MANAJEMEN RISIKO TEKNOLOGI INFORMASI MENGGUNAKAN ISO 31000 BERBASIS KERANGKA KERJA PENGUJIAN PENETRASI ISSAF

SKRIPSI

Program Studi Sistem Informasi

Jenjang Sarjana

Oleh :

Muhammad Egi Pedianza

09031382126132

JURUSAN SISTEM INFORMASI

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2024

LEMBAR PENGESAHAN

SKRIPSI

MANAJEMEN RISIKO TEKNOLOGI INFORMASI MENGGUNAKAN ISO 31000 BERBASIS KERANGKA KERJA PENGUJIAN PENETRASI ISSAF

Sebagai salah satu syarat untuk penyelesaian

studi di Program Studi Sistem Informasi S1

Oleh:

Muhammad Egi Perdianza 09031382126132

Mengetahui,
Ketua Jurusan Sistem Informasi,

Ahmad Rifai, S.T., M.T.
NIP. 19791020201021003

Palembang, 30 Desember 2024
Pembimbing,

Mgs. Afriyan Firdaus, M.IT
NIP. 198202122006041003

HALAMAN PERNYATAAN BEBAS PLAGIAT

Yang bertanda tangan di bawah ini:

Nama	:	Muhammad Egi Perdianza
NIM	:	09031382126132
Program Studi	:	Sistem Informasi Reguler
Judul Skripsi	:	Manajemen Risiko Teknologi Informasi Menggunakan ISO 31000 Berbasis Kerangka Kerja Pengujian Penetrasi ISSAF

Hasil Pengecekan iThenticate/Turnitin: 17%

Menyatakan bahwa laporan skripsi saya merupakan hasil karya saya sendiri dan bukan penjiplakan atau plagiat. Apabila ditemukan unsur penjiplakan atau plagiat dalam laporan skripsi ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya sesuai dengan ketentuan yang berlaku.

Demikian pernyataan ini saya buat dengan sebenarnya dan tidak ada paksaan oleh siapapun.

Palembang, 30 Desember 2024

Muhammad Egi Perdianza
NIM. 09031382126132

HALAMAN PERNYATAAN INTEGRITAS

Yang bertanda tangan di bawah ini:

Nama	:	Muhammad Egi Perdianza
NIM	:	09031382126132
Judul Publikasi	:	*Information Technology Risk Management Using ISO 31000 Based on the ISSAF Penetration Testing Framework*
DOI	:	https://orcid.org/0009-0004-6297-4668

Dengan ini menyatakan publikasi saya dengan judul:

Information Technology Risk Management Using ISO 31000 Based on the ISSAF Penetration Testing Framework yang diusulkan pada INOVTEK Polbeng - Seri Informatika : The Journal of Innovation and Technology Polbeng Series on Informatics, Volume 9, No. 2 (2024) bersifat original dan saya dapat bertanggungjawab pada setiap proses submisi publikasi tersebut.

Bilamana di kemudian hari ditemukan ketidaksesuaian dengan pernyataan ini, maka saya bersedia dituntut dan diproses sesuai dengan ketentuan yang berlaku. Demikian surat pernyataan ini dibuat dengan sesungguhnya dan sebenarnya.

Mengetahui,
Dosen Pembimbing

Mgs. Afriyan Firdaus, M.IT
NIP. 198202122006041003

Palembang, 30 Desember 2024
Menyatakan,

Muhammad Egi Perdianza
NIM. 09031382126132

HALAMAN PERSETUJUAN

Telah diterima jurnal di Sistemasi: Jurnal Sistem Informasi pada:

Hari : **Minggu**

Tanggal : **17 November 2024**

Nama : **Muhammad Egi Perdianza**

NIM : **09031382126132**

Judul : ***Information Technology Risk Management Using ISO 31000 Based on the ISSAF Penetration Testing Framework***

Tim Pembimbing :

1. **Pembimbing : Mgs. Afriyan Firdaus, M.IT**

Mengetahui,
Ketua Jurusan Sistem Informasi

Ahmad Rifai, S.T., M.T.
NIP. 19791020201021003

HALAMAN PERSEMBAHAN DAN MOTTO

"Every line of code holds the potential for a flaw, every flaw brings a challenge, and within the challenge lies the essence of security.."

