman prosedur tindakan perbaikan dan pencegahan, dan prosedur penanganan insiden / gangguan keamanan informasi.

Untuk menjamin keamanan data dari user dalam aplikasi tanda tangan digital di PrivyID maka diperlukan audit keamanan didalamnya. Standar yang digunakan untuk melakukan audit keamanan data tersebut adalah Standar SNI

ISO 27001. Penggunaan standar ini dalam audit keamanan dikarenakan sifatnya yang fleksibel dan mudah dikembangankan sesuai kebutuhan, tujuan, dan persyaratan keamanan organisasi/perusahaan. SNI ISO 27001 merupakan dokumen standar Sistem Manajemen Keamanan Informasi (SMKI) atau Information Security Management Systems (ISMS) yang memberikan gambaran secara umum mengenai apa saja yang seharusnya dilakukan dalam usaha pengimplementasian konsep tata kelola keamanan informasi di dalam sebuah oraganisasi.

Maka dari itu penulis ingin mengambil tema audit keamanan dalam manajemen data dengan judul "Audit Keamanan Data User Pada Aplikasi Tanda Tangan Digital PrivyID Dengan Menggunakan Standar SNI – ISO 27001". Dengan adanya penelitian tentang audit kemanan ini diharapkan mampu menambah referensi tentang audit kemanan data user pada setiap aplikasi dan sistem.

1.2. Rumusan Masalah

Berdasarkan penjelasan pada latar belakang diatas, maka perumusan masalah yang didapat yaitu:

a. Bagaimana memberikan penilaian tentang keamanan data user pada aplikasi tanda tangan digital PrivyID dengan menggunakan Standar SNI – ISO 27001.

b. Bagaimana merekomendasikan hasil temuan yang sesuai dengan kondisi riil pada keamanan data user pada aplikasi tanda tangan digital PrivyID dengan menggunakan Standar SNI – ISO 27001.

1.3. Tujuan dan Manfaat Penelitian

1.3.1. Tujuan Penelitian

a. Menghasilkan penilaian audit keamanan data user pada aplikasi tanda tangan digital PrivyID dengan menggunakan Standar SNI – ISO 27001
b. Menghasilkan rekomendasi tata kelola keamanan data user dari hasil temuan sesuai kondisi riil pada aplikasi tanda tangan digital PrivyID dengan menggunakan Standar SNI – ISO 27001

1.3.2. Manfaat Penelitian

a. Mengoptimalkan keamanan data user pada aplikasi dan sistem di aplikasi tanda tangan digital di PrivyID
b. Menghasilkan dokumen temuan dan rekomendasi dari hasil audit keamanan aplikasi tanda tangan digital di PrivyID yang dapat digunakan sebagai dokumentasi pengembangan keamanan data user yang ada.

1.4. Batasan Penelitian

a. Data-data yang dilakukan dalam analisis dan pembuatan masalah adalah data yang diperoleh dari observasi dan wawancara.

b. Analisis yang digunakan adalah metode penilaian (scoring) dengan pendekatan sesuai standar SNI ISO 27001 yaitu maturity level model.
c. Sasaran area kontrol pengamanan dari SNI ISO 27001 yang digunakan adalah Kebijakan Keamanan (A.5), Organisasi Keamanan Informasi (A.6), Pengelolaan Aset (A.7), Manajemen Komunikasi dan Operasi (A.10), Pengendalian Akses (A.11), Akuisisi, pengembangan dan pemeliharaan dari sistem informasi (A.12), Kesesuaian (A.15).
d. Output yang dihasilkan berupa temuan dan rekomendasi hasil audit keamanan data user aplikasi tanda tangan digital di PrivyID.

1.5. Keaslian Penelitian

Penelitian tentang audit sistem informasi telah banyak dilakukan sebelumnya. Namun perbedaan penelitian ini adalah dari pengambilan studi kasus atau objek yang penelitian, serta sasaran area kontrol pengamanan dari SNI ISO 27001. Sedangkan penelitian yang membahas tentang tentang Audit Keamanan Data User Pada Aplikasi Tanda Tangan Digital Privyid Dengan Menggunakan Standar SNI-ISO 27001 belum pernah dilakukan.

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 Keamanan Data Pada Aplikasi Tanda Tangan Digital di PT. PrivyID adalah:

1. Peneliti berhasil melakukan audit menggunakan standar SNI ISO-27001 dan menghasilkan analisis nilai kematangan menggunakan maturity level yang menunjukkan bahwa tingkat keamanan data user pada aplikasi tanda tangan digital PrivyID yaitu sebesar 2,8 (Defined Process), yang artinya proses telah didokumentasikan dan dikomunikasikan, prosedur telah distandarisasi, didokumentasikan, dan dikomunikasikan melalui pelatihan. Proses berada pada keadaan diamanatkan namun kecil kemungkinan penyimpangan dapat terdeteksi.
2. Rekomendasi audit keamanan data pada aplikasi tanda tangan digital untuk setiap proses klausul berhasil disusun berdasarkan analisa hasil audit untuk mengembangkan dan memperbaiki pengelolaan yang diterapkan.

6.2. Saran

Dari keseluruhan penelitian yang telah dilakukan tentunya tidak terlepas dari kekurangan dan kelemahan yang harus diperbaiki dan ditingkatkan.

1. Hendaknya dilakukan audit internal menggunakan standar SNI ISO 27001 secara rutin oleh pihak manajemen PT. Privy Identitas Digital Yogyakarta agar dapat melakukan pengembangan dalam pengelolaan keamanan data dan sistem informasi yang lebih baik.
2. Seluruh Manajemen, baik pimpinan, dan karyawan PT. Privy Identitas Digital Yogyakarta perlu lebih memahami pentingnya manajemen keamanan data dalam mendukung proses kerja guna mencapai visi misi dan tujuan yang ada.

