

Analisis Tingkat Keamanan Informasi: Studi Komparasi Framework Cobit 5 Subdomain Manage Security Services (DSS05) dan NIST SP 800 – 55

Eko Handoyo

Email: ekokurro17@gmail.com

Universitas Muhammadiyah Lamongan

Diterima: 13 Oktober 2020 | Direvisi: 20 Oktober 2020 | Disetujui: 29 Oktober 2020
©2020 Program Studi Teknik Informatika Fakultas Ilmu Komputer,
Universitas Muhammadiyah Riau, Indonesia

Abstrak

Teknologi informasi merupakan bagian yang sangat penting dari organisasi. Teknologi informasi diharapkan dapat memberikan keuntungan yang baik bagi perusahaan. Namun seiring dengan perkembangan teknologi, seringkali hal tersebut dimanfaatkan oleh beberapa pihak yang tidak bertanggung jawab yang dapat mengakibatkan munculnya ancaman dan resiko dari penggunaan teknologi. Organisasi perlu mengukur tingkat keamanan informasi untuk mengidentifikasi kelemahan dan ancaman sistem terhadap organisasi. Standar untuk mengukur keamanan informasi adalah *COBIT 5 subdomain manage security services (DSS05)* dan *NIST SP 800-55* revisi 1. Penelitian ini membandingkan kedua standar tersebut. Analisis komparatif menggunakan analisis kualitatif berdasarkan tiga aspek dalam keamanan informasi yaitu kerahasiaan, integritas, dan ketersediaan. Berdasarkan hasil analisis diperoleh kelebihan dan kekurangan masing-masing standar.

Kata kunci: *Ancaman, COBIT 5, Keamanan, NIST, Teknologi*

Information Analysis of Security Level: Cobit 5 Subdomain Framework Comparison Study Manage Security Services (DSS05) and NIST SP 800 - 55

Abstract

Information technology is a very important part of the organization. IT is expected to provide a good profit for the company. However, as technology evolves, it is often exploited by some irresponsible parties that can lead to the emergence of threats and risks from the use of technology. The organization needs to measure the level of information security to identify the system's weaknesses and threats to the organization. Standards for measuring information security are COBIT 5 subdomain manage security services (DSS05) and NIST SP 800-55 revision 1. This study is comparing the two standards. Comparative analysis uses qualitative analysis based on three aspects in information security that are confidentiality, integrity, and availability. Based on the analysis result obtained the advantages and disadvantages of each standard.

Keywords: *COBIT 5, NIST, Security, Technology, Threat*

1. PENDAHULUAN

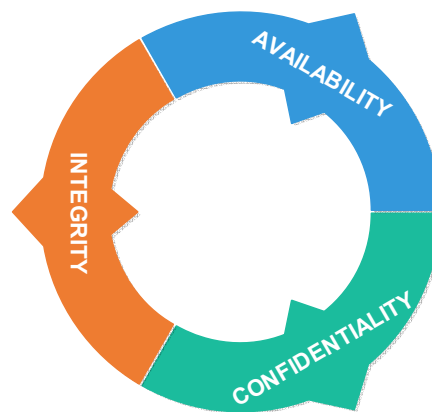
Perkembangan teknologi informasi saat ini maju dengan pesat, perkembangan teknologi juga mulai mengeksodus hampir seluruh kehidupan manusia. Teknologi informasi merupakan suatu bagian yang sangat penting bagi perusahaan atau lembaga. Perusahaan atau lembaga menempatkan teknologi informasi sebagai suatu hal yang dapat mendukung pencapaian rencana strategis perusahaan untuk mencapai sasaran visi, misi dan tujuan perusahaan atau lembaga tersebut. Teknologi informasi akan mendapatkan hasil yang efektif apa bila menggunakan tata kelola yang baik dalam penggunaannya[1].

Sistem informasi merupakan sistem yang berisi jaringan SPD (sistem pengolahan data), yang dilengkapi kanal-kanal komunikasi yang digunakan dalam sistem organisasi data[2]. Sistem informasi sendiri di harapkan mampu memberikan keuntungan yang baik untuk perusahaan. Namun, seiring perkembangannya teknologi sering kali dimanfaatkan oleh beberapa pihak yang tidak bertanggungjawab yang dapat menyebabkan munculnya ancaman dan resiko dari penggunaan teknologi[3].

Penerapan keamanan informasi dimaksudkan untuk mengatasi segala masalah dan kendala baik secara teknis maupun secara non-teknis[4]. Keamanan informasi adalah suatu keharusan[5]. Masalahnya penting karena jika informasi tersebut dapat diakses oleh orang-orang yang tidak bertanggung jawab maka akurasi informasi akan meragukan bahkan bisa menyesatkan informasi[6]. Masalah keamanan memicu mekanisme untuk mengendalikan akses ke jaringan untuk melindunginya dari penyusup[7].

