PENGGUNAAN KERANGKA KERJA SNI ISO/IEC 27001:2013 UNTUK IMPLEMENTASI TATA KELOLA KEAMANAN INFORMASI ARSIP DIGITAL PEMERINTAH BERBASIS KOMPUTASI AWAN (ARSIP NASIONAL RI)

Dicky Rutanaji [1], Sri Suning Kusumawardani [2], Wing Wahyu Winarno [3]
[1.]Mahasiswa, Jurusan Teknik Elektro dan Teknologi Informasi
[2,3] Dosen, Jurusan Teknik Elektro dan Teknologi Informasi
Universitas Gadjah mada
Jl. Grafika no.2 Kampus UGM 55281, Yogyakarta, Indonesia
[1)]dicky.rutanaji@mail.ugm.ac.id, [2)]suning@ugm.ac.id [3)]wing@mail.ugm.ac.id

ABSTRAK

E-government saat ini sudah menjadi kebutuhan dalam penyelenggaraan pemerintah. Hal tersebut dapat tercipta salah satunya dengan adanya tata kelola kelola data pemerintahan yang baik, efisien, transparan, inovatif dan patisipatif. Salah satu unsur yang terdapat dalam tata kelola TI adalah tata kelola keamanan informasi. Tata kelola keamanan informasi merupakan panduan kebijakan yang mengarahkan dan mengatur aktivitas keamanan informasi di sebuah organisasi. Arsip Nasional RI sebagai salah satu institusi negara masih belum mempunyai tata kelola keamanan informasi arsip digital pemerintah berbasis komputasi awan untuk dijadikan panduan dalam keamanan informasinya. Penelitian ini dilakukan dengan melakukan identifikasi tingkat keamanan informasi sesuai dengan SNI ISO/IEC 27001:2013 di lingkungan Arsip Nasional RI untuk kemudian digunakan sebagai kerangka kerja dalam implementasi tata kelola keamanan informasi arsip digital pemerintah berbasis komputasi awan.
Kata kunci *:* tata kelola, keamanan informasi, SNI ISO/IEC 27001:2013, komputasi awan

ABSTRACT

E-government is now a necessity in the administration of the government. It can be created by one of them with good governance governance governance, efficient, transparent, innovative and patisipatif. One of the elements contained in IT governance is information security governance. Information security governance is a policy guide that directs and regulates information security activities within an organization. National Archives of RI as one of the state institutions still do not have the governance of information security of government digital archives based on cloud computing to be a guide in information security. This research was conducted by identifying the level of information security in accordance with SNI ISO / IEC 27001: 2013 in the environment of National Archives of Indonesia to be used as a framework in the implementation of information security governance of government digital archives based on cloud computing.
Keywords: *governance, information security, SNI ISO / IEC 27001: 2013, cloud computing*

PENDAHULUAN

Arsip Nasional RI sebagai Lembaga Kearsipan Nasional dibawah koordinasi langsung oleh Presiden RI mempunyai tugas untuk memberikan informasi kepada lembaga negara dan masyarakat yang autentik dan utuh[1]. Selain itu Arsip Nasional RI juga dapat berperan sebagai

pusat data dan informasi dari seluruh aktivitas pemerintah dan lembaga negara sehingga seluruh data pemerintahan terintegrasi dengan mudah sehingga dapat diakses untuk bahan pengambilan keputusan dan untuk meningkatkan layanan publik yang prima.

Salah satu indikator keberhasilan penerapan *e-government* adalah dengan adanya tata kelola data (*good governance*) pemerintahan yang baik, efisien, transparan, inovatif dan patisipatif[2]. Menurut survei yang telah dilaksanakan oleh Waseda terkait *e-government ranking* pada tahun 2014 menyatakan bahwa *cloud computing* merupakan salah satu tren baru dalam mengembangkan *e-government*[3], dan pada tahun 2015 Waseda menjadikan *cloud computing* sebagai salah satu sub-indikator *Network Preparedness*/*Digital Infrastructure Indicator*[4].

