# ANALISIS DAN PENERAPAN SISTEM MANAJEMEN KEAMANAN INFORMASI SIMHP BPKP MENGGUNAKAN STANDAR ISO 27001

**Muhammad Bakri[1)], Nia Irmayana[2)]**

*[1)2)]Sistem Informasi, Universitas Teknokrat Indonesia*
*Jl. H.Z.A. Pagaralam, No 9-11, Labuhanratu,Bandarlampung*
*Email : muhammadbakri@teknokrat.ac.id[1)], nia.irmayana@yahoo.com[2)]*

**Abstrak**

*Kantor bagian Program dan Pelaporan (Prolap) menggunakan beberapa sistem untuk melaporkan hasil pengawasan salah satunya Sistem Informasi Manajemen Hasil Pengawasan (SIMHP). Kompleksitas pada SIMHP harus dipandang dari berbagai sudut pandang, terutama aspek keamanan yang nantinya mendukung ketahanan aplikasi SIMHP tersebut. Salah satu pengendalian yang secara khusus mengedepankan faktor keamanan informasi saat ini adalah ISO (Intenational Organization for Standardization) 27001. ISO 27001 merupakan standar untuk mengaudit keamanan sebuah sistem informasi dan digunakan sebagai acuan untuk menghasilkan dokumen (temuan dan rekomendasi). ISO 27001 memiliki kelebihan yaitu standar ini sangat fleksibel yang dikembangkan tergantung kebutuhan organisasi, tujuan organisasi, persyaratan keamanan dan juga SNI ISO 27001 menyediakan sertifikat implementasi Sistem Manajemen Keamanan Informasi (SMKI) yang diakui secara nasional dan internasional yang disebut Information Security Management System (ISMS). Penelitian ini berfokus pada penilaian dan pemetaan permasalahan keamanan terhadap aset informasi pada SIMHP. Pendekatan tersebut akan digunakan sebagai pedoman dalam membuat rancangan model pengendalian keamanan informasi menggunakan ISO 27001.*

***Kata kunci:*** *BPKP, Prolap, SIMHP, ISO 27001, Keamanan Informasi*

## 1. Pendahuluan

Kantor bagian Prolap menggunakan beberapa sistem untuk melaporkan hasil pengawasan yaitu *Integrate Performance Management System (IPMS)*, Sistem Informasi Manajemen Hasil Pengawasan (SIMHP). IPMS merupakan sebuah sistem yang bertugas untuk mengolah data penyiapan bahan penyusunan rencana dan program kegiatan. SIMHP merupakan alat atau aplikasi untuk mengolah data hasil pengawasan yang meliputi hasil pengawasan berbasis audit dan bermanfaat untuk kemudahan penyajian informasi kepada para *stakeholder*. Salah satu fokus utama dalam pengelolaan hasil pengawasan di BPKP adalah SIMHP. SIMHP memegang peran penting dalam pelaksaan kegiatan pengawasan keuangan dan pembangunan Provinsi Lampung. Seiring perkembangan teknologi dan kebutuhan informasi yang semakin signifikan, SIMHP telah dikembangkan secara mandiri oleh BPKP sejak Tahun 2000 . SIMHP digunakan sebagai acuan pembuatan rekapitulasi laporan hasil pengawasan (LHP) bulanan yang terdiri dari Temuan Pemeriksaan (TP), Temuan Pemeriksaan yang Sudah Ditindak Lanjuti (TPL), Temuan Pemeriksaan yang Belum Ditindak Lanjuti (TPB), Tindak Lanjut Hasil Pengawasan dan Hambatannya, Perkembangan Audit Investigasi Kasus Tindak Pidana Korupsi (TPK), dan Hambatan Kelancaran Pembangunan (HKP).

Sistem keamanan SIMHP memerlukan beberapa pendekatan dalam penerapannya. Salah satu penerapan yang dapat dilakukan adalah dengan membangun pengendalian yang fokus pada aspek yang terkandung dalam keamanan. Pengendalian yang dimaksud adalah pengendalian perusahaan yang mengedepankan keterkaitan antara proses bisnis dengan langkah-langkah keamanan. Saat ini terdapat beberapa kerangka kerja pengendalian keamanan yang dapat digunakan untuk membangun pengendalian tersebut (Ermana, Tanuwijaya and Mastan, 2013). Salah satu pengendalian yang secara khusus mengedepankan faktor keamanan informasi saat ini adalah ISO (Intenational Organization for Standardization) 27001 (Anarkhi, Ali and Kurnia, 2013).

