ANALISIS TINGKAT KEMATANGAN SISTEM MANAJEMEN KEAMANAN INFORMASI DIREKTORAT JENDERAL PERBENDAHARAAN DIUKUR DENGAN MENGGUNAKAN INDEKS KEAMANAN INFORMASI (STUDI KASUS: APLIKASI SPAN)

Rifqi Akmal Syarif [1], Agung Nugroho[2]

[1]Direktorat Jenderal Perbendaharaan, Kementerian Keuangan
Email: rifqiy.akmal@gmail.com

[2]Politeknik Keuangan Negara STAN, Kementerian Keuangan
Email: agungnugroho@stan.ac.id

Abstract

Implementation of Information Security Management System (ISMS) is one of the internal control measures to minimize risk and information security threats such as information leakage, application malfunction, loss of data, and low performance of IT networks. Several incidents related to information security have already occurred in the implementation of Treasury System and the State Budget (SPAN) within the Directorate General of Treasury. Therefore, Directorat General of Treasury has made efforts to implement information security in accordance with Ministry of Finance Decree No. 479 / KMK.01 / 2010 on Policy and Management System Standards Information security. In this study, Index KAMI which was published by the Directorate of Information Security, Ministry of Communication and Information has been used to evaluate the maturity level of SPAN's information security. Six key areas examined in this study are the role and the importance of ICT, information security governance, risk management, information security, information security management framework, management of information assets, technology of information security. The results showed that the maturity level of SPAN implementation is still at Level II (basic framework implementation). Of the six key areas analyzed, information security technology scored the highest (83%). However, risk management still shows low score that need special attention from the Directorate General of Treasury.

Keywords: information security management system, information security maturity level

Abstrak

Penerapan Sistem Manajemen Keamanan Informasi (SMKI) merupakan salah satu upaya pengendalian internal yang mampu meminimalisasi risiko dan ancaman keamanan informasi seperti kebocoran informasi, kerusakan aplikasi, kehilangan data, dan kinerja jaringan TI yang melambat. Beberapa insiden terkait keamanan informasi telah terjadi dalam implementasi aplikasi Sistem Perbendaharaan dan Anggaran Negara (SPAN) pada Direktorat Jenderal Perbendaharaan. Oleh karena itu, Direktorat Jenderal Perbendaharaan yang merupakan unit eselon I di lingkungan Kementerian Keuangan, telah berupaya untuk menerapkan keamanan informasi sesuai dengan Keputusan Menteri Keuangan Nomor 479/KMK.01/2010 tentang Kebijakan dan Standar Sistem Manajemen Keamanan Informasi. Dalam penelitian ini, Indeks Keamanan Informasi yang disusun oleh Direktorat Keamanan Informasi Kementerian Komunikasi dan Informasi digunakan sebagai alat untuk mengukur tingkat kematangan keamanan informasi tersebut. Enam area kunci yang diteliti dalam penelitian ini yaitu peran dan tingkat kepentingan TIK, tata kelola keamanan informasi, pengelolaan risiko keamanan informasi, kerangka kerja pengelolaan keamanan informasi, pengelolaan aset informasi, dan teknologi keamanan informasi. Hasil penelitian menunjukkan bahwa tingkat kematangan implementasi aplikasi SPAN masih berada pada level II dimana keamanan informasi berada pada klasifikasi penerapan kerangka dasar (Aktif). Dari keenam area kunci yang dianalisis, teknologi dan keamanan informasi memperoleh skor

tertinggi (83%), namun skor untuk pengelolaan risiko masih menunjukkan nilai yang rendah dan perlu memperoleh perhatian Khusus bagi Dirjen Perbendaharaan.

Kata Kunci: Sistem Manajemen Keamanan Informasi, Level kematangan keamanan informasi

1. LATAR BELAKANG

Sistem Perbendaharaan dan Anggaran Negara (SPAN) adalah sebuah sistem aplikasi yang dibuat dalam rangka mewujudkan terbentuknya *e-government* yang merupakan sub-program dari program reformasi keuangan publik terbesar dalam sejarah di Indonesia dalam modernisasi penganggaran dan perbendaharaan. SPAN diharapkan mampu menyediakan informasi yang komprehensif dan dapat dipercaya sehingga perlu adanya pengendalian internal menyeluruh yang mampu menjaga sistem informasi (SPAN) dari berbagai macam risiko atau ancaman keamanan informasi seperti kebocoran informasi, kerusakan aplikasi, kehilangan data, dan kinerja jaringan TI yang melambat.

Salah satu bentuk pengendalian internal yang mampu meminimalisasi risiko dan ancaman keamanan informasi adalah dengan cara menerapkan Sistem Manajemen Keamanan Informasi (SMKI). SMKI menurut ISO/IEC 27001:2009 (2009, 3) didefinisikan sebagai bagian dari sistem manajemen secara keseluruhan, berdasarkan pendekatan risiko bisnis, untuk menetapkan, menerapkan, mengoperasikan, memantau, mengkaji, meningkatkan dan memelihara keamanan informasi. Oleh karena itu, dalam rangka pengendalian keaman informasi tersebut, Direktorat Jenderal Perbendaharaan mengguna-kan acuan berupa Keputusan Menteri Keuangan Nomor 479/KMK.01/2010 tentang Kebijakan dan Standar Sistem Manajemen Keamanan Informasi di Lingkungan Kementerian Keuangan. KMK ini telah mengadopsi 11 sasaran pengendalian yang ada di ISO/IEC 27001:2005 atau Standar Nasional Indonesia (SNI) ISO/IEC 27001:2009. Penerapan SMKI diharapkan mampu menjamin pelaksanaan kegiatan pengelolaan keuangan negara dengan aman.

Sistem Manajemen Keamanan Informasi pada Direktorat Jenderal Perbendaharaan khususnya terkait aplikasi SPAN dapat diukur, dianalisis, dan dievaluasi tingkat kesiapan atau kematangan pengamanan informasinya menggunakan Indeks Keamanan Informasi (Indeks KAMI) yang diterbitkan oleh Tim Direktorat Keamanan Informasi Kementerian Komunikasi dan Informatika. Indeks KAMI merupakan alat untuk mengukur, menganalisis, dan meng-evaluasi tingkat kesiapan atau kematangan pengamanan informasi yang ada di suatu instansi yang sesuai dengan persyaratan pengamanan yang tercantum dalam standar ISO/IEC 27001.