" - "

Skripsi ini dipersembahkan untuk

- Allah SWT
- Diriku Sendiri
- Kedua Orang Tua, Saudara dan Keluarga Besar
- Dosen Jurusan Sistem Informasi
- Fakultas Ilmu Komputer, Universitas Sriwijaya
- Sahabat dan Rekan Seperjuangan Penulis Selama Menempuh Pendidikan

KATA PENGANTAR

Segala puji dan syukur penulis panjatkan kepada Allah Swt. karena berkat rahmat, hidayah dan karunia-Nya penulis dapat menyelesaikan Tugas Akhir yang berjudul **"MANAJEMEN RISIKO TEKNOLOGI INFORMASI MENGGUNAKAN ISO 31000 BERBASIS KERANGKA KERJA PENGUJIAN PENETRASI ISSAF"**. Tugas Akhir ini merupakan salah satu syarat mata kuliah Skripsi dan penulis membuat tugas akhir sebagai syarat untuk menyelesaikan jenjang Pendidikan strata satu pada Program Studi Sistem Informasi Fakultas Ilmu Komputer Universitas Sriwijaya. Dalam menyelesaikan Tugas Akhir ini, penulis banyak memperoleh bimbingan, bantuan, dukungan dan doa dari berbagai pihak sehingga dapat menyelesaikan laporan ini. Oleh karena itu dalam kesempatan ini penulis ingin mengucapkan terima kasih kepada :

1. Allah SWT. Yang telah memberikan anugrah berupa kesehatan, kesempatan dan juga ilmu yang bermanfaat sehingga penulis dapat melaksanakan dan menyelesaikan tugas akhir ini.
2. Kedua orang tua yang senantiasa mendoakan, memberi dukungan baik secara mental maupun finansial sebagai motivasi saya untuk menyelesaikan tugas akhir ini tepat waktu.
3. Bapak Prof. Dr. Erwin, S.Si., M.Si. selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Ahmad Rifai.S.T., M.T. selaku Ketua Jurusan Sistem Informasi Fa Fakultas Ilmu Komputer Universitas Sriwijaya
5. Bapak Mgs. Afriyan Firdaus, M.IT. selaku Dosen Pembimbing Tugas Akhir yang senantiasa memberikan arahan, dukungan, dan ilmu yang bermanfaat

selama proses penelitian dan juga selaku dosen pembimbing akademik yang selalu membimbing saya dari awal perkuliahan hingga akhir perkuliahan.

6. Segenap Dosen Fakultas Ilmu Komputer Universitas Sriwijaya yang telah membekali ilmu kepada penulis sehingga penulis bisa menjalani dan menyelesasikan tugas akhir dengan baik.
7. Teman-teman dan sahabat yang telah membantu dan memberikan dukungan sehingga penulis dapat menyelesaikan tugas akhir ini.

Penulis berharap semoga laporan tugas akhir ini dapat bermanfaat untuk kita semua khususnya mahasiswa Fakultas Ilmu Komputer Universitas Sriwijaya. Penulis juga menyadari bahwa laporan ini masih memiliki kesalahan dan jauh dari kata sempurna. Oleh karena itu, penulis sangat membutuhkan dan mengharapkan saran dan kritik dari pembaca serta saran yang berisfat membangun agar dapat menjadi lebih baik kedepannya

Palembang, 30 Desember 2024
Penulis

Muhammad Egi Perdianza
NIM. 09031382126132

MANAJEMEN RISIKO TEKNOLOGI INFORMASI MENGGUNAKAN ISO 31000 BERBASIS KERANGKA KERJA PENGUJIAN PENETRASI ISSAF

Oleh

Muhammad Egi Perdianza

09031382126132

ABSTRAK

Keamanan informasi sangat penting bagi lembaga pendidikan tinggi yang mengelola sejumlah besar data sensitive pada era digital. Insiden kebocoran data di sektor akademik Indonesia mencapai 2.217 pada tahun 2021. Laman situs web universitas yang memiliki 36 layanan sistem informasi berbasis web ditemukan telah mengalami defacement(Hariyadi & Nastiti, 2021). Serangan SQL Injection dan XSS yang dapat mengakibatkan kebocoran data, manipulasi sistem, hingga gangguan layanan akademik juga kerap terjadi. Serangan ini menegaskan pentingnya langkah keamanan ketat untuk melindungi data dan menjaga reputasi pendidikan. Penelitian ini menilai risiko keamanan situs web Universitas XYZ menggunakan ISSAF dan ISO 31000. ISSAF diterapkan dalam empat tahap: pengumpulan informasi, pemetaan jaringan, identifikasi kerentanan, dan pengujian penetrasi dengan penyesuaian untuk sistem web universitas. ISO 31000 digunakan untuk mengevaluasi keparahan risiko, menghasilkan klasifikasi dua risiko tinggi, enam sedang, dan dua belas rendah.. Temuan ini memberi wawasan luas bagi institusi pendidikan dalam memperkuat keamanan siber mereka. Implementasi

langkah-langkah tepat tidak hanya meningkatkan perlindungan data tetapi juga membangun kepercayaan dan reputasi. Keamanan informasi proaktif menjadi aset penting bagi keberlanjutan dan kredibilitas lembaga pendidikan tinggi di era digital yang rentan ini.