Keamanan informasi dapat dicapai dengan menerapkan seperangkat control yang sesuai, termasuk kebijakan, proses, prosedur, struktur organisasi serta fungsi perangkat lunak dan perangkat keras. Kontrol ini perlu ditetapkan, diterapkan, dimonitor, direview, ditingkatkan dimana yang perlu untuk memastikan bahwa tujuan bisnis dan keamanan yang spesifik bagi organisasi dipenuhi[8].

Penerapan keamanan informasi dimaksudkan untuk mengatasi segala masalah dan kendala baik secara teknis maupun non-teknis seperti faktor ketersediaan (*availability*), kerahasiaan (*confidentiality*), dan kesatuan (*integrity*) [9]. Availability focus pada penggunaan sumber daya dalam kerangka waktu yang diinginkan. Confidentiality merujuk pada data tidak dapat diakses atau ditampilkan terhadap orang yang tidak berhak. Integrity fokus pada perlindungan melawan perubahan yang tidak diinginkan. Tindakan teknis dan administrasi keamanan dibutuhkan untuk mencapai tiga karakteristik ini. Dapat disimpulkan bahwa keamanan informasi adalah perlindungan karakteristik informasi (*confidentiality, integrity, dan availability*) baik itu dalam memproses informasi, menyimpan serta mengirimkannya dalam upaya untuk menjaga keberlangsungan dan memperluas kesempatan bisnis. Seperti pada gambar 1.



Gambar 1. Aspek keamanan informasi

Keamanan sistem informasi yang baik harus menerapkan *standar deming cycle of quality* [10]. Dalam area keamanan sistem informasi terdapat 4 poin *deming cycle of quality* yaitu:

1. *Plan* (Merencanakan): keamanan berencana untuk pindah postur yang reaktif ke postur proaktif.
2. *Develop* (Mengembangkan): Keamanan adalah serangkaian proses yang harus dilakukan dikembangkan mengikuti patokan keamanan.
3. *Check* (Periksa): Keamanan dikontrol melalui tes audit dan penetrasi, dan metode yang paling umum.
4. *Act* (Tindakan): Semua aktivitas kontrol dilakukan selama fase "Periksa" kemungkinan akan menyoroti sejumlah malfungsi yang perlu disediakan untuk tindakan korektif, tindakan pencegahan dan tindakan perbaikan.

COBIT 5 adalah produk terbaru dari ISACA yang diterbitkan tahun 2012, diperuntukkan tata kelola organisasi teknologi informasi. COBIT 5 memberikan framework yang komprehensif untuk membantu enterprise mencapai tujuan dalam governance dan management dari enterprise IT [11].

NIST (*National Institute Standards Technology*) merupakan salah satu lembaga pemerintahan Amerika Serikat yang bekerja sama dengan badan-badan federal lainnya untuk meningkatkan pemahaman terhadap pelaksanaan FISMA (*Federal Information Security Management Act*) dalam melindungi informasi dan sistem informasi serta menerbitkan standar dan pedoman yang memberikan dasar untuk program keamanan informasi yang kuat. NIST melakukan tanggung jawab hukum melalui Divisi Keamanan Komputer dari Laboratorium Teknologi Informasi (*Information Technology Laboratory - ITL*). NIST mengembangkan standar, metrik, pengujian, dan program validasi untuk mempromosikan, mengukur, dan memvalidasi keamanan sistem informasi[12].

Dalam penelitian ini akan membahas perbandingan dua standar untuk mengukur keamanan informasi, yaitu COBIT 5 subdomain manage security services (DSS05) dan NIST SP 800-55. Tujuan dari penelitian ini adalah untuk mendapatkan hasil analisis perbandingan terhadap COBIT 5 subdomain manage security services (DSS05) dan NIST SP 800-55. Diharapkan hasil tersebut bisa dijadikan bahan pertimbangan untuk mempersiapkan langkah-langkah untuk penguanaan stanadrisasi dalam sebuah audit keamanan sistem informasi sesuai dengan kebutuhan dan keadaan yang ada.