2. RUANG LINGKUP PENELITIAN

Ruang lingkup yang diteliti terbatas pada Sistem Manajemen Keamanan Informasi Direktorat Jenderal Perbendaharaan khususnya yang terkait aplikasi SPAN. Terdapat enam area kunci yang diteliti dalam penelitian ini yaitu: peran dan tingkat kepentingan TIK; tata kelola keamanan informasi; pengelolaan risiko keamanan informasi; kerangka kerja pengelolaan keamanan informasi; pengelolaan aset informasi; dan teknologi keamanan informasi.

3. RUMUSAN MASALAH PENELITIAN

Bagaimana tingkat ketergantungan Sistem Manajemen Keamanan Informasi Ditjen Perbendaharaan khususnya pada aplikasi SPAN dan bagaimana pula tingkat kesiapan atau kematangan Sistem Manajemen Keamanan Informasi Ditjen Perbendaharaan khususnya pada aplikasi SPAN.

4. TUJUAN DAN MANFAAT PENELITIAN

Penelitian ini bertujuan untuk mengetahui tingkat ketergantungan Sistem Manajemen Keamanan Informasi Ditjen Perbendaharaan khususnya pada aplikasi SPAN, tingkat kesiapan atau kematangan Sistem Manajemen Keamanan Informasi Ditjen Perbendaharaan khususnya pada aplikasi SPAN.

Melalui penelitian ini, diharapkan dapat digunakan sebagai bahan pertimbangan untuk melakukan perbaikan pada area-area yang belum

memenuhi standar keamanan informasi bagi pimpinan organisasi yang bertanggung jawab dalam proses bisnis SPAN, dan dapat menjadi bahan referensi dalam melakukan penelitian selanjutnya di masa mendatang mengenai Sistem Manajemen Keamanan Informasi pada Instansi Penyelenggara Pelayanan Publik.

5. LANDASAN TEORI

5.1. Keamanan Informasi

Keamanan informasi dapat diartikan sebagai upaya untuk mengamankan aset informasi dari segala macam ancaman yang mungkin terjadi untuk mengurangi risiko negatif yang diterima. Menurut definisi SNI ISO/IEC 27001:2009 (2009,10), keamanan informasi didefinisikan sebagai penjagaan kerahasiaan, integritas, dan ketersediaan informasi; sebagai tambahan, sifat/keadaan informasi lainnya seperti keaslian, akuntabilitas, nirsangkal dan kehandalan dapat juga dimasukkan.

Keamanan informasi memiliki beberapa aspek yang menjadi perhatian utama yang wajib dipahami dalam penerapannya. Beberapa aspek tersebut sering dipahami sebagai C.I.A *triangle* model yang terdiri dari *confidentiality, integrity*, dan *availability*. Chad Perrin menjelaskan dalam "The CIA *Triad*" bahwa keamanan informasi seharusnya: (1) dapat menjamin bahwa hanya mereka yang memiliki hak yang boleh mengakses informasi tertentu (c*onfidentiality/* kerahasiaan), (2) dapat menjamin kelengkapan informasi dan menjaga dari korupsi, kerusakan, atau ancaman lain yang menyebabkan berubah informasi dari aslinya (*Integrity*), dan dapat menjamin pengguna dapat mengakses informasi kapanpun tanpa adanya gangguan dan tidak dalam format yang tidak bisa digunakan (*availability*/ketersediaan).

Sementara itu, keamanan informasi dapat terancam karena orang, organisasi, mekanisme, atau peristiwa yang memiliki potensi untuk membahayakan sumber daya informasi perusahaan. Ancaman dapat bersifat internal ataupun eksternal, dan dapat bersifat tidak disengaja maupun disengaja (McLeod dan Schell 2004, 244). Jenis-jenis ancaman atas keamanan sistem informasi pun beragam, baik yang berasal dari dalam organisasi maupun dari luar. Jenis ancaman terhadap keamanan informasi menurut ISO/IEC FIDIS 27005:2008 dapat berupa kerusakan fisik (api, air, polusi); peristiwa alam (iklim, seismik, vulkanik); hilangnya layanan penting (tenaga listrik, AC, telekomunikasi); kompromi informasi (menguping, pencurian media, pengambilan bahan dibuang); kegagalan teknis (peralatan, perangkat lunak, saturasi kapasitas); dan kompromi fungsi (kesalahan dalam penggunaan, penyalahgunaan hak, penolakan tindakan. Sementara itu, jika ditinjau dari klasifikasi asal *(origin)* ancaman, menurut ISO/IEC FIDIS 27005:2008, ancaman dapat bersifat sesuatu yang disengaja untuk tujuan spionase atau pengolahan data ilegal, bersifat kebetulan (kegagalan peralatan, kegagalan perangkat lunak), berasal dari lingkungan (peristiwa alam, hilangnya pasokan listrik), atau merupakan suatu kelalaian.

5.2. Sistem Manajemen Keamanan Informasi (SMKI)

Sistem Manajemen Keamanan Informasi (SMKI) adalah seperangkat kebijakan berkaitan dengan manajemen keamanan informasi atau teknologi informasi yang terkait dengan risiko-risiko. Penerapan SMKI didasari atas prinsip bahwa organisasi harus merancang, menerapkan dan memelihara seperangkat kebijakan, proses dan sistem untuk mengelola risiko aset informasinya, sehingga memastikan tingkat risiko yang dapat diterima oleh keamanan informasi.

Menurut SNI ISO/IEC 27001:2009 yang merupakan versi Indonesia dari ISO/IEC 27001:2005, menguraikan bahwa:

> "Sistem Manajemen Keamanan Informasi merupakan suatu bentuk susunan proses yang dibuat berdasarkan pendekatan risiko bisnis untuk merencanakan (Plan), meng-implementasikan dan mengoperasikan (Do), memonitoring dan meninjau (*Check*), serta memelihara dan meningkatkan atau mengembangkan (*Act*) terhadap keamanan informasi perusahaan."

Susunan proses Sistem Manajemen Keamanan Informasi (SMKI) menurut SNI ISO/IEC 27001:2009 sering disingkat dengan "Plan-Do-Check-Act" (PDCA) atau dikenal dengan istilah *Deming Cycle*.

SNI ISO/IEC 27001 dikembangkan dengan pendekatan proses sebagai suatu model bagi penetapan, penerapan, pengoperasian, pemantauan, tinjau ulang *(review),* pemeliharaan dan peningkatan Sistem Manajemen Keamanan Informasi. Pendekatan proses mendorong pengguna menekankan pentingnya pemahaman persyaratan keamanan informasi organisasi dan kebutuhan terhadap kebijakan serta sasaran keamanan informasi, penerapan dan pengoperasian kontrol untuk mengelola risiko keamanan informasi dalam konteks risiko bisnis organisasi secara keseluruhan, pemantauan dan tinjau ulang kinerja dan efektivitas SMKI, dan peningkatan berkelanjutan berdasarkan pada pengukuran tingkat ketercapaian sasaran. (KEMKOMINFO 2011, 10).

