Penyusunan Panduan Pengelolaan Keamanan Informasi Untuk *Firewall Configuration* Berdasarkan Kerangka Kerja PCI DSS v.3.1 dan COBIT 5

Bagus Puji Santoso[1)], Eva Hariyanti[2)], Eto Wuryanto[3)]

[1)3)] *Program Studi S1 Sistem Informasi, Fakultas Sains dan Teknologi, Universitas Airlangga Surabaya*

[1)]bagus.puji_12@fst.unair.ac.id

[2)]eva.hariyanti@fst.unair.ac.id

[3)]etowuryanto@gmail.com

Abstrak — **Sistem keamanan informasi harus dilindungi dari segala macam serangan dan usaha penyusupan oleh pihak yang tidak berhak. Salah satu mekanisme yang dapat diterapkan dalam meningkatkan keamanan informasi adalah dengan menggunakan *firewall. Firewall* merupakan sebuah mekanisme pengamanan yang dilakukan dengan cara melakukan kegiatan penyaringan paket data yang masuk dan keluar jaringan. Sehingga untuk dapat mengelola keamanan informasi dengan baik, dibutuhkan suatu tata kelola TI. Salah satu tata kelola TI yang dimaksud adalah berupa penyusunan panduan pengelolaan keamanan informasi. Penelitian ini bertujuan untuk membuat sebuah referensi keamanan informasi berupa panduan pengelolaan keamanan informasi untuk *firewall configuration* yang mengacu pada standar PCI DSS v.3.1 dan COBIT 5 dengan mengambil studi kasus di DSIK Universitas Airlangga. Penyusunan panduan pengelolaan keamanan informasi untuk *firewall configuration* dilakukan dalam tiga tahap. Tahap pertama adalah penyusunan prosedur pengelolaan keamanan informasi untuk *firewall configuration* yang terdiri dari tahap analisis pemetaan proses, tahap penyusunan prosedur dan tahap penentuan peran dan deskripsi kerja. Tahap kedua adalah tahap verifikasi panduan yang dilakukan melalui pemberian kuesioner penilaian. Tahap ketiga adalah tahap perbaikan panduan. Tahap perbaikan ini dilakukan untuk memperbaiki kekurangan yang dihasilkan saat verifikasi. Hasil verifikasi menunjukkan bahwa sebanyak 42,86% responden menyatakan panduan pengelolaan yang dibuat, secara operasional sangat mudah untuk dilaksanakan**

Kata Kunci— **COBIT 5, Keamanan Sistem Informasi, PCI DSS v.3.1, Panduan Pengelolaan**

Abstract— ***Information security systems must be protected from all attacks and interuptions by an unauthorized user. Firewall is a mechanism that can be applied to improve the security information which done by filtering data packets that enter and exit the network. IT governance is needed to manage good information security. IT governance can use to make the arrangement of guidelines for the management of information security. This research aims to create a reference guide to information security such as an information security management guide for firewall configuration that refers to the framework of PCI DSS v.3.1 and COBIT 5 by taking a case study at the DSIK Universitas Airlangga.Arrangement of guidelines for information security management for firewall configuration will be done in three stages. The first stage was the arrangement of information security management procedures for firewall configuration which consists of mapping analysis stage process, arrangement procedure's stage and determining roles and job description's stage. In the second stage was the verification of the information security management guidance using a questionnaire. The third stage was improvement of the information security management guidance. These improvements was done to correct deficiencies that were produced when verification. The verification results show that 42.86% of respondents said that management guidelines are operationally very easy to be implemented.***

Keywords— **COBIT 5, *Information Security*, PCI DSS v.3.1, *Management Guide*.**

Article history:
Received 31 May 2016; Received in revised form 28 July 2016; Accepted 5 August 2016; Available online 28 October 2016

I. PENDAHULUAN

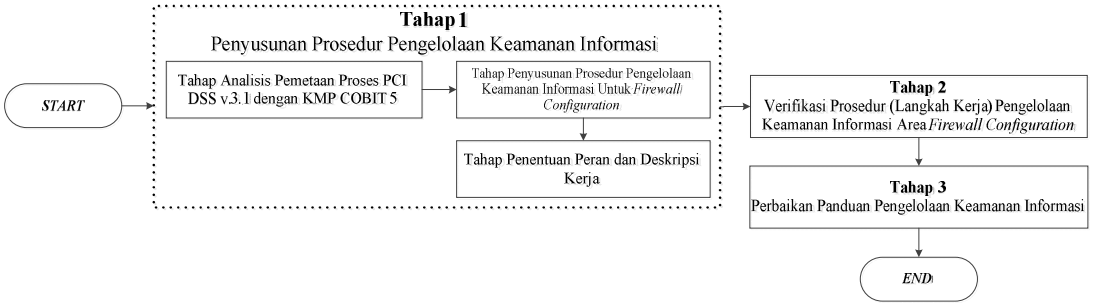
Keamanan informasi merupakan bagian dari sebuah sistem yang sangat penting untuk menjaga validitas dan integritas data serta menjamin ketersediaan layanan bagi penggunaannya. Sistem keamanan informasi harus dilindungi dari segala macam serangan dan usaha - usaha penyusupan atau pemindaian oleh pihak yang tidak berhak. Salah satu mekanisme yang dapat diterapkan dalam meningkatkan keamanan informasi adalah dengan menggunakan *firewall. Firewall* merupakan sebuah mekanisme pengamanan yang dilakukan dengan cara melakukan kegiatan penyaringan paket data yang masuk dan keluar jaringan. Sehingga untuk dapat mengelola keamanan informasi dengan baik, dibutuhkan suatu tata kelola TI. Salah satu tata kelola TI yang dimaksud adalah berupa penyusunan panduan pengelolaan keamanan informasi. Tata Kelola TI merupakan sebuah konsep yang dikembangkan oleh *IT Governance Institute* (ITGI) sebagai bagian integral dari tata kelola perusahaan, yang terdiri dari struktur organisasi dan kepemimpinan, serta proses yang memastikan bahwa organisasi TI

