Volume 15 | Desember 2016 | ISSN 2085 - 7993

In Search

Pendidikan, Penelitian & Pengabdian Masyarakat

Informatic, Science, Entrepreneur, Applied Art, Research, Humanism

In Search
Pendidikan, Penelitian & Pengabdian Masyarakat
Volume 15 | Desember 2016 | ISSN 2085 - 7993

In Search

Pendidikan Pelatihan & Pengabdian Masyarakat

Informatic, Science, Entrepreneur, Applied Art, Research, Humanism

Susnan tim In Search

Pelindung
Dr. Ir. Bob Foster, M.M.

Pengarah
Drs. Muh. Deni Johansyah, M.M.

Penanggung Jawab
Emil R. Kaburuan, S.T., MA., Ph.D.

Redaksi
Sabilla Saberina, S.E.

Anggota Redaksi
Yesica Wawoh, S.E., M.Si.
Sinta Hartini P., S.I.Kom., M.Si.
Annisa Theo Sophi, S.Psi.
Ratih Hardiantini, S.Kom., M.A.B

Sirkulasi
Elis Rostalina

In Search
diterbitkan oleh LPPM UNIBI
Jl. Soekarno Hatta 643 Bandung
Telp. 022 4265399
Fax. 022 4209308
e-mail : lppm_unibi@unibi.ac.id

Catatan Redaksi

In Search

In Search, media informasi pendidikan, penelitian dan pengabdian Universitas Informatika dan Bisnis Indonesia (UNIBI), hadir guna memasilitasi Tridharma Perguruan Tinggi dan memberikan wawasan dan pengetahuan bagi pembacanya.

Pembaca yang budiman, edisi yang saat ini berada di tangan pembaca adalah edisi ke limabelas, terdiri dari tujuh artikel hasil penelitian dan telaah pustaka dari berbagai bidang ilmu yaitu informatika, enterpreneur, ekonomi, manajemen, akuntansi, dan humaniora. Juga kami sertakan liputan kegiatan pendidikan, penelitian dan pengabdian yang berlangsung di UNIBI.

Semoga kehadiran In Search menjadi pemicu prestasi kita.

Redaksi,

Konten

PENGGUNAAN DUA KERANGKA KERJA UNTUK AUDIT KEAMANAN SISTEM INFORMASI

Titan Parama Yoga, M.Kom

Fakultas Teknologi dan Informatika, Universitas Informatika dan Bisnis Indonesia
Jl. Soekarno Hatta No. 643 Bandung, Jawa Barat, Indonesia

Email : titanparamayoga@unibi.ac.id

Abstrak

Sistem Informasi yang baik adalah sistem informasi yang dapat memberikan kemudahan, pelayanan terbaik dan ketepatan dalam hal pemberian informasi namun pada kenyataannya masih sering didapati sistem informasi yang belum maksimal dalam hal memberikan kemudahan, pelayanan terbaik dan ketepatan untuk pemberian informasi. Hal tersebut dikarenakan sistem informasi mendapat atau memiliki berbagai permasalahan khususnya dari keamanan sistem informasi. Audit keamanan sistem informasi adalah salah satu cara untuk mengetahui tingkat keamanan sistem informasi tersebut. Hasil dari audit keamanan sistem informasi dapat berupa rekomendasi untuk pihak yang berwenang terhadap keamanan sistem informasi untuk selanjutnya ditindaklanjuti untuk melakukan perbaikan-perbaikan sehingga sistem informasi dapat berjalan maksimal. Pada proses audit keamanan sistem informasi terkadang sebagian auditor tidak cukup puas hanya dengan menggunakan satu kerangka kerja penilaian. Di beberapa kasus terkadang auditor menggunakan dua bahkan lebih kerangka kerja penilaian. Tujuan dari penggunaan dua atau lebih kerangka kerja penilaian adalah untuk lebih menyempurnakan atau memdapatkan penilaian terbaik karena dinilai oleh dua atau lebih kerangka kerja penilaian. Kata Kunci : *Pendidikan dan pelatihan, motivasi kerja, insentif, kinerja pegawai*

Kata kunci *:* *Sistem Informasi, Audit, Keamanan, Kerangka kerja*

Abstract

[Title in English : Application of Fourier Series on Radio Signal Analysis] *Good information system is an information system that can provide convenience, best service and accuracy in terms of providing information but in reality they are often found to information systems is not maximized in terms of providing convenience, best service and accuracy for the provision of information. That is because the system gets information or have a variety of issues, especially on the security of information systems. Audit security of information systems is one way to determine the level of security of information systems. The results of a security audit of information systems can be either on the authorities to the security of information systems to further followed to make improvements so that the system can run up information. In the process of auditing information systems security auditors sometimes some are not quite satisfied just by using the assessment framework. In some cases, auditors sometimes use two or even more assessment framework. The purpose of the use of two or more assessment framework is to further refine or clearance can best ratings as judged by two or more assessment framework.*Keywords: *Education and trainning, job motivation, incentive, employee performance.*

Keywords: *Information Systems, Audit, Security, Frameworks*

1. PENDAHULUAN

Saat ini, salah satu aset terbesar dari suatu organisasi adalah informasi karena informasi merupakan sumber daya yang bisa dimanfaatkan oleh sebuah organisasi untuk menetapkan keputusan dan untuk berkembangnya suatu organisasi . Bahkan dengan informasi, sebuah organisasi dapat memberikan sebuah bentuk pelayanan terbaiknya bagi konsumennya.

Pengorganisasian sebuah informasi menjadi suatu hal yang penting untuk bisa menciptakan sebuah informasi yang bukan hanya baik namun juga memiliki nilai. Nilai sebuah informasi ditentukan oleh kemudahan memperoleh informasi, bersifat luas dan lengkap, memiliki ketelitian dan keamanan, memiliki kecocokan dengan penerima, memiliki ketepatan waktu, jelas, luwes, dapat dibuktikan, dapat diukur dan tidak berdasarkan atas dugaan atau prasangka (Burch Jr and Grudnitski, 1979).

Untuk mengorganisasikan informasi maka dirancanglah sesuah sistem pengorganisasian informasi yang sering kita sebut sistem informasi. Sistem Informasi bukan hanya tempat untuk pengorganisasian informasi tapi juga sumber informasi itu sendiri yang dibutuhkan oleh semua bagian dalam sebuah organisasi karena sistem informasi diciptakan dan dibangun dengan memiliki keterkaitan dan keterhubungan dengan semua bagian dengan harapan bisa mempertemukan semua kebutuhan dari semua bagian.

Namun sejalan dengan waktu, terkadang sebuah sistem informasi yang sebenarnya diharapkan dapat memberikan dan menghasilkan informasi yang bernilai pada prakteknya sering memiliki kendala untuk fungsi utama tersebut. Kendala tersebut bisa berasal dari dalam sistem informasi itu sendiri atau pun dari luar sistem. Kendala tersebut bisa saja mengganggu sistem informasi untuk memberikan informasi yang bernilai.

Untuk mengatasi hal tersebut maka yang harus dilakukan adalah memperbaiki sistem informasi itu sendiri. Namun memperbaiki tidak bisa dilakukan hanya pada bagian yang bermasalah saja karena itu tidak menyelesaikan masalah secara keseluruhan. Proses perbaikan harus dimulai dari menilai sistem informasi itu. Proses penilaian sistem informasi sering disebut audit sistem informasi.

Audit sistem informasi sedang gencar dilakukan oleh semua organisasi. Hal ini dikarenakan bukan hanya untuk mengetahui nilai dari sebuah informasi tapi juga kebutuhan terhadap sebuah sistem informasi yang baik dan dapat melayani kebutuhan setiap pemangku kepentingan sangat tinggi. Kategori sebuah sistem informasi yang baik adalah adanya jaminan keamanan dari sistem informasi itu sendiri.

Audit sistem informasi adalah suatu cara untuk mengetahui tingkat keamanan dan kemampuan sistem tersebut menghadapi gangguan. Gangguan terhadap keamanan sistem informasi banyak sumbernya, bisa bersumber dari eksternal sistem maupun internal sistem itu sendiri. Oleh karena itu, audit terhadap keamanan sistem informasi merupakan hal yang harus selalu dilakukan dan mendapatkan perhatian yang khusus dari setiap pengelola sistem informasi.

Audit sistem informasi bergantung kepada pemilihan kerangka kerja untuk proses audit tersebut. Pemilihan kerangka kerja audit yang tepat juga mempengaruhi penilaian dari tingkat keamanan sistem informasi itu sendiri.