Persyaratan utama yang harus dipenuhi SNI ISO/IEC 27001:2009 menurut KEMKOMINFO (2011,11) meliputi Sistem Manajemen Keamanan Informasi (kerangka kerja, proses dan dokumentasi), tanggung jawab manajemen, audit internal SMKI, manajemen reviu SMKI, dan peningkatan berkelanjutan. Selain persyaratan utama yang harus dipenuhi, SNI ISO/IEC 27001:2009 menetapkan sasaran kontrol dan kontrol-kontrol keamanan informasi yang meliputi 11 area pengamanan, yaitu: (1) Kebijakan keamanan informasi; (2) Organisasi keamanan informasi; (3) Manajemen aset; (4) Sumber daya manusia menyangkut keamanan informasi; (5) Keamanan fisik dan lingkungan; (6) Komunikasi dan manajemen operasi; (7) *Access control*; (8) Penggandaan/akuisisi, pengembangan dan pemeliharaan sistem informasi; (9) Pengelolaan insiden keamanan informasi; (10) Manajemen kelangsungan usaha *(business continuity management);* dan (11) Kepatuhan.

5.3. Hasil Penelitian Sebelumnya

Terdapat beberapa penelitian sebelumnya yang relevan dengan yang mengangkat tema Keamanan Sistem Informasi. Fajrin Agustian (2011) pada penelitian yang berjudul "Kajian Tingkat Kematangan Sistem Manajemen Keamanan Informasi menggunakan Indeks KAMI (Studi Kasus: Kantor Pusat Direktorat Jenderal Pajak)", menghasilkan kesimpulan bahwa tingkat ketergantungan terhadap Teknologi Informasi dan Komunikasi pada Kantor Pusat DJP menunjukkan angka 43 atau berada pada tingkat "kritis" dan tingkat kesiapan pengamanan informasi menunjukkan angka 349 atau dinyatakan "perlu perbaikan". Selain itu tingkat kematangan SMKI berada pada tingkat kematangan II. Selanjutnya, Soenardi dan Ichsan (2013) dalam penelitiannya yang berjudul "Analisis Kematangan Sistem Manajemen Keamanan Informasi Badan Pendidikan dan Pelatihan Keuangan Diukur Menggunakan Indeks Keamanan Informasi", menghasilkan kesimpulan akhir bahwa tingkat kelengkapan dan kematangan Sistem Manajemen Keamanan Informasi Badan Pendidikan dan Pelatihan Keuangan masih rendah. Penyebab rendahnya tingkat kelengkapan dan kematangan SMKI di BPPK yaitu: a) Konsep SMKI relatif baru dikenal di Indonesia, khususnya di lingkungan instansi pemerintah, kondisi ini menyebabkan rendahnya tingkat *awareness* dari pimpinan dan pegawai BPPK tentang arti penting SMKI, b) Hingga saat ini proses bisnis BPPK masih berbasis *paper-based*, sehingga budaya pendokumentasian data dan informasi serta penjagaan keamanan dan kerahasiaannya sulit untuk diterapkan secara optimal dan menyeluruh, c) Pengembangan aplikasi dan infrastruktur pendukungnya masih bersifat reaktif dan belum didasarkan pada perencanaan jangka menengah/panjang, akibatnya IT belum menjadi salah satu fasilitas pendukung yang instrumental dalam pelaksanaan tugas-tugas administratif di lingkungan BPPK. Hasil penelitian yang hampir sama juga diperoleh oleh Afrianto, Suryana, Sufa'atin (2015) dalam penelitian yang berjudul "Pengukuran dan Evaluasi Keamanan Informasi Menggunakan Indeks KAMI – SNI ISO/IEC 27001:2009 - Studi Kasus Perguruan Tinggi X" dimana tingkat kematangan keamanan informasi Perguruan Tinggi X berada pada level I+ s/d II+, dimana untuk mendapatkan sertifikasi ISO/IEC 27001:2009 level keamanan informasi adalah minimal III.

6. GAMBARAN UMUM SISTEM PERBENDAHARAAN dan ANGGARAN NEGARA (SPAN)

Dengan terbitnya Paket Undang-Undang Keuangan Negara yaitu UU No. 17/2003 tentang Keuangan Negara, UU No. 1/2004 tentang

Perbendaharaan Negara, dan UU No. 15/2004 tentang Pemeriksaan Pengelolaan dan Tanggung Jawab Keuangan Negara, maka dimulailah reformasi manajemen keuangan pemerintah di Indonesia. Pengejawantahan reformasi manajemen keuangan pemerintah tersebut adalah dengan disusunnya Government Financial Management & Revenue Admin Project (GFMRAP) yang mencakup beberapa bidang, yaitu *Public Financial Management (PFM), Revenue Administration, Governance and Accountability,* dan *Project Governance and Implementation*. Salah satu bagian dari GFMRAP yaitu *Public Financial Management* (PFM) memiliki perhatian khusus salah satunya adalah terkait dengan modernisasi anggaran dan perbendaharaan. Modernisasi tersebut diimplementasikan dalam bentuk Sistem Perbendaharaan dan Anggaran Negara (SPAN).

SPAN adalah suatu sistem manajemen informasi keuangan yang terintegrasi (IFMIS), yang mencakup keseluruhan proses pengelolaan keuangan negara, mulai dari persiapan, pelaksanaan, hingga pelaporan anggaran. Pembangunan SPAN dimulai dengan penyempurnaan proses bisnis (BPI), yang secara iteratif disesuaikan dengan kemampuan *IT system*, dan sejalan dengan peraturan perundangan maupun *best practices* berlaku. Pengintegrasian proses bisnis SPAN dilaksanakan dengan penyatuan *database* dan automasi proses bisnis ke dalam *process flow IT system* yang terintegrasi. Fungsi utama SPAN antara lain adalah fungsi penyusunan anggaran, manajemen DIPA, manajemen komitmen, manajemen penerimaan dan pembayaran, manajemen kas, serta akuntansi dan pelaporan. SPAN bekerja secara *real-time* dan *online* dalam pengelolaan keuangan negara dengan menghubungkan *users* dari unit-unit yang terlibat.

