ANALISIS KEAMANAN DATA PEGAWAI MENGGUNAKAN PENDEKATAN ISO/IEC 27001: 2013

(Studi Kasus :PT.Indonesia Power UPJP Kamojang)

TUGAS AKHIR

Disusun sebagai salah satu syarat untuk kelulusan Program Strata 1,
di Program Studi Teknik Informatika, Universitas Pasundan Bandung

oleh :

Valentina Gobasi
NRP : 13.304.0168

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS PASUNDAN BANDUNG
MARET 2019

LEMBAR PENGESAHAN

LAPORAN TUGAS AKHIR

Telah diujikan dan dipertahankan dalam Sidang Sarjana Program Studi Teknik Informatika Universitas Pasundan Bandung, pada hari dan tanggal sidang sesuai berita acara sidang, tugas akhir dari :

Nama : Valentina Gobasi

Nrp : 13.304.0168

Dengan judul:

"ANALISIS KEAMANAN DATA PEGAWAI MENGGUNAKAN PENDEKATAN ISO/ IEC 27001 : 2013"

(Studi Kasus : PT. Indonesia Power UPJP Kamojang)

Bandung, 02 Maret 2019

Menyetujui,

Pembimbing Utama,

(Rita Rijayanti, S.T., M.T.)

ABSTRAK

Keamanan informasi telah menjadi hal yang sangat penting dalam dunia bisnis yang menggunakan teknologi informasi (TI), perannya dalam melakukan kegiatan operasional sehari-hari dapat dikatakan tidak terganti, karena hampir seluruh kegiatan yang dilakukan melibatkan penggunaan teknologi informasi. Namun tidak selamanya dalam penggunaan teknologi informasi sesuai dengan harapan,misalnya keamanan informasi mengalami masalah terkait kerahasiaannya (*confidentiality)*, keutuhannya (*integrity*), dan ketersediaannya (*availability)* dalam penggunaanya muncul berbagai risiko yang dapat mengakibatkan kerugian yang besar bagi perusahaan hingga merugi, risiko-risiko yang timbul ini harus ditangani agar masalah yang ditimbulkan tidak menyebabkan kerugian pada perusahaan sehingga dapat menjamin kelanjutan bisnis, serta memberikan keuntungan bagi organisasi (Riyanarto dan Irsyat, 2009).

Penelitian ini dilakukan untuk dapat membantu mengurangi masalah keamanan informasi di PT. Indonesia Power UPJP Kamojang, sehingga dapat meminimalisir terjadinya ancaman atau risiko yang dapat membahayakan atau merugikan PT. Indonesia Power UPJP Kamojang. Penelitian dilakukan dengan melalukan studi literatur serta memahami konsep-konsep keamanan informasi. Selanjutnya dilakukan analisis risiko yaitu untuk mengetahui seberapa besar risiko yang akan diterima oleh organisasi dan merekomendasikan keamanan data pegawai PT. Indonesia Power UPJP Kamojang yang di dalamnya memaparkan tentang mekanisme penanganan keamanan terhadap setiap ancaman yang akan mengakibatkan risiko di kemudian hari.

Hasil akhir dari penelitian ini adalah sebuah rekomendasi untuk identifikasi risiko keamanan data pegawai PT. Indonesia Power UPJP Kamojang berdasarkan standar ISO/IEC 27001:2013.

Kata Kunci : Keamanan Informasi, Risiko, Teknologi Informasi, ISO/IEC 27001:2013

ABSTRACT

Information security has become a very important thing in the world of business that uses information technology (IT), it's role in carrying out daily operations can be said not to be replaced, because almost all activities carried out involve the use of information technology. But not always in the use of information technology in accordance with expectations, for example information security has problems related to confidentiality, integrity and availability in the use of a variety of risks arise that can lead to large losses for the company to lose money, these arising risks must be addressed so that the problems caused do not cause harm to the company so that it can guarantee the continuation of the business, provide benefits for the organization (Riyanarto dan Irsyat, 2009).