ISO 27001 merupakan standar untuk mengaudit keamanan sebuah sistem informasi dan digunakan sebagai acuan untuk menghasilkan dokumen (temuan dan rekomendasi). ISO 27001 memiliki 133 kontrol keamanan informasi, dan pada pelaksanaannya perusahaan dapat memilih kontrol mana yang paling relevan dengan kondisi di lapangan (Wiryana *et al.*, 2012). Namun pemilihan bukan pekerjaan yang mudah, karena banyak parameter yang harus dijadikan pertimbangan. ISO 27001 memiliki kelebihan yaitu standar ini sangat fleksibel yang dikembangkan tergantung kebutuhan organisasi, tujuan organisasi, persyaratan keamanan dan juga SNI ISO 27001 menyediakan sertifikat implementasi Sistem Manajemen Keamanan Informasi (SMKI) yang diakui secara nasional dan internasional yang disebut Information Security Management System (ISMS) (Kusuma, 2014).

Tantangan selanjutnya adalah pemetaan kompleksitas aset informasi yang terkait sistem pengolahan data hasil

pengawasan dan berkaitan dengan masalah kepedulian terhadap keamanan aset informasi tersebut. Hal ini harus dinilai dengan pendekatan lain yang terkait. Penelitian ini berfokus pada penilaian dan pemetaan permasalahan keamanan terhadap aset informasi pada SIMHP. Pendekatan tersebut akan digunakan sebagai pedoman dalam membuat rancangan model pengendalian keamanan informasi menggunakan ISO 27001. Selain itu, pedoman penanganan terhadap ancaman keamanan informasi tersebut harus dirancang sesuai kebutuhan proses bisnis.

## 2. Pembahasan

Standar Internasional ini menetapkan persyaratan untuk penetapan, penerapan, pemeliharaan, dan perbaikan Sistem Manajemen Keamanan Informasi dalam konteks organisasi secara berkesinambungan. Standar ini juga mencakup persyaratan untuk assesment dan penanganan kendali keamanan informasi yang disesuaikan dengan kebutuhan organisasi. Persyaratan standar ini bersifat umum dan ditujukan untuk diaplikasikan pada semua organisasi tanpa memperhatikan jenis, ukuran, dan sifatnya (BSI UK, 2014). Adapun Klausa dalam ISO/IEC 27001: 2013 terdiri dari 7 Klausa yaitu:

1. Klausa 4 Konteks Organisasi
2. Klausa 5 Kepemimpinan
3. Klausa 6 Perencanaan
4. Klausa 7 Pendukung
5. Klausa 8 Operasi
6. Klausa 9 Evaluasi Kinerja
7. Klausa 10 Peningkatan

Dalam ISO/IEC 27001: 2013 terdiri dari:

14 Kontrol Area: area topik inti yang membahas tentang aspek keamanan informasi, 34 Kontrol Tujuan: Tujuan Pengendalian, 114 Kontrol: Kontrol berlaku untuk diimplementasikan pada Sistem Manajemen Keamanan Informasi.

Daftar area kontrol (Annex A):

1. A.5: Kebijakan Keamanan Informasi
2. A.6: Keamanan Informasi Organisasi
3. A.7: Keamanan sumber daya manusia
4. A.8: Pengelolaan Aset
5. A.9: Akses Kontrol
6. A.10: Cryptographic
7. A.11: Keamanan Fisik dan lingkungan
8. A.12: Operasi keamanan
9. A.13: Komunikasi Keamanan
10. A.14: Akuisisi sistem, pengembangan, dan pemeliharaan
11. A.15: Supplier Relationship
12. A.16: Manajemen Insiden Keamanan Informasi
13. A.17: Aspek Keamanan Information of Business Continuity Management
14. A.18: Kepatuhan

Berdasarkan hasil pengendalian yang dirancang pada sistem manajemen keamananan informasi, maka dihasilkan temuan sebagai berikut.

