Jurnal Riset Multidisiplin dan Inovasi Teknologi
E-ISSN 3024-8582 P-ISSN 3024-9546
Volume 2 Issue 01, January 2024, Pp. 327-373
DOI: https://doi.org/10.59653/jimat.v2i01.500

Analisis Resiko Keamanan Informasi Website Repository Digital Library Menggunakan Framework ISO/IEC 27001 & 27002: Studi Kasus Perguruan tinggi X

Aulia Faradilla Setyowardhani[1], Ida Nurlela[2], Jenyta Primaranti[3], Valerian Ghrandiaz[4], Yulhendri[5*]
Universitas Esa Unggul, Indonesia | minefaraulia@gmail.com[1]
Universitas Esa Unggul, Indonesia| nuida037@gmail.com[2]
Universitas Esa Unggul, Indonesia | pjenyta@gmail.com[3]
Universitas Esa Unggul, Indonesia| ghrandiaz@gmail.com[4]
Universitas Esa Unggul, Indonesia| yulhendri@esaunggul.ac.id[5]
Correspondence Author*

Abstract

The continuous evolution of digital repositories in the era of globalization, especially in context of higher education digital libraries, poses security risks that raise concerns among users. Existence of sensitive user data that requires protection by universities adds to this concern. This research aims to conduct comprehensive analysis of information security risks associated with digital library repository websites. This research seeks to identify potential vulnerabilities, threats that could compromise the confidentiality, integrity and availability of digital assets stored in repositories. Through detailed risk analysis, this research provides actionable insights and recommendations to improve the information security posture of digital libraries using the ISO/IEC 27001 and 27002 IT governance framework specifically tailored to information security standards. This research uses a literature review and interviews with responsible parties at the University of X's digital library repository. Findings show that the use of tools such as Acunetix helps identify vulnerabilities in web repositories. Risk mitigation in digital library web repositories involves the application of ISO/IEC 27001, 27002 standards, which results in specific risk mitigation actions. For example, universities should create policies to monitor information technology assets, ensuring regular monitoring to protect technology assets. In addition, for Database Management System (DBMS) management (e.g., MySQL, PostgreSQL, Oracle, Ms SQL Server), colleges must facilitate easy access and storage of information. By implementing the recommendations obtained from this research, higher education institutions can ensure safe environment for users accessing digital library web repositories, thereby reducing concerns about the security of their information.

Keywords: *Information Security, ISO/IEC 27001, ISO/IEC 27002, Repository Digital Library, Risk Analysis*

Abstrak

Evolusi repositori digital yang terus menerus di era globalisasi, khususnya dalam konteks perpustakaan digital perguruan tinggi, menimbulkan risiko keamanan yang menimbulkan kekhawatiran di kalangan pengguna. Adanya data pengguna yang sensitif dan membutuhkan perlindungan oleh perguruan tinggi menambah kekhawatiran ini. Penelitian ini bertujuan untuk melakukan analisis komprehensif tentang risiko keamanan informasi yang terkait dengan situs web repositori perpustakaan digital. Penelitian ini berupaya mengidentifikasi potensi kerentanan dan ancaman yang dapat membahayakan kerahasiaan, integritas, dan ketersediaan aset digital yang disimpan dalam repositori. Melalui analisis risiko yang terperinci, penelitian ini memberikan wawasan dan rekomendasi yang dapat ditindaklanjuti untuk meningkatkan postur keamanan informasi perpustakaan digital dengan menggunakan kerangka kerja tata kelola TI ISO/IEC 27001 dan 27002 yang secara khusus disesuaikan dengan standar keamanan informasi. Penelitian ini menggunakan tinjauan literatur dan wawancara dengan pihak-pihak yang bertanggung jawab di repositori perpustakaan digital Universitas X. Temuan menunjukkan bahwa penggunaan alat seperti Acunetix membantu mengidentifikasi kerentanan dalam repositori web. Mitigasi risiko di repository web perpustakaan digital melibatkan penerapan standar ISO/IEC 27001 dan 27002, yang menghasilkan tindakan mitigasi risiko yang spesifik. Sebagai contoh, perguruan tinggi harus membuat kebijakan untuk memantau aset teknologi informasi, memastikan pemantauan rutin untuk melindungi aset teknologi. Selain itu, untuk manajemen Sistem Manajemen Basis Data (DBMS) (misalnya, MySQL, PostgreSQL, Oracle, Ms SQL Server), perguruan tinggi harus memfasilitasi akses dan penyimpanan informasi yang mudah. Dengan menerapkan rekomendasi yang diperoleh dari penelitian ini, perguruan tinggi dapat memastikan lingkungan yang aman bagi pengguna yang mengakses repository web perpustakaan digital, sehingga mengurangi kekhawatiran tentang keamanan informasi mereka.