Telah banyak kerangka kerja yang menawarkan bentuk penilaian dan hasil penilaian yang bisa digunakan oleh organisasi untuk mengetahui tingkat keamanan dari sistem informasinya dan selama ini juga kita telah menggunakan beberapa kerangka kerja tersebut untuk penilaian sistem informasi kita namun selama ini kita hanya menggunakan satu jenis kerangka kerja untuk sekali proses penilaian sistem informasi.

Ada alternatif lain untuk penilaian atau audit sistem informasi. Alternatif tersebut adalah dengan menggabungkan dua jenis kerangka kerja untuk sekali proses audit sistem informasi. Banyak alasan dalam penggabungan dua jenis kerangka kerja tersebut, bisa dikarenakan kerangka kerja yang satu tidak dapat berdiri sendiri atau dikarenakan kerangka kerja yang satu belum memenuhi sisi bisnis. Intinya dari dua penggabungan dua kerangka kerja ini adalah saling melengkapi.

2. TINJAUAN PUSTAKA

Audit

Definisi umum dari audit adalah bahwa "*Auditing is an independent investigation of some particular activity*" namun bila dilihat dari sejarah, maka audit berasal dari bahasa latin yaitu *Audire* atau dalam bahasa inggrisnya adalah *to hear.* (Gondodiyoto, 2007).

Sistem Informasi

Definisi sistem informasi yang didefinisikan oleh Robert A. Leitch dan K. Roscoe Davis di bukunya yaitu *Accounting Information System* dan dikutip oleh Jogiyanto Hartono pada bukunya yang berjudul Analisis dan Desain Sistem Informasi

*Sistem informasi adalah suatu sistem didalam suatu organisasi yang mempertemukan kebutuhan pengolahan transaksi harian, mendukung operasi, bersifat manajerial dan kegiatan strategis dari suatu organisasi dan menyediakan pihak luar tertentu dengan laporan-laporan yang diperlukannya (*Hartono, 1989)

Audit Sistem Informasi

Dikutip dari buku *Information system control and auditing* karangan Ron Weber (Yaher dkk, 2012) dikatakan bahwa Audit Sistem Informasi adalah Proses pengumpulan dan evaluasi bukti-bukti untuk

menentukan apakah sistem komputer yang digunakan telah dapat melindungi aset milik organisasi, mampu menjaga integritas data, dapat membantu pencapaian tujuan organisasi secara efektif, serta menggunakan sumber daya yang dimiliki secara efisien

Keamanan Sistem Informasi

Menurut Riyanarto Sarno dan Irsyat Iffano dibukunya yang berjudul Sistem Manajemen Keamanan Informasi seperti yang dikutip oleh Annisa Destiara Yaner dkk dikatakan bahwa keamanan sistem informasi adalah penjagaan informasi dari seluruh ancaman yang mungkin terjadi dalam upaya untuk memastikan atau menjamin kelangsungan bisnis, meminimalisasi resiko bisnis dan memaksimalkan atau mempercepat pengembalian investasi dan peluang bisnis (Yaner dkk, 2012).

3. PEMBAHASAN

Telah banyak penelitian maupun jurnal yang melakukan proses audit sistem informasi dengan menggabungkan dua kerangka kerja. Dengan berbagai alasan mereka menggabungkan dua kerangka kerja tersebut. Seperti yang dikutip dari jurnal "Audit Keamanan SIMAK berdasarkan ISO 27002 (Studi Kasus : FE UNUD)" , bahwa penggabungan yang melalui proses pemetaan antara kerangka kerja COBIT 4.1 dan ISO 27002 menghasilkan proses audit yang lebih luas dan lebih dalam dibandingkan kerangka kerja lain (Bless, Yulius C. N. Sasmita, Gusti Made Arya. Cahyawan, A. A. Kt. Agung, 2014). Sedangkan pada jurnal "Audit Keamanan Sistem Informasi berdasarkan standar ISO 27002 (Studi Kasus : PT. Aneka Jaya Baut Sejahtera)" mengatakan bahwa metode ISO 27002 digunakan untuk mengidentifikasi tingkat kematangan penerapan pengamanan dengan kategorisasi yang mengacu pada kerangka kerja COBIT atau CCMI (*Capability Marturity Model For Integration*). Tingkat kematangan ini nantinya akan digunakan sebagai alat untuk melaporkan pemetaan dan pemeringkatan kesiapan keamanan informasi. (Halim, Marliana. Tanuwijaya, Haryanto. Mastan, Ignatius Adrian, 2012).

Berbeda dengan jurnal "*Governance Audit Of Application Procurement Using COBIT Framework*" yang menggabungkan antara kerangka kerja COBIT dan ITIL, mengatakan bahwa COBIT dan kerangka ITIL menyediakan cara yang efektif dalam memahami kebutuhan dan prioritas tata kelola TI dengan menyelesaikan satu sama lain. Peran COBIT dalam proses pengukuran kinerja melalui proses IT pengukuran kematangan, dengan mengukur tingkat kematangan saat ini dan perbaikan proses masa depan dengan menetapkan target pencapaian kedewasaan menuju peningkatan besar sedangkan ITIL menggambarkan apa faktor kunci keberhasilan dalam kinerja layanan untuk meningkatkan kepuasan pengguna. ITIL mendukung praktik terbaik dari manajemen TI dan lebih fokus pada metode dan menentukan aliran proses telah dilakukan. Sebagai kerangka kerja, keduanya dapat dikombinasikan untuk diterapkan dalam organisasi. (Krisanthi, Gusti Ayu Theresia. Sukarsa, I Made. Bayupati, I Putu Agung. 2014)

Intinya, apapun jenis kerangka kerja yang akan digabungkan semuanya untuk memperoleh proses dan penilaian audit yang lebih sempurna, lebih baik dan lebih luas.

Namun apakah penggabungan dua kerangka itu tanpa didasari standar atau aturan yang ada. Jawabannya tentu saja tidak. Penggabungan dua kerangka kerja untuk penilaian tingkat keamanan sistem informasi harusnya mematuhi standar atau aturan yang telah ada. Salah satu standar atau aturan yang ada adalah adanya tahapan pemetaan antara dua kerangka kerja tersebut. Pemetaan antar dua kerangka kerja untuk menilai tingkat keamanan sistem informasi harus berdasarkan kesamaan dari kontrol terhadap keamanan sistem informasi. Dari berbagai literatur, banyak yang menjelaskan dan membahas 20 kontrol keamanan kritis yang dapat menjadi acuan untuk proses pemetaan setiap kerangka kerja. Kontrol keamanan kritis yang berjumlah 20 adalah standar yang menyatukan domain-domain standar penilaian dari masing masing kerangka kerja.

Tabel 1. 20 Critical Security Controls (Sumber : www.auditscript.com)

20 Critical Security Controls	
Critical Security Control #1	Inventory of Authorized and Unauthorized Devices
Critical Security Control #2	Inventory of Authorized and Unauthorized Software
Critical Security Control #3	Secure Configurations for Hardware and Software
Critical Security Control #4	Continuous Vulnerability Assessment and Remediation
Critical Security Control #5	Controlled Use of Administrative Privileges
Critical Security Control #6	Maintenance, Monitoring, and Analysis of Audit Logs

Critical Security Control #7	Email and Web Browser Protections
Critical Security Control #8	Malware Defenses
Critical Security Control #9	Limitation and Control of Network Ports
Critical Security Control #10	Data Recovery Capability
Critical Security Control #11	Secure Configurations for Network Devices
Critical Security Control #12	Boundary Defense
Critical Security Control #13	Data Protection
Critical Security Control #14	Controlled Access Based on the Need to Know
Critical Security Control #15	Wireless Access Control
Critical Security Control #16	Account Monitoring and Control
Critical Security Control #17	Security Skills Assessment and Appropriate Training to Fill Gaps
Critical Security Control #18	Application Software Security
Critical Security Control #19	Incident Response and Management
Critical Security Control #20	Penetration Tests and Red Team Exercises

Inilah 20 *critical security controls* yang menjadi acuan bukan hanya pemetaan, tapi juga lingkup penilaian keamanan sistem informasi dan juga untuk penentuan kerangka kerja mana saja yang dapat digabungkan. Penggabungan ini merujuk pada keterkaitan masing-masing domain pada setiap kerangka kerja dengan *critical security controls* tertentu. Panduannya dapat dilihat dari tabel 2 sampai tabel 21.