SPAN bertujuan meningkatkan efisiensi, efektivitas, akuntabilitas dan transparansi di bidang pengelolaan anggaran dan perbendaharaan negara melalui penyempurnaan proses bisnis dan pemanfaatan teknologi yang terintegrasi. Selain itu, dalam rangka mendukung program reformasi penganggaran dan perbendaharaan negara, SPAN bertujuan mengendalikan anggaran negara, aset, dan kewajiban pemerintah pusat, menyediakan informasi yang komprehensif, dapat dipercaya, dan tepat waktu tentang keuangan pemerintah; dan memudahkan pengambilan keputusan dalam manajemen keuangan pemerintah (Direktorat Transformasi Perbendaharaan, 2013).

Sistem Perbendaharaan dan Anggaran Negara (SPAN) digunakan oleh beberapa instansi di Kementerian Keuangan dan mempengaruhi ribuan satuan kerja di seluruh penjuru daerah di Indonesia. Organisasi yang terkait dan terkena dampak implementasi SPAN antara lain yaitu: *Direktorat Jenderal Anggaran, beserta seluruh unit teknis di bawahnya; Direktorat Jenderal Perbendaharaan, beserta unit teknis di bawahnya termasuk (30 Kanwil dan 177 KPPN);* Sekretariat Jenderal Kementerian Keuangan c.q. Pusat Sistem Informasi dan Teknologi Keuangan (PUSINTEK); Unit Eselon I lain yang terkait dengan BA 999; Seluruh Kementerian/Lembaga (kurang-lebih 36.000 Satker); dan Bank Indonesia dan perbankan nasional.

*S*ebagai sebuah sistem pengelolaan keuangan yang terintegrasi, SPAN mengintegrasikan tiga tahap proses bisnis pada Kementerian Keuangan yaitu perencanaan, pelaksanaan, dan pertanggungjawaban anggaran. Ketiga proses bisnis tersebut terdiri dari beberapa modul seperti modul *Spending Authority (SA), Budget Commitment (BC), Payment Management (PM), Government Receipt (GR), Cash Management (CM),* dan *Modul General Ledger & Reporting (GL)* yang digunakan oleh Ditjen Anggaran dan Ditjen Perbendaharaan sesuai dengan kewenangannya masing-masing.

7. GAMBARAN UMUM SISTEM MANAJEMEN KEAMANAN INFORMASI (SMKI) DI DIREKTORAT JENDERAL PERBENDAHARAAN

Sistem Manajemen Keamanan Informasi pada Direktorat Jenderal Perbendaharaan berpedoman pada peraturan induk terkait SMKI yaitu Keputusan Menteri Keuangan Nomor 479/KMK.01/2010 tentang Kebijakan dan Standar Sistem Manajemen Keamanan Informasi di Lingkungan Kementerian Keuangan. Peraturan turunan SMKI dalam bentuk Peraturan Dirjen (Perdirjen) belum dibuat seperti halnya yang sudah dilakukan oleh Direktur Jenderal Pajak (DJP) dalam bentuk PER-41/PJ/2010 tanggal 25 Agustus 2010. Hal ini mengakibatkan

belum ditetapkannya pembagian peran, tugas, dan tanggung jawab dalam pengelolaan keamanan informasi di Direktorat Jenderal Perbendaharaan.

Kebijakan dan Standar SMKI di Lingkungan Kementerian Keuangan dalam Keputusan Menteri Keuangan Nomor 479/KMK.01/2010 terdiri dari 11 (sebelas) sasaran pengendalian yaitu Pengendalian Umum, Organisasi Keamanan Informasi, Pengelolaan Aset Informasi, Keamanan Sumber Daya Manusia, Keamanan Fisik dan Lingkungan, Pengelolaan Komunikasi dan Operasional, Akses, Keamanan Informasi dalam Pengadaan, Pengembangan, dan Pemeliharaan Sistem Informasi, Pengelolaan Gangguan Keamanan Informasi, Keamanan Informasi dalam Pengelolaan Kelangsungan Kegiatan dan Kepatuhan. Kebijakan dan Standar SMKI di Lingkungan Kementerian Keuangan dikoordinasikan oleh *Chief Information Officer* (CIO) Kementerian Keuangan sekaligus berperan sekaligus sebagai oleh *Chief Information Security Officer* (CISO) Kementerian Keuangan.

Dalam melaksanakan tugasnya, CISO Kementerian Keuangan membentuk Tim Keamanan Informasi Kementerian Keuangan yang diketuai oleh CISO Kementerian Keuangan dan beranggotakan para CISO unit Eselon I, Koordinator Keamanan Informasi Kementerian Keuangan serta Petugas Keamanan Informasi Kementerian Keuangan. *Chief Information Security Officer* (CISO) Unit Eselon I dilakukan oleh *Chief Information Officer* (CIO) Unit Eselon I. Dalam hal CIO unit Eselon I belum ditetapkan oleh pimpinan Unit Eselon I, maka peran CIO Unit Eselon I dilaksanakan oleh Para Sekretaris Direktorat Jenderal, Para Sekretaris Badan, Sekretaris Inspektorat Jenderal, dan Kepala Unit TIK Sekretariat Jenderal. Dalam hal Direktorat Jenderal Perbendaharaan, peran CIO unit Eselon I dilaksanakan oleh Sekretaris Direktorat Jenderal Perbendaharaan.

Secara *ex-officio* peran *Chief Information Officer* (CIO) sekaligus *Chief Information Security Officer* (CISO) pada Direktorat Jenderal Perbendaharaan dilakukan oleh Sekretariat Direktorat Jenderal Perbendaharaan, namun dalam pelaksanaan di lapangan tidak ditemukan bagian atau subbagian yang mempunyai tugas pokok dan fungsi terkait manajemen keamanan informasi. Berdasarkan Peraturan Menteri Keuangan Nomor 206/PMK.01/2014 tentang Organisasi dan Tata Kerja Kementerian Keuangan diketahui juga bahwa pada Sekretariat Direktorat Jenderal Perbendaharaan tidak terdapat uraian tugas dan fungsi bagian atau subbagian yang terkait dengan manajemen keamanan informasi.