DAFTAR PUSTAKA

Arens dan Loebbecke. 2003. *Auditing Pendekatan Terpadu*. Edisi Indonesia. Jakarta: Penerbit Salemba Empat.

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

Hakim, Rachmad S, dan Sutarto. 2009. *Mastering JavaTM Konsep Pemrograman dan Penerapannya Untuk Membuat Software Aplikasi*. Jakarta: PT. Elex Media Komputindo.

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

Irawan, Arif Fajar.2013.Skripsi. *Sistem Keamanan Pesan Pada Android Gingerbread (2.3.4) Dengan Algoritma Luc*. Jember: Universitas Jember.

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

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

Mulyadi dan Puradiredja, Kanaka. 1998. *Auditing*. Jakarta: Penerbit Salemba Empat.

Santoso, Harip. 2010. *Aplikasi Web/asp.net + cd*. Jakarta: PT. Elex Media Kompitindo

Sarno, Riyanarto dan Iffano, Irsyat. 2009. *Sistem Manajemen Keamanan Informasi*. Surabaya: ITS Press.

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

Tipton, Harold F and Micki, Krause. 2005. *Handbook of Information Security Management*. CRC Press LLC.

Wandani, Henny, Budiman, Muhammad Andri, dan Sharif, Amer, M.Kom.2012.*Implementasi Sistem Keamanan Data dengan Menggunakan Teknik Steganografi End of File (EOF) dan Rabin Public Key Cryptosystem*. Sumatera Utara: Universitas Sumatera Utara.

Wibowo, Muhamad Prabu.2008.*Analisis Tingkat Kematangan (Maturity Level) Pengawasan dan Evaluasi Kinerja Teknologi Informasi Otomasi Perpustakaan Dengan Cobit (Control Objective For Information and Releated Technology): Studi Kasus di Perpustakaan Universitas Indonesia*. Universitas Indonesia.

LAMPIRAN A SURAT IJIN PENELITIAN

KEMENTERIAN AGAMA REPUBLIK INDONESIA
UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA YOGYAKARTA
FAKULTAS SAINS DAN TEKNOLOGI
Alamat: Jln. Marsda Adisucipto telephon 0274519739 fax 0274540971
http://saintek.uin-suka.ac.id Yogyakarta 55281

Nomor : B-2263 /Un.02/DST.1/PN.01.1/11/2017 14 Nopember 2017
Sifat : Penting
Lamp : 1 bendel proposal
Hal : Permohonan Izin Penelitian

Kepada:
Yth. CEO PT Privy ID
Bapak Marshall Pribadi
Di Jl.Kemang Raya No.34 Kemang Jakarta Selatan

Assalamu'alaikum Wr.Wb.

Kami beritahukan bahwa untuk memenuhi penyusunan tugas akhir/skripsi yang berjudul " Audit Keamanan Data User pada Aplikasi Tanda Tangan Digital Privyid dengan Menggunakan Standar SNI-ISO 27001" diperlukan penelitian.
Oleh karena itu, kami mengajukan permohonan kepada PT.Privy ID berkenan memberikan izin penelitian bagi mahasiswa kami,

Nama : Harry Mustika Hadi
NIM : 13650006
Program Studi : Tehnik Informatika
Alamat : Sangkal RT003 Bangunharjo Sewon Bantul Yogyakarta
untuk mengadakan penelitian di : PT.Privy Identitas Digital Yogyakarta
Metode pengumpulan data : Observasi dan wawancara
Adapun waktunya mulai tanggal : 19 November 2017 S.d 30 Desember 2017

Memohon untuk melakukan observasi dan wawancara pengumpulan data di PT Privy Identitas Digital Yogyakarta.
Sebagai bahan pertimbangan bersama ini kami lampirkan :

1. Proposal Skripsi
2. Fotocopy Kartu Tanda Mahasiswa (KTM)
3. Fotocopy Kartu Rencana Studi (KRS)

Demikian surat permohonan ini disampaikan, atas diperkenankannya diucapkan terimakasih.

Wassalamu'alaikum Wr.Wb.

a.n. Dekan,
Wakil Dekan Bidang Akademik,

Agung Fatwanto

Tembusan:
Dekan (sebagai laporan)

LAMPIRAN B AUDIT CHARTER

AUDIT CHARTER

Project ID : SNI-ISO 27001-Audit-01

Project Name : Audit Keamanan Data

Auditor : Harry Mustika Hadi

Penelitian ini berkaitan dengan keamanan data pada aplikasi tanda tangan digital di PT. PrivyID ini menggunakan parameter SNI ISO 27001. Penelitian ini berfokus pada klausul Kebijakan Keamanan, Organisasi Keamanan Informasi, Pengelolaan Aset, Manajemen Komunikasi dan Operasi, Pengendalian Akses, Akuisisi serta pengembangan dan pemeliharaan dari sistem informasi, Kesesuaian.

Project Schedule : Februari

Stakeholder List :

Jabatan	Responden	Audit Clause
CTO	Guritno Adi Saputro, S.Kom.	A.5 Kebijakan Keamanan A.5.1 A.6 Organisasi Keamanan Informasi A.6.1 A.7 Pengelolaan Aset A.7.2
VP IT DEV	Puji Rahmadiyanto, S.T.	A.10 Manajemen Komunikasi dan Operasi A.10.1 A.10.5 A.11 Pengendalian Akses

		A.11.3 A.11.5
Lead Web	Reky Susanto, S.Kom.	A.10 Manajemen Komunikasi dan Operasi A.10.4 A.12 Akuisisi, pengembangan, dan pemeliharaan dari sistem informasi A.12.1 A,12.3
Lead Mobile	Anna Arthdi Putra, S.Kom.	A.12 Akuisisi, pengembangan, dan pemeliharaan dari sistem informasi A.12.2 A,12.5
VP PRODUCT	Patar Hutajulu, A.Md.	A.15 Kesesuaian A.15.1 A.15.2

Yogyakarta, 8 Februari 2018

Mengetahui, Chief Technology Officer

PT. Privy ID

Auditor

Guritno Adi Saputro, S.Kom.