e-ISSN 2443-2555

tersebut mendukung strategi dan tujuan organisasi (IT Governance., 2003). Adapun definisi lain dari Tata Kelola TI yaitu merupakan penilaian kapasitas organisasi oleh dewan direksi, manajemen eksekutif, dan manajemen teknologi informasi dalam rangka mendukung bisnisnya (Grembergen, 2002). Dengan adanya Tata Kelola TI maka pengamanan aset, pemeliharaan integritas data, dapat mendorong pencapaian tujuan organisasi secara efektif dan menggunakan sumber daya secara efisien. Tata Kelola TI merupakan salah satu pilar utama dari *Good Corporate Governance* (GCG), maka dalam pelaksanaan Tata Kelola TI yang baik sangat diperlukan standar tata kelola Tl dengan mengacu pada standar tata kelola TI internasional yang telah diterima secara luas dan teruji implementasinya (Komalasari & Perdana, 2014). Tata kelola TI termasuk di dalamnya adalah kemanan informasi. Contoh dari keamanan informasi antara lain (Sarno & Iffano, 2009) : (a) *Physical Security* adalah keamanan informasi yang memfokuskan pada strategi untuk mengamankan individu atau anggota organisasi, aset fisik, dan tempat kerja dari berbagai ancaman yang meliputi bahaya kebakaran, akses tanpa otorisasi, dan bencana alam; (b) *Personal Security* adalah keamanan informasi yang berhubungan dengan keamanan personil. Biasanya saling berhubungan dengan ruang lingkup *physical security;* (c) *Operational Security* adalah keamanan informasi yang membahas bagaimana strategi suatu organisasi untuk mengamankan kemampuan organisasi tersebut untuk beroperasi tanpa gangguan; (d) *Communication Security* adalah keamanan informasi yang bertujuan mengamankan media komunikasi, teknologi komunikasi serta apa yang masih ada di dalamnya. Serta kemampuan untuk memanfaatkan media dan teknologi komunikasi untuk mencapai tujuan organisasi; dan (d) *Network Security* adalah keamanan informasi yang memfokuskan pada bagaimana pengamanan peralatan jaringannya, data organisasi, jaringan dan isinya, serta kemampuan untuk menggunakan jaringan tersebut dalam memenuhi fungsi komunikasi data organisasi.

Penerapan tata kelola TI dapat dilakukan dengan menggunakan berbagai kerangka kerja. Kerangka kerja yang digunakan pada penelitian ini adalah *Payment Card Industry Data Security Standard* (PCI DSS) dan *Control Objective for Information and Related Technology* (COBIT). PCI DSS adalah sebuah standar keamanan yang dikembangkan bertujuan untuk meningkatkan keamanan data pemegang kartu (seperti kartu kredit, kertu debit, ATM), dan memberikan fasilitas pengadopsian pengamanan data secara konsisten serta global. PCI DSS menyediakan dasar persyaratan teknis dan operasional yang dirancang untuk melindungi data pemegang kartu (Cian & Mark, 2009). Sedangkan COBIT merupakan suatu panduan *best practice* untuk Tata kelola TI yang dapat membantu auditor, pengguna, dan manajemen, untuk menjembatani *gap* antara risiko bisnis, kebutuhan kontrol dan masalah-masalah teknis TI.

Berdasarkan hasil penelitian sebelumnya yang menggunakan penggabungan 2 kerangka kerja yaitu PCI DSS dan ISO 27001, menyebutkan bahwa penggabungan standar PCI DSS dan ISO 27001 dapat menghasilkan *best practices* keamanan informasi. Penggabungan dua atau lebih kerangka kerja dapat digunakan untuk saling melengkapi standar keamanan informasi lainnya (Lovrić, 2012). Pelaksanaan proses keamanan informasi pada PCI DSS memungkinkan penggunaan dari COBIT 5 untuk mendukung pemenuhan standar keamanan PCI DSS v.3.1 (Beissel, 2014). COBIT 5 membantu perusahaan dalam tata kelola dan manajemen perusahaan IT secara umum dan pada saat yang sama mendukung kebutuhan untuk memenuhi persyaratan keamanan dengan memungkinkan proses operasional dan kegiatan manajemen. Pemetaan COBIT 5 memungkinkan proses keamanan untuk persyaratan PCI DSS v.3.1 yang memfasilitasi penerapan secara simultan dan membantu menciptakan sinergi dalam perusahaan. Dalam memenuhi tata kelola TI yang baik yang mengacu pada standar PCI DSS v.3.1 dan COBIT 5, maka melalui penelitian ini akan dibuat sebuah panduan pengelolaan keamanan informasi yang bersifat umum dan menyeluruh untuk *firewall configuration* yang terdiri dari prosedur keamanan informasi. Panduan pengelolaan keamanan



