AUDIT KEAMANAN SISTEM INFORMASI AKADEMIK MENGGUNAKAN COBIT 5 PADA UNIVERSITAS SULTAN AGENG TIRTAYASA

SKRIPSI

Disusun sebagai salah satu syarat untuk memperoleh Gelar Sarjana Teknik (S.T)

Disusun oleh:

NURFITRIANI ROMADHONA

NPM. 3332180052

JURUSAN TEKNIK ELEKTRO

FAKULTAS TEKNIK

UNIVERSITAS SULTAN AGENG TIRTAYASA

2024

LEMBAR PERNYATAAN KEASLIAN SKRIPSI

Dengan ini saya sebagai penulis Skripsi berikut:

Judul	: Audit Keamanan Sistem Informasi Akademik Menggunakan COBIT 5 Pada Universitas Sultan Ageng Tirtayasa.
Nama Mahasiswa	: Nurfitriani Romadhona
NPM	: 3332180052
Fakultas/Jurusan	: Teknik/Teknik Elektro

Menyatakan dengan sesungguhnya bahwa Skripsi tersebut di atas adalah benar-benar hasil karya asli saya dan tidak memuat hasil karya orang lain, kecuali dinyatakan melalui rujukan yang benar dan dapat dipertanggungjawabkan. Apabila di kemudian hari ditemukan hal-hal yang menunjukkan bahwa sebagian atau seluruh karya ini bukan karya saya, maka saya bersedia dituntut melalui hukum yang berlaku. Saya juga bersedia menanggung segala akibat hukum yang timbul dari pernyataan yang secara sadar dan sengaja saya nyatakan melalui lembar ini.

Cilegon, 1 Desember 2023

Nurfitriani Romadhona

NPM. 3332180052

LEMBAR PENGESAHAN

Dengan ini ditetapkan bahwa Skripsi berikut:

Judul	: Audit Keamanan Sistem Informasi Akademik Menggunakan COBIT 5 Pada Universitas Sultan Ageng Tirtayasa.
Nama Mahasiswa	: Nurfitriani Romadhona
NPM	: 3332180052
Fakultas/Jurusan	: Teknik/Teknik Elektro

Telah diuji dan dipertahankan pada tanggal 1 Desember 2023 melalui Sidang Skripsi di Fakultas Teknik Universitas Sultan Ageng Tirtayasa Cilegon dan dinyatakan LULUS.

Dewan Penguji

	Tanda Tangan
Pembimbing I : Prof. Dr. Ir. Supriyanto, S.T., M.Sc., IPM	.....
Pembimbing II : Anis Fuad S.Sos., M.Si	.....
Penguji I : Masjudin, S.T., M.Eng.	.....
Penguji II : Fadil Muhammad, S.T., M.T.	.....

Mengetahui,
Ketua Jurusan

Dr. Rommi Wiryadinata, S.T., M.Eng
NIP. 198307032009121006

PRAKATA

Puji syukur saya panjatkan kepada Tuhan Yang Maha Esa, karena atas berkat dan rahmat-Nya, saya dapat menyelesaikan laporan Skripsi dengan judul "Audit Keamanan Sistem Informasi Akademik Menggunakan COBIT 5 Pada Universitas Sultan Ageng Tirtayasa". Penulisan laporan Skripsi ini merupakan salah satu syarat untuk dapat menyelesaikan program studi S1 dan untuk mencapai gelar Sarjana Teknik Jurusan Teknik Elektro, Universitas Sultan Ageng Tirtayasa. Saya menyadari bahwa tanpa bantuan dan bimbingan dari berbagai pihak sangatlah sulit bagi saya untuk menyelesaikan laporan Skripsi ini. Oleh karena itu, saya mengucapkan terima kasih kepada:

1. Orang tua dan keluarga saya yang selalu memberikan dukungan dan doa.
2. Bapak Dr. Romi Wiryadinata, S.T., M.Eng., sebagai Dosen Pembimbing Akademik dan Ketua Program Studi Teknik Elektro, Fakultas Teknik, Universitas Sultan Ageng Tirtayasa.
3. Bapak Prof. Dr. Ir. Supriyanto, S.T., M.Sc., IPM., sebagai Dosen Pembimbing I Skripsi yang telah memberikan arahan dan bimbingannya kepada penulis untuk menyelesaikan Skripsi.
4. Bapak Anis Fuad, S.Sos., M.Si., sebagai Dosen Pembimbing II Skripsi sekaligus kepala UPT. Pusat Data dan Informasi yang telah memberikan arahan dan bimbingannya kepada penulis untuk menyelesaikan Skripsi.