A. Dokumen Temuan

| Klausa | Kontrol | Implementasi | Justifikasi | Unit Kerja |
|---|---|---|---|---|
| A.5 *Security Policy* | | | | |
| A.5.1 *Information Security Policy* | | | | |
| A.5.1.1 | *Information Security Policy Dokumen* | YA | Membuat dokumen kebijakan keamanan informasi | Manajemen Tertinggi |
| A.5.1.2 | *Review of the Information security policy* | TIDAK | Membuat dokumentasi hasil mereview kebijakan keamanan informasi | Manajemen Tetinggi |
| A.6 *Organization of Information Security* | | | | |
| A.6.1 *Internal Organization* | | | | |
| A.6.1.1 | *Management commitment to information security* | TIDAK | Membuat dokumentasi komitmen manajemen terhadap keamanan informasi | Administrator |

B. Pemetaan Ruang Lingkup

Pemangku kepentingan yang relevan harus diidentifikasi dan harus berpartisipasi dalam mendefinisikan lingkup pengendalian. Para pemangku kepentingan yang relevan mungkin internal atau eksternal ke unit organisasi, seperti manajer proyek, manajer sistem informasi, atau pengambil keputusan keamanan informasi.

Organisasi dapat mempertimbangkan membatasi jumlah hasil pengendalian yang harus dilaporkan kepada pengambil keputusan dalam jangka waktu tertentu untuk memastikan kemampuan nya untuk melakukan perbaikan SMKI berdasarkan hasil pengendalian yang dilaporkan. Sebuah jumlah yang berlebihan yang dilaporkan Hasil pengendalian akan berdampak pada kemampuan pembuat keputusan untuk memfokuskan upaya dan memprioritaskan kegiatan perbaikan di masa depan.

C. Kebijakan, Prosedur, Instruksi dan Dokumentasi yang Belum Diterapkan (Rekomendasi)

Berdasarkan hasil temuan-temuan audit keamanan informasi, maka diperoleh beberapa kebijakan, prosedur, dan instruksi yang perlu diterapkan pada BPKP Provinsi Lampung terutama pada kantor Sub Bagian Prolap sebagai acuan pengamanan sistem informasi yang terdapat pada Aplikasi SIMHP mengingat pentingnya data-data yang terdapat di dalam aplikasi SIMHP. Beberapa kebijakan, prosedur, dan instruksi tersebut adalah:

1. Kebijakan clear desk and clear screen,
   a. Personal Computer maupun laptop harus selalu dalam keadaan terkunci /logged off dengan dilengkapi password ketika pegawai meninggalkan meja.
   b. Layar komputer diarahkan dan diatur agar orang lain yang tidak berkepentingan tidak dapat melihat apa yang sedang dikerjakan pegawai.
   c. Log Off otomatis diatur dalam kondisi aktif, sehingga layar monitor terkunci jika tidak ada aktivitas dalam periode waktu tertentu.
   d. Pastikan PC atau laptop sudah dalam keadaan mati ketika jam kerja berakhir.
   e. Untuk dokumen yang sudah tidak terpakai, dihancurkan dengan mesin penghancur (*paper shredder*)
2. Kebijakan kepemilikan asset,
3. Kebijakan dan prosedur untuk melindungi informasi yang berkaitan dengan interkoneksi sistem informasi bisnis,
4. Prosedur pemusnahan media yang tidak diperlukan,
5. Prosedur pemantauan penggunaan fasilitas pengolahan informasi,
6. Prosedur pengamanan fasilitas log dan informasi log hasil pemantauan dan pengawasan dari gangguan dan akses yang tidak sah,
7. Prosedur perlindungan informasi,
8. Prosedur pemeliharaan peralatan untuk memastikan ketersediaan dan integritas layanan,
9. Prosedur pendaftaran dan pembatalan dalam pemberian dan pencabutan akses terhadap seluruh layanan dan sistem informasi,
10. Prosedur penanganan risiko terhadap informasi organisasi dan fasilitas pengolahan informasi dari proses bisnis yang melibatkan pihak-pihak eksternal,
11. Dokumentasi sistem yang sudah terlindungi atas akses yang tidak sah,
12. Dokumentasi yang disesuaikan dan diproyeksikan untuk pemenuhan kapasitas mendatang, guna memastikan kinerja sistem,
13. Dokumentasi log audit untuk membantu investigasi dimasa mendatang,
14. Dokumentasi dan melaporkan setiap kelemahan atas sistem atau layanan,
15. Dokumentasi perjanjian untuk pertukaran informasi,
16. Dokumentasi semua asset dengan jelas dan inventaris semua asset penting,
17. Dokumentasi penggunaan asset.

