ANALISIS MATURITY LEVEL KEAMANAN INFORMASI BERDASARKAN DOMAIN APO13 DAN DSS05 FRAMEWORK COBIT 5 (STUDI KASUS BAGIAN PRANATA KOMPUTER DINAS KESEHATAN KAB. SUMEDANG)

SKRIPSI

Disusun Oleh:

Yudi Hendri Taufik

A3.1800050

PROGRAM STUDI SISTEM INFORMASI (S1)

FAKULTAS TEKNOLOGI INFORMASI

UNIVERSITAS SEBELAS APRIL (UNSAP)

2022

ANALISIS MATURITY LEVEL KEAMANAN INFORMASI BERDASARKAN DOMAIN APO13 DAN DSS05 FRAMEWORK COBIT 5 (STUDI KASUS BAGIAN PRANATA KOMPUTER DINAS KESEHATAN KAB. SUMEDANG)

SKRIPSI

Diajukan Untuk Memenuhi Salah Satu Syarat Kelulusan
Jenjang Strata 1 (S1) Program Studi Sistem Informasi
Fakultas Teknologi Informasi Universitas Sebelas April (Unsap)

Disusun Oleh:

Yudi Hendri Taufik

A3.1800050

PROGRAM STUDI SISTEM INFORMASI (S1)

FAKULTAS TEKNOLOGI INFORMASI

UNIVERSITAS SEBELAS APRIL (UNSAP)

2022

PERNYATAAN KEASLIAN SKRIPSI

Saya yang bertanda tangan dibawah ini:

Nama	:	Yudi Hendri Taufik
NIM	:	A3.1800050
Alamat	:	Jl. Gandasoli No. 06, Kiarapandak RT/RW 15/05, Desa Rancamanggung, Kec. Tanjungsiang, Kab. Subang, Jawa Barat

Dengan ini menyatakan bahwa skripsi dengan judul:
ANALISIS MATURITY LEVEL KEAMANAN INFORMASI BERDASARKAN DOMAIN APO13 DAN DSS05 FRAMEWORK COBIT 5 (STUDI KASUS BAGIAN PRANATA KOMPUTER DINAS KESEHATAN KAB. SUMEDANG) merupakan hasil karya sendiri yang belum pernah dipublikasikan baik secara keseluruhan maupun sebagian, dalam bentuk karya ilmiah. Skripsi ini sepenuhnya merupakan karya intelektual saya dan seluruh sumber yang menjadi rujukan dalam skripsi ini telah saya sebutkan sesuai kaidah akademik yang berlaku umum, termasuk para pihak yang telah memberikan kontribusi pemikiran pada isi, kecuali yang menyangkut ekspresi kalimat dan desain penulisan.
Demikian pernyataan ini saya nyatakan benar dan penuh tanggung jawab dan integritas.

Sumedang, Juli 2022

Yang menyatakan,

Yudi Hendri Taufik

ABSRTAK

Teknologi informasi telah dipandang sebagai alat yang dapat membantu rencana strategis karena keberhasilan institusi dalam mencapai visi, misi, dan tujuannya. Peranan teknologi informasi tersebut mengharuskan penerapan tata kelola yang baik dalam penggunaannya sehingga kemudian dapat dinilai dan dievaluasi. Dengan pengenalan pemanfaatan TIK, penyebaran informasi, dan inovasi dapat dilakukan dengan cara yang berdampak pada pembangunan sebuah negara. Selain manfaat, dalam penggunaannya TIK juga dapat memberikan risiko yang dapat membahayakan keamanan informasi dan bersifat merugikan. Laporan menyebutkan (*id-SIRTII/CC*) per Maret 2022, telah terjadi 39 juta kali serangan siber dengan menggunakan *malware*, sektor Pemerintah Daerah menjadi sektor terbanyak terjadi peretasan. Risiko lain selain yang berasal dari luar perusahaan antara lain risiko kegagalan teknis, bencana alam, dan ancaman dari dalam organisasi. Ancaman dari dalam organisasi, umumnya dilakukan oleh pengguna sistem pada instansi (*user*) baik disengaja maupun tidak disengaja. Keamanan informasi adalah menjaga informasi dari berbagai kemungkinan ancaman dalam upaya untuk menjamin keberlangsungan bisnis, meminimasi risiko bisnis, dan memaksimalkan atau mempercepat pengembalian investasi dan peluang bisnis. Berdasarkan alasan tersebut maka dilakukan penelitian analisis tingkat kematangan keamanan informasi, metode yang digunakan adalah domain APO13 dan DSS05 *framework* COBIT 5 dengan tujuan untuk mengetahui sejauh mana manajemen keamanan informasi dilakukan. Hasil dari penelitian ini meunjukkan bahwa keseluruhan *maturity level* Bagian Pranta Komputer Dinkes Kab. Sumedang untuk seluruh proses yang ada adalah 2.528 (*Established*) dengan *gap* antara kondisi saat ini (*as is*) dengan kondisi yang diharapkan (*to be*) adalah 2.318, kondisi tersebut menunjukkan bahwa proses yang berjalan telah mendukung pencapaian tujuan dan memiliki standar dalam ruang lingkup organisasi secara keseluruhan.