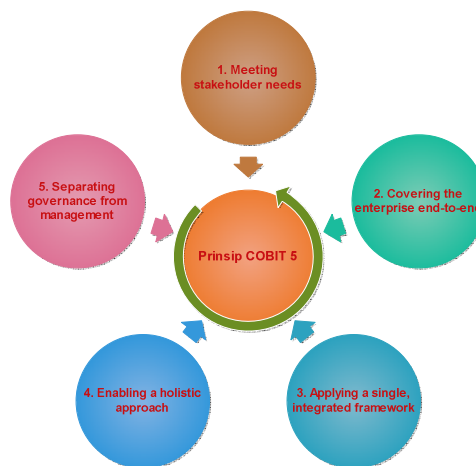
2. METODE PENELITIAN

Dalam penelitian ini menyajikan perbandingan dua standar untuk mengukur keamanan informasi, yaitu COBIT 5 subdomain manage security services (DSS05) dan NIST SP 800-55. Masing - masing standar mempunyai kelebihan dan kekurangan. Metode penelitian yang digunakan adalah studi pustaka. Analisa dilakukan menggunakan analisa kualitatif berdasar kan tiga aspek dalam keamanan informasi yaitu *confidentiality*, *integrity*, dan *availability*.

3. HASIL DAN PEMBAHASAN

Pada bagian ini akan dijelaskan hasil analisis terhadap COBIT 5 subdomain manage security services (DSS05) dan NIST SP 800-55 dengan analisa kualitatif berdasarkan tiga aspek dalam keamanan informasi yaitu *confidentiality*, *integrity*, dan *availability*. Dimana dengan berdasarkan ketiga aspek keamanan teknolgi informasi tersebut apakah kedua standar tersebut sudah mamenuhi dalam aspek – aspek keamanan teknologi informasi.

COBIT (*Control Objectives for Information and related Technology*) adalah suatu panduan standar praktek manajemen teknologi informasi dan sekumpulan dokumentasi best practices untuk tata kelola TI yang dapat membantu auditor, manajemen, dan pengguna untuk menjembatani pemisah (gap) antara risiko bisnis, kebutuhan pengendalian, dan permasalahan-permasalahan teknis[13]. COBIT 5 yang dirilis pada tahun 2012. COBIT merupakan kombinasi dari prinsip-prinsip yang telah ditanamkan yang dilengkapi dengan balance scorecard dan dapat digunakan sebagai acuan model (seperti COSO) dan disejajarkan dengan standar industri, seperti ITIL, CMM, BS779, ISO 9000. Seperti pada gambar 2.

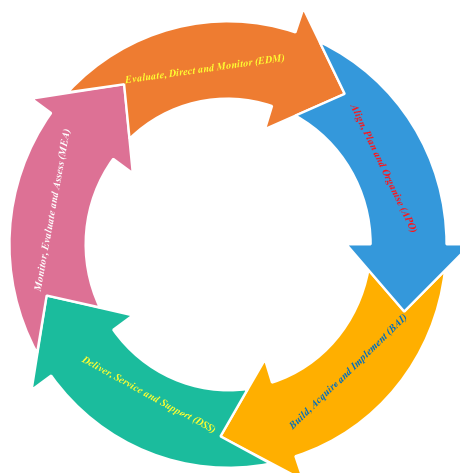


Gambar 2. Prinsip COBIT 5

COBIT 5 memungkinkan teknologi informasi untuk mengatur dan mengelola secara menyeluruh dalam perusahaan, dengan mempertimbangkan penuh bisnis dan bidang fungsional teknologi informasi dari tanggung jawab dan mempertimbangkan kepentingan terkait teknologi informasi[14].

1. Tahap 1 – *Initiate Progamme*.
2. Tahap 2 – *Define Problems and Opportunities*.
3. Tahap 3 – *Define Road Map*.
4. Tahap 4 – *Plan Progamme*.
5. Tahap 5 – *Execute Plan*.
6. Tahap 6 – *Release Benefits*.
7. Tahap 7 – *Review Effectivenes*.

Dalam COBIT 5 dibagi dalam 5 domain utama seperti pada gambar 3.



Gambar 3. Domain COBIT 5

1. *Evaluate, Direct and Monitor (EDM)* adalah kegiatan megevaluasi, mengarahkan dan memonitoring semua kegiatan teknologi informasi di organisasi tersebut.
2. *Align, Plan and Organise (APO)* adalah kegiatan merencanakan teknologi informasi dalam organisasi tersebut.
3. *Build, Acquire and Implement (BAI)* adalah kegiatan membangun teknologi informasi diorganisasi tersebut.
4. *Deliver, Service and Support (DSS)* adalah kegiatan menjalankan teknologi infromasi diorganisasi tesebut.
5. *Monitor, Evaluate and Assess (MEA)* adalah kegiatan memonitoring teknologi yang sedang berjan pada organisi tersebut.