Tabel 2. ***Critical Security Control #1 : Inventory of Authorized and Unauthorized Devices Mapping***
(Sumber : www.auditscript.com)

Frame work	NIST 800-53 rev4	NIST Core Framework	DHS CDM Program	ISO 27002:2013	ISO 27002:2005	NSA MNP	UK ICO Protecting Data	PCI DSS 3.1	PCI DSS 3.0	HIPAA
Domain	• CA-7: Continuous Monitoring • CM-8: Information System Component Inventory • IA-3: Device Identification and Authentication • SA-4: Acquisition Process • SC-17: Public Key Infrastructure Certificates • SI-4: Information System Monitoring • PM-5: Information System Inventory	• ID.AM-1 • ID.AM-3 • ID.AM-4 • PR.DS-3	HWAM: Hardware Asset Management	• A.8.1.1 • A.9.1.2 • A.13.1.1	• A.7.1.1 • A.10.6.1 - A.10.6.2 • A.11.4.6	• Map Your Network • Baseline Management • Document Your Network • Personal Electronic Device Management • Network Access Control • Log Management	Inappropriate locations for processing data	2,4	2,4	• 164.310(b): Workstation Use - R • 164.310(c): Workstation Security - R
Frame work	FFIEC Examiners Handbook	FFIEC Cybersecurity Assessment Tool (CAT)	COBIT 5	NERC CIP v5	NERC CIP v4	NERC CIP v3	Cloud Security Alliance	FY15 FISMA Metrics	ITIL 2011 KPIs	AICPA's GAPP
Domain	Host Security User Equipment Security (Workstation, Laptop, Handheld)	Domain 3: Cybersecurity Controls - Preventative Controls Domain 3: Cybersecurity Controls - Detective Controls	• APO13: Manage Security • DSS05: Manage Security Services • BAI09: Manage Assets	CIP-002-5 R1 CIP-002-5 R2	• CIP-002-4 R1 • CIP-002-4 R2 • CIP-002-4 R3 • CIP-003-4 R5 • CIP-004-4 R4 • CIP-005-4 R2 • CIP-006-4 R3	• CIP-002-3 R1 • CIP-002-3 R2 • CIP-002-3 R3 • CIP-002-3 R4 • CIP-003-3 R5 • CIP-004-3 R4 • CIP-005-3 R2 • CIP-006-3 R3	• DCS-01 • MOS-09 • MOS-15	1: System Inventory 2: Continuous Monitoring	Information Security Management	• 7.2.2 • 8.2.1 • 8.2.2

Tabel 3. Critical Security Control #2 : Inventory of Authorized and Unauthorized Software Mapping
(Sumber : www.auditscript.com)

Frame work	NIST 800-53 rev4	NIST Core Framework	DHS CDM Program	ISO 27002:2013	NSA MNP	UK ICO Protecting Data	PCI DSS 3.1	PCI DSS 3.0	HIPAA
Domain	• CA-7: Continuous Monitoring • CM-2: Baseline Configuration • CM-8: Information System Component Inventory • CM-10: Software Usage Restrictions • CM-11: User-Installed Software • SA-4: Acquisition Process • SC-18: Mobile Code • SC-34: Non-Modifiable Executable Programs • SI-4: Information System Monitoring • PM-5: Information System Inventory	• ID.AM-2 • PR.DS-6	• HWAM: Hardware Asset Management • SWAM: Software Asset Management	• A.12.5.1 • A.12.6.2	• Baseline Management • Executable Content Restrictions • Configuration and Change Management	Decommissioning of software or services	2,4	2,4	• 164.310(b): Workstation Use - R • 164.310(c): Workstation Security - R
Frame work	FFIEC Examiners Handbook	FFIEC Cybersecurity Assessment Tool (CAT)	COBIT 5	NSA Top 10	Cloud Security Alliance	FY15 FISMA Metrics	ITIL 2011 KPIs	AICPA's GAPP	Australian Top 35
Domain	Host Security User Equipment Security (Workstation, Laptop, Handheld)	Domain 3: Cybersecurity Controls - Preventative Controls Domain 3: Cybersecurity Controls - Detective Controls	• APO13: Manage Security • DSS05: Manage Security Services Assets	Application Whitelisting	• CCC-04 • MOS-3 • MOS-04 • MOS-15	1: System Inventory 2: Continuous Monitoring	Information Security Management	• 7.2.2 • 8.2.1	• 1 • 14 • 17

Tabel 4. Critical Security Control #3 : Secure Configurations for Hardware and Software Mapping
(Sumber : www.auditscript.com)

Frame work	NIST 800-53 rev4	NIST Core Framework	DHS CDM Program	FFIEC Examiners Handbook	FFIEC Cybersecurity Assessment Tool (CAT)	NSA MNP	NSA Top 10	GCHQ 10 Steps
Domain	• CA-7: Continuous Monitoring • CM-2: Baseline Configuration • CM-3: Configuration Change Control • CM-5: Access Restrictions for Change • CM-6: Configuration Settings • CM-7: Least Functionality • CM-8: Information System Component Inventory • CM-9: Configuration Management Plan • CM-11: User-Installed Software • MA-4: Nonlocal Maintenance • RA-5: Vulnerability Scanning • SA-4: Acquisition Process • SC-15: Collaborative Computing Devices • SC-34: Non-Modifiable Executable Programs • SI-2: Flaw Remediation • SI-4: Information System Monitoring	• PR.IP-1	CSM: Configuration Settings Management	• CIP-002-5 R1 • CIP-002-5 R2	• Domain 3: Cybersecurity Controls - Preventative Controls • Domain 3: Cybersecurity Controls - Detective Controls	• Patch Management • Baseline Management • Data-at-Rest Protection • Configuration and Change Management	• Set a Secure Baseline Configuration • Take Advantage of Software Improvements 2,4	Secure Configuration

Frame work	PCI DSS 3.1	PCI DSS 3.0	ISO 27002:2013	ISO 27002:2005	COBIT 5	NERC CIP v5	NERC CIP v4	NERC CIP v3
Domain	• 2.2 • 2.3 • 6.2 • 11.5	• 2.2 • 2.3 • 6.2 • 11.5	• A.14.2.4 • A.14.2.8 • A.18.2.3	• A.15.2.2	• APO13: Manage Security • DSS05: Manage Security Services	• CIP-007-5 R2 • CIP-010-5 R2	• CIP-003-4 R6 • CIP-007-4 R3	• CIP-003-3 R6 • CIP-007-3 R3

Frame work	HIPAA	ITIL 2011 KPIs	AICPA's GAPP	Australian Top 35	Cloud Security Alliance	UK Cyber Essentials	FY15 FISMA Metrics
Domain	• 164.310(b): Workstation Use - R • 164.310(c): Workstation Security – R	Information Security Management	• 7.2.2 • 8.2.1	• 2-5 • 21	• IVS-07 • MOS-15 • MOS-19 • TVM-02	• Secure Configuration • Patch Management	2: Continuous Monitoring

Tabel 5. Critical Security Control #4 : Continuous Vulnerability Assessment and Remediation Mapping
(Sumber : www.auditscript.com)

Frame work	NIST 800-53 rev4	NIST Core Framework	FFIEC Examiners Handbook	FFIEC Cybersecurity Assessment Tool (CAT)	NSA MNP	NSA Top 10	UK ICO Protecting Data	UK Cyber Essentials
Domain	• CA-2: Security Assessments • CA-7: Continuous Monitoring • RA-5: Vulnerability Scanning • SC-34: Non-Modifiable Executable Programs • SI-4: Information System Monitoring • SI-7: Software, Firmware, and Information Integrity	• ID.RA-1 • ID.RA-2 • PR.IP-12 • DE.CM-8 • RS.MI-3	Host Security User Equipment Security (Workstation, Laptop, Handheld)	• Domain 3: Cybersecurity Controls - Preventative Controls • Domain 3: Cybersecurity Controls - Detective Controls	• Patch Management • Log Management • Configuration and Change Management	• Take Advantage of Software Improvements	Software Updates	• Patch Management
Frame work	**PCI DSS 3.1**	**PCI DSS 3.0**	**ISO 27002:2013**	**ISO 27002:2005**	**COBIT 5**	**NERC CIP v5**	**NERC CIP v4**	**NERC CIP v3**
Domain	• 6.1 • 6.2 • 11.2	• 6.1 • 6.2 • 11.2	• A.12.6.1 • A.14.2.8	• A.12.6.1 • A.13.1.2 • A.15.2.2	• APO13: Manage Security • DSS05: Manage Security Services	• CIP-007-5 R2 • CIP-010-5 R3	• CIP-005-4 R4 • CIP-007-4 R3 • CIP-007-4 R8	• CIP-005-3 R4 • CIP-007-3 R3 • CIP-007-3 R8
Frame work	**HIPAA**	**ITIL 2011 KPIs**	**AICPA's GAPP**	**DHS CDM Program**	**FY15 FISMA Metrics**	**Australian Top 35**	**Cloud Security Alliance**	
Domain	• 164.310(b): Workstation Use - R • 164.310(c): Workstation Security - R	Information Security Management	• 7.2.2 • 8.2.1	VUL: Vulnerability Management	2: Continuous Monitoring	• 2-3	• IVS-05 • MOS-15 • MOS-19 • TVM-02	