This research is conducted to help reduce the problem of information security at PT. Indonesia Power UPJP Kamojang, so it can minimize the occurrence of threat or risk that can harm or harm the PT. Indonesia Power UPJP Kamojang. Research is done by conducting literature studies as well as understanding information security concepts. Furthermore, risk analysis is done to find out how big the risks will be accepted by the organization and recommend employee data security at PT. Indonesia Power UPJP Kamojang in which describes the mechanism of handling security against any threats that will lead to risk in the future.

The end result of this research is a recommendation to identify employee data security risk at PT. Indonesia Power UPJP Kamojang based on ISO/IEC 27001:2013 standard.

Keywords : Information Security, Risk, Information Technology, ISO/IEC 27001:2013.

DAFTAR ISI

UNIVERSITAS
PASUNDAN

BAB 1
PENDAHULUAN

Pada bab ini berisi Latar Belakang Masalah, Identifikasi masalah, Tujuan Tugas Akhir, Lingkup Tugas Akhir dan Sistematika Penulisan Tugas Akhir.

1.1. Latar Belakang

Keamanan data pada saat ini menjadi hal yang sangat penting terutama terhadap organisasi yang menggunakan Teknologi Informasi (TI) sebagai pendukung proses bisnisnya. Kinerja TI akan terganggu jika keamanan informasi sebagai aspek penting mengalami masalah terkait kerahasiaannya (*confidentiality*), keutuhannya (*integrity*), dan ketersediaannya (*availability*). (Riyanarto dan Irsyat, 2009) [SAR09].

Ancaman terhadap keamanan data di PT. Indonesia Power semakin meningkat dengan adanya penyalahgunaan pada data Pegawai di PT. Indonesia Power oleh pihak yang tidak berhak. Data tersebut adalah data keuangan dan data pegawai yang sangat penting bagi proses bisnis Indonesia Power oleh karena itu jika terjadi kehilangan, kerusakan atau bahkan pengubahan data akan sangat berdampak bagi kelangsungan proses bisnis di PT. Indonesia Power. Data merupakan segala fakta yang dapat dijadikan bahan untuk menyusun suatu informasi (Arikunto, 2002) [DEF16], dengan kata lain data merupakan bagian dari informasi yang harus dilindungi keamanannya. Maka dari itu perlu menerapkan kebijakan yang tepat untuk melindungi segala bentuk informasi dari ancaman yang dapat membahayakan atau merugikan organisasi, dalam pelaksanaan keamanan informasi diperlukan Sistem Manajemen Keamanan Informasi (SMKI) agar keamanan informasi dapat dikelola sesuai standar yang ada. Oleh karena itu, perlu diterapkan atau diimplementasikan sebagai panduan yang memberikan arahan dalam menjaga aset penting yang dianggap sensitif bagi organisasi.

Oleh sebab itu permasalahan tersebut mendorong penulis untuk merekomendasikan keamanan informasi berdasarkan standar ISO/IEC 27001:2013 pada data pegawai PT. Indonesia Power. Standar yang digunakan adalah standar keamanan informasi ISO/IEC 27001, standar ISO/IEC 27001 merupakan suatu standar Internasional dalam menerapkan Sistem Manajemen Keamanan Informasi (SMKI) dan disesuaikan untuk menangani kebutuhan keamanan tertentu, secara umum standar ini merupakan sebuah *framework* untuk membuat, menerapkan, melaksanakan, memonitoring, menganalisa dan memelihara serta mendokumentasikan Sistem Manajemen Keamanan Informasi (SMKI) (Riyanarto dan Irsyat, 2009) [SAR09].

1.2 Identifikasi Masalah

Berdasarkan latar belakang yang telah dipaparkan sebelumnya, maka permasalahan yang akan dibahas dalam tugas akhir ini adalah :

1 Bagaimana cara melindungi data Pegawai PT. Indonesia Power UPJP dari ancaman yang dapat membahayakan atau merugikan organisasi.

1.3 Tujuan Tugas Akhir

Tujuan dari penelitian tugas akhir ini adalah mengidentifikasi risiko dan merekomendasikan kontrol berdasarkan standar ISO/IEC 27001: 2013 yang sesuai untuk diaplikasikan di PT. Indonesia Power UPJP Kamojang .