Semakin cepat pertumbuhan teknologi informasi untuk mendukung kegiatan *e-government* dalam hal ini pertumbuhan kebutuhan akan data arsip digital pada sebuah instansi pemerintah sangatlah besar maka isu akan keamanan informasi tidak dapat untuk dihindari. Keamanan informasi merupakan tindakan melindungi informasi dan sistem informasi dari akses, penggunaan, pengungkapan, gangguan, modifikasi, teliti, inspeksi, rekaman atau kehancuran[5].

Jika salah satu insiden keamanan informasi ini terjadi pada Arsip Nasional RI maka akan secara langsung mempengaruhi kinerja dari Arsip Nasional RI dalam melaksanakan tugas dan fungsi pokoknya dengan baik. Jadi setiap organisasi pasti membutuhkan sebuah tata kelola keamanan informasi (*Information Security* Governance) untuk berbagi aset informasi yang ada secara aman dan terpercaya sehingga secara tidak langsung menjadi elemen utama dan pendukung dalam strategi bisnis dari organisasi tersebut[6].

Dalam pembuatan tata kelola keamanan informasi terdapat berbagai macam framework yang dapat digunakan antara lain ISO 27001, ISO 27002, COSO, COBIT, ITIL dan lain-lain. Untuk saat ini yang paling cocok untuk diterapkan dalam pengembangan proses keamanan informasi yaitu SNI ISO/IEC 27001:2013. SNI ISO/IEC 27001:2013 merupakan suatu standar Internasional dalam menerapkan sistem manajemen kemanan informasi atau lebih dikenal dengan *Information Security Management Systems* (ISMS)[7].

Di lingkungan Arsip Nasional sendiri saat ini terdapat sekitar beberapa sistem informasi yang digunakan, baik itu yang sudah digunakan maupun masih tahap pengembangan ke arah komputasi awan. Semua sistem informasi yang ada tidak luput dari berbagai risiko dan ancaman yang ada terkait dengan keamanan informasinya. Akan tetapi sampai dengan saat ini di lingkungan Arsip Nasional RI masih belum ada kebijakan secara spesifik mengatur berkaitan dengan keamanan informasi.

Maka untuk meminimalisir resiko tersebut salah satunya dengan pembuatan sebuah rancangan model dokumen kebijakan tata kelola keamanan informasi pada sistem informasi berbasis komputasi awan di Arsip Nasional RI yang sesuai dengan SNI ISO/IEC 27001:2013 agar dapat mengurangi dampak dari resiko terjadinya kehilangan integritas, kerahasiaan, dan ketersediaan dari sebuah informasi.

Penelitian ini dilakukan berdasarkan tinjauan penelitian sebelumnya yang terkait tentang tata kelola keamanan informasi yaitu antara lain:

1. Kurniasih [8] melakukan penelitian mengenai perancangan tata kelola keamanan informasi untuk proses pengelolaan aset informasi (studi kasus BPK RI). Tujuan dari penelitian ini adalah sebuah rancangan peraturan pelaksanaan keamanan informasi sesuai dengan ISO 27001:2009 di BPK RI. Penelitian ini menggunakan metode kuesioner dalam pengumpulan data dan *member checking* dalam pengujiannya.
2. Utomo [9] melakukan penelitian mengenai pembuatan tata kelola keamanan informasi kontrol akses berbasis iso/iec 27001:2005 pada KPPN Surabaya I . Tujuan dari penelitian ini adalah menghasilkan dokumen manual dan prosedur keamanan informasi berdasarkan aset dan resiko yang dimiliki oleh KPPN Surabaya I. Peneltiian ini menggunakan metode studi literatur peraturan dan kebijakan yang ada di KPPN Surabaya I.