Kata kunci: Keamanan Informasi, ISO/IEC 27001, ISO/IEC 27002, Repository Digital Library, Analisis Risiko

Pendahuluan

Dalam bidang repository digital yang terus berkembang, khususnya dalam tingkat perguruan tinggi, pentingnya keamanan informasi yang kuat tidak dapat diabaikan. Seiring dengan pergeseran menuju digitalisasi yang lebih luas pada perpustakaan dan sumber daya akademis, kerentanan repository digital terhadap risiko keamanan menjadi perhatian kritis.

Tujuan utama dari penelitian ini adalah untuk melakukan analisis komprehensif terhadap risiko keamanan informasi yang terkait dengan situs web repository perpustakaan digital dalam konteks lembaga pendidikan tinggi, khususnya perguruan tinggi X. Dengan menggunakan kerangka kerja ISO/IEC 27001 & 27002 yang telah ditetapkan, penelitian ini juga bertujuan untuk mengidentifikasi potensi kerentanan dan ancaman yang dapat membahayakan kerahasiaan, integritas, dan ketersediaan aset digital yang tersimpan di dalam repository. dengan melakukan penelitian risiko yang terperinci, penelitian ini memberikan

wawasan dan rekomendasi yang dapat ditindaklanjuti untuk meningkatkan postur keamanan informasi perpustakaan digital. (Hermawan, 2019)

Penerapan standar ISO/IEC 27001 dan ISO/IEC 27002 dapat dilakukan ketika membangun sistem manajemen keamanan informasi (Disterer, 2013). ISO/IEC 27001 merupakan standar yang diterapkan untuk mendukung manajemen dalam merancang dan mengimplementasikan keamanan informasi yang sesuai dengan peraturan. ISO/IEC 27002, di sisi lain, berfungsi sebagai standar untuk menentukan operasi dan pemanfaatan sistem pendukung (ISO/IEC 27001 dan ISO/IEC 27002, 2013). ISO/IEC 27001 berfokus pada penetapan kebijakan berdasarkan penilaian risiko dan kebutuhan pengguna, sedangkan ISO/IEC 27002 berkonsentrasi pada penerapan prosedur yang didefinisikan dengan jelas (ISO/IEC 27001 dan ISO/IEC 27002, 2013). Penelitian yang dilakukan oleh Georg Diesterer berjudul "ISO/IEC 27000, 27001, dan 27002 untuk Manajemen Keamanan Informasi" menyoroti pentingnya menilai kapabilitas masalah keamanan, yang menandakan inisiatif penting dalam manajemen teknologi informasi (TI). Protokol keamanan standar dapat digunakan untuk menyebarluaskan dan memelihara sistem manajemen keamanan informasi yang kuat. Standar ISO/IEC 27000, 27001, dan 27002 telah diadopsi dan disesuaikan berdasarkan protokol-protokol ini. Perusahaan yang menerapkan standar ISO/IEC 27001 menerima sertifikasi ISMS/SMKI pihak ketiga, yang menunjukkan keamanan yang telah dievaluasi dan bukti-bukti yang tersedia (Disterer, 2023).

A. Keamanan Informasi

Keamanan informasi adalah upaya untuk mencegah ancaman seperti pencurian data, akses tidak sah, dan kerusakan sistem informasi. Ancaman keamanan informasi dapat berasal dari berbagai sumber, seperti hacker, virus komputer, kegagalan sistem, kejahatan siber, dan masalah keamanan lainnya. (Putra et al., 2016).

Bisnis atau organisasi dapat melindungi data pelanggan dengan menetapkan kebijakan dan pedoman yang jelas, memberikan pelatihan dan penilaian risiko yang teratur, menggunakan teknologi keamanan, dan menerapkan praktik keamanan yang ketat seperti otentikasi pengguna, enkripsi data, dan pemantauan aktivitas. Untuk membantu organisasi dan individu menghindari serangan siber dan kehilangan data sensitif, penting bagi mereka untuk menyadari pentingnya keamanan informasi. (Firdani & Reza Perdanakusuma, 2019)