Kata Kunci: keamanan informasi, *Infomation System Security Assessment Framework*, pengujian penetrasi, manajemen risiko, ISO 31000

INFORMATION TECHNOLOGY RISK MANAGEMENT USING ISO 31000 BASED ON THE ISSAF PENETRATION TESTING FRAMEWORK

By

Muhammad Egi Perdianza

09031382126132

ABSTRACT

Information security is critical for higher education institutions, which manage large amounts of sensitive data in the digital age. Data breach incidents in Indonesia's academic sector reached 2,217 in 2021. A university website with 36 web-based information system services was found to have been defaced. SQL injection and XSS attacks, which can lead to data breaches, system manipulation, and disruption of academic services, are also common. These attacks underscore the importance of strong security measures to protect data and preserve the reputation of education. This research assesses the security risk of the XYZ University website using the ISSAF and ISO 31000. ISSAF was applied in four stages: information gathering, network mapping, vulnerability identification, and penetration testing with customization for university web systems. ISO 31000 was used to assess risk severity, resulting in classifications of two high, six medium, and twelve low risks. Security recommendations were developed to address the key risks and can be applied to other universities facing similar threats. The findings provide great insight for educational institutions to strengthen their cybersecurity.

Implementing appropriate measures not only improves privacy, but also builds trust and reputation. Proactive information security is becoming a critical asset for the sustainability and credibility of higher education institutions in this vulnerable digital age.

Keywords : information security, Information System Security Assessment Framework, penetration testing, risk management, ISO 31000

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

BAB I

PENDAHULUAN

1.1. Latar Belakang

Banyak institusi pendidikan tinggi Indonesia telah menggunakan website sebagai alat untuk meningkatkan kualitas informasi yang tersedia di kampus di era digital saat ini. Sebagai universitas negeri, Universitas XYZ menggunakan teknologi berbasis web untuk mendukung administrasi berbagai kegiatan akademik dan ekstrakurikuler di kampus selain menyebarkan informasi. Universitas rentan terhadap ancaman siber akibat menangani berbagai informasi pribadi sensitif dan pribadi yang bersifat rahasia milik pribadi,karyawan dan mahasiswa, termasuk data keuangan dan akademik.

Menggabungkan Kerangka Kerja Penilaian Keamanan Sistem Informasi (ISSAF) dengan ISO 31000 memberikan pendekatan komprehensif untuk keamanan situs web, yang mencakup penemuan kerentanan teknis, analisis dampak, dan manajemen risiko dengan rencana yang dipikirkan dengan matang. Sebagai kerangka kerja pengujian penetrasi, ISSAF menawarkan instruksi metodis kepada penguji tentang cara mengidentifikasi dan memanfaatkan kelemahan keamanan(Mahtuf et al., 2019). Menurut Nugraha dan Istanbul, ISO 31000 merupakan standar internasional yang fokus pada pengelolaan risiko dan membantu perusahaan menentukan, menilai, dan mengurangi risiko berdasarkan ancaman yang telah diakui (Nugraha & Istambul, 2019).

Karena institusi-institusi tersebut menangani informasi yang sensitif dan menjalankan sistem dasar vital, perguruan tinggi kerap menjadi sasaran utama serangan siber(Hina & Dominic, 2020) . Risiko pelanggaran data, perubahan

sistem, dan interupsi layanan pendidikan dipengaruhi oleh ancaman reguler termasuk serangan SQL Injection dan Cross-Site Scripting (XSS)(Priyanka & Smruthi, 2020; Vikas et al., 2023). Salah satu target utama penjahat dunia maya adalah sektor pendidikan, yang meliputi universitas. Ada indikasi meningkatnya serangan yang menargetkan sektor pendidikan di Indonesia, termasuk 2.217 insiden perusakan situs web pada tahun 2021(Siburian, 2021). Ini menunjukkan betapa pentingnya menerapkan tindakan pencegahan yang efisien serta memastikan kerahasiaan dan keutuhan data.