Domain yang berhubungan dengan keamanan teknologi informasi adalah domain DSS. Domain DSS (*Deliver, Service and Support*) merupakan sebuah domain yang digunakan dalam analisa teknologi informasi dalam area manajemen yang di dalamnya terdapat beberapa proses. Domain DSS berkaitan dengan pengiriman aktual dan dukungan layanan yang dibutuhkan, yang meliputi pelayanan, pengelolaan keamanan dan kelangsungan, dukungan layanan bagi pengguna, dan manajemen data dan fasilitas operasional[15]. Dalam Domain DSS terdapat 6 sub domain yaitu:

1. *DSS01 Manage Operations.*
2. *DSS02 Manage Service Requests and Incidents.*
3. *DSS03 Manage Problems.*
4. *DSS04 Manage Continuity.*
6. *DSS05 Manage Security Services.*
7. *DSS06 Manage Business Process Controls.*

Dalam domain DSS (*Deliver, Service and Support*) terdapat control prosedur sebanyak 38 proses Practices dan 204 Activities. Seperti pada tabel 1.

Tabel 1. Control Proses Subdomain DSS (*Deliver, Service and Support*)

Subdomain		Practices	Activities
DSS01	<i>Manage Operations</i>	5	34
DSS02	<i>Manage Service Requests and Incidents.</i>	7	24
DSS03	<i>Manage Problems.</i>	5	23
DSS04	<i>Manage Continuity.</i>	8	42
DSS05	<i>Security Services.</i>	7	49
DSS06	<i>Business Process Controls.</i>	6	32

Dalam domain DSS terdapat Subdomain DSS05 dimana subdomain ini merupakan prosedur yang lebih intensif terhadap kemandan informasi. Subdomain tersebut adalah *manage security services* (mengelola layanan keamanan) dimana subdomain ini melaksanakan beberapa akatifitas atau pernyataan sebanyak 49 pernyataan yang di kelompokkan dalam 7 proses, seperti pada tabel 2.

Tabel 2. Control Proses dan Aktivitas dalam DSS05

Practice.ID	Practice Name	Activity
DSS05.01	<i>Protect against malware</i>	6
DSS05.02	<i>Manage network and connectivity security</i>	9
DSS05.03	<i>Manage endpoint security</i>	9
DSS05.04	<i>Manage user identity and logical access</i>	8
DSS05.05	<i>Manage physical access to IT assets</i>	7
DSS05.06	<i>Manage sensitive documents and output devices</i>	5
DSS05.07	<i>Monitor the infrastructure for security-related events</i>	5

Dimana dalam DSS05 terdapat practice sebagai berikut :

1. *Protect against malware* (DSS05.01) dimana proses ini melaksanakan dan memelihara tindakan pencegahan, detektif dan perbaikan yang ada (terutama patch keamanan dan pengendalian virus terkini) di seluruh perusahaan untuk melindungi sistem informasi dan teknologi dari perangkat lunak perusak (misal, Virus, worm, spyware, spam).
2. *Manage network and connectivity security* (DSS05.02) dimana proses ini digunakan langkah-langkah keamanan dan prosedur manajemen terkait untuk melindungi informasi dari semua metode konektivitas.
3. *Manage endpoint security* (DSS05.03) dimana proses ini memastikan titik akhir (misal: Laptop, desktop, server, dan perangkat seluler dan jaringan seluler atau perangkat lunak lainnya) dijamin pada tingkat yang sama atau lebih besar dari persyaratan keamanan yang ditetapkan dari informasi yang diproses, disimpan atau dikirim.
4. *Manage user identity and logical access* (DSS05.04) dimana proses ini memastikan semua pengguna memiliki hak akses informasi sesuai dengan kebutuhan bisnis mereka dan berkoordinasi dengan unit bisnis yang mengelola hak akses mereka sendiri dalam proses bisnis.
5. *Manage physical access to IT assets* (DSS05.05) dimana proses ini menentukan dan menerapkan prosedur untuk memberi, membatasi dan mencabut akses ke bangunan, bangunan dan area sesuai kebutuhan bisnis, termasuk keadaan darurat. Akses ke bangunan, bangunan dan area harus dibenarkan, disahkan, dicatat dan dipantau. Ini harus berlaku untuk semua orang yang memasuki tempat itu, termasuk staf, staf sementara, klien, vendor, pengunjung atau pihak ketiga lainnya.
6. *Manage sensitive documents and output devices* (DSS05.06) dimana proses ini menetapkan pengamanan fisik, praktik akuntansi dan pengelolaan persediaan yang tepat atas aset TI yang sensitif, seperti formulir khusus, instrumen yang dapat dinegosiasikan, printer tujuan khusus atau token keamanan.
7. *Monitor the infrastructure for security-related events* (DSS05.07) dimana proses ini menggunakan alat deteksi intrusi, memantau infrastruktur untuk akses yang tidak sah dan memastikan bahwa setiap peristiwa diintegrasikan dengan pemantauan kejadian dan pengelolaan kejadian secara umum.