3. Sultan Aldossary dan William Alle [10] melakukan penelitian mengenai *Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions* yang menyatakan bahwa terdapat 7 (tujuh) isu keamanan data dalam komputasi awan yaitu *data loss* (kehilangan data), *data breaches* (pelanggaran data), *malicious insiders* (orang dalam dengan niat jahat), *insecure interfaces and APIs* (antarmuka tidak aman dan API), *account or Service hijacking* (pembajakan akun atau layanan), lokasi data, dan *denial of service* (pencegahan layanan sesungguhnya dari server)
4. Oscar Rebollo, Daniel Mellado, dan Eduardo Fernández-Medina [11] melakukan penelitian mengenai *A Systematic Review Of Information Security Governance Frameworks In The Cloud Computing Environment* menyatakan bahwa dalam tata kelola keamanan di lingkungan komputasi awan terdapat 2 (dua) aspek utama yaitu yang pertama berisi tinjauan literatur sistematis dilakukan untuk mengekstrak dari berbagai sumber akademik, dan kerangka ISG yang cocok untuk aplikasi dalam penyebaran *cloud computing* yang ada. Serta yang kedua berisi kerangka komparatif dengan kriteria fasilitasi analisis dan perbandingan dari mantan kerangka ISG, serta berfokus pada ciri utama dari model awan.

LANDASAN TEORI

1. Tata Kelola Keamanan Informasi

   Menurut ITGI (*IT Governance Institute)*[12] tata kelola keamanan informasi antara lain sebagai berikut:
   a. Metodologi manajemen resiko keamanan informasi
   b. Strategi keamanan yang komprehensif terkait dengan binsis dan tujuan TI
   c. Strategi keamanan yang efektif
   d. Strategi keamanan yang berbicara tentang nilai informasi yang dilindungi
   e. Kebijakan keamanan yang membahas setiap aspek strategi, kontrol dan regulasi
   f. Sebuah standar yang lengkap untuk setiap kebijakan dengan memastikan bahwa prosedur dan pedoman yang sesuai dengan kebijakan
   g. Institusi memantau proses untuk memastikan kepatuhan dan memberikan umpan balik efektifitas.
   h. Sebuah proses untuk memastikan evaluasi lanjutan dan memperbaharui kebijakan keamanan, standar, dan prosedur.
2. Sistem Manajemen Keamanan Informasi (SMKI)

   Sistem Manajemen Keamanan Informasi (SMKI) adalah cara untuk melindungi dan mengelola informasi berdasarkan pendekatan risiko bisnis yang sistematis, untuk menetapkan, menerapkan, mengoperasikan, memantau, mengkaji, memelihara, dan meningkatkan keamanan informasi. Proses dalam SMKI disusun berdasarkan resiko pendekatan bisnis untuk merencanakan (*Plan*), mengimplementasikan dan mengoperasikan (*Do*), memonitor dan meninjau ulang (*Check*) serta memelihara dan meningkatkan atau mengembangkan (*Act*) [13].

Tabel 1. Peta PDCA dalam proses SMKI [13]

Plan (Penetapan SMKI)	Menetapkan kebijakan, sasaran, proses dan prosedur SMKI yang sesuai untuk pengelolaan risiko dan perbaikan keamanan informasi agar menghasilkan hasil yang sesuai dengan kebijakan dan sasaran organisasi secara keseluruhan.
Do (Penerapan dan Pengoperasian SMKI)	Menetapkan kebijakan, sasaran, proses dan prosedur SMKI yang sesuai untuk pengelolaan risiko dan perbaikan keamanan informasi agar menghasilkan hasil yang sesuai dengan kebijakan dan sasaran organisasi secara keseluruhan.

Check (Pemantauan dan pengkajian SMKI)	Mengases dan apabila berlaku mengukur kinerja proses terhadap kebijakan, sasaran SMKI dan pengalaman praktis dan melaporkan hasilnya kepada manajemen untuk pengkajian.
Act (peningkatan dan pemeliharaan SMKI)	Mengambil tindakan korektif dan pencegahan berdasarkan hasil internal audit SMKI dan tinjauan manajemen atau informasi terkait lainnya, untuk mencapai perbaikan berkesinambungan dalam SMKI