Penulis menyadari bahwa laporan Skripsi ini masih jauh dari kata sempurna. Oleh karena itu, kritik dan saran yang membangun sangat diharapkan untuk meningkatkan wawasan kepada penulis agar menjadi lebih baik. Akhir kata, penulis mohon maaf apabila terdapat kekeliruan di dalam penulisan laporan ini. Semoga laporan Skripsi ini bermanfaat bagi penulis khusus-Nya dan pembaca pada umumnya.

Cilegon, 1 Desember 2023

Penulis

ABSTRAK

Nurfitriani Romadhona
Teknik Elektro

Audit Keamanan Sistem Informasi Akademik Menggunakan COBIT 5 Pada Universitas Sultan Ageng Tirtayasa

Teknologi informasi banyak digunakan oleh organisasi seperti industri, pemerintahan, dan pendidikan. Ancaman keamanan teknologi informasi merupakan salah satu permasalahan paling serius akhir-akhir ini. Sistem informasi akademik merupakan suatu sistem pengelolaan data dan kegiatan akademik, karena penggunaan *website* ini penting dan juga memiliki kerentanan yang dapat merugikan, seperti: serangan SQL injection, XSS, *Man-in-the-Middle* dan lain-lain. Oleh karena itu, perlu mengetahui kerentanan melalui metode pengujian penetrasi menggunakan *framework* ISSAF dan dengan audit berdasarkan COBIT 5. Hasil pengujian kerentanan pada Vega dan Owasp Zap memperoleh beberapa kerentanan yaitu *Sesion Cookie without HTTPOnly Flag, Session Cookie without Secure Flag, Session Cookie without Samesite Attribute, Client Cipher-suite Preference, Directory Listing, Missing Anti Click-jacking, SQL Injection, Absence of Anti CSRF tokens, X-Powered-By and Server HTTP Response Header Field, Strict-Transport-Security, Timestamp Disclosure-UNIX and X-Content-Type-Options*. Hasil pengujian COBIT 5 untuk domain APO13 dan DSS05 saat ini berada di level 3 *established process,* sedangkan yang diharapkan berada di level 5 *optimising process*. Dengan masing-masing gap sebesar 2 dan 1,57. Hasil simulasi menggunakan *tools* Sqlmap dengan menambahkan injeksi SQL ke *website* tidak berhasil karena keamanannya telah ditingkatkan.

Kata Kunci: Keamanan, Manajemen, ISSAF, COBIT 5.

ABSTRACT

Nurfitriani Romadhona
Electrical Engineering

Academic Information System Security Audit Using COBIT 5 at Sultan Ageng Tirtayasa University

Information technology is widely used by organizations such as industry, government, and education. Information technology security threats are one of the most serious problems these days. Academic information system is a system for managing data and academic activities, because the use of this website is important and also has vulnerabilities that can be detrimental, such as: SQL injection attacks, XSS, Man-in-the-Middle and others. Therefore, it is necessary to find out vulnerabilities through penetration testing methods using the ISSAF framework and with audits based on COBIT 5. The results of vulnerability testing on Vega and OwasP Zap revealed several vulnerabilities, namely Sesion Cookie without HTTPOnly Flag, Session Cookie without Secure Flag, Session Cookie without Samesite Attribute, Client Cipher-suite Preference, Directory Listing, Missing Anti Click-jacking, SQL Injection, Absence of Anti CSRF tokens, X-Powered-By and Server HTTP Response Header Field, Strict-Transport-Security, Timestamp Disclosure-UNIX and X-Content-Type-Options. The COBIT 5 test results for domains APO13 and DSS05 are currently at level 3 established process, while the expected is at level 5 optimizing process. With gaps of 2 and 1,57 respectively. The simulation results using the Sqlmap tool by adding SQL injection to the website were unsuccessful because the security has been improved.