Harry Mustika Hadi

NIM: 13650006

LAMPIRAN C CONTROL OBJECTIVE

CONTROL OBJECTIVE

No	Klausul	Control	Auditee
1	**A.5**	**Kebijakan Keamanan**	
	A.5.1	Kebijakan keamanan jaringan	CTO
2	**A.6**	**Organisasi dan Keamanan Informasi**	
	A.6.1	Mengelola keamanan informasi dalam organisasi.	CTO
3	**A.7**	**Pengelolaan Aset**	
	A.7.2	Klasifikasi Informasi	CTO
4	**A.10**	**Manajemen Komunikasi dan Operasi**	
	A.10.1	Memastikan pengoperasian fasilitas pengolahan informasi secara benar dan aman	VP IT DEV
	A. 10.4	Melindungi integritas dan ketersediaan informasi dan fasilitas pengolahan informasi	Lead Web
	A. 10.5	Melindungi integritas dan ketersediaan informasi dan fasilitas pengolahan informasi.	VP IT DEV
	A. 10.9	Memastikan keamananan layanan elektronik commerce dan keamanan penggunanya.	VP IT DEV
5	**A.11**	**Pengendalian akses**	
	A.11.3	Tanggung jawab pengguna	VP IT DEV
	A.11.5	Pengendalian akses sistem operasi	VP IT DEV

6	**A.12**	**Akuisisi Pemeliharaan dan Perawatan Sistem Informasi**	
	A.12.1	Persyaratan keamanan sistem jaringan	Lead Web
	A. 12.2	Mencegah kesalahan, kehilangan, modifikasi yang tidak sah atau penyalahgunaan informasi dalam aplikasi	Lead Mobile
	A.12.3	Melindungi kerahasiaan, keaslian, atau integritas informasi dengan cara kriptografi	Lead Web
	A. 12.5	Memelihara keamanan perangkat lunak sistem aplikasi dan informasi.	Lead Mobile
7	**A.15**	**Kesesuaian**	
	A.15.1	Mencegah pelanggaran terhadap undang undang, peraturan perundang-undangan atau kewajiban kontrak dan setiap persyaratan Keamanan	VP PRODUCT
	A.15.2	Pemenuhan terhadapat kebijakan kemanan dan standar, dan pemenuhan teknis	VP PRODUCT

LAMPIRAN D MASTER QUESTION

MASTER QUESTION

Klausul	Kode	Question
A.5 Kebijakan Keamanan		
5.1	Q1	Apakah sudah diterapkan kebijakan keamanan informasi?
	Q2	Apabila sudah, apakah kebijakan tesebut dipublikasikan kepada seluruh pegawai?
	Q3	Apakah ada dokumentasi kebijakan keamanan informasi?
	Q4	Apakah petugas selalu mengontrol keamanan informasi secara berkala?
	Q5	Bagaimana prosedur kebijakan keamanan informasi tesebut?
A.6 Organisasi Keamanan Informasi		
6.1	Q6	Apakah sudah ada manajeman keamanan yang aktif dalam organisasi?
	Q7	Apakah arahan yang jelas dan bertanggung jawab terhadap keamanan data yang ada?
	Q8	Apakah sudah ada koordinasi ditiap bagian organisasi dalam kegiatan keamanan data?
	Q9	Apakah ditiap bagian organisasi sudah sesuai dengan fungsi kerjanya?
	Q10	Apakah sudah ada alokasi(bagian) yang bertanggung jawab terhadap kemanan data?
	Q11	Apakah proses otorisasi pengolahan kemanan data sudah diterapkan?
	Q12	Apakah sudah ada perjanjian kerahasiaan keamanan data dalam organisasi?
	Q13	Sebelum dilakukan perjanjian kerahasiaan data, apakah sudah dilakukan identifikasi dan dikaji secara regular?

	Q14	Apakah sudah ada perjanjian kerahasiaan keamanan data dengan pihak berwenang?
	Q15	Apakah sudah ada perjanjian kerahasiaan keamanan data dengan pihak khusus penanganan keamanan data?
	Q16	Apakah sudah diterapkan pendekatan dalam organisasi dalam mengelola keamanan data jika terjadi perubahan terhadap penerapannya?
	Q17	Apakah selama ini sudah berhasil menerapkan keamanan data yang sesuai?
A.7 Pengelolaan Aset		
7.2	Q18	Apakah ada pengklasifikasian data yang dapat diakses oleh user dalam aplikasi tanda tangan digital Privy ID?
	Q19	Apakah prosedur pengklasifikasian data tersebut sudah diterapkan?
A.10 Manajemen Komunikasi dan Operasi		
10.1	Q20	Apakah pengoperasian fasilitas pengolahan informasi data (Maintenance Server) sudah dilakukan secara benar dan aman?
	Q21	Jika ada kesalahan operasi dan kesulitan teknis, apakah akan meminta bantuan pengelola/pegawai lain-nya?
	Q22	Apakah (back-up data) sudah di dipelihara serta sudah dilakukan sesuai prosedur?
	Q23	Jika ada perubahan terhadap fasilitas dan sistem pengolahan informasi apakah sudah di kontrol dan dikendalikan?
	Q24	Apakah sudah dilakukan pencatatan perubahan dan perubahan tersebut sudah disosialisasikan ke semua pihak?
	Q25	Apakah pegawai di ruang sistem informasi pengolahan data di PrivyID sudah dipisahkan menurut tugas dan tanggung jawabnya masing-masing?