National Institute of Standard And Technology (NIST) merupakan Organisasi pemerintah di Amerika Serikat dengan misi mengembangkan dan mempromosikan penilaian, standar, dan teknologi untuk meningkatkan fasilitas dan kualitas kehidupan. NIST mengeluarkan alat, teknik dan metode untuk penilaian dan perencanaan keamanan informasi berbasis risiko [16]. *National Institute of Standard And Technology (NIST) 800-55 publication* adalah sebuah standar nasional yang dikeluarkan oleh Departemen Perdagangan Amerika Serikat untuk mengukur keamanan informasi. Pengukuran ini mengindikasikan efektifitas kontrol keamanan yang diterapkan pada sistem informasi dan mendukung program keamanan informasi. Pengukuran ini juga digunakan untuk memfasilitasi pengambilan keputusan, meningkatkan performance dan meningkatkan accountabilitas melalui pengumpulan, analisa dan pelaporan data performance yang relevan. Tujuan pengukuran performance untuk memonitor status aktivitas yang diukur dan memfasilitasi peningkatan aktivitas tersebut dengan menerapkan tindakan korektif berdasarkan hasil pengukuran [17].

Pendekatan untuk mengukur efektivitas pengendalian keamanan sudah dalam pengembangan selama beberapa tahun. NIST SP 800-55, keamanan metrik panduan untuk sistem teknologi informasi, dan NIST Draft SP 800-80, panduan untuk mengembangkan metrik kinerja untuk keamanan informasi, baik ditujukan pengukuran keamanan informasi. Dokumen ini menggantikan publikasi ini dengan membangun atas mereka untuk menyelaraskan pendekatan ini dengan kontrol keamanan yang disediakan di NIST SP 800-53, direkomendasikan keamanan kontrol untuk sistem informasi federal. Dokumen tersebut juga memperluas konsep dan proses diperkenalkan dalam versi asli dari NIST SP 800-55 untuk membantu dengan penilaian pelaksanaan program keamanan informasi[18]. NIST Publikasi Khusus (SP) 800-55 Revisi 1, memperluas atas pekerjaan sebelumnya NIST di bidang langkah-langkah keamanan informasi untuk memberikan panduan program-tingkat tambahan untuk mengukur kinerja keamanan informasi dalam mendukung tujuan strategis organisasi. Proses dan metodologi yang diuraikan dalam link di dokumen ini kinerja keamanan sistem informasi untuk kinerja instansi dengan memanfaatkan proses perencanaan strategis lembaga-tingkat. Dengan demikian, proses dan metodologi membantu menunjukkan bagaimana informasi keamanan kontribusi untuk mencapai tujuan strategis lembaga dan tujuan. ukuran kinerja dikembangkan sesuai dengan panduan ini akan meningkatkan kemampuan lembaga untuk menanggapi berbagai mandat pemerintah federal dan inisiatif[18].

NIST 800-55 terdiri dari 19 bidang pengukuran yaitu :