B. Risiko Keamanan Informasi

Dalam konteks keamanan informasi, risiko keamanan informasi mengacu pada berbagai kemungkinan yang dapat muncul sebagai akibat dari pelanggaran keamanan informasi atau tindakan yang tidak diizinkan oleh pengelolaan. Pengungkapan, penggunaan, penghancuran, penolakan layanan, dan perubahan data tanpa otorisasi pengelola adalah beberapa jenis ancaman keamanan informasi. Hacker, virus komputer, kegagalan sistem, kejahatan siber, dan masalah keamanan lainnya adalah beberapa sumber potensi ancaman keamanan informasi. Karena kebocoran data dapat terjadi karena kesalahan manusia, kegagalan sistem, atau serangan siber, keamanan informasi harus diperhatikan oleh organisasi

dan individu. Selain itu, risiko keamanan informasi juga dapat berdampak pada kerahasiaan, integritas, ketersediaan, keberadaan, kepatuhan, dan keandalan sistem informasi (Ala, 2023).

Untuk mengurangi risiko keamanan informasi, penting untuk meningkatkan kesadaran terhadap keamanan informasi. Salah satu caranya adalah dengan menerapkan framework tata kelola sistem informasi dengan standar ISO/IEC 27001 & 27002 (Wicaksono & Papilaya, 2018).

C. ISO/IEC 27001

ISO/IEC 27001:2013 adalah standar keamanan informasi yang diterbitkan pada Oktober 2013 oleh ISO (Organisasi Internasional untuk Standardisasi) dan IEC (Komisi Elektroteknik Internasional). ISO/IEC 27001:2013 menjelaskan persyaratan untuk membuat, menerapkan, menjalankan, memonitor, menganalisis, serta memelihara dan mendokumentasikan standar Sistem Manajemen Keamanan Informasi (ISMS). ISO/IEC 27001:2013 menetapkan 14 Klause Utama, dan 114 kontrol yang dapat diterapkan untuk membangun ISMS (Candiwan & Priyadi, n.d.)

Dalam konteks Perguruan Tinggi X, penerapan ISO/IEC 27001 sangat penting, mengingat kompleksitas keamanan informasi di lingkungan akademik. ISO/IEC 27001 menyediakan pendekatan sistematis untuk mengelola informasi sensitif, memastikan kerahasiaan, integritas, dan ketersediaannya(Disterer, 2013b). Standar ini menetapkan kriteria untuk menetapkan, menerapkan, memelihara, dan terus meningkatkan sistem manajemen keamanan informasi (SMKI) dalam keseluruhan risiko bisnis organisasi. Memahami penerapan standar ini di perguruan tinggi dapat menjadi alat yang penting dalam menganalisis dan mengatasi tantangan keamanan informasi spesifik yang dihadapi oleh Perguruan Tinggi X.(*BAB II LANDASAN TEORI 2.1 Keamanan Informasi*, n.d.)

D. ISO/IEC 27002

International Standard Organization (ISO) 27002: 2013 merupakan standar internasional untuk dapat membandingkan antara lain kebijakan, proses, prosedur,organisasi struktur, software dan hardware. Standar Internasional mengelompokkan prasyarat keamanan informasi menjadi tiga prasyarat utama, yaitu: Information technology, Security techniques and Code of practice for information security controls yang terdiri dari 14 major division , 37 subdivision dan 114 controls (Soesanto et al., 2023).

Metode Penelitian

A. Identifikasi Masalah

Tahap awal penelitian melibatkan serangkaian kegiatan yang menjadi landasan penting bagi penelitian.Tahap pertama meliputi penentuan rumusan masalah, batasan masalah, serta tujuan dan manfaat penelitian yang dilakukan.

B. Metode Pengumpulan Data

Ada beberapa metode pengumpulan data yang dapat digunakan dalam penelitian keamanan risiko ISO 27001 dan 27002 pada digital library. Pemilihan metode

tergantung pada sifat penelitian, pertanyaan penelitian, dan tujuan penelitian. Berikut adalah observasi, studi pustaka, wawancara (Mahersmi et al., 2016).

1) **Observasi**

   Kami mengamati situs arsip perpustakaan elektronik yang dapat diakses kapan saja dan dimana saja, serta melakukan observasi untuk memperoleh data yang dikumpulkan melalui observasi langsung.Jenis observasi yang dilakukan adalah observasi non partisipan.Artinya peneliti tidak terlibat aktif dan hanya sekedar pengamat independen.

