# ANALISIS TINGKAT KEAMANAN INFORMASI : STUDI KOMPARASI FRAMWORK COBIT 5 SUBDOMAIN MANAGE SECURITY SERVICES (DSS05) DAN NIST SP 800 – 55

Rusydi Umar, Imam Riadi, Eko Handoyo

***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.***

***Index Terms*— Threat, COBIT 5, Security, NIST, Information Technology.**

## I. PENDAHULUAN

Perkembangan teknonogi 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 sebagi 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 menggunana tata kelola yang baik dalam penggunaannya(Umar, Riadi, and Handoyo 2017).

Sistem informasi merupakan sistem yang berisi jaringan SPD (sistem pengolahan data), yang dilengkapi kanal-kanal komunikasi yang digunakan dalam sistem organisasi data(Fathoni et al. 2016). 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(Kurniawan and Riadi 2018a).

Penerapan keamanan informasi dimaksudkan untuk mengatasi segala masalah dan kendala baik secara teknis maupun secara non-teknis(Rosmiati, Riadi, and Prayudi 2016). Keamanan informasi adalah suatu keharusan(Kurniawan and Riadi 2018b). Masalahnya penting karena jika informasi tersebut dapat diakses oleh orang-orang yang tidak bertanggung jawab maka akurasi informasi akan meragukan bahkan bisa menyesatkan informasi(Farida and Rahajeng 2014). Masalah keamanan memicu mekanisme untuk mengendalikan akses ke jaringan untuk melindunginya dari penyusup(Hermaduanti and Riadi 2016).

Keamanan informasi dapat dicapai dengan menerapkan seperangkat control yang sesuai, termasuk kebijakan, proses, prosedur, struktur organisasi serta fungsi perangakat lunak dan perangkat keras. Kontrol ini perlu ditetapkan, diterapkan, dimonitor, direview, ditingkatkan dimana yang perlu untuk memastikan bahwa tujuan bisnis dan keamanan yang spesfifik bagi organisasi dipenuhi(Raichel et al. 2005).

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)* (Riadi 2016). *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. Tinda kan 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 memperoses informasi, menyimpan serta mengirimkanya 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*(Elachgar et

al. 2012). Dalam area keamanan sistem informasi terdapat 4 poin *deming cycle of quality* yaitu:

- *Plan* (Merencanakan): keamanan berencana untuk pindah postur yang reaktif ke postur proaktif.
- *Develop* (Mengembangkan): Keamanan adalah serangkaian proses yang harus dilakukan dikembangkan mengikuti patokan keamanan.
- *Check* (Periksa): Keamanan dikontrol melalui tes audit dan penetrasi, dan metode yang paling umum.
- *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(Asriyanik and Hendayun 2017).

NIST (*National Institute Standards Technology*) merupakan salah satu lembaga pemerintahan Amerikas 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(Sasongko 2011).

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 pengunanan stanadrisasi dalam sebuah audit keamanan sistem informasi sesuai dengan kebutuhan dan keadaan yang ada.

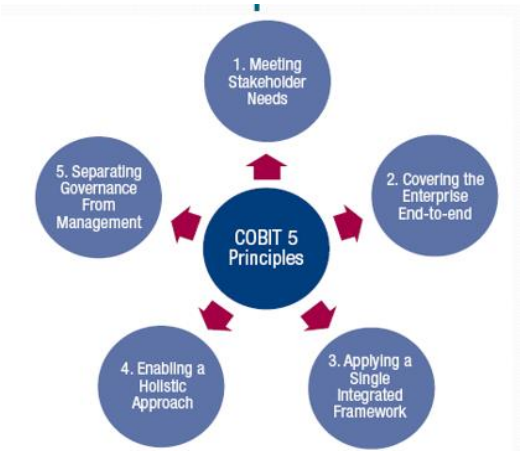
## II. METODE PENELITIAN

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.

## III. 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(Isaca 2013). *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.