Kata kunci: Teknologi Informasi, COBIT 5, Maturity Level, Keamanan Informasi.

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

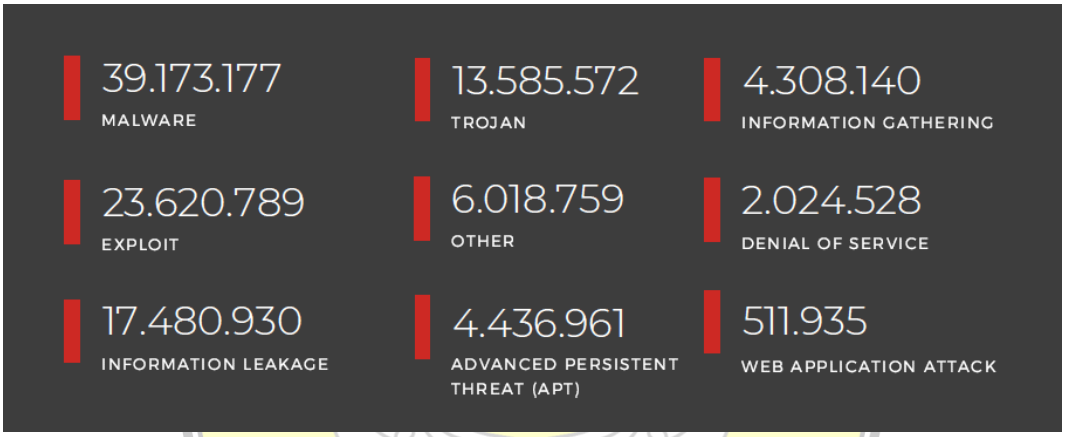
Hampir semua bidang pemerintahan dan perusahaan saat ini sangat bergantung pada teknologi informasi (Savira dan Sari, 2016), teknologi informasi tersebut perlu untuk lebih memperhatikan pola hidup masyarakat (Riadi, 2019). Dengan begitu teknologi informasi diharapkan dapat menunjang kehidupan manusia secara lebih efektif dan efisien.

Dewasa ini, teknologi informasi dipandang sebagai alat yang dapat membantu rencana strategis karena keberhasilan institusi dalam mencapai visi, misi, dan tujuannya (Riadi, 2019). Peranan teknologi informasi tersebut mengharuskan penerapan tata kelola yang baik dalam penggunaannya sehingga kemudian dapat dinilai dan dievaluasi. Selain itu, dalam penerapan teknologi informasi penting untuk menyesuaikan dengan kebutuhan agar dapat mencapai tujuan institusi yang sudah ditetapkan.

Dengan pengenalan pemanfaatan TIK, penyebaran informasi (terutama dari negara maju ke negara berkembang) dan inovasi dapat dilakukan dengan cara yang berdampak pada pembangunan sebuah negara (Vu, 2011). Banyak organisasi di Indonesia telah menggunakan teknologi informasi dan komunikasi sebagai penunjang efektifitas bisnis perusahaan. Hasil survei menunjukkan 92,95% perusahaan telah menggunakan dan memanfaatkan TIK dan 69,53% telah menggunakan fasilitas internet (BPS, 2018).