Gambar 1 Alur Metode Penelitian

informasi yang dihasilkan akan diujicobakan di DSIK Universitas Airlangga. DSIK Universitas Airlangga dipilih sebagai tempat studi kasus pada penelitian ini dikarenakan DSIK Universitas Airlangga telah menerapkan mekanisme pengamanan data dengan menggunakan *firewall.* Namun pada tahun 2015, dalam setahun *firewall* DSIK Universitas Airlangga telah ditembus oleh pihak yang tidak terotorisasi sebanyak 5 kali. Sehingga untuk saat ini, DSIK Universitas Airlangga memerlukan sebuah referensi standar keamanan informasi yang dapat digunakan sebagai bahan acuan dalam pengelolaan *firewall* yang sesuai dengan permasalahan yang dibahas dalam penelitian. Luaran dari penelitian ini berupa dokumen panduan pengelolaan keamanan informasi untuk *firewall configuration* berdasarkan kerangka kerja PCI DSS v.3.1 dan COBIT 5. Dokumen panduan pengelolaan keamanan informasi ini bersifat umum dan dapat digunakan oleh berbagai perusahaan.

II. METODE PENELITIAN

Penelitian ini dilakukan dengan 3 tahap yang terdiri dari: Tahap penyusunan prosedur pengelolaan keamanan informasi, tahap verifikasi panduan pengelolaan keamanan informasi dan tahap perbaikan panduan pengelolaan keamanan informasi. Alur metode penelitian pada penelitian ini dapat dilihat pada Gambar 1.

A. Penyusunan Prosedur Pengelolaan Keamanan Informasi

Terdapat 3 tahap dalam penyusunan prosedur pengelolaan keamanan informasi yaitu: Tahap analisis pemetaan proses PCI DSS v.3.1 (PCI Security Standards Council, 2015) (PCI Security, 2015) dengan KMP COBIT 5 (ISACA, 2012a) (ISACA, 2012b) (ISACA, 2012c), tahap penyusunan prosedur pengelolaan keamanan informasi untuk *Firewall Configutarion* dan tahap penentuan peran dan deskripsi kerja.

1) Tahap Analisis Pemetaan Proses PCI DSS v.3.1 dengan KMP COBIT 5

Pemetaan ini bertujuan untuk menentukan KMP COBIT 5 yang berkaitan langsung dengan proses PCI DSS v.3.1. Namun, sebelum melakukan pemetaan proses, terlebih dahulu akan dilakukan penyelarasan kebijakan *firewall.* Penyelarasan ini bertujuan untuk mengetahui kebijakan umum dalam penerapan *firewall* telah terdapat dalam proses PCI DSS v.3.1. Penyelarasan kebijakan dilakukan dengan memetakan kebijakan *firewall* yang terdapat pada SOP *Firewall* DEPKOMINFO (DEPKOMINFO, 2010) dengan proses PCI DSS v.3.1 (PCI Security Standards Council, 2015). Tahap selanjutnya adalah analisis proses PCI DSS v.3.1 (PCI Security Standards Council, 2015) dengan KMP COBIT 5 (ISACA, 2012c). Analisis proses dilakukan dengan cara memetakan aktivitas PCI DSS v.3.1 dan KMP COBIT 5 yang saling bersesuaian kedalam lima pendekatan bertahap dalam pengelolaan *firewall* menurut SOP *firewall* DEPKOMINFO.

2) Tahap Penyusunan Prosedur Pengelolaan Keamanan Informasi Untuk Firewall Configuration

Pada tahap ini dilakukan penyusunan prosedur pengelolaan keamanan informasi untuk *firewall configuration.* Hasil dari analisis pemetaan proses PCI DSS v.3.1 dengan KMP COBIT 5 akan digunakan sebagai acuan dalam pembuatan langkah kerja pengelolaan keamanan informasi. Prosedur pengelolaan keamanan informasi ini berisi tentang langkah kerja yang harus dilakukan dalam pengelolaan keamanan informasi berdasarkan aktivitas - aktivitas yang didapatkan dari gabungan aktivitas PCI DSS v.3.1 area *firewall configuration* dengan COBIT 5.

3) Tahap Penentuan Peran dan Deskripsi Kerja

Tahap ini dilakukan setelah melakukan tahap penyusunan prosedur pengelolaan keamanan informasi untuk *firewall configuration.* Untuk setiap aktifitas yang terdapat pada prosedur tersebut akan ditentukan peran dan tanggung jawab dan kemudian menentukan deskripsi kerja untuk setiap peran. Peran tersebut kemudian disesuaikan dengan RACI *chart* COBIT 5 (ISACA, 2012c) dan struktur organisasi pada suatu perusahaan.

B. Verifikasi Panduan Pengelolaan Keamanan Informasi

Verifikasi dilakukan untuk mengetahui apakah panduan pengelolaan keamanan informasi mudah untuk dipahami dan dapat diimplementasikan dalam organisasi atau institusi. Verifikasi dilakukan dengan mengambil studi kasus di DSIK Universitas Airlangga dan dilakukan tanpa adanya penyesuaian atau spesifikasi terhadap DSIK Universitas Airlangga. *Item* pertanyaan yang digunakan dalam kuesioner berupa pertanyaan terkait penggunaan bahasa dan kesesuaian panduan dengan kondisi DSIK Universitas Airlangga.