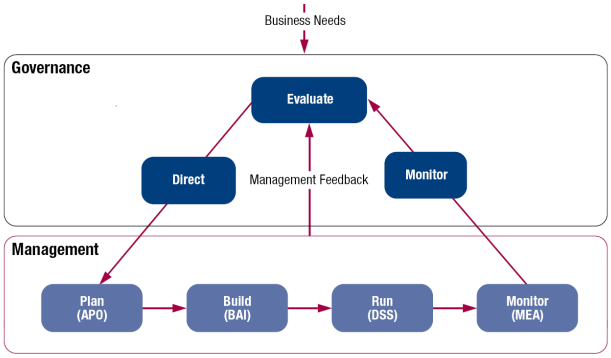



Gambar 2 Prinsip *COBIT* 5 (Isaca 2013)

COBIT 5 memungkinkan teknologi informasi untuk mengatur dan mengelola secara menyeluruh dalam perusahaan, dengan mempertimbangkan penuh bisnis dan bidang fungsional teknkologi informasi dari tanggung jawab dan mempertimbangkan kepentingan terkait teknologi informasi(Setyaningrum and Kusyanti 2018).

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 sepeti pada gambar 3.




Gambar 3 Domain *COBIT* 5 (Isaca 2013)

1. *Evaluate, Direct and Monitor (EDM)* adalah kegitan megevaluasi, mengarahkan dan memonitoring semua kegitan teknologi informasi di oraganisasi tersebut.
2. *Align, Plan and Organise (APO)* adalah kegitan merencanakan teknologi informasi dalam organisasi tersebut.
3. *Build, Acquire and Implement (BAI)* adalah kegitan membangun teknologi informasi di organisasi tersebut.
4. *Deliver, Service and Support (DSS)* adalah kegitan menjalakan teknologi infromasi do organisasi tesebut.
5. *Monitor, Evaluate and Assess (MEA)* adalah kegitan 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 menajemen 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(Firmansyah 2015). 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.*
5. DSS05 *Manage Security Services.*
6. 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 | Manage Operations | 5 | 34 |
| DSS02 | Manage Service Requests and Incidents | 7 | 24 |
| DSS03 | Manage Problems | 5 | 23 |
| DSS04 | Manage Continuity | 8 | 42 |
| DSS05 | Manage Security Services | 7 | 49 |
| DSS06 | Manage Business Process Controls | 6 | 32 |

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

Tabel 2. Control proses dan activitas dalam DSS05.

| Practice ID | Practice Name | Activity |
|---|---|---|
| DSS05.01 | Protect against malware. | 6 |
| DSS05.02 | Manage network and connectivity security. | 9 |
| DSS05.03 | Manage endpoint security. | 9 |
| DSS05.04 | Manage user identity and logical access. | 8 |
| DSS05.05 | Manage physical access to IT assets. | 7 |
| DSS05.06 | Manage sensitive documents and output devices. | 5 |
| DSS05.07 | Monitor the infrastructure for security-related events. | 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 (Mahardika 2017).

*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 (Brown and Robinson 2015).

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(Chew et al. 2008).

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(Chew et al. 2008).

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 Managemet* (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
8. *Contingency Planning* (CP) Perencanaan kontingenci 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.
9. *Identification and Authentication* (IA) bertujuan memberikan Semua pengguna sistem diidentifikasi dan dikonfirmasi di sesuai dengan kebijakan keamanan informasi.
10. *Incident Respons* (IR) Tanggapan insiden bertujuan memberikan Track, dokumen, dan laporan insiden untuk tepat pejabat organisasi dan / atau kewenangan.
11. *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.
12. *Media Protection* (MP) Proteksi media bertujuan membersihkan atau menghancurkan sistem media informasi sebelum pembuangan atau pelepasan untuk digunakan kembali.
13. *Physical and Environmental* (PE) Lingkungan fisik bertujuan mengintegrasikan perlindungan fisik dan keamanan informasi mekanisme untuk memastikan

perlindungan yang tepat dari informasi organisasi sumber.

14. *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.
15. *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.
16. *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.
17. *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.
18. *System and Communications Protection* (SC) Perlindungan sistem dan komunikasi bertujuan mengalokasikan sumber daya yang cukup untuk melindungi memadaiinfrastruktur informasi elektronik.
19. *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* (Task and Transformation n.d.).

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 (Bekti Maryuni Susanto 2013).

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 kekuranganya 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, *repetable* 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 sepeti anggaran alokasi keuangan untuk keamanan sehinggan menjamin tersedianya anggaran yang baik dalam organisasi tersebut.

COBIT 5 DSS05 mempunyai 7 Proses dan 49 Peryataan keamanan informasi. Sementara, NIST 800-55 mempunyai 19 Proses dan 60 pertanyaan kemanan 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 terdamasuk kedama kedua standar tersebut.