	Q26	Untuk mengurangi resiko insiden memodifikasi tanpa ijin atau penyalahgunaan sistem, apakah ada pengawasan dan pemantauan?
	Q27	Apakah sudah terdapat fasilitas untuk pengembangan, pengujian, dan operasional sudah dipisahkan untuk mengurangi resiko akses/perubahan yang tidak sah kedalam sistem?
10.4	Q28	Apakah pendeteksian sejak awal sudah dilakukan untuk pengendalian terhadap malicious code (malware)?
	Q29	Apakah sudah diterapkan sistem keamanan untuk mencegah serangan malicious code (malware)?
	Q30	Apakah ada prosedur yang diterapkan untuk memulikan data sistem/user jika terkena serangan malicious code (malware)?
10.5	Q31	Apakah salinan back-up dan piranti lunak yang penting sudah dilakukan secara berkala?
	Q32	Apakah fasilitas back-up sudah memadai guna memulihkan seluruh sisitem informasi jika terjadi bencana atau kegagalan?
	Q33	Catatan yang akurat dari salinan back-up dan prosedur pemulihan yang terdokumentasi apakah sudah disimpan di lokasi terpisah?
	Q34	Apakah media back-up sudah di uji secara berkala untuk memastikan bisa digunakan di situasi darurat?
A.11 Pengendalian Akses		
11.3	Q35	Apakah sudah ada prosedur validasi data pengguna?
	Q36	Apakah petugas selalu meninjau ulang terhadap hak akses user secara berkala?
	Q37	Apakah sudah ada sistem manajemen password dan sistem pengelola password untuk mengelola kwalitas password?
	Q38	Apakah user mengubah password dalam sistem tersebut?

	Q39	Adakah ada petunjuk untuk membuat kombinasi password yang baik?
	Q40	Ketika mengisi password, apakah sudah diterapkan ada sistem clear screen password?
	Q41	Apakah anda (pegawai) pernah memberikan password ke orang lain?
	Q42	Apakah anda (pegawai) pernah meninggalkan komputer tanpa logout dari sistem tanda tangan digital?
11.5	Q43	Apakah sudah ada prosedur log on?
	Q44	Apakah setiap user memiliki akun / USER ID untuk penggunaan personal masing-masing user?
	Q45	Apakah user diberikan pelatihan penggunaan aplikasi dan sistem yang benar dan aman?
	Q46	Apakah saat anda mengganti password ada kombinasi yang unik?
	Q47	Apakah ada pengamanan data user dari pengguna luar?
	Q48	Apakah ada prosedur batasan jangka waktu pemakaian akun user?
	Q49	Apakah adanya prosedur penonaktifan akun user guna memastikan tidak adanya pemakaian ulang?
	Q50	Apakah sudah ada sistem manajemen password?
	Q51	Apakah ada sosialisasi password yang interaktif?
	Q52	Bagaimana prosedur maintenance aplikasi tanda tangan digital apakah sudah berjalan dengan baik?
	Q53	Apakah aplikasi tanda tangan digital sudah menerapkan mekanisme session time out?
A.12 Akuisisi, pengembangan dan pemeliharaan dari sistem informasi		
12.1	Q54	Apakah keamanan dalam sistem yang dibangun sudah termasuk dalam bussiness statements?
	Q55	Apakah prosedur business statement sudah berjalan?

	Q56	Apakah ada kesulitan saat menerapkan prosedur tersebut?
	Q57	Pada saat sistem informasi berjalan, apakah rancangan keamanan data pada aplikasi tanda tangan digital sudah terimplementasi?
	Q58	Pada tahap perancangan sistem dan aplikasi tanda tangan digital, apakah keamanan data yang dibangun sudah termasuk dalam perancangan?
	Q59	Adakah klasifikasi pembagian tugas dalam penanganan serangan sistem dan aplikasi?
	Q60	Apabila terjadi serangan pada data aplikasi, apakah sudah diterapkan mekanisme penanganan sesuai serangannya?
	Q61	Apakah ada monitoring manajemen terhadap mekanisme pengolahan data yang ada?
	Q62	Apakah sudah ada dokumentasi mekanisme pengamanan pada data sitem?
	Q63	Apakah petugas selalu mengidentifikasi titik kelemahan aplikasi dan sistem?
	Q64	Apakah petugas melakukan pengujian ttitik kelemahan sistem yang sudah teidentifikasi?
12.2	Q65	Apakah sudah terdapat sistem validasi saat melakukan dalam aplikasi?
	Q66	Apakah sudah terdapat sistem validasi saat login dalam aplikasi?
	Q67	Apakah sudah ada pengecekan validasi jika ID yang di masukkan salah?
	Q68	Untuk memastikan keaslian identitas pendaftar, apakah sudah diterapkan validasi yang tepat?
	Q69	Apakah sudah ada perlindungan integritas pesan dalam aplikasi?

	Q70	Apakah sudah diterapkan mekanisme yang benar dalam pengendalian integritas pesan?
	Q71	Untuk memastikan bahwa pengolahan informasi yang disimpan adalah benar, apakah validasi data keluaran begitu penting?
	Q72	Apakah keluaran data dari aplikasi sudah divalidasi?
12.3	Q73	Apakah sistem keamanan dengan kriptografi dapat digunakan dalam sistem tanda tangan digital Privy ID?
	Q74	Apakah sistem sudah dilindungi dengan sistem kriptografi?
	Q75	Apakah integritas data user tidak diketahui oleh user lain?
	Q76	Apakah keamanan sistem telah diterapkan, dan dirasa aman, dan tidak ada masalah penyerangan sejauh ini?
12.5	Q77	Apakah sudah ada prosedur pengendalian perubahan yang formal?
	Q78	Apakah pengendalian perubahan harus diterapkan?
	Q79	Bila sistem operasi di ubah, apakah sistem dalam aplikasi tanda tangan digital ditinjau dan di uji kembali untuk memastikan tidak ada dampak yang merugikan?
	Q80	Apakah penting menjaga keamanan data aplikasi tanda tangan digital Privy ID ketika dilakukan perubahan sistem operasi?
	Q81	Apakah sering melakukan modifikasi perangkat lunak/aplikasi?
	Q82	Apakah modifikasi perangkat lunak/aplikasi sudah dibatasi?
	Q83	Apakah seluruh perubahan sudah dikendalikan?
	Q84	Apakah sudah dilakukan pencegahan terhadap peluang kebocoran informasi data?
	Q85	Apakah sudah dilakukan prosedur pencegahannya?
	Q86	Apakah sudah dilakukan supervisi dan dipantau pengembangan terhadap perangkat lunak/aplikasi yang dialihdayakan?