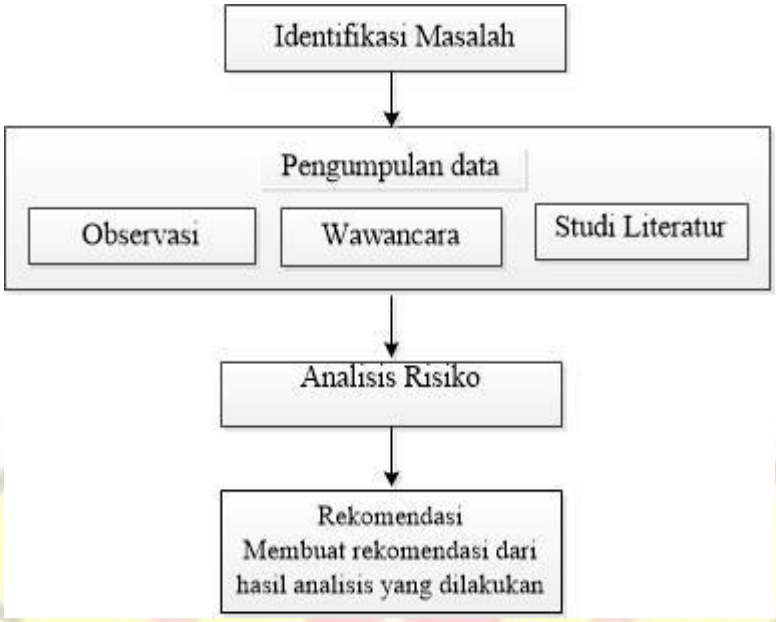
1.4 Lingkup Tugas Akhir

Agar pembahasan masalah ini terarah maka penulis memberikan batasan permasalahan pada penelitian ini. Adapun lingkup tugas akhir tersebut yaitu :

1. Penelitian dilakukan di PT.Indonesia Power , di bagian SIS
2. Fokus penelitian hanya mencakup keamanan pada data Pegawai PT. Indonesa Power, meliputi data pribadi (pegawai).
3. Menggunakan standar ISO/IEC 27001:2013 klausul 9 pada bagian Pengendalian akses (*Access control*). Namun ada beberapa bagian yang terkait dengan klausul 9, yaitu klausul 7, 10, 11, 12 pada tugas akhir.

1.5 Metodologi Tugas Akhir

Metodologi pengerjaan tugas akhir ini dapat dilihat pada Gambar 1.1 Metodologi Tugas Akhir, berikut ini merupakan penjelasan dari Gambar 1.1 :



Gambar 1.1 Metodologi Tugas Akhir

Keterangan:

Berikut ini merupakan penjelasan Metodologi Tugas Akhir.

1. Identifikasi masalah

   Pada tahap ini dilakukan pengdentifikasian masalah yang terjadi di organisasi, serta solusi sementara yang akan diusulkan untuk mengatasi masalah tersebut.

2. Pengumpulan data dilakukan dengan cara sebagai berikut :

   a. Observasi

      Observasi merupakan suatu metode pengumpulan data dengan mengadakan pengamatan secara langsung terhadap objek penelitian dengan mendatangi lokasi untuk mendapatkan data.

   b. Wawancara

      Wawancara merupakan suatu metode pengumpulan data dengan cara melalukan tanya jawab secara langsung terhadap narasumber untuk mendapatkan informasi.

   c. Studi Literatur

      Studi Literatur merupakan suatu metode pengumpulan data dan fakta denga cara mencari dan mempelajari referensi teori yang relevan dengan objek penelitian.

3. Analisis Risiko

   Analisis dapat diartikan sebagai upaya mengolah data menjadi informasi, sehingga data tersebut dapat dengan mudah dipahami untuk menjawab masalah-masalah yag berkaitan dengan kegiatan penelitian.