C. Perbaiki Panduan Pengelolaan Keamanan Informasi

Setelah melakukan tahap verifikasi panduan pengelolaan keamanan informasi maka tahap selanjutnya adalah tahap perbaikan panduan pengelolaan keamanan informasi. Tahap perbaikan ini dilakukan untuk memperbaiki kekurangan yang ditemukan pada saat tahap verifikasi.

III. HASIL DAN PEMBAHASAN

A. Penyusunan Prosedur Pengelolaan Keamanan Informasi

1) Tahap Analisis Pemetaan Proses PCI DSS v.3.1 dengan KMP COBIT 5

Pada tahap ini dilakukan studi literatur dan analisis proses PCI DSS v.3.1 dan KMP COBIT 5. Literatur PCI DSS v.3.1 yang digunakan yaitu "PCI : *Requirements and Security Assessment Procedures Version* 3.1" sedangkan literatur KMP COBIT 5 yang digunakan adalah "COBIT 5 : *Enabling Processes".* Terdapat dua langkah dalam tahap ini yaitu :

a) Tahap Penyelarasan Kebijakan Firewall

Penyelarasan kebijakan firewall dilakukan dengan memetakan kebijakan firewall yang terdapat pada SOP Firewall DEPKOMINFO dengan proses PCI DSS v.3.1. Dari hasil penyelarasan kebijakan menunjukkan bahwa terdapat proses PCI DSS v.3.1 yang bersesuaian dengan empat kebijakan dalam SOP *Firewall* DEPKOMINFO. Hasil analisis penyelarasan kebijakan *firewall* dapat dilihat pada Tabel 1.

TABEL 1. HASIL PENYELARASAN KEBIJAKAN *FIREWALL*

Kebijakan *Firewall* DEPKOMINFO	**Kode Proses**
Kebijakan Berbasis Hubungan Antar Zone	PCI-1.4, PCI-2.1, PCI-3.1, PCI-3.2, PCI-3.3, PCI-3.4 PCI-3.5, PCI-3.6, PCI-3.7, PCI-3.8.
Kebijakan Berbasis IP dan Protokol	PCI-1.6, PCI-2.1
Kebijakan Berbasis Pada Aplikasi	PCI-3.8.
Kebijakan Berbasis Pada Identitas *User*	PCI-1.5, PCI-2.3.

Dari hasil penyelarasan kebijakan menunjukkan bahwa terdapat proses PCI DSS v.3.1 yang bersesuaian dengan empat kebijakan dalam SOP *Firewall* DEPKOMINFO. Hasil analisis penyelarasan kebijakan *firewall* menunjukkan bahwa :

1. Kebijakan berbasis hubungan antar zone yang diterapkan antara lain : (a) Pemasangan *Access Rule a*ntara jaringan internal dengan *Demilitarized Zone* (DMZ), terdapat pada proses PCI DSS v.3.1 dengan kode proses PCI-1.4, PCI-3.1, dan PCI-3.2; (b) Pemasangan *Access Rule* antara jaringan internal dengan jaringan eksternal, terdapat pada proses PCI DSS v.3.1 dengan kode proses PCI-2.1, PCI-3.3, PCI-3.4, PCI-3.5, PCI-3.6, dan PCI-3.7; (c) *Routing* atau *Network Address Translation* (NAT), terdapat pada proses PCI DSS v.3.1 dengan kode proses PCI-3.8.
2. Kebijakan berbasis IP atau protokol yang diterapkan adalah hanya mengijinkan protokol IP yang dibutuhkan saja dan protokol yang tidak dibutuhkan seharusnya diblok secara *default* atau diblok setelah mengikuti beberapa pernyataan. Kebijakan ini terdapat pada proses PCI DSS v.3.1 dengan kode proses PCI-1.6 dan PCI-2.1.
3. Kebijakan berbasis pada aplikasi yang diterapkan adalah mengaktifkan fitur *proxy*. Penerapan kebijakan *firewall* berbasis pada aplikasi dapat dilakukan jika sistem *firewall* yang digunakan memiliki sistem *proxy*. Kebijakan ini terdapat pada proses PCI DSS v.3.1 dengan kode proses PCI-3.8.
4. Penerapan kebijakan *firewall* berbasis pada identitas *user* dilakukan jika *firewall* yang digunakan memiliki fitur otentikasi dan otorisasi berbasis *user account.* Pengaturan hak akses pengguna terhadap pengiriman *traffic* melalui *firewall* di atur berdasarkan *user account.* Kebijakan ini terdapat pada proses PCI DSS v.3.1 dengan kode proses PCI-1.5 dan PCI-2.3.

Semua kebijakan *firewall* yang terdapat dalam SOP *firewall* DEPKOMINFO tercakup pada proses PCI DSS v.3.1. Sehingga dapat disimpulkan bahwa didalam proses PCI DSS v.3.1 telah mencakup kebijakan umum dalam penerapan *firewall*.

b) Tahap Analisis Pemetaan Proses PCI DSS V.3.1 Dengan KMP COBIT 5

Analisis pemetaan proses dilakukan dengan cara memetakan aktivitas PCI DSS v.3.1 dan KMP COBIT berdasarkan lima pendekatan bertahap dalam pengelolaan *firewall* menurut SOP *Firewal* DEPKOMINFO. Lima pendekatan tersebut adalah Tahap Perencanaan, Tahap Konfigurasi, Tahap Pengujian, Tahap Deloyment, dan Tahap Perawatan. Hasil Pemetaan Proses PCI DSS v.3.1 dan KMP COBIT 5 dapat dilihat pada Tabel 2.