Pelaksanaan Sistem Manajemen Keamanan Informasi di Direktorat Jenderal Perbendaharaan lebih banyak dilakukan oleh Direktorat Sistem Informasi dan Teknologi Perbendaharaan (SITP). Direktorat SITP mempunyai tugas merumuskan serta melaksanakan kebijakan dan standarisasi teknis di bidang sistem informasi dan teknologi perbendaharaan. Direktorat SITP terdiri atas 6 Subdirektorat yaitu Subdirektorat Perancangan dan Pengembangan Sistem Informasi, Subdirektorat Pengelolaan Sistem Informasi Internal, Subdirektorat Pengelolaan Sistem Informasi Eksternal, Subdirektorat Pengelolaan Infrastruktur, Subdirektorat Pengelolaan Transformasi Teknologi Informasi dan Subbagian Tata Usaha. Terdapat 3 Subdirektorat yang memiliki hubungan dengan aplikasi SPAN yaitu Subdirektorat Pengelolaan Sistem Informasi Internal, Subdirektorat Pengelolaan Infrastruktur, Subdirektorat Pengelolaan Transformasi Teknologi Informasi.

Subdirektorat Pengelolaan Sistem Informasi Internal mempunyai tugas melaksanakan pengelolaan, pengamanan, *monitoring*, evaluasi, penerapan, dan pemeliharaan Sistem Informasi Internal Perbendaharaan yang salah satunya adalah aplikasi SPAN. Subdirektorat Pengelolaan Infrastruktur mempunyai tugas melaksanakan pengujian, *monitoring*, evaluasi, pengamanan, pemberian dukungan teknis, dan pengadministrasian infrastruktur sistem informasi. Subdirektorat Pengelolaan Transformasi Teknologi Informasi mempunyai tugas melaksanakan penyiapan penerapan perubahan organisasi, melaksanakan penyiapan perumusan dan penyusunan rencana strategis dan rencana kerja pengelolaan perubahan, melaksanakan operasional transformasi, melakukan *monitoring*, evaluasi, dan pelaporan akuntabilitas kinerja direktorat, perumusan pedoman, pengkajian, implementasi, pembinaan, dan pengembangan jabatan fungsional Teknologi Informasi.

Pengelolaan keamanan informasi aplikasi SPAN pada Direktorat Jenderal Perbendaharaan

secara tersirat dan tersurat sudah ada dalam tugas pokok dan fungsi pada Direktorat SITP. Pengelolaan keamanan informasi dalam bentuk SMKI akan lebih optimal bila didasari dengan sebuah peraturan khusus yang mengatur standar dan kebijakan SMKI di Direktorat Jenderal Perbendaharaan. Peraturan khusus ini diharapkan mampu memberi kejelasan mengenai pembagian peran, tugas, dan tanggung jawab dalam pengelolaan keamanan informasi di Direktorat Jenderal Perbendaharaan.

Bentuk pengelolaan keamanan informasi pada aplikasi SPAN antara lain adalah perlindungan aplikasi dengan proses enskripsi dan deskripsi, adanya mekanisme *maker* dan *checker* dimana setiap transaksi akan dilakukan oleh minimal 2 orang, yang 1 sebagai pembuat transaksi dan orang kedua akan menyetujui transaksi tersebut sehingga dengan pemisahan wewenang tersebut akan mengurangi tindakan penyalahgunaan atau kecurangan.

Aplikasi SPAN dilengkapi dengan *Disaster Recovery Center* (DRC) yang ditempatkan di Balikpapan yang berfungsi sebagai *backup* apabila terdapat masalah pada server yang ada pada *Data Center* (DC) di Jakarta. Pengamanan data dan informasi pada DC dan DRC SPAN dilengkapi oleh *Firewall, Bluecoat Web Filter*, Anti SPAM sebagai perangkat pengamanan lalu lintas data internet dan intranet dengan komputer-komputer *client*. Kemudian terdapat *Access Control Server* dan *Access Concentrator* sebagai perangkat keamanan dan manajemen konektifitas data. Ditambah lagi terdapat *Vaccine Server* dan *Security Server.*

Bentuk pengelolaan keamanan informasi aplikasi SPAN juga terdapat dalam infrastruktur pendukung yang mampu meminimalisir risiko-risiko dan dampak dari bencana seperti kebakaran, banjir, mati listrik, dan penyusup. Infrastruktur pendukung tersebut meliputi: *Uninterupted Power Supply (UPS)* sebagai perangkat *backup power* untuk server saat pasokan listrik utama terputus, *Computer Room Air Conditioning (CRAC)* yang berfungsi sebagai sistem pengatur suhu ruangan yang menjaga suhu ruangan *server* tetap stabil pada 70-74 derajat Fahrenheit plus minus 8 derajat dan *humidity* antara 45-60%, *Electricity Generator* sebagai perangkat *backup power* untuk server saat pasokan listrik utama terputus, *Fire Alarm System (Detection sensor* and *Extinguisher)* termasuk sensor api, jaringan hidran, dan alat pemadam api untuk mengantisipasi risiko kebakaran serta *Intruder Alarm* dan *Security Access System* sebagai sistem keamanan mencegah risiko masuknya penyusup kedalam ruang server. Semua perangkat pendukung tersebut telah terintegrasi dalam suatu *Integrated Facility Management System (FMS)* dan aktif selama 24 jam sehari selama setahun penuh.

Selanjutnya bentuk pengelolaan keamanan informasi aplikasi SPAN adalah pemeliharaan sistem informasi yang mencakup perangkat keras (*hardware*), perangkat lunak (*software*), perangkat jaringan *(netware)*, dan *brainware.*

a. Pemeliharaan perangkat keras dilakukan secara berkala dengan reparasi, penggantian, atau penambahan suku cadang dan komponen untuk merestorasi atau menjaga agar perangkat keras tetap bekerja dengan baik. Komponen perangkat keras sistem informasi dicek dan diservis secara periodik.
b. Pemeliharaan perangkat lunak dilakukan dengan selalu meng-*update antivirus* untuk melindungi *software* dari serangan virus yang berbahaya. Selain itu dilakukan juga kebijakan *backup* dan *recovery* sebagai usaha preventif terhadap sesuatu yang tidak diinginkan.
c. Pemeliharaan perangkat jaringan selalu dilakukan secara berkala mencakup jaringan *LAN/WAN/Wireless* yang dimiliki Direktorat Jenderal Perbendaharaan.
d. Pemeliharaan perangkat *brainware* meliputi seluruh sumber daya manusia atau pegawai di Direktorat Jenderal Perbendaharaan. Pemeliharaan *brainware* dilakukan dengan cara memberikan bimbingan teknis, pendidikan dan pelatihan secara berkala mengenai sistem informasi terbaru dan mendistribusikan buku panduan keamanan TI kepada seluruh unit vertikal di Direktorat Jenderal Perbendaharaan baik di kantor pusat maupun di kantor daerah sehingga dapat meningkatkan *security awareness* pegawai.