Keyword: Security, Management, ISSAF, COBIT 5.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Teknologi informasi merupakan bagian penting dari industri 4.0 yang dikenal dengan konsep otomatisasi melalui teknologi untuk mengurangi risiko kegagalan dan meningkatkan akurasi dan efensiensi kerja. Konsep ini diterapkan pada sektor industri, pendidikan, kesehatan dan pemerintahan [1]. Ancaman keamanan teknologi informasi merupakan salah satu permasalahan yang paling serius akhir – akhir ini. Keamanan TI adalah hal yang harus diawasi oleh semua organisasi untuk menghindari kerentanan [2]. Berdasarkan Badan Siber dan Sandi Negara (BSSN), 190 juta insiden ancaman dilakukan terhadap server web Indonesia dari Januari sampai Agustus 2020 [3].

Manajemen TI merupakan serangkaian prosedur yang memastikan implementasi TI yang tepat untuk mendukung pencapaian tujuan. Salah satu cara untuk mengetahui seberapa baik pengelolaan TI diterapkan adalah dengan mengauditnya [4]. Audit sistem informasi adalah proses terkoordinasi yang membantu, memantau, mengevaluasi cara kerja, dan memberikan perlindungan terhadap organisasi [5]. TI jelas membutuhkan suatu kerangka untuk pengolahannya. Penilaian kinerja TI dapat memanfaatkan kerangka *Control Objectives for Information and Related Technology* (COBIT) [6]. COBIT adalah pedooman manajemen TI yang mendukung administrasi, dan pengguna menggabungkan kesenjangan antara risiko dan masalah teknis [7].

Universitas Sultan Ageng Tirtayasa (UNTIRTA) merupakan perguruan tinggi negeri yang menggunakan teknologi informasi dalam proses operasionalnya. Salah satu penerapan teknologi informasi adalah Sistem Informasi Akademik (SIAKAD). *Bug* adalah kesalahan atau error yang menyebabkan suatu program tidak berfungsi dengan baik. Siakad memiliki beberapa masalah *bug* seperti SQL *injection* serta sistem jaringan yang sering gangguan ketika digunakan oleh banyak pengguna, misalnya saat pengisian

Kartu Rencana Studi (KRS), pengisian KRS perlu dilakukan berkali-kali. Untuk mengatasi permasalahan tersebut perlu adanya peningkatan keamanan dan manajemen teknologi informasi Siakad Untirta yang baik.

Potensi kerentanan termasuk *clickjacking, sql injection, XEE, Cross-site Scripting, brute force* dan lain-lain [8]. Pengujian keamanan *website* merupakan hal yang tepat dilakukan untuk memperbaiki kerentanan dan kelemahan keamanan pada *web* terkait. Salah satu metode pengujian keamanan *website* adalah penetrasi [9]. Untuk melakukan penetrasi terdapat beberapa *framework* yang digunakan, seperti *Information Systems Security Assessment Framework* (ISSAF). ISSAF adalah kerangka terstruktur mencakup beberapa tahap pengumpulan, evaluasi, dan validasi informasi tentang sistem keamanan yang telah diuji serta dianalisis secara jelas [10].

Penelitian pertama membahas mengenai evaluasi keamanan *website.* Metode yang digunakan yaitu pentest dengan memanfaatkan kerangka ISSAF. Hasil pengujian memperoleh 18 kerentanan yang ditemukan di *website* tersebut [11]. Penelitian kedua membahas evaluasi TI. Penelitian ini memanfaatkan kerangka COBIT 2019 proses BAI11. Hasilnya tingkat kemampuan yaitu level 1 (*perfomed*) sedangkan tingkat kematangan nya level 2 (*managed projects*) [12].