Hasil analisis pemetaan proses PCI DSS v.3.1 dan KMP COBIT 5 menunjukan bahwa:

1. Aktivitas PCI DSS v.3.1 dan KMP COBIT 5 yang terdapat pada tahap perencanaan telah mencakup : (a) Identivikasi ancaman dan kerentanan dalam sistem informasi; (b) Dampak potensial dari kerentanan sistem informasi; (c) Pertimbangan dalam memilih solusi *firewall* yang terdiri dari : kemampuan, pengelolaan, kinerja, dan proses integrasi *firewall* serta lingkungan fisik penempatan *firewall,* dan personil manajaemen jaringan; (d) Perencanaan kebijakan dan prosedur untuk *firewall configuration.*
2. Aktivitas PCI DSS v.3.1 dan KMP COBIT 5 yang terdapat pada tahap konfigurasi telah mencakup : (a) Instalasi perangkat lunak; (b)

TABEL 2. HASIL PEMETAAN PROSES PCI DSS V.3.1 DAN KMP COBIT 5

Tahap	Kode Proses PCI DSS v.3.1	Kode Proses COBIT 5
Perencanaan	PCI-1.1.1, PCI-1.2.1, PCI-1.3.1, PCI-1.5.1, PCI-1.6.1, PCI-1.7.1, dan PCI-3.7.1.	APO03.02-1, APO03.02-2, APO03.02-3, APO03.02-4, APO03.02-5, APO03.02-6, APO03.02-7, APO03.02-8, APO03.02-9, APO12.01-1, APO12.01-2, APO12.01-3, APO12.01-4, APO12.01-5, APO12.01-6, BAI03.03-1, BAI03.03-2, BAI03.03-3, BAI03.03-4, BAI03.03-5, BAI03.03-6, BAI03.05-1, BAI03.05-2, BAI03.05-3, BAI03.05-4, BAI03.05-5, BAI03.05-7, BAI03.05-8, BAI10.01-1, BAI10.01-2, DSS02.03-1, DSS02.03-2, DSS02.03-3, DSS05.02-5, DSS05.04-4, DSS05.04-5, DSS05.04-7, DSS06.03-1, DSS06.03-2, DSS06.03-3, DSS06.03-4, DSS06.03-5, dan DSS06.03-6.
Konfigurasi	PCI-1.4.1, PCI-2.1.1, PCI-2.1.2, PCI-2.1.3, PCI-2.2.1, PCI-2.2.2, PCI-2.3.1, PCI-2.3.2, PCI-3.2.1, PCI-3.3.1, PCI-3.4.1, PCI-3.5.1, PCI-3.6.1, PCI-3.7.1, PCI-3.8.1, dan PCI-4.1.1.	BAI10.02-1, BAI10.02-2, BAI10.03-1, BAI10.03-2, BAI10.03-3, BAI10.03-4,DSS05.02-3, DSS05.02-4,DSS05.02-6, dan DSS05.02-7.
Pengujian	PCI-1.1.1, PCI-1.1.2, PCI-1.1.3,PCI-1.2.1, PCI-1.2.2, PCI-1.3.1, PCI-1.4.1, PCI-1.4.2, PCI-1.4.3, PCI-1.5.1, PCI-1.5.2, PCI-1.6.1, PCI-1.6.2, PCI-1.6.3, PCI-2.1.1, PCI-2.1.2, PCI-2.1.3, PCI-2.3.1, PCI-2.3.2, PCI-3.1.1, PCI-3.2.1, PCI-3.3.1, PCI-3.4.1, PCI-3.5.1, PCI-3.6.1, PCI-3.7.1, PCI-3.8.1, PCI-3.8.2, PCI-4.1.1, dan PCI-4.1.2.	BAI03.05-6, BAI07.03-1, BAI07.03-2, BAI07.03-3, BAI07.03-4, BAI07.03-5, BAI07.03-6, BAI07.03-7, BAI07.03-8, BAI07.05-1, BAI07.05-2, BAI07.05-3, BAI07.05-4, BAI07.05-5, BAI07.05-6, BAI07.05-7, BAI07.05-8, BAI07.05-9, BAI07.05-10, BAI07.05-11, dan DSS05.02-3.
Deployment	PCI-5.1.1.	BAI06.01-1, BAI06.01-2, BAI06.01-3,BAI06.01-4,BAI06.01-5, BAI06.01-6, BAI06.01-7, DSS05.02-1, DSS05.02-2, dan DSS05.04-1.
Perawatan	PCI-1.7.1, PCI-1.7.2, dan PCI-5.1.1.	APO01.08-1, APO01.08-2, APO01.08-3, APO01.08-4, APO01.08-5, BAI03.10-1, BAI03.10-2, BAI03.10-3, BAI03.10-4, BAI03.10-5,DSS01.03-1, DSS01.03-2, DSS01.03-3, DSS01.03-4, DSS01.03-5, DSS01.03-6, DSS05.02-8, DSS05.02-9, DSS05.04-2, DSS05.04-3, DSS05.04-5, DSS05.04-6, DSS05.04-8, DSS05.05-1, DSS05.05-2, DSS05.05-3,DSS05.05-4, DSS05.05-5, DSS05.05-6, DSS05.05-7, DSS05.07-1, DSS05.07-2, DSS05.07-3, DSS05.07-4, DSS05.07-5, dan DSS06.03-6.