Tabel 6. Critical Security Control #5 : Controlled Use of Administrative Privileges Mapping
(Sumber : www.auditscript.com)

Frame work	NIST 800-53 rev4	NIST Core Framework	ISO 27002:2013	ISO 27002:2005	NERC CIP v4	NERC CIP v5	NERC CIP v3	COBIT 5
Domain	• AC-2: Account Management • AC-6: Least Privilege • AC-17: Remote Access • AC-19: Access Control for Mobile Devices • CA-7: Continuous Monitoring • IA-2: Identification and Authentication (Organizational Users) • IA-4: Identifier Management • IA-5: Authenticator Management • SI-4: Information System Monitoring	• PR.AC-4 • PR.AT-2 • PR.MA-2 • PR.PT-3	• A.9.1.1 • A.9.2.2 - A.9.2.6 • A.9.3.1 • A.9.4.1 - A.9.4.4	• A.11.5.1 - A.11.5.3	• CIP-002-4 R1 • CIP-002-4 R2 • CIP-002-4 R3 • CIP-003-4 R5 • CIP-004-4 R4 • CIP-005-4 R2 • CIP-006-4 R3	• CIP-002-5 R1 • CIP-002-5 R2	• CIP-002-3 R1 • CIP-002-3 R2 • CIP-002-3 R3 • CIP-002-3 R4 • CIP-003-3 R5 • CIP-004-3 R4 • CIP-005-3 R2 • CIP-006-3 R3	• APO13: Manage Security • DSS05: Manage Security Services
Frame work	**FFIEC Cybersecurity Assessment Tool (CAT)**	**FFIEC Examiners Handbook**	**UK Cyber Essentials**	**Cloud Security Alliance**	**PCI DSS 3.1**	**PCI DSS 3.0**	**NSA Top 10**	**Australian Top 35**
Domain	• Domain 3: Cybersecurity Controls - Preventative Controls • Domain 3: Cybersecurity Controls - Detective Controls	Authentication and Access Controls	• Access Control	• DCS-01 • MOS-09 • MOS-15	• 2.1 • 7.1 - 7.3 • 8.1 - 8.3 • 8.7	• 2.1 • 7.1 - 7.3 • 8.1 - 8.3 • 8.7	• Control Administrative Privileges	• 4 • 9 • 11 • 25
Frame work	**FY15 FISMA Metrics**	**ITIL 2011 KPIs**	**AICPA's GAPP**	**NSA MNP**	**HIPAA**	**UK ICO Protecting Data**		**GCHQ 10 Steps**
Domain	3: Identity Credential and Access Management	Information Security Management	• 7.2.2 • 8.2.1 • 8.2.2	• User Access • Baseline Management • Log Management	• 164.310(b): Workstation Use - R • 164.310(c): Workstation Security - R	• Configuration of SSL and TLS • Default Credentials		Monitoring

Tabel 7. Critical Security Control #6 : Maintenance, Monitoring, and Analysis of Audit Logs Mapping
(Sumber : www.auditscript.com)

Frame work	NIST 800-53 rev4	NIST Core Framework	HIPAA	FFIEC Cybersecurity Assessment Tool (CAT)	FFIEC Examiners Handbook	ISO 27002:2005	ISO 27002:2013
Domain	• AC-23: Data Mining Protection • AU-2: Audit Events • AU-3: Content of Audit Records • AU-4: Audit Storage Capacity • AU-5: Response to Audit Processing Failures • AU-6: Audit Review, Analysis, and Reporting • AU-7: Audit Reduction and Report Generation • AU-8: Time Stamps • AU-9: Protection of Audit Information • AU-10: Non-repudiation • AU-11: Audit Record Retention • AU-12: Audit Generation • AU-13: Monitoring for Information Disclosure • AU-14: Session Audit • CA-7: Continuous Monitoring • IA-10: Adaptive Identification and Authentication • SI-4: Information System Monitoring	• PR.PT-1 • DE.AE-3 • DE.DP-1 • DE.DP-2 • DE.DP-3 • DE.DP-4 • DE.DP-5	• 164.308(a)(1): Security Management Process - Information System Activity Review R • 164.308(a)(5): Security Awareness and Training - Log-in Monitoring A	• Domain 2: Threat Intelligence & Collaboration - Monitoring and Analyzing • Domain 3: Cybersecurity Controls - Detective Controls	• Security Monitoring	• A.10.10.1 - A.10.10.6	• A.12.4.1 - A.12.4.4 • A.12.7.1
Frame work	**COBIT 5**	**ITIL 2011 KPIs**	**PCI DSS 3.1**	**PCI DSS 3.0**	**NERC CIP v5**	**NERC CIP v4**	**NERC CIP v3**
Domain	• APO13: Manage Security • DSS05: Manage Security Services	• Information Security Management	• 10.1 - 10.7	• 10.1 - 10.7	• CIP-007-5 R4	• CIP-005-4 R3 • CIP-007-4 R6	• CIP-005-3 R3 • CIP-007-3 R6
Frame work	**NV Gaming MICS v7 2015**	**Cloud Security Alliance**	**Australian Top 35**	**AICPA's GAPP**	**NSA MNP**	**DHS CDM Program**	**GCHQ 10 Steps**
Domain	System Parameters	• IVS-01 • IVS-03	• 15-16 • 35	• 7.2.2 • 8.2.1	• Log Management	• Generic Audit Monitoring	Monitoring

Tabel 8. Critical Security Control #7 : Email and Web Browser Protections Mapping
(Sumber : www.auditscript.com)

Frame work	NIST 800-53 rev4	NIST Core Framework	FFIEC Examiners Handbook	FFIEC Cybersecurity Assessment Tool (CAT)	COBIT 5	NERC CIP v5	NERC CIP v4	NERC CIP v3
Domain	• CA-7: Continuous Monitoring • CM-2: Baseline Configuration • CM-3: Configuration Change Control • CM-5: Access Restrictions for Change • CM-6: Configuration Settings • CM-7: Least Functionality • CM-8: Information System Component Inventory • CM-9: Configuration Management Plan • CM-11: User-Installed Software • MA-4: Nonlocal Maintenance • RA-5: Vulnerability Scanning • SA-4: Acquisition Process • SC-15: Collaborative Computing Devices • SC-34: Non-Modifiable Executable Programs • SI-2: Flaw Remediation • SI-4: Information System Monitoring	• PR.IP-1	Host Security User Equipment Security (Workstation, Laptop, Handheld)	• Domain 3: Cybersecurity Controls - Preventative Controls • Domain 3: Cybersecurity Controls - Detective Controls	• APO13: Manage Security • DSS05: Manage Security Services • BAI09: Manage Assets	• CIP-002-5 R1 • CIP-002-5 R2	• CIP-002-4 R1 • CIP-002-4 R2 • CIP-002-4 R3 • CIP-003-4 R5 • CIP-004-4 R4 • CIP-005-4 R2 • CIP-006-4 R3	• CIP-002-3 R1 • CIP-002-3 R2 • CIP-002-3 R3 • CIP-002-3 R4 • CIP-003-3 R5 • CIP-004-3 R4 • CIP-005-3 R2 • CIP-006-3 R3
Frame work	**NSA MNP**	**FY15 FISMA Metrics**	**ITIL 2011 KPIs**	**NSA Top 10**	**ISO 27002:2013**	**ISO 27002:2005**	**PCI DSS 3.1**	**PCI DSS 3.0**
Domain	• Patch Management • Baseline Management • Data-at-Rest Protection • Configuration and Change Management	2: Continuous Monitoring	Information Security Management	• Set a Secure Baseline Configuration • Take Advantage of Software Improvements	• A.8.1.1 • A.9.1.2 • A.13.1.1	• A.7.1.1 • A.10.6.1 - A.10.6.2 • A.11.4.6	• 2.2 • 2.3 • 6.2 • 11.5	• 2.2 • 2.3 • 6.2 • 11.5
Frame work	**HIPAA**	**Cloud Security Alliance**	**Australian Top 35**	**UK Cyber Essentials**	**GCHQ 10 Steps**	**AICPA's GAPP**	**DHS CDM Program**	
Domain	• 164.310(b): Workstation Use - R • 164.310(c): Workstation Security – R	• IVS-07 • MOS-15 • MOS-19 • TVM-02	• 2 • 5 • 17-20 • 31	• Secure Configuration • Patch Management	• Secure Configuration	• 7.2.2 • 8.2.1 • 8.2.2	• HWAM: Hardware Asset Management	