COBIT 5 DSS05 tidak menjelaskan langkah-langkah dalam mengukur keamanan informasi tetapi memberikan panduan dalam menerapakan hasil audit dengan menggadopsi *Maturity Level*. NIST 800-55 selain berisi panduan mengukur keamanan informasi juga menjelaskan menjelaskan langkah-langkah mengukur keamanan informasi tetapi tidak memberikan panduan terhadap keputusan akhir audit sehingga membutuhakan 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 beberapa kesamaan dalam prosedur dan terdapat perbedaan dalam prosedur yang ada dalam proses audit keamanan informasi. Seperti pada tabel 3.

Tabel 3. Perbandingan *Sceurity 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* |

| | | |
|---|---|---|
| | | *Awareness and Training* |
| Aspek Keamanan TI | COBIT 5 DSS05 | NIST SP 800-55 |
| | | *Audit and Accountability* |
| | | *Certification, Accreditation, and Security Assessments* |
| *integrity* | *Protect against malware* | *System and Information Integrity* |
| | | *Maintenance* |
| | | *Risk Assessnent* |
| | | *Vulnerability Management* |
| *availability* | *Manage sensitive documents and output devices* | *System and Communications Protection* |
| | *Manage physical access to IT assets* | *Physical and Environmental* |
| | | *Security Budget* |
| | | *System and Services Acquisition* |
| | | *Contingency Planning* |

Dari tabel 1 dapat di analisi 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 di dapatkan bahwa metode NIST SP 800-55 memiliki kompleksitas dalam prosedur dari pada COBIT 5 DSS05.

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*.

## IV. PENUTUP

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. Jika organisasi itu belum menerapkan manajemen keamanan informasi, bisa menggunakan COBIT 5 seperti pada sebuah oranisasi yang ingin membuat dan mengimplemantasikan sebuah sistem informasi akademik baru di sebuah kampus .

Namun apabila organisasi itu 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 pelaksanaanya 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


Asriyanik, and Mokhamad Hendayun. 2017. "Tata Kelola Teknologi Informasi Pada Perguruan Tinggi Menggunakan Control Objective for Information & Related Technology ( COBIT ) 5." *Jurnal Teknik Informatika dan Sistem Informasi* 3(April): 206–16.

Bekti Maryuni Susanto. 2013. "Mengukur Keamanan Informasi : Studi Komparasi ISO 27002 Dan NIST 800-55." In *Seminar Nasional Teknologi Informasi Dan Komunikasi 2013 (SENTIKA 2013)*,.

Brown, Anthony, and Will Robinson. 2015. 1 *Security Metrics Guide for Information Technology Systems*.

Chew, Elizabeth et al. 2008. *Performance M Easurement Guide for Information Security*.

Elachgar, Hicham, Brahim Boulafdour, Meryem Makoudi, and Boubker Regragui. 2012. "Information Security, 4TH Wave." *Journal of Theoretical and Applied Information Technology* 43(1): 1–7.

Farida, Siti Ida, and Elsy Rahajeng. 2014. "Usulan Model Tata Kelola Teknologi Informasi Pada Domain Monitor , Evaluate And Assess Dengan Metode Framework COBIT 5." *Studi Informatika :Jurnal Sistem Informasi* 7(2): 1–10.

Fathoni, Listya Febri et al. 2016. "Application Information System Based Health Services Android." *Jurnal Ilmu Teknik Elektro Komputer dan Informatika (JITEKI)* 2(1): 39–48.

Firmansyah, Devie. 2015. "Pengukuran Kapabilitas Pengelolaan Sistem Informasi Sub Domain Deliver , Service , Support 01 Menggunakan Framework Cobit 5 Studi Kasus : Politeknik Komputer Niaga LPKIA Bandung." *Konferensi Nasional Sistem & Informatika 2015*: 689–95.

Hermaduanti, Ninki, and Imam Riadi. 2016. "Automation Framework for Rogue Access Point Mitigation in Ieee 802.1X-Based WLAN." *Journal of Theoretical and Applied Information Technology* 93(2): 287–96.