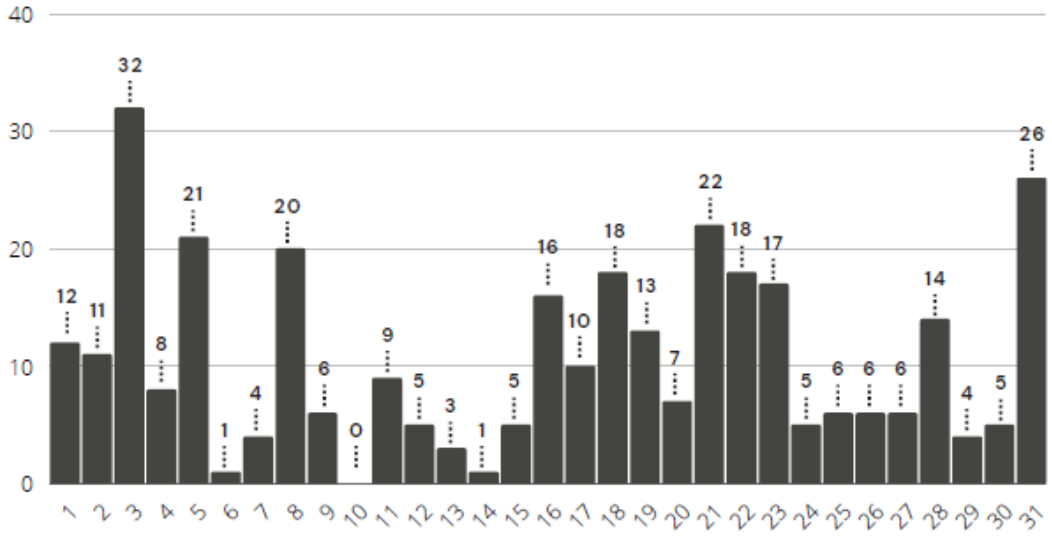
Selain manfaat, dalam penggunaannya TIK juga dapat memberikan risiko yang dapat membahayakan keamanan informasi dan bersifat merugikan. Kerusakan ini dapat berupa pelanggaran privasi dan pencurian informasi yang bersifat profit daripada hanya

mengubah konfigurasi sistem komputer atau informasi yang disimpan, seperti hal yang biasanya terjadi ketika terkena virus (Mauladani, 2017). Pencurian informasi dilakukan hacker menggunakan banyak metode, seperti dengan penyebaran *malware* (*worm*, *virus, trojan horse* atau *spyware*), aktivitas *social engineering* (pengiriman spam atau pembuatan situs palsu) serta lainnya (Mauladani, 2017). Sebagian besar dari metode *hacking* tersebut, pelaku memakai media internet serta membuatkan *file* untuk mengelabui korbannya.



GAMBAR 1. 1 KLASIFIKASI SERANGAN SIBER PER MARET 2022 DI INDONESIA (SUMBER: ID-SIRTII/CC)

Laporan menyebutkan di Indonesia sendiri per-Maret 2022 kemarin, telah terjadi setidaknya 39 juta kali serangan siber dengan menggunakan *malware*.



GAMBAR 1. 2 KASUS PERETASAN SITUS PER MARET 2022 DI INDONESIA (SUMBER: ID-SIRTII/CC)

Selain itu, terjadi pula peretasan terhadap situs dengan total 331 kasus peretasan yang didominasi oleh sektor pemerintahan daerah. Sektor pemerintah daerah menjadi sektor yang paling banyak terjadi peretasan pada bulan Maret 2022, yaitu 133 kasus peretasan, kemudian disusul oleh sektor akademik dengan 76 kasus, dan swasta dengan 54 kasus peretasan.

Risiko lain selain yang berasal dari luar perusahaan antara lain risiko kegagalan teknis, bencana alam, dan ancaman dari dalam organisasi (Mauladani, 2017). Ancaman dari dalam organisasi, umumnya dilakukan oleh pengguna sistem pada instansi (*user*) baik disengaja maupun tidak disengaja. Kelalaian atau ketidaktahuan *user* ini bertanggung jawab atas 63 persen dari pelanggaran keamanan informasi yang terjadi, hal ini dapat menciptakan peluang untuk ancaman yang tidak diinginkan untuk muncul (bahkan 20 persen mengatakan sengaja dengan alasan pekerjaan mereka menjadi lebih efektif dan efisien) (Mauladani, 2017).

Sebagian besar ancaman dari risiko-risiko yang disebutkan sebelumnya dapat berdampak merugikan apabila terjadi. Informasi adalah sumber daya berharga yang harus dijaga keamanannya, untuk mengamankan informasi, upaya dilakukan dengan memperhatikan aspek-aspek keamanan dari semua perangkat pendukung, fasilitas pemrosesan informasi, dan jaringan (Prasetyowati *et al.*, 2019). Keberlangsungan aktivitas organisasi akan terancam karena dampak yang ditimbulkan seperti kerugian finansial, terganggunya aktivitas bisnis, masalah peraturan/hukum dan penurunan reputasi organisasi (Hardy, 2014).