Tabel 9. Critical Security Control #8 : Malware Defenses Mapping
(Sumber : www.auditscript.com)

Frame work	NIST 800-53 rev4	NIST Core Framework	NSA MNP	NSA Top 10	FFIEC Examiners Handbook	FFIEC Cybersecurity Assessment Tool (CAT)	Australian Top 35	Cloud Security Alliance
Domain	• CA-7: Continuous Monitoring • SC-39: Process Isolation • SC-44: Detonation Chambers • SI-3: Malicious Code Protection • SI-4: Information System Monitoring • SI-8: Spam Protection	• PR.PT-2 • DE.CM-4 • DE.CM-5	• Device Accessibility • Virus Scanners and Host Intrusion Prevention Systems • Security Gateways, Proxies, and Firewalls • Network Security Monitoring • Log Management	• Use Anti-Virus File Reputation Services • Enable Anti-Exploitation Features	• Host Security • User Equipment Security (Workstation, Laptop, Handheld)	• Domain 2: Threat Intelligence & Collaboration - Monitoring and Analyzing • Domain 3: Cybersecurity Controls - Preventative Controls • Domain 3: Cybersecurity Controls - Detective Controls	• 7 • 17 • 22 • 26 • 30	• MOS-01 • MOS-15 • TVM-01 • TVM-03
Frame work	**HIPAA**	**AICPA's GAPP**	**GCHQ 10 Steps**	**COBIT 5**	**ISO 27002:2013**	**ISO 27002:2005**	**FY15 FISMA Metrics**	**ITIL 2011 KPIs**
Domain	• 164.308(a)(5): Security Awareness and Training - Protection from Malicious Software A • 164.310(d)(1): Device and Media Controls - Accountability A • 164.310(b): Workstation Use - R • 164.310(c): Workstation Security - R	• 7.2.2 • 8.2.1	• Removable Media Controls • Malware Protection	• APO13: Manage Security • DSS05: Manage Security Services	• A.8.3.1 • A.12.2.1 • A.13.2.3	• A.10.4.1 - A.10.4.2 • A.10.7.1	4: Anti Phishing and Malware Defense	• Information Security Management
Frame work	**UK Cyber Essentials**	**PCI DSS 3.1**	**PCI DSS 3.0**	**NERC CIP v5**	**NERC CIP v4**	**NERC CIP v3**		
Domain	• Malware Protection	• 5.1 - 5.4	• 5.1 - 5.4	• CIP-007-5 R3	• CIP-007-4 R4	• CIP-007-3 R4		

Tabel 10. Critical Security Control #9 : Limitation and Control of Network Ports Mapping
(Sumber : www.auditscript.com)

Frame work	NIST 800-53 rev4	NIST Core Framework	FFIEC Cybersecurity Assessment Tool (CAT)	FFIEC Examiners Handbook	ISO 27002:2013	ISO 27002:2005	Australian Top 35	COBIT 5
Domain	• AC-4: Information Flow Enforcement • CA-7: Continuous Monitoring • CA-9: Internal System Connections • CM-2: Baseline Configuration • CM-6: Configuration Settings • CM-8: Information System Component Inventory • SC-20: Secure Name /Address Resolution Service (Authoritative Source) • SC-21: Secure Name /Address Resolution Service (Recursive or Caching Resolver) • SC-22: Architecture and Provisioning for Name/Address Resolution Service • SC-41: Port and I/O Device Access • SI-4: Information System Monitoring	• PR.AC-5 • DE.AE-1	• Domain 3: Cybersecurity Controls - Preventative Controls • Domain 3: Cybersecurity Controls - Detective Controls	• Network Security	• A.9.1.2 • A.13.1.1 • A.13.1.2 • A.14.1.2	• A.10.6.1 - A.10.6.2 • A.11.4.4	• 2 • 3 • 12 • 13 • 27	• APO13: Manage Security • DSS05: Manage Security Services

Frame work	UK ICO Protecting Data	Cloud Security Alliance	NV Gaming MICS v7 2015	ITIL 2011 KPIs	NSA Top 10	NSA MNP	DHS CDM Program	GCHQ 10 Steps
Domain	• Decommissioning of software or services • Unnecessary Services	• DSI-02 • IVS-06 • IPY-04	• Network Security and Data Protection	• Information Security Management	• Limit Workstation-to-Workstation Communication	• Baseline Management • Configuration and Change Management	• Boundary Protection	• Network Security

Frame work	HIPAA	PCI DSS 3.1	PCI DSS 3.0	NERC CIP v5	NERC CIP v4	NERC CIP v3	AICPA's GAPP
Domain	• 164.310(b): Workstation Use - R • 164.310(c): Workstation Security - R	• 1,4	• 1,4	• CIP-007-5 R1	• CIP-007-4 R2	• CIP-007-3 R2	• 7.2.2 • 8.2.1

Tabel 11. Critical Security Control #10 : Data Recovery Capability Mapping
(Sumber : www.auditscript.com)

Frame work	NIST 800-53 rev4	NIST Core Framework	FFIEC Examiners Handbook	FFIEC Cybersecurity Assessment Tool (CAT)	Cloud Security Alliance	COBIT 5	NERC CIP v4	NERC CIP v3
Domain	• CP-9: Information System Backup • CP-10: Information System Recovery and Reconstitution • MP-4: Media Storage	• PR.IP-4	• Encryption	• Domain 3: Cybersecurity Controls - Preventative Controls	• MOS-11	• APO13: Manage Security • DSS05: Manage Security Services	• CIP-009-4 R4 • CIP-009-4 R5	• CIP-009-3 R4 • CIP-009-3 R5
Frame work	**HIPAA**	**ISO 27002:2013**	**ISO 27002:2005**	**NSA MNP**	**PCI DSS 3.1**	**PCI DSS 3.0**	**AICPA's GAPP**	**NV Gaming MICS v7 2015**
Domain	• 164.308(a)(7): Contingency Plan - Data Backup Plan R • 164.308(a)(7): Contingency Plan - Disaster Recovery Plan R • 164.308(a)(7): Contingency Plan - Testing and Revision Procedure A • 164.310(d)(1): Device and Media Controls - Data Backup and Storage A	• A.10.1.1 • A.12.3.1	• A.10.5.1 • A.10.8.3	• Backup Strategy	• 4.3 • 9.5 - 9.7	• 4.3 • 9.5 - 9.7	• 7.2.2 • 8.2.1	• Backups

Tabel 12. Critical Security Control #11 : Secure Configurations for Network Devices Mapping
(Sumber : www.auditscript.com)

Frame work	NIST 800-53 rev4	NIST Core Framework	DHS CDM Program	ISO 27002:2013	ISO 27002:2005	Cloud Security Alliance	UK Cyber Essentials	UK ICO Protecting Data
Domain	• AC-4: Information Flow Enforcement • CA-3: System Interconnections • CA-7: Continuous Monitoring • CA-9: Internal System Connections • CM-2: Baseline Configuration • CM-3: Configuration Change Control • CM-5: Access Restrictions for Change • CM-6: Configuration Settings • CM-8: Information System Component Inventory • MA-4: Nonlocal Maintenance • SC-24: Fail in Known State • SI-4: Information System Monitoring	• PR.AC-5 • PR.IP-1 • PR.PT-4	• CSM: Configuration Settings Management • Boundary Protection	• A.9.1.2 • A.13.1.1 • A.13.1.3	• A.10.6.1 - A.10.6.2 • A.11.4.5 • A.11.4.7 • A.11.5.1 - A.11.5.3	• DSI-02 • IAM-03 • IVS-06 • IVS-09 • MOS-19 • TVM-02	• Boundary firewalls and internet gateways • Secure Configuration • Patch Management	• Software Updates • Inappropriate locations for processing data
Frame work	**NSA MNP**	**NSA Top 10**	**GCHQ 10 Steps**	**NERC CIP v5**	**NERC CIP v4**	**NERC CIP v3**	**FFIEC Examiners Handbook**	**FFIEC Cybersecurity Assessment Tool (CAT)**
Domain	• Map Your Network • Patch Management • Baseline Management • Document Your Network • Security Gateways, Proxies, and Firewalls • Configuration and Change Management	• Set a Secure Baseline Configuration • Segregate Networks and Functions	• Secure Configuration • Network Security	• CIP-005-5 R1 • CIP-007-5 R2	• CIP-003-4 R6 • CIP-004-4 R4 • CIP-005-4 R2 • CIP-006-4 R3 • CIP-007-4 R3	• CIP-003-3 R6 • CIP-004-3 R4 • CIP-005-3 R2 • CIP-006-3 R3 • CIP-007-3 R3	• Network Security	• Domain 3: Cybersecurity Controls - Preventative Controls • Domain 3: Cybersecurity Controls - Detective Controls
Frame work	**FY15 FISMA Metrics**	**Australian Top 35**	**ITIL 2011 KPIs**	**AICPA's GAPP**	**PCI DSS 3.1**	**PCI DSS 3.0**	**NV Gaming MICS v7 2015**	**COBIT 5**
Domain	• 3: Identity Credential and Access Management	• 2 • 3 • 10	• Information Security Management	• 7.2.2 • 8.2.1	• 1.1 - 1.2 • 2.2 • 6.2	• 1.1 - 1.2 • 2.2 • 6.2	• Network Security and Data Protection	• APO13: Manage Security • DSS05: Manage Security Services • BAI10: Manage Configuration