Isaca. 2013. *A Business Framework for the Governance*

*and Management of Enterprise IT*. www.isaca.org.
Kurniawan, Endang, and Imam Riadi. 2018a. "Analisis Tingkat Keamanan Sistem Informasi Akademik Berdasarkan Standar ISO 27002 : 2013 Menggunakan SSE-CMM." *Jurnal Ilmia Penelitian Teknologi dan Penerapan Sistem Informasi* 2(1): 12–23.
Kurniawan, Endang, and Imam Riadi. 2018b. "Security Level Analysis of Academic Information Systems Based on Standard ISO 27002:2003 Using SSE-CMM." *International Journal of Computer Science and Information Security (IJCSIS)* 16(1): 139–47. http://arxiv.org/abs/1802.03613%0Ahttp://dx.doi.org/10.13140/RG.2.2.20925.15840.
Mahardika, Fathoni. 2017. "Manajemen Risiko Keamanan Informasi Menggunakan Framework NIST SP 800-30 Revisi 1 (Studi Kasus: STMIK Sumedang)." *JURNAL INFORMATIKA : Jurnal Pengembangan IT* 2(2): 1–8. http://ejournal.poltektegal.ac.id/index.php/informatika/article/view/484.
Raichel, L et al. 2005. *INTERNATIONAL STANDARD ISO / IEC*.
Riadi, Imam. 2016. "Analisis Keamanan Informasi Berdasarkan Kebutuhan Teknikal Dan Operasional Mengkombinasikan Standar ISO 27001 : 2005 Dengan Maturity Level ( Studi Kasus Kantor Biro Teknologi Informasi PT . XYZ )." *Seminar Nasional Teknologi Informasi Dan Multimedia 2016* 6(6): 6–7.
Rosmiati, Imam Riadi, and Yudi Prayudi. 2016. "A Maturity Level Framework for Measurement of Information Security Performance Imam Riadi." *International Journal of Computer Applications* 141(8): 975–8887.
Sasongko, Nanang. 2011. "Pengujian Keamanan Transaksi Cloud Computing Pada Layanan Software as a Services ( SaaS ) Menggunakan Kerangka Kerja NIST SP800-53A." *Seminar Nasional Aplikasi Teknologi Informasi (SNATI)* 2011(Snati): 134–39.
Setyaningrum, Novia Dwi, and Ari Kusyanti. 2018. "Evaluasi Manajemen Risiko Teknologi Informasi Menggunakan Framework COBIT 5 ( Studi Kasus : PT . Kimia Farma ( Persero ) Tbk – Plant Watudakon )." *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer* 2(1): 143–52.
Task, Joint, and Force Transformation. *Security and Privacy Controls for Federal Information Systems and Organizations Security and Privacy Controls for Federal Information Systems and Organizations*.
Umar, Rusydi, Imam Riadi, and Eko Handoyo. 2017. "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*, Seminar Nasional Teknologi Informasi dan Komunikasi - SEMANTIKOM 2017 ANALISIS, 41–48.

**Rusydi Umar**, merupakan dosen di prodi teknik infromatika Universitas Ahmad Dahlan Yogjakarta. Dengan jabatan fugsional Lektor / III.D, mendapatkan gelar S1 dari Teknik Elektro UGM Yogykarta – Indonesia, S2 Teknik Informatika ITB Bandung – Indonesia, S3 Dept. Computer, Information Science School of Mathematics and Information Sciences University of Hyderabad – India. Dengan bidang penelitian Grid Computing, Cloud Computing, Software Engineering. **Imam Riadi**, merupakan dosen di prodi sistem informasi Universitas Ahmad Dahlan Yogjakarta. Dengan jabatan fugsional Lektor, mendapatkan gelar S1 dari Universitas Negeri Yogyakarta, S2 Ilmu Komputer Universitas Gadjah Mada, S3 Ilmu Komputer Universitas Gadjah Mada. Dengan bidang keahlian Jaringan Komputer, Sekuritas Komputer, Administrasi Sistem dan Jaringan, Organisasi dan Arsitektur Komputer, Forensik Digital. **Eko Handoyo**, Merupakan mahasiswa Magister Teknik Informatika Universitas Ahmad Dahlan Yogyakarta. Mendapatkan gelar S1 dari Universitas Trunojoyo Madura. Dengan spsifikasi bidang sistem Informasi.

Rusydi Umar , S.T., M.T, Ph.D. Prodi teknik infromatika Universitas Ahmad Dahlan Yogjakarta. Dr. Imam Riadi, S.Pd., M.Kom. Prodi sistem informasi Universitas Ahmad Dahlan Yogjakarta. Eko Handoyo Magister Teknik Informatika Universitas Ahmad Dahlan Yogyakarta.