A.15 Kesesuaian		
15.1	Q87	Apakah dilakukan pemutakhiran sistem informasi dan organisasi sesuai dengan peraturan undang undang?
	Q88	Apakah prosedur sudah sesuai dengan peraturan hukum tentang hak kekayaan intelektual?
	Q89	Apakah perangkat lunak sudah memiliki hak paten?
	Q90	Apakah organisasi sudah dilindungi peraturan hukum?
	Q91	Apakah perlindungan data dan kerhasiaannya sudah dijamin oleh hukum?
	Q92	Apakah data yang ada dan digunakan dijamin legalitas sesuai hukum?
	Q93	Apakah pengendalian dan penerapan kriptografi sudah sesuai dangan peraturan yang ada?
15.2	Q94	Apakah kemanan data yang ada sudah sesuai dengan standar yang diterapkan?

LAMPIRAN E FORM QUESTION

FORM QUESTIONS

Document ID : FQ

Document Name : Form Question

Dokumen ini digunakan sebagai acuan pemetaan pertanyaan yang akan digunakan saat proses audit

Form Question 1 (FQ1): CTO

Q1, Q2, Q3, Q4, Q5, Q6, Q7, Q8, Q9, Q10, Q11, Q12, Q13, Q14, Q15, Q16, Q17, Q18, Q19

Form Question 2 (FQ2): VP IT DEV

Q20, Q21, Q22, Q23, Q24, Q25, Q26, Q27, Q31. Q32, Q33, Q34, Q35, Q36, Q37, Q38, Q39, Q40, Q41, Q42, Q43, Q44, Q45, Q46, Q47, Q48, Q49, Q50, Q51, Q52, Q53,

Form Question 3 (FQ2): Lead Web

Q28, Q29, Q30, Q54, Q55, Q56, Q57, Q58, Q59, Q60, Q61, Q62, Q63, Q64, Q71, Q72, Q73, Q74,, Q75, Q76

Form Question 4 (FQ2): Lead Mobile

Q65, Q66, Q67, Q68, Q69, Q70, Q71, Q72, Q77, Q78, Q79, Q80, Q81, Q82, Q83, Q84, Q85, Q86

Form Question 5 (FQ3): VP PRODUCT

Q87, Q88, Q89, Q90, Q91, Q92, Q93, Q94

LAMPIRAN F MATURITY MODEL

MATURITY MODEL

No	Tingkat Kematangan	Definisi
1	0 – (Non-Exisent)	Proses manajemen tidak diterapkan sama sekali. Semua proses tidak dapat diidentifikasi dan dikenali. Status kesiapan keamanan informasi tidak diketahui.
2	1 – (Initial/Ad Hoc)	Mulai adanya pemahaman mengenai perlunya pengelolaan keamanan informasi. Penerapan langkah pengamanan masih bersifat reaktif, tidak teratur, tidak mengacu kepada keseluruhan resiko yang ada, tanpa alur komunikasi, dan kewenangan yang jelas dan tanpa pengawasan, Kelemahan teknis dan nonteknis tidak teridentifikasi dengan baik, pihak yang terlibat tidak menyadari tanggung jawab mereka.
3	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.
4	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.
5	4 – (Managed and Measuble	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.
6	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 Data Pada Aplikasi Tanda Tangan Digital

PT. Privy Identitas Digital Yogyakarta

Menggunakan Standar SNI ISO 27001

Document ID : FQ1-CTO

Project Name : Audit Keamanan Data User Pada Aplikasi Tanda Tangan Digital PrivyID Dengan Menggunakan Standar SNI-ISO 27001

Auditor : Harry Mustika Hadi

Auditee : Guritno Adi Saputro, S.Kom

Description : Lembar kertas kerja audit ini merupakan bagian dari penelitian tugas akhir mahasiswa Program Studi Teknik Informatika, UIN Sunan Kalijaga Yogyakarta. Lembar kerja audit ini digunakan untuk mengevaluasi manajemen yang diterapkan oleh pengelola kemanan data aplikasi tanda tangan digital di PT. Privy ID Yogyakartwa.

Date : 8 Februari 2018

Responsible : Chief Technology Officer (CTO)

CTO

Guritno Adi Saputro, S.Kom

Auditor

Harry Mustika Hadi

FQ1-CTO								
No	**Code**	**Questions**	**Score**					
			0	**1**	**2**	**3**	**4**	**5**
1	Q1	Apakah sudah diterapkan kebijakan keamanan informasi?						
2	Q2	Apabila sudah, apakah kebijakan tesebut dipublikasikan kepada seluruh pegawai?						
3	Q3	Apakah ada dokumentasi kebijakan keamanan informasi?						
4	Q4	Apakah petugas selalu mengontrol keamanan informasi secara berkala?						
5	Q5	Bagaimana prosedur kebijakan keamanan informasi tesebut?						
6	Q6	Apakah sudah ada manajeman keamanan yang aktif dalam organisasi?						
7	Q7	Apakah arahan yang jelas dan bertanggung jawab terhadap keamanan data yang ada?						
8	Q8	Apakah sudah ada koordinasi ditiap bagian organisasi dalam kegiatan keamanan data?						