1. *Security Budget* bertujuan menyediakan sumber daya yang diperlukan untuk benar mengamankan agen informasi dan sistem informasi.
2. *Vulnerability Management* bertujuan memastikan lingkungan keamanan dan akuntabilitas yang komprehensif untuk personil, fasilitas, dan produk.
3. *Access Control (AC)* bertujuan untuk membatasi informasi, sistem, dan akses komponen untuk individu atau mesin yang dapat diidentifikasi, diketahui, kredibel, dan berwenang.
4. *Awareness and Training (AT)* bertujuan untuk memastikan bahwa personil organisasi dilatih secara memadai untuk melaksanakan tugas-tugas yang berhubungan dengan keamanan informasi ditugaskan mereka dan tanggung jawab.
5. *Audit and Accountability (AU)* bertujuan membuat, melindungi, dan mempertahankan sistem audit informasi catatan sejauh diperlukan untuk memungkinkan pemantauan, analisis, investigasi, dan pelaporan kegiatan yang melanggar hukum, tidak sah, atau tidak pantas.
6. *Certification, Accreditation, and Security Assessments (CA)* Penilaian sertifikasi, akreditasi, dan keamanan bertujuan memastikan semua sistem informasi telah disertifikasi dan diakreditasi sebagai diperlukan.
7. *Configuration Management (CM)* Manajemen konfigurasi bertujuan membangun dan mempertahankan konfigurasi dasar dan persediaan sistem informasi organisasi (termasuk hardware, software, firmware, dan dokumentasi) sepanjang hidup pengembangan sistem masing-masing
2. *Contingency Planning (CP)* Perencanaan kontingensi bertujuan membangun, memelihara, dan secara efektif melaksanakan rencana untuk tanggap darurat, operasi backup, dan recovery pasca bencana untuk sistem informasi organisasi untuk memastikan ketersediaan informasi penting sumber daya dan kelangsungan operasi dalam situasi darurat.
3. *Identification and Authentication (IA)* bertujuan memberikan Semua pengguna sistem diidentifikasi dan dikonfirmasi di sesuai dengan kebijakan keamanan informasi.
4. *Incident Respons (IR)* Tanggapan insiden bertujuan memberikan Track, dokumen, dan laporan insiden untuk tepat pejabat organisasi dan / atau kewenangan.
5. *Maintenance (MA)* Pemeliharaan bertujuan melakukan perawatan berkala dan tepat waktu pada sistem informasi organisasi dan memberikan kontrol yang efektif pada alat, teknik, mekanisme, dan personil digunakan untuk melakukan sistem informasi pemeliharaan.
6. *Media Protection (MP)* Proteksi media bertujuan membersihkan atau menghancurkan sistem media informasi sebelum pembuangan atau pelepasan untuk digunakan kembali.
7. *Physical and Environmental (PE)* Lingkungan fisik bertujuan mengintegrasikan perlindungan fisik dan keamanan informasi mekanisme untuk memastikan perlindungan yang tepat dari informasi organisasi sumber.
8. *Planning (PL)* Perencanaan bertujuan mengembangkan, dokumen, memperbarui secara berkala, dan melaksanakan rencana keamanan untuk sistem informasi organisasi yang menggambarkan keamanan kontrol di tempat atau direncanakan untuk sistem informasi, dan aturan-aturan perilaku untuk individu mengakses sistem ini.
9. *Personnel Security (PS)* Keamanan personal bertujuan memastikan bahwa individu menempati posisi tanggung jawab dalam organisasi dapat dipercaya dan memenuhi keamanan didirikan kriteria untuk posisi tersebut.
10. *Risk Assessnent (RA)* Penilaian resiko bertujuan menilai berkala risiko untuk operasi organisasi (Termasuk misi, fungsi, gambar, atau reputasi), aset organisasi, dan individu yang dihasilkan dari pengoperasian sistem informasi organisasi.
11. *System and Services Acquisition (SA)* Akuisisi sistem dan pelayanan bertujuan memastikan penyedia pihak ketiga mempekerjakan keamanan yang memadai langkah-langkah untuk melindungi informasi, aplikasi, dan / atau jasa outsourcing dari organisasi.
12. *System and Communications Protection (SC)* Perlindungan sistem dan komunikasi bertujuan mengalokasikan sumber daya yang cukup untuk melindungi memadai infrastruktur informasi elektronik.
13. *System and Information Integrity (SI)* Integritas sistem dan informasi bertujuan memberikan perlindungan dari kode berbahaya di tepat lokasi dalam sistem informasi organisasi, memonitor sistem informasi peringatan keamanan dan nasihat, dan mengambil tindakan yang tepat dalam menanggapi.

Secara garis besar pengukuran keamanan informasi menggunakan NIST 800-55 merujuk pada kontrol keamanan pada NIST 800-53. Kontrol keamanan pada NIST 800-53 meliputi tiga kelas yaitu, *technical, operational dan management* [19]. Implementasi pengukuran keamanan informasi melibatkan penerapan pengukuran untuk memonitor *performance control* keamanan informasi dan menggunakan hasilnya untuk menginisiasi tindakan peningkatan performance. Implementasi pengukuran keamanan informasi terdiri dari enam fase, yaitu persiapan pengumpulan data, pengumpulan data, identifikasi tindakan korektif, mengembangkan kasus bisnis, mendapatkan sumber daya dan menerapkan tindakan korektif [20].

COBIT 5 DSS05 merupakan standar yang memberikan petunjuk praktis dalam melaksanakan manajemen keamanan informasi termasuk didalamnya mengukur keamanan informasi. Sementara, NIST 800-55 revisi 1 merupakan standar nasional Amerika Serikat dalam mengukur keamanan informasi pada sebuah organisasi. Masing-masing standar memiliki kelebihan dan kekurangannya sendiri-sendiri. COBIT 5 dapat digunakan oleh sebuah organisasi yang tadinya belum menerapkan manajemen keamanan informasi, sedangkan NIST digunakan untuk mengukur keamanan informasi organisasi yang sudah menerapkan manajemen keamanan informasi. Seperti yang disyaratkan oleh NIST 800-55, performance yang akan diukur harus siap didapatkan melalui performance yang konsisten, repeatable dan terdokumentasi. COBIT 5 DSS05 hanya menilai proses bukan

teknologi maupun kuantitasnya. Sehingga pengukuran keamanan informasi menggunakan COBIT 5 tidak menunjukkan tingkat kematangan organisasi secara spesifik. Sementara NIST SP 800 – 55 memberikan proses yang lebih detail dan spesifik dalam beberapa bidang. Contohnya seperti anggaran alokasi keuangan untuk keamanan sehingga menjamin tersedianya anggaran yang baik dalam organisasi tersebut.