Bentuk pengelolaan keamanan informasi aplikasi SPAN yang terakhir adalah pengelolaan gangguan atau insiden keamanan TI melalui *service desk* SPAN. *Service desk* SPAN terbagi dalam tiga lapisan pelayanan *(3 tiers)*. Lapis

pertama adalah *operator*, yakni pegawai yang telah di-*training* untuk menangani gangguan yang dapat dipandu via telepon dan sudah ada *knowledge base*. *Knowledge base* ini akan selalu dibuat apabila ada permasalahan baru, sehingga apabila ada permasalahan yang sama muncul lagi, maka penyelesaiannya akan jauh lebih cepat. Lapis kedua terdiri terdiri dari Tim IT dan Tim Bisnis Proses dari Ditjen Anggaran dan Ditjen Perbendaharaan. Lapis ketiga adalah tenaga ahli dan level pimpinan. Ketika sebuah gangguan masih tidak terselesaikan pada lapis kedua, maka gangguan tersebut akan di-*eskalasi* ke lapis tiga, dimana sudah melibatkan tim ahli dari masing-masing kompetensi.

8. HASIL PENELITIAN

Hasil penelitian diperoleh melalui proses penilaian dalam Indeks KAMI yang dilakukan dengan menggunakan 2 (dua) metode yaitu jumlah (kelengkapan) bentuk pengamanan dan tingkat kematangan proses pengelolaan pengamanan informasi. Metode pertama akan mengevaluasi sejauh mana Dirjen Perbendaharaan sudah menerapkan pengamanan sesuai dengan kelengkapan kontrol yang diminta oleh standar ISO/IEC 27001:2009. Metode yang kedua merupakan perluasan dari evaluasi kelengkapan dan digunakan untuk mengidentifikasi tingkat kematangan penerapan pengamanan dengan kategorisasi yang mengacu kepada tingkatan kematangan yang digunakan oleh kerangka kerja COBIT *(Control Objective for Information and related Technology)* atau CMMI *(Capability Maturity Model for Integration)*. Hasil akhir penelitian yang diperoleh melalui 2 (dua) metode penilaian tersebut dapat dilihat dalam 3 (tiga) instrumen berikut ini:

8.1. Tabel nilai masing-masing area

Nilai berisikan total skor untuk tiap area yang dievaluasi dapat dilihat pada Tabel 1.

Berdasarkan informasi Tabel 1 dapat diketahui bahwa:

a. Tingkat ketergantungan terhadap TIK (aplikasi SPAN) pada Direktorat Jenderal Perbendaharaan masuk ke dalam klasifikasi kritis. Hal ini karena jumlah skor/nilai pada bagian I kuesioner mengenai peran/ tingkat kepentingan TIK sebesar 46 yang masuk ke dalam klasifikasi kritis. (Lihat Tabel 2).
b. Level tingkat kematangan
   1) Bagian II mengenai tata kelola keamanan informasi mendapatkan jumlah skor 89 dan berada pada level/ tingkat kematangan III+.
   2) Bagian III mengenai pengelolaan risiko keamanan informasi mendapatkan jumlah skor 30 dan berada pada level/ tingkat kematangan II.
   3) Bagian IV mengenai kerangka kerja keamanan informasi mendapatkan jumlah skor 106 dan berada pada level/ tingkat kematangan II.
   4) Bagian V mengenai pengelolaan aset informasi mendapatkan jumlah skor 112 dan berada pada level/ tingkat kematangan II.

Tabel 1. Nilai Akhir Area Keamanan Informasi

Area	Skor
Peran/Tingkat Kepentingan TIK	46
Tata Kelola	89
Pengelolaan Risiko	30
Kerangka Kerja Keamanan Informasi	106
Pengelolaan Aset Informasi	112
Teknologi dan Keamanan Informasi	92

Sumber: Data diolah dengan Indeks KAMI versi 2.3

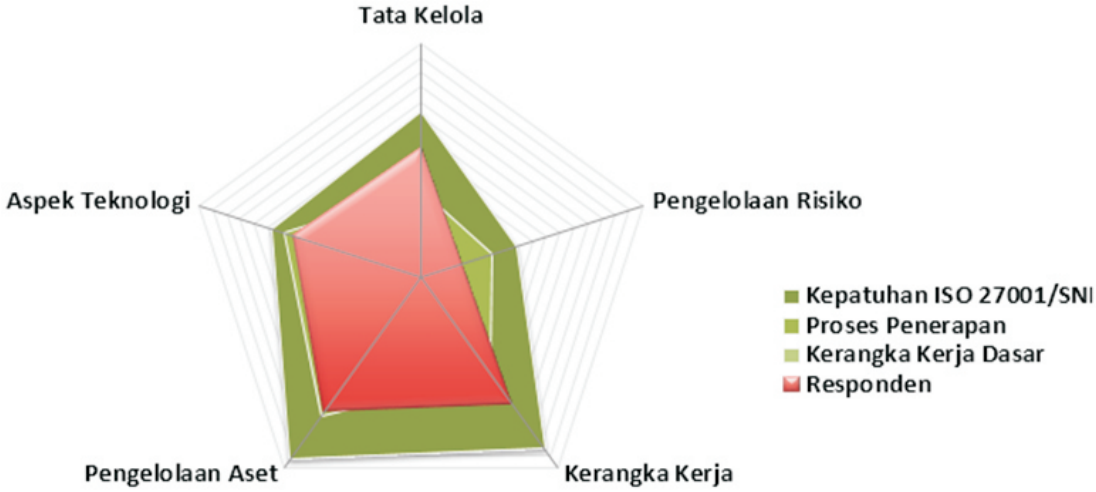
Skor	Tata Kelola	Pengelolaan Risiko	Kerangka Kerja	Pengelolaan Aset	Teknologi
Skor Maksimal	114	69	144	153	108
Persentase	78%	43%	74%	73%	85%

Tabel 2. Persentase Capaian Skor Responden

Skor	Tata Kelola	Pengelolaan Risiko	Kerangka Kerja	Pengelolaan Aset	Teknologi
Skor Penelitian	89	30	106	112	92
Skor Maksimal	114	69	144	153	108
Persentase	78%	43%	74%	73%	85%

Sumber: Data diolah dari Indeks KAMI

Gambar 2. Diagram Radar Hasil Akhir Penilaian Area Keamanan Informasi



Sumber: Data diolah dengan Indeks KAMI versi 2.3

5) Bagian VI mengenai teknologi dan keamanan informasi mendapatkan jumlah skor 92 dan berada pada level/ tingkat kematangan II+.