3. SNI ISO/IEC 27001:2013

Standar Nasional Indonesia ISO/IEC 27001:2013 merupakan sebuah standar internasional keamanan informasi yang memuat persyaratan-persyaratan yang harus dipenuhi dalam usaha menggunakan konsep-konsep keamanan informasi yang berlaku secara internasional pada sebuah organisasi[13]. SNI ISO/IEC 27001:2013 mensyaratkan penetapan sasaran kontrol dan kontrolkontrol keamanan informasi meliputi 14 area pengamanan sebagai berikut:

a. Kebijakan keamanan informasi
b. Organisasi keamanan informasi
c. Sumber daya manusia menyangkut keamanan informasi
d. Manajemen aset
e. Akses kontrol
f. Kriptografi
g. Keamanan fisik dan lingkungan
h. Keamanan operasi
i. Kemanaan Komunikasi
j. Pengadaan/akuisisi, pengembangan dan pemeliharaan sistem informasi
k. Hubungan dengan pemasok
l. Pengelolaan insiden keamanan informasi
m. Manajemen kelangsungan usaha (business continuity management)
n. Kepatuhan

4. Keamanan Data di Cloud Computing

Beberapa poin penting dalam proses pengamanan data di cloud computing [14] antara lain:

a. Proteksi Data

Ketika kita sudah memutuskan untuk adopsi atau migrasi data ke Cloud, yang yang diperhatikan adalah bagaimana penyedia layanan Cloud memberikan proteksi terhadap data kita. Dengan metode apa mereka melakukan proteksi sehingga kita yakin data aman, selain itu lokasi penyimpanan data juga adalah pertimbangan penting dimana ini hubungannya dengan DC.

b. Security Control

Setelah data kita betul-betul terproteksi, selanjutnya adalah bagaimana keamanan dari akses terhadap data kita (role), bagaimana prosedurnya sehingga hanya orang-orang yang berhak saja yang bisa akses data kita.

c. Compliance

Standar yang diterapkan pada penyedia layanan Cloud Computing, misalnya untuk keamanan data menggunakan ISO/IEC 27001:2013, untuk penyediaan layanan memakai ITIL, COBIT, Cloud Security Alliance, termasuk regulasi internasioanl dan pemerintah.

d. Multi-tenancy

Salah satu sifat Cloud computing adalah resource sharing, nah bagaimana ketika ada penyewa lain terdapat melakukan kecurangan atau bocor, apa imbasnya terhadap data kita disana, ini harus dipertimbangkan.

e. Security Governance

Ini lebih kepada policy governance dari penyedia layanan atau kita sebagai pemakai layanan, harus dijabarkan dan governance-nya paka apa harus didefinisikan disini.

METODE

Penelitian ini merupakan metode yang menggunakan hasil dari kualitatif yang dipakai sebagai data/informasi utama. Proses tahapan dalam penelitian kualitatif yaitu pengumpulan data dimulai dari wawancara, studi literatur, dan dokumen internal untuk mengetahui strategi yang tepat untuk keamanan informasi di Arsip Nasional RI berdasarkan proses dalam SNI ISO/IEC 27001:2013.

Berikut ini langkah-langkah perancangan tata kelola keamanan informasi yang meliputi:

1. Melakukan identifikasi awal

   Identifikasi awal merupakan sebuah proses awal dalam tahapan penelitian untuk memperoleh dan menganganalisis secara mendalam permasalahan yang ada di Arsip Nasional RI sehingga dapat menjamin operasional menggunakan teknologi informasi.
2. Mengumpulkan data

   Pengumpulan data dilakukan untuk mendapatkan gambaran besar dan terperinci tentang kondisi saat ini aset yang mendukung pelaksanaan dan pengelolaan teknologi informasi melalui observasi serta wawancara kepada pejabat di lingkup Pusat Data Arsip Nasional RI.
3. Menentukan model tata kelola keamanan informasi

   Dalam tahapan ini akan dilakukan penentuan model tata kelola keamanan informasi yang sesuai dengan kondisi Sistem Manajemen Keamanan Informasi di lingkungan Arsip Nasional dan hasil identifikasi awal dan pengumpulan data yang sudah dilakukan sebelumnya.
4. Melakukan perancangan tata kelola keamanan informasi

   Perancangan tata kelola keamanan informasi ini terdiri dari 2 tahapan yaitu
   a. Menetapkan Sistem Manajemen Keamanan Informasi