Tabel 13. Critical Security Control #12 : Boundary Defense Mapping
(Sumber : www.auditscript.com)

Frame work	NIST 800-53 rev4	NIST Core Framework	ISO 27002:2005	ISO 27002:2013	DHS CDM Program	Cloud Security Alliance	UK Cyber Essentials	UK ICO Protecting Data
Domain	• Map Your Network • Network Architecture • Baseline Management • Document Your Network • Personal Electronic Device Management • Security Gateways, Proxies, and Firewalls • Remote Access Security • Network Security Monitoring • Log Management	• 10-11 • 18-20 • 23 • 32-34	• A.10.6.1 - A.10.6.2 • A.10.10.2 • A.11.4.2 • A.11.4.5 • A.11.4.7 • A.11.5.1 - A.11.5.3 • A.11.7.1 - A.11.7.2	• A.9.1.2 • A.12.4.1 • A.12.7.1 • A.13.1.1 • A.13.1.3 • A.13.2.3	• Boundary Protection	• DSI-02 • IVS-01 • IVS-06 • IVS-09 • MOS-16	• Boundary firewalls and internet gateways	• Configuration of SSL and TLS • Inappropriate locations for processing data
Frame work	**NSA MNP**	**NSA Top 10**	**GCHQ 10 Steps**	**NERC CIP v5**	**NERC CIP v4**	**NERC CIP v3**	**FFIEC Examiners Handbook**	**FFIEC Cybersecurity Assessment Tool (CAT)**
Domain	• Map Your Network • Network Architecture • Baseline Management • Document Your Network • Personal Electronic Device Management • Security Gateways, Proxies, and Firewalls • Remote Access Security • Network Security Monitoring • Log Management	• Segregate Networks and Functions	• Home and Mobile Working • Monitoring • Network Security	• CIP-005-5 R1 • CIP-005-5 R2 • CIP-007-5 R4	• CIP-005-4 R3 • CIP-007-4 R6	• CIP-005-3 R3 • CIP-007-3 R6	• Network Security • Security Monitoring	• Domain 2: Threat Intelligence & Collaboration - Monitoring and Analyzing • Domain 3: Cybersecurity Controls - Preventative Controls • Domain 3: Cybersecurity Controls - Detective Controls
Frame work	**FY15 FISMA Metrics**	**Australian Top 35**	**ITIL 2011 KPIs**	**AICPA's GAPP**	**PCI DSS 3.1**	**PCI DSS 3.0**	**NV Gaming MICS v7 2015**	**COBIT 5**
Domain	• 3: Identity Credential and Access Management • 6: Network Defense • 7: Boundary Protection	• 10-11 • 18-20 • 23 • 32-34	• Information Security Management	• 7.2.2 • 8.2.1 • 8.2.2	• 1.1 - 1.3 • 8.3 • 10.8 • 11.4	• 1.1 - 1.3 • 8.3 • 10.8 • 11.4	• Network Security and Data Protection • Remote Access	• APO13: Manage Security • DSS05: Manage Security Services

Tabel 14. Critical Security Control #13 : Data Protection Mapping
(Sumber : www.auditscript.com)

Frame work	NIST 800-53 rev4	NIST Core Framework	Australian Top 35	ISO 27002:2013	ISO 27002:2005	ITIL 2011 KPIs	COBIT 5	NSA MNP
Domain	• AC-3: Access Enforcement • AC-4: Information Flow Enforcement • AC-23: Data Mining Protection • CA-7: Continuous Monitoring • CA-9: Internal System Connections • IR-9: Information Spillage Response • MP-5: Media Transport • SA-18: Tamper Resistance and Detection • SC-8: Transmission Confidentiality and Integrity • SC-28: Protection of Information at Rest • SC-31: Covert Channel Analysis • SC-41: Port and I/O Device Access • SI-4: Information System Monitoring	• PR.AC-5 • PR.DS-2 • PR.DS-5 • PR.PT-2	• 26	• A.8.3.1 • A.10.1.1 - A.10.1.2 • A.13.2.3 • A.18.1.5	• A.10.7.1 • A.12.3.1 - A.12.3.2 • A.12.5.4 • A.15.1.6	• Information Security Management	• APO13: Manage Security • DSS05: Manage Security Services	• Network Architecture • Device Accessibility • Security Gateways, Proxies, and Firewalls • Network Security Monitoring

Frame work	HIPAA	Cloud Security Alliance	GCHQ 10 Steps	FY15 FISMA Metrics	AICPA's GAPP	NV Gaming MICS v7 2015	FFIEC Examiners Handbook	FFIEC Cybersecurity Assessment Tool (CAT)
Domain	• 164.308(a)(4): Information Access Management - Isolating Health care Clearinghouse Function R • 164.310(d)(1): Device and Media Controls - Accountability A • 164.312(a)(1): Access Control - Encryption and Decryption A • 164.312(e)(1): Transmission Security - Integrity Controls A • 164.312(e)(1): Transmission Security - Encryption A	• DSI-02 • DSI-05 • EKM-01 - EKM-04 • MOS-11	• Removable Media Controls	• 5: Data Protection	• 7.2.2 • 8.2.1 • 8.2.2 • 8.2.6	• Network Security and Data Protection	• Encryption • Data Security	• Domain 3: Cybersecurity Controls - Preventative Controls • Domain 3: Cybersecurity Controls - Detective Controls

Frame work	NERC CIP v5	PCI DSS 3.1	PCI DSS 3.0
Domain	• CIP-011-5 R1	• 3.6 • 4.1 - 4.3	• 3.6 • 4.1 - 4.3

Tabel 15. Critical Security Control #14 : Controlled Access Based on the Need to Know Mapping
(Sumber : www.auditscript.com)

Frame work	NIST 800-53 rev4	NIST Core Framework	ISO 27002:2013	ISO 27002:2005	UK Cyber Essentials	UK ICO Protecting Data	NSA Top 10	NSA MNP
Domain	• AC-1: Access Control Policy and Procedures • AC-2: Account Management • AC-3: Access Enforcement • AC-6: Least Privilege • AC-24: Access Control Decisions • CA-7: Continuous Monitoring • MP-3: Media Marking • RA-2: Security Categorization • SC-16: Transmission of Security Attributes • SI-4: Information System Monitoring	• PR.AC-4 • PR.AC-5 • PR.DS-1 • PR.DS-2 • PR.PT-2 • PR.PT-3	• A.8.3.1 • A.9.1.1 • A.10.1.1	• A.10.7.1 • A.10.10.1 - A.10.10.3 • A.11.4.5 • A.11.4.7 • A.11.6.1 - A.11.6.2 • A.12.5.4	• Access Control	• Inappropriate locations for processing data	• Segregate Networks and Functions	• Network Architecture • Device Accessibility • User Access • Data-at-Rest Protection • Log Management