Akibatnya keamanan informasi dimaksudkan untuk mempertahankan sistem dari ancaman, maka dari itu pengawasan terhadap keamanan informasi sangat penting (Kurniawan, 2018), tak terkecuali Dinas Kesehatan Kabupaten Sumedang (Dinkes Kab. Sumedang). Dinkes Kab. Sumedang merupakan Satuan Kerja Perangkat Daerah (SKPD) yang memiliki fokus memberikan pelayanan kesehatan kepada masyarakat. Dinkes Kab. Sumedang tahun 2019 – 2023 memiliki visi yaitu "Terwujudnya masyarakat sumedang yang sejahtera, agamis, maju profesional dan kreatif (SIMPATI) pada tahun 2023". Seperti halnya organisasi lain, Dinkes Kab. Sumedang juga memanfaatkan berbagai fasilitas TIK dalam menjalankan aktivitas bisnisnya. Bahkan Dinkes Kab. Sumedang memiliki perhatian lebih terhadap TIK dengan membuat kebijakan pembangunan kesehatan mengacu pada sasaran yang tertuang dalam rancangan Rencana Pembangunan Jangka Menengah Daerah (RPJMD) periode 2019 – 2023, seperti: Penerapan sistem informasi kesehatan. Pada pelaksanaan tujuan strategis tersebut, Dinkes Kab. Sumedang menggunakan beragam fasilitas TIK berupa perangkat keras seperti laptop, komputer, perangkat jaringan dan sebagainya, selain itu terdapat pula sistem

informasi seperti website dinas, e-Puskesmas, e-Office Dinkes, Sistem Informasi Manajemen (SIM) Kepegawaian, SIM Keuangan, dan lainnya.

Dalam mengelola, mengkoordinasikan, mengendalikan, dan mengembangkan berbagai fasilitas TIK tersebut, terutama yang berafiliasi dengan teknologi serta sistem informasi, Dinkes Kab. Sumedang mempunyai bagian spesifik yaitu Sub Bagian Program, akan tetapi pada tahun 2022 ini, Pemerintah Kabupaten (Pemkab) Sumedang melakukan penyederhanaan birokrasi yang menyebabkan Sub Bagian Program dialih fungsikan, sekaligus terjadi perubahan Tugas Pokok Fungsi (Tupoksi) pengelolaan TI menjadi tanggung jawab bagian Pranata Komputer, dan Bagian Pranata Komputer ini bertanggung jawab langsung kepada Kepala Sub Bagian dan Sekretaris Dinas.

Bagian Pranata Komputer ada pada setiap SKPD yang ada di Kabupaten Sumedang, untuk Dinkes sendiri Bagian Pranata Komputer bertanggung jawab langsung kepada kepala Sub Bagian Umum, Aset, dan Kepegawaian. Salah satu peran Bagian Pranata Komputer adalah memastikan bahwa setiap teknologi serta sistem informasi yang dipergunakan di setiap divisi/bagian beroperasi sebagaimana mestinya dan bebas dari setiap resiko. Sebab apabila suatu insiden keamanan informasi terjadi, maka secara langsung maupun tidak langsung dapat menghambat aktivitas. Oleh karena itu kondisi yang stabil dan terjaganya aspek keamanan informasi seperti *confidentiality* (kerahasiaan), *integrity* (integritas) dan *availability* (ketersediaan) sudah sebagai harga mati bagi Sub Bagian Program demi memenuhi segala aktivitas bisnis yang ada.

Setelah dilakukan observasi, didapat beberapa permasalahan khususnya pada Bagian Pranata Komputer dan sistem informasi yang ada di Dinkes Kab.

Sumedang seperti website dinas, e-Puskesmas, dan e-Office Dinkes. Masalah yang ditemui tersebut adalah staf yang mengelola sistem informasi tersebut tidak hanya mengelola TI akan tetapi memiliki pekerjaan rangkap, selain itu ada pula staf yang mempunyai tanggung jawab terhadap sistem informasi akan tetapi staf tersebut bukan dari bagian yang seharusnya mempunyai tanggung jawab terhadap sistem informasi. Hal ini tentu saja akan mengakibatkan pengelolaan sistem yang ada menjadi tidak fokus.