      Dalam tahapan penetapan Sistem Manajemen Keamanan Informasi ini akan menjelaskan cakupan dokumen pada proses penetapan kebijakan Sistem Manajemen Keamanan Informasi menggunakan ISO 27001:2013
   b. Menerapkan dan Mengoperasikan Sistem Manajemen Keamanan Informas

      Dalam tahapan penerapan dan pengoperasian Sistem Manajemen Keamanan Informasi ini akan menjelaskan cakupan dokumen pada proses penerapan dan pengoperasian kebijakan Sistem Manajemen Keamanan Informasi menggunakan ISO 27001:2013 dan sesuai dengan kebutuhan vital dari keamanan informasi arsip digital menggunakan komputasi awan.

HASIL

1. Hasil Identifikasi Awal

   Arsip Nasional RI mempunyai tugas yang sangat penting dalam penyelenggaraan pemerintahan saat ini karena Arsip sendiri memiliki fungsi yang sangat vital sebagai memori kolektif bangsa, selain itu ANRI juga berperan sebagai pembina Kearsipan Nasional sesuai dengan Pasal 8 Ayat 1 Undang-Undang Nomor 43 Tahun 2009.

   Sesuai dengan kondisi saat ini dimana lonjakan volume arsip yang tercipta dalam bentuk digital maupun arsip yang sebelumnya berbentuk konvensional untuk kemudian dilakukan alih media ke dalam bentuk digital dan untuk aksesbilitasnya sudah ke arah komputasi awan akan tetapi ANRI dari sisi keamanan informasinya masih belum mempunyai sebuah prosedur untuk pengamanan serta pengedaliannya. Dalam hal ini ANRI masih belum mempunyai sebuah tata kelola keamanan informasi bagi arsip digital yang sudah terletak di komputasi awan untuk diberikan perlindungan terhadap hal-hal yang tidak diinginkan.

2. Hasil Pengumpulan Data

Hasil dari pengumpulan data yang sudah dilakukan terdapat 4 (empat) aset yang mendukung dalam pelaksanaan dan pengelolaan teknologi informasi dan komunikasi di lingkungan Arsip Nasional RI yaitu sebagai berikut:

a. Aset Kebijakan

   Arsip Nasional RI masih belum mempunyai sebuah kebijakan yang mengatur tentang tata kelola keamanan informasi pada sistem informasi berbasis komputasi awan. Sehingga hal ini Arsip Nasional RI berpotensi mengalami insiden dan ancaman ganguan terhadap keamanan informasi arsip digital yang sudah ada.

b. Aset Kelembagaan

   Arsip Nasional sudah mempunyai unit kerja yang mempnyai tugas dan fungsi pokok dalam melaksanakan penyusunan dan pelaksanaan kebijakan teknis pelaksanaan, pemberian bimbingan, dan pengendalian di bidang data dan informasi serta pengelolaan perangkat Teknologi Informasi dan Komunikasi, serta pengembangan sistem informasi adalah Pusat Data dan Informasi. Sesuai dengan tugas dan fungsi dari Pusat Data dan Informasi maka sebenarnya secara otomatis untuk masalah keamanan informasi arsip digital pemerintath berbasis komputasi awan sudah menjadi kewenangan dan kewajibannya.

c. Aset Aplikasi

   Arsip Nasional RI sampai dengan saat ini sudah mengembangkan berbagai sistem informasi dan aplikasi yang digunakan untuk melaksanakan tugas fungsi pokoknya dalam mendukung terciptanya *Good Governance serta untuk* melayani kepentingan eksternal (masyarakat/pemerintah) maupun internal dalam Arsip Nasional RI sendiri.

d. Aset Infrastruktur

   Arsip Nasional RI sesuai dengan kondisi saat ini sudah memiliki *data center* yang pengelolaannya dilakukan oleh unit Pusat Data dan Informasi. Adapun *data center* yang ada sudah mempunyai standar spesifikasi yang tinggi sesuai dengan fungsinya dalam tempat penyimpanan aplikasi. Akan tetapi Arsip Nasional RI sampai dengan saat ini masih belum mempunyai *Disaster Recovery Plan (DRP)* dan *Disaster Recovery Center (DRC)* yang berfungsi sebagai tempat backup data dan aplikasi di lokasi yang berbeda dengan lokasi *data center* yang utama. Sehingga rentan sekali terjadi kehilangan dan kerusakan data di server *data center* utama apabila nanti terjadi kejadian yang tidak diinginkan semisal bencana alam dan lain sebagainya.