Frame work	HIPAA	DHS CDM Program	Australian Top 35	PCI DSS 3.1	PCI DSS 3.0	COBIT 5	FFIEC Examiners Handbook	FFIEC Cybersecurity Assessment Tool (CAT)
Domain	• 164.308(a)(1): Security Management Process - Information System Activity Review R • 164.308(a)(4): Information Access Management - Isolating Health care Clearinghouse Function R • 164.308(a)(4): Information Access Management - Access Authorization A • 164.312(a)(1): Access Control - Encryption and Decryption A • 164.312(c)(1): Integrity - Mechanism to Authenticate Electronic Protected Health Information A • 164.312(a)(1): Access Control - Automatic Logoff A • 164.312(d): Person or Entity Authentication - R • 164.312(e)(1): Transmission Security - Integrity Controls A • 164.312(e)(1): Transmission Security - Encryption A	• TRUST: Access Control Management • PRIV: Privileges	• 26	• 1.3 - 1.4 • 4.3 • 7.1 - 7.3 • 8.7	• 1.3 - 1.4 • 4.3 • 7.1 - 7.3 • 8.7	• APO13: Manage Security • DSS05: Manage Security Services	• Authentication and Access Controls • Encryption • Data Security	• Domain 3: Cybersecurity Controls - Preventative Controls • Domain 3: Cybersecurity Controls - Detective Controls

Frame work	ITIL 2011 KPIs	Cloud Security Alliance	AICPA's GAPP	NERC CIP v5	NERC CIP v4	NERC CIP v3	NV Gaming MICS v7 2015	GCHQ 10 Steps
Domain	• Information Security Management	• DSI-02 • IVS-09 • MOS-11	• 7.2.2 • 8.2.1 • 8.2.2 • 8.2.6	• CIP-005-5 R1 • CIP-005-5 R2 • CIP-007-5 R4 • CIP-011-5 R1	• CIP-003-4 R5 • CIP-004-4 R4 • CIP-005-4 R2 • CIP-006-4 R3	• CIP-003-3 R5 • CIP-004-3 R4 • CIP-005-3 R2 • CIP-006-3 R3	• Network Security and Data Protection	• Managing User Privileges • Network Security

Tabel 16. Critical Security Control #15 : Wireless Access Control Mapping
(Sumber : www.auditscript.com)

Frame work	NIST 800-53 rev4	ISO 27002:2013	GCHQ 10 Steps	COBIT 5	Cloud Security Alliance	ITIL 2011 KPIs	FFIEC Examiners Handbook	FFIEC Cybersecurity Assessment Tool (CAT)
Domain	• AC-18: Wireless Access • AC-19: Access Control for Mobile Devices • CA-3: System Interconnections • CA-7: Continuous Monitoring • CM-2: Baseline Configuration • IA-3: Device Identification and Authentication • SC-8: Transmission Confidentiality and Integrity • SC-17: Public Key Infrastructure Certificates • SC-40: Wireless Link Protection • SI-4: Information System Monitoring	• A.10.1.1 • A.12.4.1 • A.12.7.1	• Monitoring • Network Security	• APO13: Manage Security • DSS05: Manage Security Services	• IVS-01 • IVS-06 • IVS-12 • MOS-11	• Information Security Management	• Network Security • Encryption • Security Monitoring	• Domain 3: Cybersecurity Controls - Preventative Controls • Domain 3: Cybersecurity Controls - Detective Controls

Frame work	NSA MNP	AICPA's GAPP	PCI DSS 3.1	PCI DSS 3.0	NERC CIP v5	NERC CIP v4	NERC CIP v3	NV Gaming MICS v7 2015
Domain	• Map Your Network • Baseline Management • Document Your Network • Personal Electronic Device Management • Network Access Control	• 7.2.2 • 8.2.1 • 8.2.2	• 4.3 • 11.1	• 4.3 • 11.1	• CIP-007-5 R4	• CIP-005-4 R3 • CIP-007-4 R6	• CIP-005-3 R3 • CIP-007-3 R6	• Network Security and Data Protection

Tabel 17. Critical Security Control #16 : Account Monitoring and Control Mapping
(Sumber : www.auditscript.com)

Frame work	NIST 800-53 rev4	NIST Core Framework	DHS CDM Program	ISO 27002:2013	ISO 27002:2005	NSA MNP	FFIEC Examiners Handbook	FFIEC Cybersecurity Assessment Tool (CAT)
Domain	• AC-2: Account Management • AC-3: Access Enforcement • AC-7: Unsuccessful Logon Attempts • AC-11: Session Lock • AC-12: Session Termination • CA-7: Continuous Monitoring • IA-5: Authenticator Management • IA-10: Adaptive Identification and Authentication • SC-17: Public Key Infrastructure Certificates • SC-23: Session Authenticity • SI-4: Information System Monitoring	• PR.AC-1 • PR.AC-4 • PR.PT-3	• CRED: Credentials and Authenticati on Management	• A.9.1.1 • A.9.2.1 - A.9.2.6 • A.9.3.1 • A.9.4.1 - A.9.4.3 • A.11.2.8	• A.8.3.3 • A.11.2.1 • A.11.2.3 - A.11.2.4 • A.11.3.1 - A.11.3.3 • A.11.5.1 - A.11.5.3	• User Access • Baseline Management • Log Management	• Authentication and Access Controls	• Domain 3: Cybersecurity Controls - Preventative Controls • Domain 3: Cybersecurity Controls - Detective Controls
Frame work	**HIPAA**	**COBIT 5**	**NERC CIP v5**	**NERC CIP v4**	**NERC CIP v3**	**Cloud Security Alliance**	**FY15 FISMA Metrics**	**NV Gaming MICS v7 2015**
Domain	• 164.308(a)(1): Security Management Process - Information System Activity Review R • 164.308(a)(4): Information Access Management - Access Authorization A • 164.308(a)(4): Information Access Management - Access Establishment and Modification A • 164.308(a)(5): Security Awareness and Training - Password Management A • 164.312(a)(1): Access Control - Unique User Identification R • 164.312(a)(1): Access Control - Automatic Logoff A • 164.312(d): Person or Entity Authentication - R • 164.312(e)(1): Transmission Security - Integrity Controls A • 164.312(e)(1): Transmission Security - Encryption A	• APO13: Manage Security • DSS05: Manage Security Services	• CIP-005-5 R1 • CIP-005-5 R2 • CIP-007-5 R4	• CIP-005-4 R3 • CIP-007-4 R5 • CIP-007-4 R6	• CIP-005-3 R3 • CIP-007-3 R5 • CIP-007-3 R6	• IAM-02 • IAM-09 - IAM-12 • MOS-14 • MOS-16 • MOS-20	• 3: Identity Credential and Access Management	• System Parameters • User Accounts • Generic User Accounts • Service & Default Accounts

Frame work	ITIL 2011 KPIs	AICPA's GAPP	Australian Top 35	GCHQ 10 Steps	UK Cyber Essentials	UK ICO Protecting Data	PCI DSS 3.1	PCI DSS 3.0
Domain	• Information Security Management	• 7.2.2 • 8.2.1	• 25	• Managing User Privileges	• Access Control	• Configuration of SSL and TLS	• 7.1 - 7.3 • 8.7 - 8.8	• 7.1 - 7.3 • 8.7 - 8.8

Tabel 18. Critical Security Control #17 : Security Skills Assessment and Appropriate Training to Fill Gaps Mapping (Sumber : www.auditscript.com)

Frame work	NIST 800-53 rev4	NIST Core Framework	DHS CDM Program	NERC CIP v5	NERC CIP v4	NERC CIP v3	FFIEC Examiners Handbook	FFIEC Cybersecurity Assessment Tool (CAT)
Domain	• AT-1: Security Awareness and Training Policy and Procedures • AT-2: Security Awareness Training • AT-3: Role-Based Security Training • AT-4: Security Training Records • SA-11: Developer Security Testing and Evaluation • SA-16: Developer-Provided Training • PM-13: Information Security Workforce • PM-14: Testing, Training, & Monitoring • PM-16: Threat Awareness Program	• PR.AT-1 • PR.AT-2 • PR.AT-3 • PR.AT-4 • PR.AT-5	• BEHV: Security-Related Behavior Management	• CIP-004-5 R1 • CIP-004-5 R2	• CIP-004-4 R1 • CIP-004-4 R2	• CIP-004-3 R1 • CIP-004-3 R2	• Personnel Security	• Domain 1: Cyber Risk Management & Oversight - Training and Culture • Domain 3: Cybersecurity Controls - Preventative Controls
Frame work	**HIPAA**	**COBIT 5**	**ISO 27002:2013**	**ISO 27002:2005**	**GCHQ 10 Steps**	**Cloud Security Alliance**	**ITIL 2011 KPIs**	**AICPA's GAPP**
Domain	• 164.308(a)(5): Security Awareness and Training - Security Reminders A • 164.308(a)(5): Security Awareness and Training - Protection from Malicious Software A • 164.308(a)(5): Security Awareness and Training - Log-in Monitoring A • 164.308(a)(5): Security Awareness and Training - Password Management A	• APO13: Manage Security • DSS05: Manage Security Services	• A.7.2.2	• A.8.2.2	• User Education & Awareness	• HRS-10 • MOS-05	• Information Security Management	• 1.2.9 • 1.2.10 • 7.2.2 • 8.2.1
Frame work	**FY15 FISMA Metrics**	**PCI DSS 3.1**	**PCI DSS 3.0**	**Australian Top 35**	**NSA MNP**			
Domain	• 8: Training and Education	• 12,6	• 12,6	• 28	• Training			