Diharapkan website Universitas XYZ agar lebih terlindungi terhadap gangguan eksternal serta mendukung kelancaran kelangsungan operasional kampus (Hasan et al., 2017). Sementara penerapan metode keamanan seringkali tidak optimal, memungkinkan peretas untuk mengeksploitasi kelemahan sistem (Sahu & Tomar, 2017; Tedyyana, Ahmad, et al., 2024), evaluasi kerentanan berkala diperlukan dengan melakukan pengujian penetrasi yang sistematis serta pengelolaan risiko secara menyeluruh untuk menentukan tipe-tipe kerentanan yang ada pada website Universitas XYZ. Selain itu, keefektifan penggunaan ISSAF dan ISO 31000 untuk pengelolaan risiko dievaluasi, dan saran-saran strategis dikembangkan dalam memperkuat perlindungan situs online dan menghindari pengungkapan informasi atau serangan cyber di masa depan.

1.2. Rumusan Masalah

Berdasarkan latar belakang yang telah dipaparkan, penelitian ini merumuskan masalah mengenai cara penerapan Kerangka Kerja Penilaian Keamanan Sistem Informasi (ISSAF serta ISO 31000 untuk mengidentifikasi celah keamanan serta

mengatur risiko yang terkait dengan website Universitas XYZ demi mengurangi dampak serangan siber dan melindungi kerahasiaan data.

1.3. Tujuan Penelitian

Adapun tujuan dari Penelitian ini bertujuan untuk mengidentifikasi kerentanan keamanan yang ada pada situs web Universitas XYZ, menganalisis risiko dengan memanfaatkan ISSAF dan ISO 31000, serta menyusun rekomendasi strategis guna memperkuat keamanan dan mengurangi risiko terhadap ancaman siber.

1.4. Manfaat Penelitian

Penelitian ini diharapkan dapat menjadi acuan untuk meningkatkan keamanan sistem informasi pada situs web Universitas XYZ, menyediakan panduan praktis dalam penerapan ISSAF dan ISO 31000, serta menjadi evaluasi dan referensi bagi pengelola sistem informasi di perguruan tinggi lain dalam menangani ancaman keamanan siber.

1.5. Batasan Masalah

Penelitian ini dibatasi pada ruang lingkup sebagai berikut:

1. Evaluasi kerentanan dilakukan terhadap situs web Universitas XYZ menggunakan pendekatan simulasi berdasarkan data publik yang tersedia.
2. Pengujian penetrasi dengan kerangka kerja ISSAF dibatasi pada tahap Information gathering, network mapping, vulnerability identification, and penetration tanpa melakukan eksploitasi lebih lanjut terhadap sistem target.
3. Evaluasi risiko menggunakan ISO 31000 didasarkan pada analisis hasil simulasi dan pemetaan kerentanan, dengan pendekatan teoretis terhadap konteks risiko.

4. Rekomendasi difokuskan pada strategi mitigasi risiko tingkat tinggi dan sedang, tanpa mencakup implementasi langsung atau pengujian terhadap langkah mitigasi yang diusulkan.
5. Penelitian tidak mencakup analisis terhadap infrastruktur non-web, seperti aplikasi mobile, perangkat keras, atau jaringan internal universitas.

DAFTAR PUSTAKA

Bacudio, A. G., Yuan, X., Bill Chu, B. T., & Jones, M. (2011). An Overview of Penetration Testing. *International Journal of Network Security & Its Applications*, *3*(6), 19–38. https://doi.org/10.5121/ijnsa.2011.3602

Hariyadi, D., & Nastiti, F. E. (2021). Analisis Keamanan Sistem Informasi Menggunakan Sudomy dan OWASP ZAP di Universitas Duta Bangsa Surakarta. *Jurnal Komtika (Komputasi Dan Informatika)*, *5*(1), 35–42. https://doi.org/10.31603/komtika.v5i1.5134

Hasan, M. Z., Hussain, M. Z., Taimoor, M., & Chughtai, A. (2017). Penetration Testing In System Administration. *INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH*, *6*(06). www.ijstr.org

Hina, S., & Dominic, P. D. D. (2020). Information security policies' compliance: a perspective for higher education institutions. In *Journal of Computer Information Systems* (Vol. 60, Issue 3, pp. 201–211). Taylor and Francis Inc. https://doi.org/10.1080/08874417.2018.1432996

Hutagalung, R. H., Nugroho, L. E., & Hidayat, R. (2017). Analisis Uji Penetrasi Menggunakan ISSAF. *Hacking Digit. Forensics Expo*, 32–40.

Mahtuf, F. R., Hatta, P., & Wihidiyat, E. S. (2019). Pengembangan Laboratorium Virtual untuk Simulasi Uji Penetrasi Sistem Keamanan Jaringan. *Journal of Information Technology and Computer Science (JOINTECS)*, *4*(1).