COBIT 5 DSS05 mempunyai 7 Proses dan 49 Pernyataan keamanan informasi. Sementara, NIST 800-55 mempunyai 19 Proses dan 60 pertanyaan keamanan informasi. COBIT 5 DSS05 memiliki proses yang lebih sedikit dibandingkan dengan NIST 800-55 revisi 1. Meskipun ketiga aspek keamanan informasi, yaitu confidentiality, integrity, dan availability, sudah terdmasuk kedua standar tersebut. COBIT 5 DSS05 tidak menjelaskan langkah-langkah dalam mengukur keamanan informasi tetapi memberikan panduan dalam menerapkan hasil audit dengan mengadopsi *Maturity Level*. NIST 800-55 selain berisi panduan mengukur keamanan informasi juga menjelaskan langkah-langkah mengukur keamanan informasi tetapi tidak memberikan panduan terhadap keputusan akhir audit sehingga membutuhkan refrensi perhitungan lain. Dari analisis yang dilakukan di dapatkan hasil perbandingan antara COBIT 5 DSS05 dan NIST SP 800-55. Dimana dalam perbandingan tersebut terdapat beberpa kesamaan dalam prosedur dan terdapat perbedaan dalam prosedur yang ada dalam proses audit keamanan informasi. Seperti pada tabel 3.

Tabel 3. Perbandingan *Security Metrics* COBIT 5 DSS05 dan NIST SP 800-55

Aspek Keamanan TI	COBIT 5 DSS05	NIST SP 800-55
confidentiality	Manage user identity and logical access	Access Control
		Identification and Authentication
		Personnel Security
		Planning
	Manage network and connectivity security	Configuration Managemet
	Manage endpoint security	Media Protection
	Monitor the infrastructure for security-related	Incident Respons
integrity	Protect against malware	Awareness and Training
		Audit and Accountability
		Certification, Accreditation, and Security Assessments
		System and Information Integrity
		Maintenance
availability	Manage sensitive documents and output devices	Risk Assessment
		Vulnerability Management
		System and Communications Protection
		Physical and Environmental
		Security Budget
Manage physical access to IT assets	System and Services Acquisition	
	Contingency Planning	

Dari tabel 1 dapat di analisis bahwa COBIT 5 DSS05 dan NIST SP 800-55 sama – sama sudah menganut dan menerapkan aspek-aspek keamanan informasi yaitu *confidentiality, integrity dan availability*. Dari tabel 1 juga didapatkan bahwa metode NIST SP 800-55 memiliki kompleksitas dalam prosedur dari pada COBIT 5 DSS05.

4. KESIMPULAN

Aspek keamanan confidentiality bisa dijumpai dalam kedua metode, dimana COBIT 5 DSS05 terdapat *manage user identity and logical access, manage network and connectivity security, manage endpoint security, monitor the infrastructure for security-related*. Sementara pada NIST SP 800-55 tedapat *access control, identification and authentication, personnel security, planning, configuration managemet, media protection, incident respons, awareness and training, audit and accountability, certification, accreditation, and security assessments*. Aspek keamanan integrity bisa dijumpai dalam kedua metode, baik COBIT 5 DSS05 dan NIST SP 800 – 55 revisi 1. Dimana dalam COBIT 5 DSS05 terdapat pada subdomain *protect against malware*. Sedangkan pada NIST SP 800 -55 revisi 1 terdapat klausul *system and information integrity, maintenance, risk assessnent, vulnerability management*. Aspek keamanan availability juga bisa di jumpai dalam kedua metode, dimana COBIT 5 DSS 05 terdapat *manage sensitive documents and output devices, manage physical access to IT assets*. Sedangkan dalam NIST SP 800-55 terdapat *system and communications protection, physical and environmental, security budget, system and services acquisition, contingency planning*.

Masing-masing standard memiliki kelebihan dan kekurangan masing – masing. Standar mana yang akan kita gunakan, sangat tergantung dari kondisi organisasi yang akan kita audit, apakah organisasi itu sudah menerapkan manajemen keamanan informasi atau belum. Organisasi yang sudah menerapkan manajemen keamanan informasi, bisa menggunakan NIST 800-55 seperti sebuah organisasi yang sudah mengimplemantasikan sebuah sistem informasi akademik sehingga memerlukan sebuah audit dalam pelaksanaannya untuk menjaga keamanan infrmasi organisasi tersebut. Karena memiliki kelebihan dan kekurangan, sangat dimungkinkan penelitian selanjutnya menggabungkan kedua standar ini untuk mengelola keamanan informasi. Sehingga di dapatkan perbandingan yang lebih akurat.