9	Q9	Apakah ditiap bagian organisasi sudah sesuai dengan fungsi kerjanya?						
10	Q10	Apakah sudah ada alokasi(bagian) yang bertanggung jawab terhadap kemanan data?						
11	Q11	Apakah proses otorisasi pengolahan kemanan data sudah diterapkan?						
12	Q12	Apakah sudah ada perjanjian kerahasiaan keamanan data dalam organisasi?						
13	Q13	Sebelum dilakukan perjanjian kerahasiaan data, apakah sudah dilakukan identifikasi dan dikaji secara regular?						
14	Q14	Apakah sudah ada perjanjian kerahasiaan keamanan data dengan pihak berwenang?						
15	Q15	Apakah sudah ada perjanjian kerahasiaan keamanan data dengan pihak khusus penanganan keamanan data?						
16	Q16	Apakah sudah diterapkan pendekatan dalam organisasi dalam mengelola keamanan data jika terjadi perubahan terhadap penerapannya?						

17	Q17	Apakah selama ini sudah berhasil menerapkan keamanan data yang sesuai?						
18	Q18	Apakah ada pengklasifikasian data yang dapat diakses oleh user dalam aplikasi tanda tangan digital Privy ID?						
19	Q19	Apakah prosedur pengklasifikasian data tersebut sudah diterapkan?						

Lembar Kertas Kerja Audit

Audit Keamanan Data Pada Aplikasi Tanda Tangan Digital

PT. Privy Identitas Digital Yogyakarta

Menggunakan Standar SNI ISO 27001

Document ID : FQ2-VP IT DEV

Project Name : Audit Keamanan Data User Pada Aplikasi Tanda Tangan Digital PrivyID Dengan Menggunakan Standar SNI-ISO 27001

Auditor : Harry Mustika Hadi

Auditee : Puji Rahmadiyanto, S.T.

Description : Lembar kertas kerja audit ini merupakan bagian dari penelitian tugas akhir mahasiswa Program Studi Teknik Informatika, UIN Sunan Kalijaga Yogyakarta. Lembar kerja audit ini digunakan untuk mengevaluasi manajemen yang diterapkan oleh pengelola kemanan data aplikasi tanda tangan digital di PT. PrivyID Yogyakarta.

Date : 19 Februari 2018

Responsible : VP IT DEV

VP IT DEV

Puji Rahmadiyanto, S.T.

Auditor

Harry Mustika Hadi

FQ2-VP IT DEV									
No	**Code**	**Questions**	**Score**						
			0	**1**	**2**	**3**	**4**	**5**
1	Q20	Apakah pengoperasian fasilitas pengolahan informasi data (Maintenance Server) sudah dilakukan secara benar dan aman?						
2	Q21	Jika ada kesalahan operasi dan kesulitan teknis, apakah akan meminta bantuan pengelola/pegawai lain-nya?						
3	Q22	Apakah (back-up data) sudah di dipelihara serta sudah dilakukan sesuai prosedur?						
4	Q23	Jika ada perubahan terhadap fasilitas dan sistem pengolahan informasi apakah sudah di kontrol dan dikendalikan?						
5	Q24	Apakah sudah dilakukan pencatatan perubahan dan perubahan tersebut sudah disosialisasikan ke semua pihak?						
6	Q25	Apakah pegawai di ruang sistem informasi pengolahan data di PrivyID sudah dipisahkan menurut tugas dan tanggung jawabnya masing-masing?						

7	Q26	Untuk mengurangi resiko insiden memodifikasi tanpa ijin atau penyalahgunaan sistem, apakah ada pengawasan dan pemantauan?						
8	Q27	Apakah sudah terdapat fasilitas untuk pengembangan, pengujian, dan operasional sudah dipisahkan untuk mengurangi resiko akses/perubahan yang tidak sah kedalam sistem?						
9	Q31	Apakah salinan back-up dan piranti lunak yang penting sudah dilakukan secara berkala?						
10	Q32	Apakah fasilitas back-up sudah memadai guna memulihkan seluruh sisitem informasi jika terjadi bencana atau kegagalan?						
11	Q33	Catatan yang akurat dari salinan back-up dan prosedur pemulihan yang terdokumentasi apakah sudah disimpan di lokasi terpisah?						
12	Q34	Apakah media back-up sudah di uji secara berkala untuk memastikan bisa digunakan di situasi darurat?						
13	Q35	Apakah sudah ada prosedur validasi data pengguna?						
14	Q36	Apakah petugas selalu meninjau ulang terhadap hak akses user secara berkala?						
15	Q37	Apakah sudah ada sistem manajemen password dan sistem pengelola password untuk mengelola kwalitas password?						

16	Q38	Apakah user mengubah password dalam sistem tersebut?						
17	Q39	Adakah ada petunjuk untuk membuat kombinasi password yang baik?						
18	Q40	Ketika mengisi password, apakah sudah diterapkan ada sistem clear screen password?						
19	Q41	Apakah anda (pegawai) pernah memberikan password ke orang lain?						
20	Q42	Apakah anda (pegawai) pernah meninggalkan komputer tanpa logout dari sistem tanda tangan digital?						
21	Q43	Apakah sudah ada prosedur log on?						
22	Q44	Apakah setiap user memiliki akun / USER ID untuk penggunaan personal masing-masing user?						
23	Q45	Apakah user diberikan pelatihan penggunaan aplikasi dan sistem yang benar dan aman?						
24	Q46	Apakah saat anda mengganti password ada kombinasi yang unik?						
25	Q47	Apakah ada pengamanan data user dari pengguna luar?						
26	Q48	Apakah ada prosedur batasan jangka waktu pemakaian akun user?						

27	Q49	Apakah adanya prosedur penonaktifan akun user guna memastikan tidak adanya pemakaian ulang?						
28	Q50	Apakah sudah ada sistem manajemen password?						
29	Q51	Apakah ada sosialisasi password yang interaktif?						
30	Q52	Bagaimana prosedur maintenance aplikasi tanda tangan digital apakah sudah berjalan dengan baik?						
31	Q53	Apakah aplikasi tanda tangan digital sudah menerapkan mekanisme session time out?						