3. Penentuan Model Tata Kelola Keamanan Informasi

   Pemilihan SNI ISO/IEC 27001:2013 karena didalamnya berisi prosedur yang sesuai prinsip keamanan informasi yaitu *confidentiality* (kerahasiaan), *integrity* (keutuhan), *authentication* (keaslian), dan *avability* (ketersediaan).

   Manfaat SNI ISO/IEC 27001:2013 Keamanan Informasi Manfaat Tata Kelola Keamanan Informasi untuk organsiasi atau instansi/lembaga

   a. Mampu menerapkan tatakelola keamanan informasi secara efektif, efisien, dan konsisten dengan pendekatan berbasis risiko.
   b. Mampu melakukan penilaian mandiri (selfassessment) secara berkala melalui mekanisme audit internal
   c. Mampu menyusun sistem dokumentasi minimum yang diperlukan untuk menerapkan tata kelola keamanan informasi.
   d. Membantu memberikan pemahaman pentingnya keamanan informasi pada karyawan, stakeholder dan masyarakat umum.

   Dokumen pada Klausul Kontrol SNI ISO/IEC 27001:2013 dapat dilihat pada Tabel 2 berikut ini:

Tabel 2.14. (Empat Belas) Klausul Kontrol SNI ISO/IEC 27001:2013

No	Domain Klausul	Sasaran
1	Kebijakan Keamanan Informasi	Untuk memberikan arahan dan dukungan manajemen untuk keamanan informasi sesuai dengan persyaratan bisnis dan regulasi serta hukum yang relevan
2	Organisasi Keamanan Informasi	Untuk membentuk kerangka kerja manajemen untuk mengendalikan implementasi, dan operasi keamanan informasi serta untuk menjamin keamanan teleworking dalam organisasi
3	Keamanan Sumber Daya Manusia	Untuk memastikan bahwa setiap pegawai memahami peran dan tanggung jawab mereka di dalam organisasi
4	Manajemen Aset	Untuk mengenali aset organisasi dan menetapkan tanggung jawab perlindungan yang sesuai dengan organisasi
5	Kendali Akses	Untuk memastikan pengendalian dari setiap informasi
6	Kriptografi	Untuk memastikan penggunaan kriptografi secara tepat dan efektif dalam melindungi kerahasian, keaslian dan keutuhan sebuah informasi
7	Keamanan Fisik dan Lingkungan	Untuk mencegah akses fisik dari pihak yang tidak berkewenangan sehingga dapat menimbulkan kerusakan terhadap informasi dan fasilitas pengolah informasi di dalam organisasi
8	Keamanan Operasi	Untuk menjamin operasi fasilitas pengolahan informasi yang baik dan benar
9	Keamanan Komunikasi	Untuk menjamin perlindungan keamanan informasi dalam jaringan dan fasilitas pendukung pengolah informasi
10	Akuisisi, Pengembangan dan Perawatan Sistem	Untuk memastikan bahwa keamanan merupakan bagian yang utuh dari informasi
11	Hubungan Pemasok	Untuk memastikan perlindungan dari aset organsisasi yang dapat diakses oleh pemasok
12	Manajemen Insiden Keamanan Informasi	Untuk memastikan kejadian dan kelemahan keamanan sistem informasi terkait dengan sistem informasi dilakukan sinkronisasi sehingga dimungkinkan tindakan koreksi yang tepat waktu
13	Aspek Keamanan Informasi dari Keberlangsungan Bisnis	Untuk menghadapi gangguan kegiatan bisnis dan untuk melindungi proses bisnis kritis dari efek kegagalan utama SI atau bencana dan untuk memastikan keberlanjutannya secara tepat waktu
14	Kesesuaian	Untuk mencegah pelanggaran terhadap undang-undang atau kewajiban kontrak dan setiap persyaratan keamanan