Penelitian ketiga membahas menganalisa keamanan *webserver*, Metode yang digunakan yaitu *penetration testing* dengan domain *information gathering, vulnerability assessment, gaining* dan *maintaining,* serta *clearing track.* Hasil pengujian memperoleh 10 kerentanan, ditemukan beberapa *port* yang terbuka dan dalam mensimulasikan ancaman, berhasil memperoleh nama pengguna dan kata sandi [13]. Penelitian keempat membahas mengaudit Siakad, penelitian ini memanfaatkan kerangka COBIT 5 proses APO12, APO13, serta DSS05. Hasil dari penelitian tingkat kapabilitas adalah APO12 yaitu level 1, APO13 level 2, dan DSS05 level 2, artinya telah melaksanakan dan mengimplementasikan proses TI hingga memperoleh tujuan [14].

Penelitian kelima membahas pengujian penetrasi aplikasi *web* menggunakan serangan injeksi SQL. Penelitian ini menggunakan metode *black-*

box dengan *framework Open Web Application Security Project* (OWASP). Hasil pengujian terhadap 10 situs dilakukan, 80% *web* yang di uji memiliki kelemahan terhadap serangan SQL injeksi [15].

Berdasarkan latar belakang, penelitian ini melakukan audit keamanan sistem informasi akademik di Untirta dengan melakukan pengujian layanan manajemen dan keamanan Siakad menggunakan COBIT 5 serta pengujian penetrasi menggunakan *framework* ISSAF. Hasil dari penelitian akan memperoleh rekomendasi dan diperlukan untuk menerapkan manajemen serta layanan keamanan yang lebih baik.

1.2 Rumusan Masalah

Berdasarkan latar belakang diketahui rumusan masalah dalam penelitian:

1. Bagaimana keamanan layanan siakad di Untirta berdasarkan hasil *penetration testing* menggunakan kerangka kerja ISSAF?
2. Berapa hasil kapabilitas level manajemen keamanan di Untirta dengan kerangka COBIT 5?
3. Bagaimana rekomendasi untuk Siakad agar memiliki kontrol keamanan yang baik dan benar?

1.3 Tujuan Penelitian

Berikut merupakan tujuan yang akan dicapai dalam penelitian ini:

1. Mengetahui keamanan siakad di Untirta dengan *penetration testing* menggunakan kerangka kerja ISSAF.
2. Mengetahui tingkat kapabilitas level layanan manajemen keamanan menggunakan kerangka kerja COBIT 5.
3. Memberikan rekomendasi berdasarkan hasil penelitian untuk meningkatkan keamanan dan tata kelola layanan manajemen Siakad di Untirta.

1.4 Manfaat Penelitian

Manfaat dari penelitian ini adalah:

1. Bagi peneliti, dapat dijadikan pengetahuan mengenai keamanan Siakad dengan *penetration testing* menggunakan kerangka ISSAF dan mengetahui nilai kapabilitas manajemen keamanan TI dengan COBIT 5.
2. Bagi akademisi, dapat dijadikan referensi untuk penelitian selanjutnya terkait audit keamanan dengan kerangka ISSAF dan COBIT 5.
3. Bagi Universitas, dapat dijadikan evaluasi dan acuan untuk Universitas mengenai keamanan dan manajemen TI berdasarkan *penetration testing* dengan kerangka ISSAF dan COBIT 5.

1.5 Batasan Masalah

Agar permasalahan tetap fokus dan mudah untuk dipahami, berikut merupakan beberapa batasan masalah:

1. Pengujian audit keamanan Siakad dilaksanakan di Untirta.
2. Penilaian keamanan Siakad menggunakan *penetration testing* dan kerangka ISSAF dengan 4 langkah yaitu *Information Gathering, Network Mapping, Vulnerability Assessment,* dan *penetration testing.*
3. Melakukan *penetration testing* menggunakan sistem operasi Kali Linux. *Tools* yang digunakan untuk *information gathering* yaitu Whois, Dnsrecon, Whatweb, dan Sslscan. *Network mapping* menggunakan Nmap. *Vulnerability assessment* menggunakan Vega dan Owasp Zap, *penetration testing* berupa simulasi serangan sql *injection* menggunakan Sqlmap.
4. Penilaian manajemen keamanan dengan kerangka COBIT 5 yang fokus pada 2 domain yaitu *Align, Plan, and Organise* subdomain pengelolaan keamanan dan *Deliver, Security and Support* subdomain pengelolaan layanan keamanan.
5. Hasil penelitian ini memberikan rekomendasi terhadap pengelolaan manajemen dan keamanan TI.