8.2. Diagram radar dengan lima sumbu sesuai area pengamanan.

Diagram radar dimaksudkan untuk menggambarkan hubungan antara kepatuhan terhadap standar yang ditetapkan oleh ISO 27001/SNI dan KMK Nomor 479 Tahun 2010, status penerapan, kerangka kerja dasar, dan skor dari masing-masing area. Diagram radar untuk tiap area yang dievaluasi sebagai berikut:

Pada Gambar 2, diagram berwarna merah muda merupakan kondisi Sistem Manajemen Keamanan Informasi (SMKI) Direktorat Jenderal Perbendaharaan berdasarkan hasil pengisian kuesioner oleh para responden/ informan. Berdasarkan Gambar 2 tersebut dapat dicermati bahwa:

a. Berdasarkan kelima area keamanan informasi yang diamati, tampak bahwa Direktorat Jenderal Perbendaharaan telah memiliki aspek teknologi keamanan informasi dan tata kelola keamanan informasi yang jauh lebih baik dibanding area keamanan lainnya (paling mendekati standar yang ditetapkan dalam ISO 27001 dan KMK 479/2010).
b. Berdasarkan kelima area keamanan informasi yang diamati, tampak bahwa area terlemah SMKI Direktorat Jenderal Perbendaharaan terdapat pada area penge-lolaan risiko keamanan informasi (masih sangat jauh dari standar yang ditetapkan dalam ISO 27001 dan KMK 479/2010).

8.3. Bar Chart Tingkat Kelengkapan Penerapan Standar ISO27001

Bar Chart dimaksudkan untuk menggambarkan status kesiapan atau kelengkapan pengamanan informasi berdasarkan standar ISO 27001. *Bar chart* hasil akhir penilaian area keamanan informasi dapat dilihat pada Gambar 3.

Gambar 3. *Bar Chart* Hasil Akhir Penilaian Area Keamanan Informasi

Sumber: Data diolah dengan Indeks KAMI versi 2.3

Dari Gambar 3 dapat diketahui bahwa status kesiapan atau kelengkapan pengamanan informasi Direktorat Jenderal Perbendaharaan berdasarkan standar ISO 27001 berada di area warna kuning atau berarti masih "Memerlukan Perbaikan". Sebagai padanan terhadap standar ISO/IEC 2700:2005, tingkat kematangan yang diharapkan untuk ambang batas minimum kesiapan sertifikasi adalah tingkat III+ (berada pada area warna hijau).

9. SIMPULAN

a. Tingkat ketergantungan terhadap Teknologi Informasi dan Komunikasi (aplikasi SPAN) pada Direktorat Jenderal Perbendaharaan menunjukkan angka 46 atau berada pada tingkatan "kritis".
b. Tingkat kesiapan atau kelengkapan pengamanan informasi Direktorat Jenderal Perbendaharaan berdasarkan standar ISO 27001 menunjukkan angka 370 dari total keseluruhan 588 dan berada di area warna kuning atau berarti masih "Memerlukan Perbaikan".
c. Tingkat kematangan Sistem Manajemen Keamanan Informasi Direktorat Jenderal Perbendaharaan berdasarkan hasil pengumpulan data menggunakan kuesioner Indeks KAMI adalah Tingkat II atau dalam klasifikasi Penerapan Kerangka Dasar (AKTIF), yang memiliki arti antara lain:
    a) Pengamanan sudah diterapkan walaupun sebagian besar masih di area teknis dan belum adanya keterkaitan langkah pengamanan untuk mendapatkan strategi yang efektif.
    b) Proses pengamanan berjalan tanpa dokumentasi atau rekaman resmi.
    c) Langkah pengamanan operasional yang diterapkan bergantung kepada pengetahuan dan motivasi individu pelaksana.
    d) Bentuk pengamanan secara keseluruhan belum dapat dibuktikan efektivitasnya.
    e) Kelemahan dalam manajemen pengamanan masih banyak ditemukan dan tidak dapat diselesaikan dengan tuntas oleh pelaksana maupun pimpinan sehingga menyebabkan dampak yang sangat signifikan.
    f) Manajemen pengamanan belum mendapatkan prioritas dan tidak berjalan secara konsisten.
    g) Pihak yang terlibat kemungkinan besar masih belum memahami tanggung jawab mereka.

10. SARAN

1. Peningkatan aspek pengelolaan risiko keamanan informasi karena aspek ini merupakan aspek dengan hasil penilaian terendah di antara kelima aspek keamanan informasi. Untuk itu, perlu ditingkatkan dengan cara sebagai berikut:
    a. Pembuatan Pedoman Pelaksanaan Manajemen Risiko Keamanan Informasi di Lingkungan Direktorat Jenderal Perbendaharaan.
    b. Mengkaji ulang profil risiko berikut bentuk mitigasinya secara berkala, untuk memastikan akurasi dan validitasnya.
    c. Melakukan pemantauan secara berkala status penyelesaian langkah mitigasi risiko, untuk memastikan penyelesaian atau kemajuan kerjanya.
2. Peningkatan aspek tata kelola keamanan informasi dengan cara sebagai berikut:
    a. Memetakan secara lengkap dan jelas peran pelaksana pengamanan informasi dalam sebuah uraian jabatan.
    b. Mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi dalam sebuah peraturan tertulis.
    c. Memastikan bahwa pelaksana pengelolaan keamanan informasi memenuhi persyaratan/standar kompetensi dan keahlian sesuai dengan peraturan.
    d. Mendefinisikan paramater, metrik dan mekanisme pengukuran kinerja pengelolaan keamanan informasi bagi pejabat dan pelaksana pengamanan informasi.

e. Menerapkan pengukuran kinerja pengelolaan keamanan informasi bagi pejabat dan pelaksana pengamanan informasi.