Pengkonfigurasian kebijakan *firewall;* (c)Konfigurasi sistem pencatatan dan *alert;* (d)Pengkonfigurasian *firewall* ke dalam arsitektur jaringan.

3. Aktivitas PCI DSS v.3.1 dan KMP COBIT 5 yang terdapat pada tahap pengujian telah mencakup : (a) Pengujian konektivitas, *rulset, traffic,* kompabilitasaplikasiserta daftar layanan yang digunakan; (b) Manajemen jaringan. Telah mengidentifikasi peran dan tanggung jawab dari tim manajemen jaringan; (c) Pengujian kinerja yang mencakup jumlah maksimum koneksi simultan dan *throughput* yang di*support* oleh *firewall* serta keamanan *firewall.*
4. Proses dan aktivitas PCI DSS v.3.1 dan KMP COBIT 5 yang terdapat pada tahap implementasi telah mencakup : (a) Analisis dampak dari penerapan *firewall;* (b) Kebijakan dan keamanan *firewall;* (c) Pembagian hak akses untuk manajemen jaringan.
5. Aktivitas PCI DSS v.3.1 dan KMP COBIT 5 yang terdapat pada tahap perawatan telah mencakup : (a) Instalasi *patch* untuk perangkat *firewall;* (b) Pembaharuan terhadap kebijakan untuk menghadapi jenis ancaman yang baru teridentifikasi; (c) Pemantauan kinerja *firewall* dan *log* untuk memastikan bahwa pengguna mematuhi kebijakan keamanan; (d) Pengujian secara periodik untuk memverifikasi bahwa aturan *firewall* berfungsi seperti yang diharapkan; (e) Penyimpanan *log* jaringan.

Semua aktivitas telah terpetakan dalam lima pendekatan bertahap pengelolaan *firewall*. Luaran dari analisis tersebut akan digunakan sebagai panduan dalam menyusun prosedur pengelolaan keamanan informasi untuk *firewall configuration.*

2) Tahap Penyusunan Prosedur Pengelolaan Keamanan Informasi Untuk Firewall Configuration

Penyusunan prosedur pengelolaan keamanan informasi untuk *firewal configuration* dilakukan dengan menggunakan hasil analisis pemetaan proses PCI DSS v.3.1 dan KMP COBIT 5, seperti yang telah dilakukan dalam Tabel 2. Aktivitas tersebut akan dijadikan sebagai bahan acuan dalam menyusun pedoman prosedur. Pedoman prosedur disusun berupa langkah kerja. Penyusunan langkah kerja dalam pedoman prosedur dilakukan dengan menggunakan kombinasi aktivitas PCI DSS v.3.1 dan KMP COBIT 5. Sebagai contoh : aktivitas PCI DSS v.3.1 dengan kode aktivitas PCI-1.1 yang berbunyi: "Terdapat sebuah prosedur yang terdokumentasi untuk menyetujui dan menguji semua koneksi jaringan dan perubahan pada *firewall* serta konfigurasi router". Aktivitas PCI-1.1 dapat dikombinasikan dengan aktivitas KMP COBIT 5 dengan kode aktivitas BAI10.01-1 yang berbunyi : "Menentukan dan menyetujui ruang

lingkup dan tingkat rincian manajemen konfigurasi". Sehingga langkah kerja yang terbentuk dari kombinasi dua aktivitas yang masih saling berkaitan ini adalah :

1. Buat prosedur untuk menyetujui semua perubahan pada koneksi jaringan.
2. Tentukan dan setujui ruang lingkup dan tingkat rincian manajemen konfigurasi.

Proses pengkombinasian aktivitas PCI DSS v.3.1 dengan KMP COBIT 5 untuk tahap perencanaan dapat dilihat pada Tabel 3. Proses pengkombinasian aktivitas juga dilakukan untuk tahap konfigurasi, pengujian, *deployment* dan tahap perawatan.

TABEL 3. HASIL PENGKOMBINASIAN AKTIVITAS PCI DSS V.3.1 DENGAN KMP COBIT 5

Tahap	Kombinasi Aktivitas PCI DSS v.3.1 dengan KMP COBIT 5
Perencanaan	(APO12.01-1), (APO12.01-2 & APO12.01-3),(APO12.01-4), (APO12.01-5), (APO12.01-6), (BAI03.03-1), (BAI03.03-2), (BAI03.03-3), (DSS02.03-1), (PCI-1.1 & BAI10.01-1), (DSS02.03-2), (DSS02.03-3), (BAI03.03-4 & PCI-1.6), (BAI03.03-5 & BAI03.05-7), (BAI03.03-6), (BAI03.05-1, BAI03.05-2 & BAI03.05-5), (BAI03.05-3), (BAI03.05-4), (BAI03.05-8 & DSS05.02-5), (BAI10.01-2), (APO03.02-1, APO03.02-4 & PCI-1.2.1), (PCI-1.3.1 & DSS05.04-7), (APO03.02-2, APO03.02-3 & PCI-3.7.1), (APO03.02-5 & APO03.02-6), (APO03.02-7), (APO03.02-8, APO03.02-9), (DSS06.03-1, DSS06.03-2 & PCI-1.5), (DSS06.03-3, DSS05.04-4 & DSS05.04-5), (DSS06.03-3, DSS05.04-4 & DSS05.04-5), (DSS06.03-4), (DSS06.03-5), (PCI-1.7.1 & DSS06.03-6)