Menanggapi masalah ancaman keamanan informasi yang sudah dijelaskan sebelumnya, pihak Dinkes Kab. Sumedang sudah seharusnya melakukan analisis terkait seberapa matang tingkat keamanan informasi yang ada, salah satunya dapat dilakukan dengan menggunakan *Control Objectives for Information and related Technology* (COBIT).

COBIT merupakan standar praktik manajemen teknologi informasi dan sekumpulan dokumentasi *best practices* untuk tata kelola TI yang dapat membantu auditor, manajemen, dan pengguna untuk menjembatani pemisah (*gap*) antara resiko bisnis, kebutuhan pengendalian, dan permasalahan-permasalahan teknis (ISACA, 2012). Publikasi terbaru dari standar ini adalah COBIT 2019 dan Versi sebelumnya adalah COBIT 5. COBIT 5 didasarkan pada lima prinsip kunci untuk tata kelola dan manajemen TI perusahaan. Kelima prinsip ini memungkinkan perusahaan untuk membangun sebuah kerangka tata kelola dan manajemen yang efektif dan efisien, yang dapat mengoptimalkan investasi dan penggunaan TI untuk mendapatkan keuntungan bagi para stakeholder (ISACA, 2012).

Adapun domain yang berhubungan dengan keamanan teknologi informasi adalah domain APO (*Align, Plan, and Organize*) pada subdomain APO13 *Manage*

Security dan domain DSS (*Deliver, Service, and Support*) pada sub-domain DSS05 *Manage Security Services*. Untuk itu perlu dilakukan observasi dan wawancara. COBIT memiliki kelebihan sebagai *framework* tata kelola karena dapat mengintegrasikan sistem keamanan informasi ke dalam tata kelola TI yang lebih luas. Pengelolaan teknologi informasi ini menjadi suatu kebutuhan yang sangat penting untuk organisasi yang menggunakan teknologi informasi sebagai landasan dasar proses kerja perusahaan tersebut (Helmiawan, 2017).

Didasari latar belakang yang dipaparkan, perlu untuk dilakukan "**Analisis Maturity Level Keamanan Informasi Berdasarkan Domain APO13 dan DSS05 *Framework* COBIT 5**".

1.2 Identifikasi Masalah

Berdasarkan penjelasan singkat pada latar belakang, maka permasalahan yang akan dibahas pada penelitian ini adalah sebagai berikut:

1. Belum adanya evaluasi keamanan informasi pada Bagian Pranata Komputer Dinkes Kab. Sumedang menggunakan *framework* COBIT 5.
2. Belum diketahui dengan jelas risiko keamanan yang dihadapi oleh Bagian Pranata Komputer Dinkes Kab. Sumedang.
3. Belum diketahui tingkat kematangan keamanan informasi dari Bagian Pranata Komputer Dinkes Kab. Sumedang.

1.3 Batasan Masalah

Berdasarkan identifikasi masalah yang telah diuraikan, agar permasalahan yang dibahas tidak melebar ke topik lain maka perlu diberikan batasan masalah, yaitu sebagai berikut:

1. Pelaksanan analisis keamanan informasi dilakukan pada Bagian Pranata Komputer pada Sub Bagian Umum, Aset, dan Kepegawaian Dinkes Kab. Sumedang.
2. Penelitian dilakukan untuk menganalisis tingkat kematangan keamanan informasi.
3. Metode yang digunakan adalah *framework* COBIT 5 dengan domain APO13 dan DSS05.

1.4 Perumusan Masalah

Berdasarkan penjelasan singkat pada latar belakang, maka rumusan masalah yang menjadi topik bahasan adalah sebagai berikut:

1. Bagaimana mengidentifikasi, menganalisis, dan mengevaluasi tingkat kematangan keamanan informasi Bagian Pranata Komputer Dinkes Kab. Sumedang melalui manajemen risiko keamanan informasi menggunakan domain APO13 dan DSS05 COBIT 5?
2. Bagaimana menghitung *Maturity Level* keamanan informasi pada Bagian Pranata Komputer Dinkes Kab. Sumedang?
3. Bagaimana rekomendasi berdasarkan perhitungan maturity level menggunakan domain APO13 dan DSS05 COBIT 5?