1.6 Sistematika Penulisan

Penulisan laporan skripsi, terdiri dari 5 bab. Bab I Pendahuluan memuat latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah, dan sistematika penulisan. Bab II Landasan Teori memuat teori-teori yang relevan serta tinjauan pustaka yang memuat referensi-referensi yang digunakan. Bab III Metodologi Penelitian meliputi alur penelitian, metode dan alat yang digunakan dalam penelitian. Bab IV Hasil dan Pembahasan memuat penjelasan dan analisis yang diperoleh dari penelitian yang dilakukan. Bab V Penutup memuat kesimpulan yang dapat diambil dari penelitian dan saran untuk penelitian ini.

DAFTAR PUSTAKA

[1] Novianto, F., dan M. U. Siregar, "Evaluation of E-Government Using COBIT 5 Framework (Case Study of Sistem Database Pemasyarakatan Implementation in Ministry of Law and Human Rights in The Special Region of Yogyakarta)," *IJID: International Journal of Information for Development*, vol. 8, no. 2, pp. 74-83, 2019.

[2] Yunus, M., "Analisis Kerentanan Aplikasi Berbasis Web Menggunakan Kombinsasi Security Tools Project Berdasarkan Owasp Versi 4," *Jurnal Ilmiah Informatika Komputer*, vol. 24, no. 1, 2019.

[3] Budi, E., D. Wira, dan A. Infantono, "Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0," *Prosiding Seminar Nasional Sains Teknologi dan Inovasi Indonesia* , vol. 3, pp. 223-234, 2021.

[4] Tangka, G. M. W., A. T. Liem, dan J. Y. Mambu, "Information Technology Governance Audit Using The COBIT 5 Framework at XYZ University," *Proceedings on 2nd International Conference on Cybernetics and Intelligent System (ICORIS)*, 2020.

[5] Nugroho, H., "A Review on Information System Audit Using COBIT Framework," *International Journal of Applied Information Technology*, vol. 3, no. 2, 2019.

[6] Riantini, F. I., dan D. I. Mulyana, "Implementasi Tata Kelola Teknologi Informasi Menggunakan Framework COBIT 5 Pada Direktorat Jendral Bea dan Cukai," *Journal Sekolah Tinggi Ilmu Komputer Cipta Karya Informatika*, vol. 12, no. 1, 2019.

[7] Handoyo, E., R. Umar, and I. Riadi, "Analysis Security of SIA Based DSS05 on COBIT 5 Using Capability Maturity Model Intetgration," *Scientific Journal of Informatics*, vol. 6, no. 2, 2019.

[8] Andriyani, S., M. F. Sidiq, dan B. P. Zen, "Analisis Celah Keamanan Pada Website Dengan Metode Penetration Testing Dan Framework Issaf Pada

Website SMK Al-Kautsar," *LEDGER: Journal Informatic and Information Technology,* vol. 2, no. 1, 2023.

[9] Wiradarma, A. A. B. A., dan G. M. A. Sasmita, "IT Risk Management Based on ISO 31000 and OWASP Framework Using OSINT at The Information Gathering Stage (Case Study: X Company)," *International Journal Computer Network and Information Security,* vol. 12, pp. 17-29, 2019.

[10] Rusdan, M., D. T. H. .Manurung dan F. K. Genta, "Evaluation of Wireless Network Security Using Information System Security Assessment Framework (ISSAF) (Case Study: PT. Keberlanjutan Strategis Indonesia)," *Test Engineering & Management,* vol. 83, pp. 15714 - 15719, 2020.