4. Perancangan Tata Kelola Keamanan Informasi
   a. Penetapan Sistem Manajemen Keamanan Informasi

      Dalam proses penetapan dokumen kebijakan keamanan informasi di Arsip Nasional RI mendapatkan acuan kepada beberapa sasaran pengendalian yang terdapat pada standar SNI/ISO/IEC 27001:2013. Cakupan dokumen pada proses menetapkan kebijakan SMKI dapat dilihat pada Tabel 3 berikut ini:

Tabel 3. Cakupan Dokumen Pada Proses Menetapkan Kebijakan SMKI

No	Klausul SNI 27001:2013	Nama Dokumen	Cakupan Dokumen
1	5.1	Kebijakan Umum Keamanan Informasi	Dokumen kebijakan keamanan informasi antara lain berisi: ❖ Tujuan dan ruang lingkup keamanan informasi ❖ Persetujuan terhadap kebijakan dan program keamanan informasi ❖ Organisasi dan aset informasi
2	8.2.1	Klasifikasi Informasi	Berisi tentang petunjuk cara melakukan klasifikasi informasi yang ada di instansi / lembaga dan disusun dengan memperhatikan nilai penting dan kritikalitas informasi sebuah instansi untuk mendapatkan perlindungan yang layak berdasarkan kepentingan di dalam sebuah organisasi

b. Penerapan dan Pengoperasian Sistem Manajemen Keamanan Informasi

Sesuai dengan topik dari penelitian ini yaitu keamanan informasi pada sistem informasi berbasis komputasi awan maka peneliti selain mengacu kepada SNI ISO/IEC 27001:2013, dan juga didapatkan dari studi literatur *National Institute Of Standard And Technology* **(**NIST) serta *Cloud Security Alliance* (CSA) berkaitan dengan keamanan informasi di komputasi awan yang menghasilkan poin-poin utama yaitu antara lain

1) *Virtualization Privacy Security* yaitu bagaimana cara penganganan terhadap isu-isu di virtual seperti contohnya teleworking.
2) *Identifitaction, authentication and authorization* yaitu bagaimana cara menjamin akses kontrol terhadap akses informasi.
3) *Application security* yaitu bagaimana prosedur terkait dengan keamanan informasi secara keseluruhan dari aplikasi yang berjalan di atas komputasi awan.
4) *Incident response* yaitu bagaimana membuat pengelolaan dan penanganan respon terhadap insiden keamanan informasi.

Pada tahapan proses penerapan dan pengoperasian dokumen kebijakan keamanan informasi mengacu kepada beberapa sasaran pengendalian yang terdapat pada standar SNI ISO/IEC 27001:2013 maka penelitian ini menghasilkan 4 (empat) dokumen kebijakan antara lain sebagai berikut:

1) Kebijakan Teleworking,
2) Kebijakan Bisnis Untuk Pengendalian Akses,
3) Manajemen Pengendalian Akses Sistem dan Aplikasi,
4) Manajemen Insiden Keamanan Infromasi dan Perbaikan.

Cakupan dokumen pada proses proses menerapkan dan mengoperasikan SMKI dapat dilihat pada Tabel 4 berikut ini:

Tabel 4. Cakupan dokumen pada proses penerapan dan pengoperasian kebijakan SMKI

No	Klausul SNI	Nama Dokumen	Cakupan Dokumen

	27001:2013		
1	A.6.2.2	Kebijakan Teleworking	Berisi tentang kebijakan dan langkah-langkah keamanan pendukung harus diterapkan untuk melindungi informasi yang diakses, diproses atau disimpan di dalam teleworking
2	A.9.1	Kebijakan Bisnis Untuk Pengendalian Akses	Berisi Persyaratan akses kontrol terhadap informasi dan fasilitas sistem informasi (aplikasi, sistem operasi, internet, email dan akses ruang *Data Center*).
3	A.9.4	Manajemen Pengendalian Akses Sistem dan Aplikasi	Berisi tentang kendali akses sistem dan aplikasi yang dapat di instal pada komputer pegawai di Arsip Nasional RI karena berkaitan dengan kebutuhan dan fungsi dari sistem dan aplikasi terhadap pekerjaan setiap pegawai.
4	A.16.1	Manajemen Insiden Keamanan Infromasi dan Perbaikan	Berisi tentang manajemen insiden keamanan informasi yang didalamnya terdapat tanggung jawab prosedur, pelaporan kejadian dan kelemahan yang ada, dan keputusan terhadap kejadian tersebut.