1.5 Tujuan dan Manfaat Penelitian

1.5.1 Tujuan Penelitian

Berikut adalah beberapa tujuan dilakukannya penelitian ini berdasarkan perumusan masalah yang ada:

1. Mengidentifikasi, menganalisis, dan mengevaluasi tingkat kematangan keamanan informasi Bagian Pranata Komputer Dinkes Kab. Sumedang menggunakak domain APO13 dan DSS05 COBIT 5.
2. Mengetahui *Maturity Level* keamanan informasi pada Bagian Pranata Komputer Dinkes Kab. Sumedang.

3. Mengetahui rekomendasi yang dihasilkan berdasarkan perhitungan maturity level menggunakan domain APO13 dan DSS05 COBIT 5.

1.5.2 Manfaat Penelitian

Manfaat yang ingin dicapai dalam penelitian ini adalah:

1. Bagi Peneliti

   Dengan penelitian ini, peneliti dapat menambah wawasan dan pengetahuan serta mengetahui proses analisis tingkat kematangan keamanan informasi khususnya dengan menggunakan *framework* COBIT 5.

2. Bagi Dinas Kesehatan Kabupaten Sumedang

   Membantu pihak Dinkes Kab. Sumedang khususnya Bagian Pranata Komputer dalam menjaga keamanan informasi, serta memberikan gambaran acuan dalam pengembangan sistem dan pengelolaan risiko keamanan informasi.

3. Bagi Pembaca

   Dengan adanya penelitian ini diharapkan dapat membantu dan menambah referensi pembaca mengenai analisis tingkat kematangan keamanan informasi khususnya menggunakan domain APO13 dan DSS05 *framework* COBIT 5 serta diharapkan bermanfaat bagi penelitian selanjutnya.

1.6 Sistematika Penulisan

Penyusunan laporan skripsi ini dilakukan dengan sistematika penulisan yang dibagi menjadi lima (5) bab, adapun uraian dari masing-masing bab tersebut adalah sebagai berikut:

BAB I PENDAHULUAN

Pada bab 1 terdapat beberapa sub-bab yaitu Latar Belakang, Identifikasi Masalah, Batasan Masalah,

Perumusan Masalah, Tujuan dan Manfaat Penelitian, Metodologi Penelitian, dan Sistematika Penelitian.

BAB II KAJIAN PUSTAKA

Pada bab ini menguraikan teori mengenai hal-hal yang berhubungan dan yang dipakai dalam penelitian.

BAB III ANALISIS SISTEM

Bab ini membahas tentang metodologi yang digunakan untuk membahas dan menganalisis penelitian yang dilakukan. Metode pengumpulan data yang digunakan adalah observasi, wawancara, dan analisis dokumen.

BAB IV HASIL DAN PEMBAHASAN

Bab ini membahas secara lengkap mengenai analisis keamanan Informasi berdasarkan *framework* COBIT 5 dan perhitungan *maturity level* Bagian Pranata Komputer Dinas Kesehatan Kabupaten Sumedang.

BAB V KESIMPULAN DAN SARAN

Pada bab ini berisi tentang kesimpulan-kesimpulan dari penelitian dengan kritik dan saran untuk penelitian selanjutnya.

DAFTAR PUSTAKA

Akbar, Y. H., Putri, N., & Helmiawan, M. A. (2018). Audit Sistem Informasi Akademik STMIK Sumedang Menggunakan Framework COBIT 5. *J-Sin's*, *1*(1).

Chazar, C. (2017) "Standar Manajemen Keamanan Informasi Berbasis ISO/IEC 27001: 2005," *Jurnal Informasi*, VII(2), hal. 48–57.

Helmiawan, M. A. (2017) "COBIT 5 UNTUK MANAJEMEN TEKNOLOGI INFORMASI & PROSES BISNIS PERUSAHAAN," *No. June*. doi: 10.24036/ib.v1i1.12.

Imany, Y. D. *et al.* (2019) "Evaluasi Tata Kelola Keamanan Informasi menggunakan COBIT 5 pada Domain APO13 dan DSS05 (Studi pada PT Gagas Energi Indonesia)," 3(6), hal. 5926–5935.

Komalasari, R. dan Perdana, I. (2014) "Audit Keamanan Informasi Bagian Teknologi Informasi PT PLN (Persero) DJBB Menggunakan SNI ISO / IEC," hal. 201–216.