D. Pengujian Atribut

Setiap atribut yang sudah ditentukan sebelumnya harus dilakukan pengujian terlebih dahulu apakah atribut tersebut sudah sesuai dan dapat digunakan sebagai pengendalian dalam sistem manajemen keamanan informasi. Salah satu pengujian yang dapat dilakukan adalah uji validasi sistem oleh ahli.

Validasi sistem oleh ahli dilakukan dengan mendemokan sistem di depan Judgement Experts. Validasi sistem dilakukan oleh 1 orang ahli yaitu ahli keamanan informasi BPKP Lampung untuk menentukan kelayakan dokumen pengendalian sebelum diimplementasikan di lapangan dan memberikan masukan untuk perbaikan sistem.

Dalam pengujian menggunakan expert judgement dibuat dokumen pengendalian keamanan informasi berdasarkan ISO 27001 dalam bentuk paper.

Selain itu juga penjelasan peneliti tentang pengendalian dan keterkaitannya dengan pihak expert. Kemudian pihak expert menganalisa dan memberi penilaian atau pendapat.

## 3. Kesimpulan

Kesimpulan dari penelitian ini adalah sebagai berikut:

1. Perancangan Sistem Manajemen Keamanan Informasi (SMKI) yang dibuat meliputi keseluruhan proses SMKI.
2. Telah dihasilkan katalog temuan-temuan SMKI yang dibuat berdasarkan dari standar Internasional yang diterapkan oleh ISO 27001:2013.
3. Pemataan telah dilakukan dengan cara mengidentifikasi artifak keamanan informasi pada SIMHP, melakukan kuisioner dan wawancara terhadap Kepala Sub Bagian Prolap dan Administrator SIMHP.
4. Pemodelan SMKI telah dilakukan dengan cara mengidentifikasi kendali-kendali keamanan informasi.
5. Langkah pelaksanaan audit keamanan sistem informasi dilakukan dengan pembuatan pernyataan, identifikasi asset informasi, pembuatan pertanyaan, penentuan kendali berdasarkan temuan-temuan SMKI.

Saran yang diberikan dari penelitian ini adalah sebagai berikut:

1. Untuk penelitian berikutnya perlu dilakukan penelitian terkait pengembangan pengendalian lebih lanjut keamanan informasi dengan layanan teknologi informasi.

2. Untuk penelitian berikutnya perlu dilakukan penerapan secara menyeluruh pengendalian Sistem Manajemen Keamanan Informasi di Badan Pengawasan Keuangan dan Pembangunan Provinsi Lampung.
3. Penelitian yang lebih lanjut atas penelitian ini diharapkan dapat mendefinisikan ukuran-ukuran performa yang lebih mendetil dari sistem manajemen keamanan informasi untuk Aplikasi SIMHP menurut maturity model sehingga manajemen BPKP Perwakilan Lampung dapat menilai apakah pengelolaan keamanan informasi SIMHP sudah mencapai performa yang diharapkan atau belum.

**Daftar Pustaka**

ANARKHI, P. G., ALI, A. H. N. AND KURNIA, I. (2013) 'Penyusunan Perangkat Audit Keamanan Informasi Aplikasi Berbasis Web Menggunakan ISO/IEC 27001 Klausul Kendali Akses', *JURNAL TEKNIK POMITS*, 1(1), pp. 1–5.

BSI UK (2014) 'Moving from ISO/IEC 27001:2005 to ISO/IEC 27001:2013'. United Kingdom: BSI.

ERMANA, F., TANUWIJAYA, H. AND MASTAN, I. A. (2013) *Audit Keamanan Sistem Informasi Berdasarkan Standar ISO 27001 pada PT. BPR Jatim*. Surabaya.

KUSUMA, R. A. (2014) *Audit Keamanan Sistem Informasi Berdasarkan Standar SNI-ISO 27001*. Yogyakarta.

WIRYANA, I. M. *ET AL*. (2012) *Bakuan Audit Keamanan Informasi Kemenpora*.