SIMPULAN

Dari hasil penelitian yang sudah ada dapat berikan kesimpulan antara lain sebagai berikut:

1. Hasil dari penelitian ini dengan adanya SNI ISO/IEC 27001:2013 dapat digunakan untuk panduan implementasi pengelolaan keamanan informasi arsip digital pemerintah menggunakan komputasi awan di lingkungan Arsip Nasional RI. Dimana sesuai dengan indentifikasi awal yang ada masih belum menjadi perhatian dari unit kerja dalam hal ini Pusat Data dan Informasi yang menangani pengelolaan teknologi informasi dan komunikasi.
2. Penelitian ini merupakan sebagian kecil dari penelitian tesis penulis dengan judul Perancangan Tata Kelola Keamanan Informasi Arsip Digital Pemerintah Berbasis Komputasi Awan Menggunakan SNI ISO/IEC 27001:2013 (Kasus Arsip Nasional Republik Indonesia).

DAFTAR PUSTAKA

[1] "Undang-Undang Nomor 43 Tahun 2009 Tentang Kearsipan," 2009

[2] Violeta Madzova, Krste Sajnoski And Ljupco Davcev, "*E-Government As An Efficient Tool Towards Good Governance (Trends And Comparative Analysis Throughout Worldwide Regions And Within West Balkan Countries),*" *Balkan Social Science Review*, Vol. 1, Juni 2013, 157-174

[3] Obi, T,. "*WASEDA – IAC 10th International E-Government Ranking 2014*," Tokyo, 2014

[4] Obi, T,. "*WASEDA – IAC 10th International E-Government Ranking Survey 2015*," Tokyo, 2015

[5] Simson Garfinkel, "*PGP: Pretty Good Privacy*," O'Reilly & Associates, Inc., 1995

[6] Ohki, Eijiroh, et al. "*Information security governance framework." Proceedings of the first ACM workshop on Information security governance*. ACM, 2009.

[7] Arora, Varun. "*Comparing different information security standards: COBIT vs ISO 27001." Línea. Disponible en Carnegie Mellon University, Qatar*:(http://qatar. cmu. edu/media/assets/CPUCIS2010-1. pdf) (2010).

[8] Nia Kurniasih, perancangan tata kelola keamanan informasi untuk proses pengelolaan aset informasi (Studi Kasus BPK RI), MTI Thesis, Universitas Gadjah Mada : Yogyakarta, 2013

[9] Utomo, Margo, Ahmad Holil Noor Ali, and Irsal Affandi. "Pembuatan Tata Kelola Keamanan Informasi Kontrol Akses Berbasis ISO/IEC 27001: 2005 Pada Kantor Pelayanan Perbendaharaan Surabaya I." *Jurnal Teknik ITS* 1.1 (2012): A288-A293.

[10] Sultan Aldossary and William Allen "*Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions" (IJACSA) International Journal of Advanced Computer Science and Applicatio*ns,Vol. 7, No. 4, 2016

[11] Rebollo, Oscar, Daniel Mellado, and Eduardo Fernández-Medina. "*A Systematic Review of Information Security Governance Frameworks in the Cloud Computing Environment*." J. UCS 18.6 (2012): 798-815.

[12] ITGI"Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition,"2016

[13] Sarno, R & Iffano, Sistem Manajemen Keamanan Informasi, Surabaya, Percetakan ITS Press, 2009

[14] Josyula, Venkata, Malcolm Orr, and Greg Page. *Cloud computing: Automating the virtualized data center*. Cisco Press, 2011.