Lembar Kertas Kerja Audit

Audit Keamanan Data Pada Aplikasi Tanda Tangan Digital

PT. Privy Identitas Digital Yogyakarta

Menggunakan Standar SNI ISO 27001

Document ID : FQ3-Lead Web

Project Name : Audit Keamanan Data User Pada Aplikasi Tanda Tangan Digital PrivyID Dengan Menggunakan Standar SNI-ISO 27001

Auditor : Harry Mustika Hadi

Auditee : Reky Susanto, S.Kom.

Description : Lembar kertas kerja audit ini merupakan bagian dari penelitian tugas akhir mahasiswa Program Studi Teknik Informatika, UIN Sunan Kalijaga Yogyakarta. Lembar kerja audit ini digunakan untuk mengevaluasi manajemen yang diterapkan oleh pengelola kemanan data aplikasi tanda tangan digital di PT. PrivyID Yogyakarta.

Date : 19 Februari 2018

Responsible : Lead Web

Lead Web

Reky Susanto, S.Kom.

Auditor

Harry Mustika Hadi

FQ3-Lead Web								
No	**Code**	**Questions**	**Score**					
			0	**1**	**2**	**3**	**4**	**5**
1	Q28	Apakah pendeteksian sejak awal sudah dilakukan untuk pengendalian terhadap malicious code (malware)?						
2	Q29	Apakah sudah diterapkan sistem keamanan untuk mencegah serangan malicious code (malware)?						
3	Q30	Apakah ada prosedur yang diterapkan untuk memulikan data sistem/user jika terkena serangan malicious code (malware)?						
4	Q54	Apakah keamanan dalam sistem yang dibangun sudah termasuk dalam bussiness statements?						
5	Q55	Apakah prosedur business statement sudah berjalan?						
6	Q56	Apakah ada kesulitan saat menerapkan prosedur tersebut?						
7	Q57	Pada saat sistem informasi berjalan, apakah rancangan keamanan data pada aplikasi tanda tangan digital sudah terimplementasi?						

8	Q58	Pada tahap perancangan sistem dan aplikasi tanda tangan digital, apakah keamanan data yang dibangun sudah termasuk dalam perancangan?						
9	Q59	Adakah klasifikasi pembagian tugas dalam penanganan serangan sistem dan aplikasi?						
10	Q60	Apabila terjadi serangan pada data aplikasi, apakah sudah diterapkan mekanisme penanganan sesuai serangannya?						
11	Q61	Apakah ada monitoring manajemen terhadap mekanisme pengolahan data yang ada?						
12	Q62	Apakah sudah ada dokumentasi mekanisme pengamanan pada data sitem?						
13	Q63	Apakah petugas selalu mengidentifikasi titik kelemahan aplikasi dan sistem?						
14	Q64	Apakah petugas melakukan pengujian ttitik kelemahan sistem yang sudah teidentifikasi?						
15	Q73	Apakah sistem keamanan dengan kriptografi dapat digunakan dalam sistem tanda tangan digital Privy ID?						
16	Q74	Apakah sistem sudah dilindungi dengan sistem kriptografi?						

17	Q75	Apakah integritas data user tidak diketahui oleh user lain?						
18	Q76	Apakah keamanan sistem telah diterapkan, dan dirasa aman, dan tidak ada masalah penyerangan sejauh ini?						

Lembar Kertas Kerja Audit

Audit Keamanan Data Pada Aplikasi Tanda Tangan Digital

PT. Privy Identitas Digital Yogyakarta

Menggunakan Standar SNI ISO 27001

Document ID : FQ4-Lead Mobile

Project Name : Audit Keamanan Data User Pada Aplikasi Tanda Tangan Digital PrivyID Dengan Menggunakan Standar SNI-ISO 27001

Auditor : Harry Mustika Hadi

Auditee : Anna Arthdi Putra, S.Kom.

Description : Lembar kertas kerja audit ini merupakan bagian dari penelitian tugas akhir mahasiswa Program Studi Teknik Informatika, UIN Sunan Kalijaga Yogyakarta. Lembar kerja audit ini digunakan untuk mengevaluasi manajemen yang diterapkan oleh pengelola kemanan data aplikasi tanda tangan digital di PT. PrivyID Yogyakarta.

Date : 19 Februari 2018

Responsible : Lead Mobile

Lead Mobile

Anna Arthdi Putra, S.Kom.

Auditor

Harry Mustika Hadi

FQ4-Lead Mobile									
No	**Code**	**Questions**	**Score**						
			0	**1**	**2**	**3**	**4**	**5**
1	Q65	Apakah sudah terdapat sistem validasi saat melakukan dalam aplikasi?						
2	Q66	Apakah sudah terdapat sistem validasi saat login dalam aplikasi?						
3	Q67	Apakah sudah ada pengecekan validasi jika ID yang di masukkan salah?						
4	Q68	Untuk memastikan keaslian identitas pendaftar, apakah sudah diterapkan validasi yang tepat?						
5	Q69	Apakah sudah diterapkan validasi saat memasukkan data?						
6	Q70	Apakah sudah diterapkan validasi saat melakukan pengolahan data yang disimpan?						
7	Q71	Untuk memastikan bahwa pengolahan informasi yang disimpan adalah benar, apakah validasi data keluaran begitu penting?						

8	Q72	Apakah keluaran data dari aplikasi sudah divalidasi?						
9	Q77	Apakah sudah ada prosedur pengendalian perubahan yang formal?						
10	Q78	Apakah pengendalian perubahan harus diterapkan?						
11	Q79	Bila sistem operasi di ubah, apakah sistem dalam aplikasi tanda tangan digital ditinjau dan di uji kembali untuk memastikan tidak ada dampak yang merugikan?						
12	Q80	Apakah penting menjaga keamanan data aplikasi tanda tangan digital Privy ID ketika dilakukan perubahan sistem operasi?						
13	Q81	Apakah sering melakukan modifikasi perangkat lunak/aplikasi?						
14	Q82	Apakah modifikasi perangkat lunak/aplikasi sudah dibatasi?						
15	Q83	Apakah seluruh perubahan sudah dikendalikan?						
16	Q84	Apakah sudah dilakukan pencegahan terhadap peluang kebocoran informasi data?						
17	Q85	Apakah sudah dilakukan prosedur pencegahannya?						
18	Q86	Apakah sudah dilakukan supervisi dan dipantau pengembangan terhadap perangkat lunak/aplikasi yang dialihdayakan?						