Kurniawan, E. (2018) "SECURITY LEVEL ANALYSIS OF ACADEMIC INFORMATION SYSTEMS BASED ON STANDARD ISO 27002 : 2013 USING SSE-CMM," (February). doi: 10.13140/RG.2.2.20925.15840.

Mauladani, F. (2017) "Perancangan Sistem Manajemen Keamanan Informasi (Smki) Berdasarkan Sni Iso / Iec 27001 : 2013 Dan Sni Iso / Iec 27005 : 2013 (Studi Kasus Direktorat Pengembangan Teknologi Dan Sistem Informasi - Institut Teknologi Sepuluh Nopember)," 2013.

Prasetyowati, D. D. *et al.* (2019) "Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Berdasarkan ISO/IEC 27001:2013 pada Politeknik Ilmu Pelayaran Semarang," *JOINS (Journal of Information System)*, 4(1), hal. 65–75. doi: 10.33633/joins.v4i1.2429.

Riadi, I. (2017) "Forensic Analysis and Prevent of Cross Site Scripting in Single Victim Attack Using Open Web Application Security Project (OWASP) Framework FORENSIC ANALYSIS AND PREVENT OF CROSS SITE SCRIPTING IN SINGLE VICTIM ATTACK USING OPEN WEB APPLICATION SECURITY," (April).

Riadi, I. (2019) "Analisis Keamanan Sistem Informasi Berdasarkan Framework COBIT 5 Menggunakan Capability Maturity Model Integration (CMMI)," 9(October), hal. 47–54. doi: 10.21456/vol9iss1pp47-54.

Richard, L. (2019) "Glossary of Key Information Security Terms," (July).

S, F. *et al.* (2015) "Toward an Effective Information Security Risk Management of Universities' Information Systems Using Multi Agent Systems, Itil, Iso 27002, Iso 27005," 5 No. 6(June 2014), hal. 114–118. Tersedia pada:

https://www.researchgate.net/profile/Ljubomir-Jerinic/publication/270510381_Teaching_Introductory_Programming_Agent-based_Approach_with_Pedagogical_Patterns_for_Learning_by_Mistake/links/54ac4f3a0cf21c477139d3ab/Teaching-Introductory-Programming-Agent-bas.

Santoso, B. P., Hariyanti, E. dan Wuryanto, E. (2016) "Penyusunan Panduan Pengelolaan Keamanan Informasi Untuk Firewall Configuration Berdasarkan Kerangka Kerja PCI DSS v.3.1 dan COBIT 5," *Journal of Information Systems Engineering and Business Intelligence*, 2(2), hal. 67. doi: 10.20473/jisebi.2.2.67-73.

Savira, R. B. dan Sari, W. S. (2016) "Analisis IT Governance dengan Domain MEA01 Dalam Pelaksanaan E-Health Menggunakan Kerangka Kerja COBIT 5 pada Dinas Kesehatan Provinsi Jawa Tengah," *Techno*, 15(1), hal. 48–57.

Vu, K. M. (2011) "ICT as a source of economic growth in the information age: Empirical evidence from the 19962005 period," *Telecommunications Policy*. Elsevier, 35(4), hal. 357–372. doi: 10.1016/j.telpol.2011.02.008.

Wood, P. *et al.* (2015) "2015 Internet Security Threat Report, Volume 20," 20(April). Tersedia pada: http://www.symantec.com/content/en/us/enterprise/other_resources/21347933_GA_RPT-internet-security-threat-report-volume-20-2015.pdf.

Hardy, G. Mark (2014) *Risk, Loss and Security Spending in the Financial Sector: A SANS Survey*, SANS Institute, Bethesda. Tersedia pada: https://www.sans.org/reading-room/whitepapers/analyst/risk-loss-security-spending-financial-sector-survey-34690.

Badan Pusat Statistik. (2018) "PENGGUNAAN DAN PEMANFAATAN TEKNOLOGI INFORMASI DAN KOMUNIKASI (P2TIK) 2018 SEKTOR BISNIS," *Badan Pusat Statistik*, hal. 4–7.

ISACA (2012) "COBIT 5 Enabling Process," *ISACA*.
ISACA (2012) "COBIT 5 A Business Framework for the Gorvenance and Management of Enterprise," *ISACA*.
ISACA (2012) "COBIT 5 Implementation." *ISACA*.
ISACA (2013) "COBIT 5 Process Assessment Model," *ISACA*.
ISACA (2013) "COBIT 5 Self Assessment Guide Using COBIT," *ISACA*.