[11] Sanjaya, I. G. A. S., G. M. A. Sasmita, dan D. M. S. Arsa, "Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF," *Jurnal Ilmiah Merpati,* vol. 8, no. 2, 2020.

[12] Sipayung, A. B., R. Yunis, dan Elly, "Evaluation of Information Technology Governance at Mikroskil University Using COBIT 2019 Framework with BAI11 Domain," *International Journal of Research and Applied Technology,* vol. 2, no. 2, pp. 128-143, 2022.

[13] Fahri, F., A. Fadil, dan I. Riadi, "Analisis Keamanan Webserver Menggunakan Penetration Testing," *Jurnal Informatika,* vol. 8, no. 2, 2021.

[14] Megasyah, Y., dan A. A. Arifnur., "Academic Information System Security Audits Using COBIT 5 Framework Domains APO12, APO13 AND DSS05," *Journal of Applied Engineering and Technological Science (JAETS),* vol. 1, p. 2, 2020.

[15] Alanda, A., D. Satria, M. I. Ardhana, A. A. Dahlan, dan H. A. Mooduto "Web Application Penetration Testing Using SQL Injection Attack,"

JOIV: International Journal on Informatic Visualization, vol. 5, no. 3, pp. 320-326, 2021.

[16] Simmons, G. J., "Contemporary cryptology: The science of information integrity," New York: IEEE press, 1994.

[17] Supriyanto, "Keamanan Jaringan," Serang: Untirta Press, 2017.

[18] Simarmata, J., D. Sasongko, J. I. Sihotang, dan Yuswardi, "Sistem Keamanan Data," Yayasan Kita Menulis, 2022.

[19] Ujung, A. M., dan M. I. P. Nasution, "Pentingnya Sistem Keamanan Database untuk Melindungi Data Pribadi," *JISKA: Jurnal Sistem Informasi Dan Informatika*, vol. 1, no. 2, pp. 44-47, 2023.

[20] Fogie, S., J. Grossman, R. Hansen, A. Rager, dan P. D. Petkov, "XSS Attacks: Cross-site Scripting Exploits and Defense," Syngress, 2007.

[21] Anonim, "What is the Poodle attack?," Acunetix by invicti, 1 June 2020. [Online]. Available: https://www.acunetix.com/blog/web-security-zone/what-is-poodle-attack/. [Accessed 20 December 2022].

[22] Clarke, J., "SQL Injection Attacks and Defense Second Edition," United State of America: Elsevier, 2009.

[23] Prasetyo, S. E., dan N. Hasannah, "Analisis Keamanan Website Universitas Internasional Batam Menggunakan Metode ISSAF," *Jurnal Ilmiah Informatika (JIF)*, vol. 09, no. 02, 2021.

[24] Weber, R., "Information Systems Control And Audit," London: Upper Saddle River Prentice-Hall, 1999.

[25] Anonim, "Enterprise Value: Governance of IT Investments : Getting Started with Value Management," Rolling Meadows, IL 60008 USA: ISACA, 2008.

[26] Anonim, "COBIT 5 Enabling Process," Rolling Meadows, IL 60008 USA: ISACA, 2012.

[27] Anonim "COBIT 5 Process Assesment Model (PAM) : Using COBIT 5," Rolling Meadows, IL 60008 USA: ISACA, 2012.

[28] Yandri, R., Suharjito, D. N. Utama, dan A. Zahra, "Evaluation Model for the Implementation of Information Technology Service Management using Fuzzy ITIL," *Procedia Computer Science,* vol. 157, pp. 290-297, 2019.

[29] Anonim, "Self-Assessment Guide : Using COBIT 5," Rolling Meadows, IL 60008 USA: ISACA, 2013.

[30] Wibowo, E. Y. A., "Evaluasi Tata Kelola Keamanan Teknologi Informasi Menggunakan Framework COBIT 5 dan ISO 27002 (Studi Kasus: Pusat Jaringan Komunikasi Badan Meteorologi Klimatologi dan Geofisika)," Jakarta: Fakultas Sains dan Teknologi Universitas Islam Negeri Syarif Hidayatullah Jakarta , 2019.