Lembar Kertas Kerja Audit

Audit Keamanan Data Pada Aplikasi Tanda Tangan Digital

PT. Privy Identitas Digital Yogyakarta

Menggunakan Standar SNI ISO 27001

Document ID : FQ5-VP PRODUCT

Project Name : Audit Keamanan Data User Pada Aplikasi Tanda Tangan Digital PrivyID Dengan Menggunakan Standar SNI-ISO 27001

Auditor : Harry Mustika Hadi

Auditee : Patar Hutajulu, A.Md.

Description : Lembar kertas kerja audit ini merupakan bagian dari penelitian tugas akhir mahasiswa Program Studi Teknik Informatika, UIN Sunan Kalijaga Yogyakarta. Lembar kerja audit ini digunakan untuk mengevaluasi manajemen yang diterapkan oleh pengelola kemanan data aplikasi tanda tangan digital di PT. PrivyID Yogyakarta.

Date : 19 Februari 2018

Responsible : VP PRODUCT

VP PRODUCT

Patar Hutajulu, A.Md.

Auditor

Harry Mustika Hadi

FQ5-VP PRODUCT									
No	**Code**	**Questions**	**Score**						
			0	**1**	**2**	**3**	**4**	**5**
1	Q87	Apakah dilakukan pemutakhiran sistem informasi dan organisasi sesuai dengan peraturan undang undang?						
2	Q88	Apakah prosedur sudah sesuai dengan peraturan hukum tentang hak kekayaan intelektual?						
3	Q89	Apakah perangkat lunak sudah memiliki hak paten?						
4	Q90	Apakah organisasi sudah dilindungi peraturan hukum?						
5	Q91	Apakah perlindungan data dan kerhasiaannya sudah dijamin oleh hukum?						
6	Q92	Apakah data yang ada dan digunakan dijamin legalitas sesuai hukum?						
7	Q93	Apakah pengendalian dan penerapan kriptografi sudah sesuai dangan peraturan yang ada?						
8	Q94	Apakah kemanan data yang ada sudah sesuai dengan standar yang diterapkan?						

LAMPIRAN H HASIL EVALUASI AUDIT

HASIL EVALUASI AUDIT

Klausul	Kode	Score	Score Maturity
A.5 Kebijakan Keamanan			
5.1	Q1	4	**2.8**
	Q2	2	
	Q3	3	
	Q4	2	
	Q5	3	
A.6 Organisasi Keamanan Informasi			
6.1	Q6	4	**2.9**
	Q7	3	
	Q8	3	
	Q9	3	
	Q10	3	
	Q11	2	
	Q12	3	
	Q13	3	
	Q14	4	
	Q15	1	
	Q16	3	
	Q17	3	
A.7 Pengelolaan Aset			
7.2	Q18	3	**3.0**
	Q19	3	
A.10 Manajemen Komunikasi dan Operasi			
10.1	Q20	3	**2.4**
	Q21	3	

	Q22	4	
	Q23	3	
	Q24	2	
	Q25	2	
	Q26	2	
	Q27	3	
10.4	Q28	1	
	Q29	1	
	Q30	2	
10.5	Q31	3	
	Q32	3	
	Q33	3	
	Q34	2	
A.11 Pengendalian Akses			
11.3	Q35	3	**2.5**
	Q36	3	
	Q37	2	
	Q38	2	
	Q39	2	
	Q40	3	
	Q41	3	
	Q42	3	
11.5	Q43	3	
	Q44	5	
	Q45	0	
	Q46	2	
	Q47	3	
	Q48	2	
	Q49	3	
	Q50	3	

	Q51	0	
	Q52	3	
	Q53	3	
A.12 Akuisisi, Pengembangan dan Pemeliharaan dari Sistem Informasi			
12.1	Q54	3	**2.5**
	Q55	3	
	Q56	2	
	Q57	3	
	Q58	3	
	Q59	2	
	Q60	2	
	Q61	2	
	Q62	3	
	Q63	2	
	Q64	2	
12.2	Q65	3	
	Q66	3	
	Q67	3	
	Q68	3	
	Q69	3	
	Q70	2	
	Q71	2	
	Q72	2	
12.3	Q73	3	
	Q74	3	
	Q75	3	
	Q76	3	
12.5	Q77	1	
	Q78	2	

	Q79	3	
	Q80	3	
	Q81	1	
	Q82	2	
	Q83	2	
	Q84	3	
	Q85	3	
	Q86	3	
A.15 Kesesuaian			
15.1	Q87	3	**3.5**
	Q88	4	
	Q89	3	
	Q90	5	
	Q91	4	
	Q92	3	
	Q93	3	
15.2	Q94	3	
Total Maturity			**2.8**

CURRICULUM VITAE

Nama	: Harry Mustika Hadi
Tempat, Tanggal lahir	: Bantul, 22 Maret 1995
Jenis Kelamin	: Laki-laki
Status	: Belum menikah
Agama	: Islam
Nama Ayah	: Suharno
Nama Ibu	: Umi Maryani
Alamat	: Sangkal RT03 Dk. Tarudan, Ds. Bangunharjo, Kec. Sewon, Kab. Bantul, DIY
No.HP	: 085875885611
Email	: harryhadi0@gmail.com

Riwayat Pendidikan :

2001-2007	: SD N Jurug
2007-2010	: SMP N 2 Sewon
2010-2013	: SMA N 1 Imogiri
2013-2019	: Program Studi Teknik Informatika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Sunan Kalijaga Yogyakarta