4. Rekomendasi

Rekomendasi adalah hasil dari analisis dan perancangan yang dapat digunakan untuk perbaikan peroses keamanan informasi di kemudian hari.

1.6 Sistematika Penulisan Tugas Akhir

Untuk memberikan gambaran secara jelas, maka dirancang sebuah sistematika penulisan pada laporan tugas akhir agar adanya keterhubungan antar bab dengan bab lainnya, adapun sistematika penulisan laporan tugas akhir adalah sebagai berikut :

BAB 1 PENDAHULUAN

Bab ini menjelaskan garis besar yang akan dibahas dan diselesaikan sesuai dengan tujuan yang telah dirumuskan seperti latar belakang masalah, Identifikasi masalah, Tujuan Tugas Akhir, Lingkup Tugas Akhir, Metedologi Tugas Akhir, dan Sistematika penulisan tugas akhir.

BAB 2 LANDASAN TEORI

Bab ini memaparkan teori- teori yang mendukung dan mendasari penulisan ini yaitu mengenai konsep yang diperlukan dalam penelitian.

BAB 3 SKEMA PENELITIAN

Bab ini menjelaskan mengenai tahapan penelitian tugas akhir meliputi rancangan penelitian, peta analisis dan langkah analisis, analisis masalah dan manfaat TA, analisis kegunaan konsep dan teori, tempat dan objek penelitian.

BAB 4 ANALISIS RISIKO DAN REKOMENDASI

Bab ini menjelaskan mengenai tingkat keamanan data pegawai PT. Indonesia Power UPJP Kamojang dengan melakukan penilaian risiko (risk assessment) bertujuan untuk mengetahui seberapa besar risiko yang akan diterima oleh organisasi dan menjelaskan sebuah rekomendasi keamanan informasi berdasarkan standar ISO/IEC 27001:2013.

BAB 5 KESIMPULAN DAN SARAN

Pada bab ini berisi kesimpulan yang diambil dari hasil penelitian Tugas Akhir, serta saran-saran untuk pengembangan selanjutnya, agar dapat dilakukan perbaikan-perbaikan di masa yang akan datang.

DAFTAR PUSTAKA

Daftar pustaka menjelaskan tentang sumber yang digunakan pada landasan teori dalam penulisan tugas akhir ini.

DAFTAR PUSTAKA

[DEF16] Definisi dan Pengertian Menurut Ahli, "Pengertian Data Serta Definisi Data Menurut Para Ahli", tersedia : 27 Januari 2017, http://www.definisipengertian.com/2016/01/pengertian-data-definisi-menurut-ahli.html, Januari 2016

[INT05] International Standard, *"ISEC 27001:2005 First Edition"*, 15 Oktober 2005

[INT13] International Standard, *"ISO/IEC 27001:2013 Second Edition",* 01 Oktober 2013

[KEL95] Kelleher, Kevin, Casey G., Lois D., et al, *"Cause and Effect Diagram : Plain and Simple '*, Joiner Associates Inc USA, 1995

[PEC16] PECB, *"ISO/IEC 27002:2013", 26 Februari 2016*

[SAR09] Sarno, Riyanarto., & Ifanno, Irsyat., *"Sistem Manajemen Keamanan Informasi",* ITSPress, 2009

[SOL14] Solusi Utama, "*Perbedaan ISO/IEC 27001:2005 dengan ISO/IEC 27001:2013",* tersedia *: 27* Januari 2017, http://readybisnisnet.wordpress.com/2014/06/06/perbedaan-iso-270012005-dengan-iso-270012013/, Juni 2014

[TIU17] Tiurna Rahayu "Perangcangan Keamanan Data Mahasiswa Fakultas Teknik Berdasarkan ISO/IEC 27001:2013" Unpas Bandung 2017

[VEB13] Vebriana Parmita, *"Pengantar Peluang (Probabilitas)",* tersedia : 11 Februari 2017, https://vebrianaparmita.wordpress.com/2013/11/04bab-vii-pengantar-peluang/, November 2013

[WHI12] Whitman, Michael E., *"Principles of Information Security",* Information security, 2012