Tabel 19. Critical Security Control #18 : Application Software Security Mapping
(Sumber : www.auditscript.com)

Frame work	NIST 800-53 rev4	NIST Core Framework	COBIT 5	DHS CDM Program	ISO 27002:2013	ISO 27002:2005	FFIEC Examiners Handbook	FFIEC Cybersecurity Assessment Tool (CAT)
Domain	• SA-13: Trustworthiness • SA-15: Development Process, Standards, and Tools • SA-16: Developer-Provided Training • SA-17: Developer Security Architecture and Design • SA-20: Customized Development of Critical Components • SA-21: Developer Screening • SC-39: Process Isolation • SI-10: Information Input Validation • SI-11: Error Handling • SI-15: Information Output Filtering • SI-16: Memory Protection	• PR.DS-7	• APO13: Manage Security • DSS05: Manage Security Services	• VUL: Vulnerability Management	• A.9.4.5 • A.12.1.4 • A.14.2.1 • A.14.2.6 - A.14.2.8	• A.10.1.4 • A.12.2.1 • A.12.2.4 • A.12.5.2 • A.12.5.5	• Application Security • Software Development & Acquisition	• Domain 3: Cybersecurity Controls - Preventative Controls
Frame work	**NV Gaming MICS v7 2015**	**ITIL 2011 KPIs**	**AICPA's GAPP**	**Australian Top 35**	**PCI DSS 3.1**	**PCI DSS 3.0**	**UK ICO Protecting Data**	**Cloud Security Alliance**
Domain	• In-House Software Development • Purchased Software Programs	Information Security Management	• 7.2.2 • 8.2.1	• 24	• 6.3 • 6.5 - 6.7	• 6.3 • 6.5 - 6.7	• SQL Injection	• AIS-01 • AIS-03 • AIS-04 • CCC-01 - CCC-03 • IVS-08
Frame work	**NSA MNP**							
Domain	• Training	•	•	•	•	•	•	•

Tabel 20. Critical Security Control #19 : Incident Response and Management Mapping
(Sumber : www.auditscript.com)

Frame work	NIST 800-53 rev4	NIST Core Framework	DHS CDM Program	ISO 27002:2013	ISO 27002:2005	ITIL 2011 KPIs	COBIT 5	FFIEC Cybersecurity Assessment Tool (CAT)
Domain	• IR-1: Incident Response Policy and Procedures • IR-2: Incident Response Training • IR-3: Incident Response Testing • IR-4: Incident Handling • IR-5: Incident Monitoring • IR-6: Incident Reporting • IR-7: Incident Response Assistance • IR-8: Incident Response Plan • IR-10: Integrated Information Security Analysis Team	• PR.IP-10 • DE.AE-2 • DE.AE-4 • DE.AE-5 • DE.CM-1-7 • RS.RP-1 • RS.CO-1-5 • RS.AN-1-4 • RS.MI-1-2 • RS.IM-1-2 • RC.RP-1 • RC.IM-1-2 • RC.CO-1-3	• Plan for Events • Respond to Events	• A.6.1.3 • A.7.2.1 • A.16.1.2 • A.16.1.4 - A.16.1.7	• A.6.1.6 • A.8.2.1 • A.13.1.1 • A.13.2.1 - A.13.2.2	• Information Security Management • Incident Management	• APO13: Manage Security • DSS05: Manage Security Services • DSS02: Manage Service Requests and Incidents	• Domain 5: Cyber Incident Management and Resilience - Incident Resilience Planning and Strategy • Domain 5: Cyber Incident Management and Resilience - Detection, Response, and Mitigation • Domain 5: Cyber Incident Management and Resilience - Escalation and Reporting

Frame work	HIPAA	Cloud Security Alliance	GCHQ 10 Steps	PCI DSS 3.1	PCI DSS 3.0	NERC CIP v5	NERC CIP v4	NERC CIP v3
Domain	• 164.308(a)(6): Security Incident Procedures - Response and Reporting R	• SEF-01 - SEF-05	• Incident Management	• 12.10	• 12.10	• CIP-008-5 R1 • CIP-008-5 R2 • CIP-008-5 R3	• CIP-008-4 R1 • CIP-008-4 R2	• CIP-008-3 R1 • CIP-008-3 R2

Frame work	NSA MNP	FY15 FISMA Metrics	AICPA's GAPP
Domain	• Incident Response and Disaster Recovery Plans	• 9: Incident Response	• 7.2.2 • 8.2.1

Tabel 21. Critical Security Control #20 : Penetration Tests and Red Team Exercises Mapping
(Sumber : www.auditscript.com)

Frame work	NIST 800-53 rev4	ISO 27002:2013	ISO 27002:2005	NSA MNP	PCI DSS 3.1	PCI DSS 3.0	FFIEC Cybersecurity Assessment Tool (CAT)	COBIT 5
Domain	• CA-2: Security Assessments • CA-5: Plan of Action and Milestones • CA-6: Security Authorization • CA-8: Penetration Testing • RA-6: Technical Surveillance Countermeasures Survey • SI-6: Security Function Verification • PM-6: Information Security Measures of Performance • PM-14: Testing, Training, & Monitoring	• A.14.2.8 • A.18.2.1 • A.18.2.3	• A.6.1.8 • A.15.2.2 • A.15.3.1	• Audit Strategy	• 11,3	• 11,3	• Domain 3: Cybersecurity Controls - Detective Controls	• APO13: Manage Security • DSS05: Manage Security Services • MEA02: Monitor, Evaluate and Assess the System of Internal Control

Frame work	ITIL 2011 KPIs	AICPA's GAPP
Domain	• Information Security Management	• 7.2.2 • 8.2.1 • 8.2.7

4. Kesimpulan

1. Audit terhadap keamanan sistem informasi dilakukan untuk mengetahui tingkat keamanan sebuah sistem informasi sebagai tempat menghasilkan informasi.
2. Penggabungan dua kerangka kerja untuk audit terhadap keamanan sistem informasi bertujuan untuk memperluas dan memperdalam hasil audit dengan menyediakan cara yang efektif dalam memahami kebutuhan dan prioritas tata kelola TI dengan menyelesaikan satu sama lain karena dua kerangka kerja tadi bersifat saling melengkapi
3. Penggabungan tersebut didasari atas pemetaan terhadap domain-domain dari kedua kerangka kerja yang memiliki kesamaan *Critical Security Control* nya

5. Daftar Pustaka

Bless, Yulius C. N. Gusti Made Arya Sasmita, A. A. Kt. Agung Cahyawan.2014. Audit Keamanan SIMAK berdasarkan ISO 27002, Jurnal MERPATI VOL. 2, NO. 2, Agustus 2014

Halim, Marliana. Tanuwijaya, Haryanto. Mastan, Ignatius Adrian. 2012. Audit Keamanan Sistem Informasi berdasarkan standar ISO 27002. Jurnal JSIKA. 2012

Gondodiyoto,Sanyoto. Audit Sistem Informasi + Pendekatan CobIT. Mitra Wacana Media. 2007

Krisanthi, Gusti Ayu Theresia. Sukarsa, I Made. Bayupati, I Putu Agung. 2014. Governance Audit Of
Application Procurement Using COBIT Framework, Journal of Theoretical and Applied Information Technology 20th January 2014. Vol. 59 No.2. 2014

Hartono,Jogiyanto. Analisis dan Desain Sistem Informasi. Andi Yogyakarta. 1989.

Burch Jr, John G. Grudnitski, Gary . Information System : Theory and Practice. 1979

Yaner.Annisa Destiara, Tanuwijaya.Haryanto, Sutumo.Erwin. 2012. Audit Keamanan Sistem Informasi Pada Instalasi Sistem Informasi Management (SIM-RS) Berdasarkan Standar ISO 27002 Studi Kasus di Rumah Sakit Umum Haji Surabaya, Jurnal Sistem Informasi dan Komputerisasi Akuntansi STIKOM Surabaya. Vol 1. No.1. 2012.

www.auditscipt.com, 20 April 2016, 01.30.00