3) Tahap Penentuan Peran dan Deskripsi Kerja

Penentuan peran dan deskripsi kerja ditentukan dengan menggunakan RACI *chart*, sesuai dengan aktivitas KMP COBIT 5 yang digunakan dalam menyusun langkah kerja pengelolaan keamanan informasi. Langkah kerja pada panduan pengelolaan keamanan informasi untuk *firewall configuration* membutuhkan peran yang bertanggung jawab pada kegiatan operasional, memenuhi kebutuhan dan menciptakan hasil yang diinginkan organisasi, serta membutuhkan peran yang bertanggung jawab atas keberhasilan suatu tugas. Sehingga dipilihlah peran dalam RACI *chart* yang berkategori R atau A yang digunakan dalam penentuan peran dan deskripsi kerja pada panduan pengelolaan keamanan informasi untuk *firewall configuration.*

Pemilihan kategori R atau A yang digunakan dalam penentuan peran dan deskripsi kerja didasarkan pada masing – masing deskripsi peran dan tanggung jawab RACI *chart.* Daftar alternatif peran diperoleh dari tabel RACI *chart* COBIT 5 sesuai dengan KMP yang digunakan dalam menyusun langkah kerja. Tabel RACI *chart* terdapat pada literatur "COBIT 5 : *Enabling Processes"*. Setelah melakukan penentuan peran dan deskripsi kerja langkah selanjutnya adalah membuat daftar dokumen yang dihasilkan (*work product*) dalam panduan pengelolaan keamanan informasi. Penentuan daftar *work product* disesuaikan dengan *work product* COBIT 5 yang bersesuaian dengan aktivitas yang digunakan dalam menyusun langkah kerja. Contoh luaran dari pedoman prosedur pengelolaan keamanan informasiuntuk *firewall configuration* dapat dilihat pada Gambar 2.

B. Verifikasi Panduan Pengelolaan Keamanan Informasi

Verifikasi dilakukan untuk mengetahui apakah panduan pengelolaan keamanan informasi yang telah dibuat berupa pedoman prosedur mudah untuk dipahami dan dapat diimplementasikan dalam organisasi atau institusi. Verifikasi dilakukan dengan mengambil studi kasus di DSIK Universitas Airlangga dan dilakukan tanpa adanya penyesuaian atau spesifikasi terhadap DSIK Universitas Airlangga. Verifikasi dilakukan dengan cara memberikan kuesioner penilaian terkait panduan pengelolaan keamanan informasi yang ditujukan kepada responden yang terkait dengan proses. Responden tersebut antara lain: Direktur Sistem Informasi, Kepala Seksi Integrasi Program dan Pengembangan Sistem, Kepala Seksi Jaringan, Kepala Seksi Keamanan Data, Kepala Seksi Pencitraan Informatika, Kepala Sub Direktorat Operasional Sistem Informasi serta Kepala Sub Direktorat Pengembangan Sistem. *Item* pertanyaan yang digunakan dalam kuesioner berupa pertanyaan – pertanyaan terkait penggunaan bahasa dan kesesuaian panduan dengan kondisi DSIK Universitas Airlangga.

Kuesioner yang diberikan kepada responden bertujuan untuk mengetahui tanggapan dari penanggung jawab proses yang terdapat dalam panduan pengelolaan keamanan informasi untuk *firewall configuration.* Dari pelaksanaan pengisian kuesioner penilaian, diperoleh jawaban dari responden. Kemudian dari hasil jawaban responden, dibuat sebuah rekapitulasi jawaban. Hasil rekapitulasi jawaban responden dapat dilihat pada Tabel 4. Dari hasil pengisian kuesioner verifikasi panduan pengelolaan keamanan informasi dapat diketahui bahwa sebanyak 42,86% responden menyatakan panduan pengelolaan yang dibuat, secara operasional sangat mudah untuk dilaksanakan dan sebanyak 100% responden menyatakan bahwa panduan pengelolaan keamanan informasi yang dibuat mampu menjawab kebutuhan keamanan informasi di DSIK Universitas Airlangga. Panduan pengelolaan keamanan informasi yang dibuat mampu menjawab kebutuhan keamanan informasi di DSIK Universitas Airlangga dari sisi *firewall*

configuration, namun *firewall configuration* yang optimal terkadang seringkali mengurangi kecepatan akses internet dan sangat dibutuhkannya *skill* tenaga kerja yang kompeten dan telah tersertifikasi untuk mengelola jaringan dengan sekala besar. Oleh sebab itu, dibutuhkannya kebijakan dan persiapan yang optimal dari perusahaan sebelum mengimplementasikan *firewall.*

3.1 Tahap Perencanaan

Didistribusikan Kepada : *Chief Financial Officer, Business Executives, Business Process Owners, Strategy Executive Committee, Project Management Office, Chief Risk Officer, Chief Information Security Officer, Chief Information Officer, Head Architect, Head Development, Head IT Operations, Head IT Administration, Service Manager Information, Security Manager, Business Continuity Manager, Privacy Officer*