Mirjalili, M., Nowroozi, A., & Alidoosti, M. (2014). *A survey on web penetration test*. https://www.researchgate.net/publication/270523617

Novia Rilyani, A., Firdaus W ST, Y. A., & Dwi Jatmiko, D. S. (n.d.). *Analisis Risiko Teknologi Informasi Berbasis Risk Management Menggunakan ISO 31000 (Studi Kasus : i-Gracias Telkom University) Information Technology Risk Analysis Based On Risk Management Using Iso 31000 (Case Study : i-Gracias Telkom University)*.

Nugraha, U., & Istambul, R. (2019). Implementation of ISO 31000 for Information Technology Risk Management in the Government Environment. In *International Journal of Innovation, Creativity and Change. www.ijicc.net* (Vol. 6, Issue 5). www.ijicc.net

Priyanka, A. K., & Smruthi, S. S. (2020). WebApplication Vulnerabilities:Exploitation and Prevention. *2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA)*, 729–734. https://doi.org/10.1109/ICIRCA48905.2020.9182928

Rathore, B., Brunner, M., Dilaj, M., Herrera, O., Brunati, P., Subramaniam, R., Raman, S., & Chavan, U. (2005). *Information Systems Security Assessment Framework (ISSAF) draft 0.2*.

Riadi, I., Sunardi, S., & Handoyo, E. (2019). Security Analysis of Grr Rapid Response Network using COBIT 5 Framework. *Lontar Komputer : Jurnal Ilmiah Teknologi Informasi*, 29. https://doi.org/10.24843/lkjiti.2019.v10.i01.p04

Sahu, D. R., & Tomar, D. S. (2017). Analysis of Web Application Code Vulnerabilities using Secure Coding Standards. *Arabian Journal for Science and Engineering*, *42*(2), 885–895. https://doi.org/10.1007/s13369-016-2362-5

Sanjaya, I. G. A. S., Sasmita, G. M. A., & Sri Arsa, D. M. (2020). Information technology risk management using ISO 31000 based on issaf framework penetration testing (Case study: Election commission of x city). *International Journal of Computer*

Network and Information Security, *12*(4), 30–40. https://doi.org/10.5815/ijcnis.2020.04.03

Siburian, H. (2021). *Laporan Tahunan Monitoring Keamanan Siber 2021*.

Sukapto, P., Desena, J. D. H., Ariningsih, P. K., & Susanto, S. (2018). Integration of risk engineering by ISO 31000 and safety engineering: A case study in a production floor of sport footwear industry in Indonesia. *International Journal of Simulation: Systems, Science and Technology*, *19*(4), 22.1-22.12. https://doi.org/10.5013/IJSSST.a.19.04.22

Tedyyana, A., Ahmad, A. A., Idrus, M. R., Shabli, M., Hanis, A., Abu Seman, M. A., Ghazali, O., & Abd Razak, A. H. (2024). Enhance Telecommunication Security Through the Integration of Support Vector Machines. *International Journal of Advanced Computer Science & Applications*, *15*(3).

Tedyyana, A., Ghazali, O., Asnafi, T., Purbo, O. W., Harun, N. Z., & Riza, F. (2024). Transforming the voting process integrating blockchain into e-voting for enhanced transparency and securiy. *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, *22*(2), 311–320.

Vikas, V., Saisri, G., Meghana, T. S., Harshini, A. S., & Kaveri, G. (2023). Web Security Audit and Penetration Testing: Identifying Vulnerabilities and Strengthening Website Security. *International Journal for Research in Applied Science and Engineering Technology*, *11*(7), 794–805. https://doi.org/10.22214/ijraset.2023.54658

Vito Tarigan, B., Kusyanti, A., & Yahya, W. (2017). *Analisis Perbandingan Penetration Testing Tool Untuk Aplikasi Web* (Vol. 1, Issue 3). http://j-ptiik.ub.ac.id

Wiradarm, A. A. B. A., & Sasmit, G. M. A. (2019). IT Risk Management Based on ISO 31000 and OWASP Framework using OSINT at the Information Gathering Stage (Case Study: X Company). *International Journal of Computer Network and Information Security*, *11*(12), 17–29. https://doi.org/10.5815/ijcnis.2019.12.03

Zukhrufatul Firdaus, N. (2018). *Evaluasi Manajemen Risiko Teknologi Informasi Menggunakan COBIT 5 IT Risk (Studi Kasus : PT. Petrokimia Gresik)* (Vol. 2, Issue 1). http://j-ptiik.ub.ac.id