3. Pembuatan peraturan dalam bentuk Peraturan Dirjen Perbendaharaan mengenai Standar dan Kebijakan Sistem Manajemen Keamanan Informasi di Lingkungan Direktorat Jenderal Perbendaharaan. Hal ini diperlukan dengan semakin pentingnya aspek keamanan informasi dalam pelaksanaan Sistem Perbendaharaan dan Anggaran Negara (SPAN) dalam menjalankan tugas pokok dan fungsi organisasi.
4. Pelaksanaan program audit internal keamanan informasi SPAN secara rutin. Hal ini dapat dilakukan dengan memaksimalkan fungsi Bagian Kepatuhan Internal yang selama ini belum menjangkau fungsi audit internal terkait aspek keamanan informasi.
5. Pembuatan kebijakan dan prosedur keamanan informasi dengan memastikan bahwa keseluruhan kebijakan dan prosedur keamanan informasi tersebut telah merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi.
6. Penyediaan dan penerapan mekanisme pengelolaan dokumen kebijakan dan prosedur keamanan informasi secara konsisten baik dalam bentuk *softcopy* maupun *hardcopy*. Kebijakan dan prosedur keamanan informasi yang terdokumentasi dengan baik menunjukkan bahwa suatu kontrol/sistem pengendalian telah dilakukan sesuai dengan persyaratan. Hal ini diperlukan sebagai salah satu persyaratan dalam mendapatkan sertifikat ISO Keamanan Informasi.
7. Peningkatan pemahaman tentang keamanan informasi kepada semua pihak (pegawai, pejabat, pihak ketiga) melalui berbagai media. Hal ini dilakukan untuk meningkatkan *security awareness* atau kesadaran atas keamanan informasi.
8. Penetapan rencana dan program *(blueprint)* peningkatan keamanan informasi untuk jangka menengah/panjang yang direalisasikan secara konsisten.

REFERENSI

Afrianto, Irawan, Taryana Suryana, dan Sufa'atin. 2015. *Pengukuran dan Evaluasi Keamanan Informasi Menggunakan Indeks KAMI – SNI ISO/IEC 27001:2009* - Studi Kasus Perguruan Tinggi X. Bandung: Universitas Komputer Indonesia.

Agustian, Fajrin. 2011. *Kajian Tingkat Kematangan Sistem Manajemen Keamanan Informasi menggunakan Indeks KAMI (Studi Kasus: Kantor Pusat Direktorat Jenderal Pajak)*. Tangerang Selatan: Sekolah Tinggi Akuntansi Negara.

Badan Standardisasi Nasional. 2009. SNI ISO/IEC 27001:2009 Teknologi Informasi – Teknik Keamanan – Sistem Manajemen Keamanan Informasi – Persyaratan. Jakarta: Badan Standardisasi Nasional – BSN

Committee on National Security Systems: *National Information Assurance (IA) Glossary*, CNSS *Instruction* No. 4009, 26 April 2010.

Direktorat Transformasi Perbendaharaan. 2013. Modul SPAN-SAKTI. Jakarta: Direktorat Jenderal Perbendaharaan.

Direktorat Transformasi Perbendaharaan. 2013. Slide *Overview* SPAN. Jakarta: Direktorat Jenderal Perbendaharaan.

ISO/IEC 27000:2009 (E). (2009). *Information technology - Security techniques - Information security management systems - Overview and vocabulary*. ISO/IEC.

ISO/IEC FIDIS 27005:2008. *Information technology - Security techniques-Information security risk management*. ISO/IEC.

Kementerian Komunikasi dan Informatika. 2011. *Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan*

Publik. Jakarta: Direktorat Keamanan Informasi Direktorat Jenderal Aplikasi dan Informatika Informasi Kementerian Komunikasi dan Informatika.

Kurniawan, Fanny Wahyu. 2015. *Pengukuran Indeks Keamanan Sistem Informasi Berdasarkan Standar ISO 27001 (Studi Kasus Instansi Badan Nasional Penempatan dan Perlindungan Tenaga Kerja Indonesia)*. Jakarta: Universitas Mercu Buana.

McLeod, Raymond Jr. dan George Schell. 2008. *Sistem Informasi Manajemen*, Jakarta: Indeks.

Soenardi, Iqbal dan M. Ichsan. 2013. *Analisis Kematangan Sistem Manajemen Keamanan Informasi Badan Pendidikan dan Pelatihan Keuangan Diukur Menggunakan Indeks Keamanan Informasi*. Jakarta: Badan Pendidikan dan Pelatihan Keuangan.

The Open Group. 2011. *Open Book Standard - Open Information Security Management Maturity Model (O-ISM3)*. United Kingdom: The *Open Group*.

Websites dan Sumber Lainnya

Direktorat Jenderal Perbendaharaan. Sejarah Direktorat Jenderal Perbendaharaan. http://www.djpbn.kemenkeu.go.id/portal/id/profil/profil-organisasi/sejarah.html (diakses 11 November 2015).

Direktorat Jenderal Perbendaharaan. Visi dan Misi Direktorat Jenderal Perbendaharaan. http://www.djpbn.kemenkeu.go.id/portal/id/profil/profil-organisasi/visi-misi.html (diakses 11 November 2015).

ISACA. (2008). *Glossary of terms*, 2008. *Retrieved from* http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf (diakses 6 November 2015).

Sistem Perbendaharaan dan Anggaran Negara. Project Management SPAN. http://www.span.kemenkeu.go.id/content/single-span-project-management (diakses 7 November 2015).

Sistem Perbendaharaan dan Anggaran Negara. Sejarah SPAN. http://www.span.kemenkeu.go.id/content/span-template-artikel (diakses 7 November 2015).

Sistem Perbendaharaan dan Anggaran Negara. Teknologi SPAN. http://www.span.kemenkeu.go.id/content/single-it-aplikasi (diakses 7 November 2015).

Perrin, Chad. 2008. *The CIA Triad*. 30 Juni 2008. http://www.techrepublic.com/blog/it-security/the-cia-triad/ (diakses 6 November 2015).

Peraturan Perundang-undangan

Kementerian Keuangan Republik Indonesia. 2014. Peraturan Menteri Keuangan Nomor 206/PMK.01/2014 Tahun 2014 tentang Organisasi dan Tata Kerja Kementerian Keuangan.

Kementerian Keuangan Republik Indonesia. 2010. Keputusan Menteri Keuangan Nomor 479/KMK.01/2010 Tahun 2010 tentang Kebijakan dan Standar Sistem Manajemen Keamanan Informasi di Lingkungan Kementerian.

Kementerian Keuangan Republik Indonesia. 2009. Keputusan Menteri Keuangan Nomor 72/KMK.05/2009 Tahun 2009 tentang Program Reformasi Penganggaran dan Perbendaharaan Negara.

Kementerian Keuangan Republik Indonesia. 2009. Keputusan Menteri Keuangan Nomor 512/KMK.01/2009 Tahun 2009 tentang Kebijakan dan Standar Penggunaan Akun dan Kata Sandi, Surat Elektronik, dan Internet di Lingkungan Departemen Keuangan.

Kementerian Keuangan Republik Indonesia. 2008. Keputusan Menteri Keuangan Nomor 276/KMK.05/2008 Tahun 2008 tentang Program Reformasi Sistem Perbendaharaan dan Anggaran Negara.