No	Langkah Kerja	Keluaran	Penanggung Jawab
1	Buat dan tetapkan sebuah metode yang digunakan untuk mengumpulkan, menklasifi-kasikan dan menganalisis data terkait ancaman dan kerentanan dalam sistem informasi. *Catatan : Perhatikan berbagai jenis kejadian, dan faktor-faktor ancaman dan kerentanan sistem informasi*	Data pada lingkungan operasional yang berkaitan dengan risiko	a) *Business Process Owners* b) *Project Management Office* c) *Chief Risk Officer* d) *Chief Information Security Officer* e) *Head Architect* f) *Head Development* g) *Head IT Operations* h) *Head IT Administration* i) *Service Manager* j) *Information Security Manager* k) *Business Continuity Manager* l) *Privacy Officer*
2	Simpan data ancaman kerentanan sistem informasi yang relevan di dalam lingkungan operasional internal dan eksternal yang berperan penting dalam pengelolaan risiko.	Data terkait kejadian risiko dan faktor yang berkontribusi menimbulkan risiko	
3	Buat catatan rekaman terkait risiko ancaman dan kerentanan sistem informasi yang terjadi.		
4	Analisis dan review catatan rekaman terkait risiko ancaman dan kerentanan sistem informasi yang terjadi secara rutin.	Dokumen hasil analisis risiko	
5	Lakukan pencatatan untuk setiap kejadian, masalah dan proses pengelolaan ancaman risiko dan kerentanan sistem informasi yang berdampak tehadap pencapaian manfaat TI.	Dokumen terkait kumpulan profil risiko, termasuk status tindakan manajemen risiko & Dokumen terkait skenario risiko TI	

Gambar 2 Contoh LuaranPedoman Prosedur Pengelolaan Keamanan InformasiUntuk *Firewall Configuration*

C. Perbaikan Panduan Pengelolaan Keamanan Informasi

Tahap perbaikan panduan pengelolaan keamanan informasi dilakukan untuk memperbaiki kekurangan yang ditemukan pada tahap verifikasi. Perbaikan dilakukan berdasarkan komentar yang diberikan oleh responden pada saat tahap verifikasi dilakukan. Berdasarkan komentar dari responden, dilakukan perbaikan panduan pengelolaan keamanan informasi yang meliputi : memperbaiki kesalahan pembagian peran dan tanggung jawab, dan memperbaiki tata bahasa yang digunakan dalam menyusun langkah kerja

IV. SIMPULAN

Penyusunan panduan pengelolaan keamanan informasi untuk *firewall configuration* disusun berupa langkah kerja. Literatur yang digunakan dalam menyusun panduan pengelolaan keamanan informasi adalah "PCI : *requiretments and security assessment procedures version* 3.1" dan COBIT 5 : *Enabling Processes"*. Berdasarkan hasil penelitian yang telah dilakukan, maka dapat diambil kesimpulan sebagai berikut : Hasil penyelarasan kebijakan *firewall* menurut SOP DEPKOMINFO yang terdapat pada tahap analisis pemetaan proses PCI DSS v.3.1 dengan KMP COBIT 5 dapat diketahui bahwa semua kebijakan *firewall* yang terdapat dalam SOP *firewall* DEPKOMINFO tercakup pada proses PCI DSS v.3. sedangkan Hasil analisis pemetaan proses PCI DSS v.3.1 dan KMP COBIT 5 menunjukkan bahwa semua aktivitas telah terpetakan dalam lima pendekatan bertahap pengelolaan *firewall configuration.*

Hasil pengisian kuesioner verifikasi panduan pengelolaan keamanan informasi dapat diketahui bahwa sebanyak 42,86% responden menyatakan panduan pengelolaan yang dibuat, secara operasional sangat mudah untuk dilaksanakan.

V. DAFTAR PUSTAKA

Beissel, S. (2014). *Supporting PCI DSS 3.0 Compliance With COBIT 5* (Vol. 1). USA: ISACA.

Cian, B., & Mark, G. T. (2009). PCI DSS compliance meeting the demands. *Data Protection Ireland , 2* (6), 10-13.

DEPKOMINFO. (2010). *Standard Operational Procedure Firewall.* Jakarta: Kementrian Komunikasi dan Informatika Republik Indonesia.

Grembergen, W. V. (2002). *The Balenced Scorcard and IT Governance.* USA: IT Governance Institute.

ISACA. (2012a). *A Business Framework for the Governance and Managemen tof Enterprise IT.* USA: ISACA and IT Governance Institute.

ISACA. (2012b). COBIT Process Assessment Model (PAM) Using COBIT 5. Dalam ISACA, *COBIT Process Assessment Model (PAM) Using COBIT 5.* USA.

ISACA. (2012c). *Enabling Processes.* USA: ISACA and IT Governance Institute.

IT Governance., I. (2003). *Board Briefing on IT Governance.* (2nd ed.). USA: IT Governance Institute.

Komalasari, R., & Perdana, I. (2014). Audit Keamanan Informasi Bagian Teknologi Informasi PT PLN (Persero) DJBB Menggunakan SNI ISO/IEC 27001: 2009. *Jurnal Sistem Informasi , IX* (2), 201 - 216.

Lovrić, Z. (2012). Model of Simplified Implementation of PCI DSS by Using ISO 27001 Standard. *Central European Conference on Information and Intelligent Systems* (hal. 347-493). Varazdin: University of Zagreb.

PCI Security Standards Council. (2015). *Payment Card Industry (PCI) Data Security Standard : Requirements and Security Assessment Procedures version 3.1.* USA: ISACA.

PCI Security, S. C. (2015). *Lifecycle for Changes to PCI DSS and PA-DSS* (3.1 ed.). USA: PCI Security Standards Council, LLC.

Sarno, R., & Iffano, I. (2009). *Sistem Manajemen Keamanan Informasi berbasis ISO 27001.* Surabaya: ITS Press.