DAFTAR PUSTAKA

- [1] R. Umar, I. Riadi, and E. Handoyo, "Analisis Tata Kelola Teknologi Informasi Menggunakan Framework COBIT 5 Pada Domain Delivery, Service, And Support (DSS)," in *Seminar Nasional Teknologi Informasi dan Komunikasi - SEMANTIKOM 2017*, 2017, pp. 41–48.
- [2] L. F. Fathoni et al., "Application Information System Based Health Services Android," vol. 2, no. 1, pp. 39–48, 2016.
- [3] E. Kurniawan and I. Riadi, "Analisis Tingkat Keamanan Sistem Informasi Akademik Berdasarkan Standar ISO 27002 : 2013 Menggunakan SSE-CMM," vol. 2, no. 1, pp. 12–23, 2018.
- [4] Rosmiati, I. Riadi, and Y. Prayudi, "A Maturity Level Framework for Measurement of Information Security Performance Imam Riadi," *Int. J. Comput. Appl.*, vol. 141, no. 8, pp. 975–8887, 2016.
- [5] E. Kurniawan and I. Riadi, "Security level analysis of academic information systems based on standard ISO 27002:2003 using SSE-CMM," *Int. J. Comput. Sci. Inf. Secur.*, vol. 16, no. 1, pp. 139–147, 2018.
- [6] S. I. Farida and E. Rahajeng, "Usulan Model Tata Kelola Teknologi Informasi Pada Domain Monitor , Evaluate And Assess Dengan Metode Framework COBIT 5," vol. 7, no. 2, 2014.
- [7] N. Hermaduanty and I. Riadi, "Automation framework for rogue access point mitigation in ieee 802.1X-based WLAN," *J. Theor. Appl. Inf. Technol.*, vol. 93, no. 2, pp. 287–296, 2016.
- [8] L. Raichel et al., "International Standard ISO / IEC," 2005.
- [9] I. Riadi, "Analisis keamanan informasi berdasarkan kebutuhan teknis dan operasional mengkombinasikan standar iso 27001 : 2005 dengan maturity level (Studi Kasus Kantor Biro Teknologi Informasi PT . XYZ)," *Semin. Nas. Teknol. Inf. Dan Multimed.* 2016, vol. 6, no. 6, pp. 6–7, 2016.
- [10] H. Elachgar, B. Boulafourd, M. Makoudi, and B. Regragui, "Information security, 4TH wave," *J. Theor. Appl. Inf. Technol.*, vol. 43, no. 1, pp. 1–7, 2012.
- [11] Asriyanik and M. Hendayun, "Tata Kelola Teknologi Informasi pada Perguruan Tinggi Menggunakan Control Objective for Information & Related Technology (COBIT) 5," vol. 3, no. April, pp. 206–216, 2017.
- [12] N. Sasongko, "Penguujian Keamanan Transaksi Cloud Computing pada Layanan Software as a Services (SaaS) Menggunakan Kerangka Kerja NIST SP800-53A," *Semin. Nas. Apl. Teknol. Inf.*, vol. 2011, no. Snati, pp. 134–139, 2011.
- [13] Isaca, *A Business Framework for the Governance and Management of Enterprise IT*. 2013.
- [14] N. D. Setyaningrum and A. Kusyanti, "Evaluasi Manajemen Risiko Teknologi Informasi Menggunakan Framework COBIT 5 (Studi Kasus : PT . Kimia Farma (Persero) Tbk – Plant Watudakon)," vol. 2, no. 1, pp. 143–152, 2018.
- [15] D. Firmansyah, "Pengukuran Kapabilitas Pengelolaan Sistem Informasi Sub Domain Deliver , Service , Support 01 Menggunakan Framework Cobit 5 Studi Kasus : Politeknik Komputer Niaga LPKIA Bandung," *Konf. Nas. Sist. Inform.* 2015, pp. 689–695, 2015.
- [16] F. Mahardika, "Manajemen Risiko Keamanan Informasi Menggunakan Framework NIST SP 800-30 Revisi 1 (Studi Kasus: STMIK Sumedang)," *J. Inform. J. Pengemb. IT*, vol. 2, no. 2, pp. 1–8, 2017.
- [17] A. Brown and W. Robinson, "Security Metrics Guide for Information Technology Systems," vol. 1, 2015.
- [18] E. Chew, M. Swanson, K. Stine, N. Bartol, A. Brown, and W. Robinson, "Performance Measurement Guide for Information Security," no. July, 2008.
- [19] J. Task and F. Transformation, "Security and Privacy Controls for Federal Information Systems and Organizations Security and Privacy Controls for Federal Information Systems and Organizations."
- [20] I. S. O. Dan, J. Ring, T. Pad, and K. Kun, "Menajemen informasi : studi komparasi," vol. 2013, no. Sentika, 2013.