2) **Studi Pustaka**

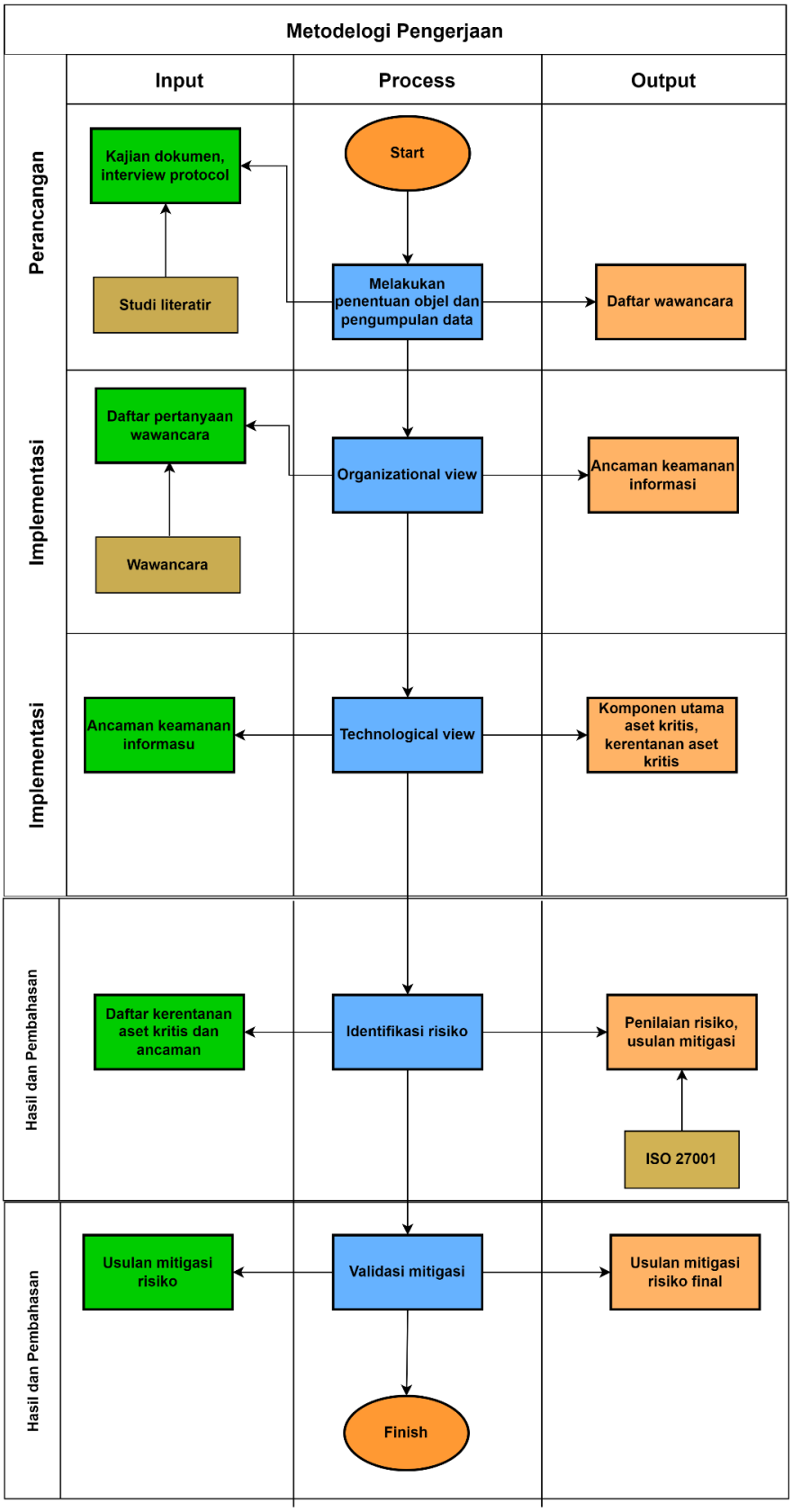
   Studi pustaka digunakan sebagai suatu metode untuk menemukan teori pendukung yang mendasari masalah yang akan diteliti dalam melakukan analisis risiko keamanan informasi, studi pustaka dilakukan dengan mempelajari teori-teori terkait dengan Analisis risiko, Keamanan Informasi, pengetahuan tentang repository digital library dan framework yang akan digunakan nantinya. Melalui studi pustaka, peneliti juga dapat memperoleh informasi dan menambah wawasan terkait dengan penelitian yang dilakukan. Penelitian ini didukung dengan berbagai sumber website, jurnal dan internet.

3) **Wawancara**

   Wawancara dilakukan 1 kali. Pada tanggal 01 Desember 2023 Wawancara dilakukan dengan Kepala Perpustakaan Perguruan Tinggi X, Kepala Perpustakaan Perguruan Tinggi X, Dan Staff IT perguruan tinggi X. Yang dilakukan secara Online, Wawancara ini diketahui informasi tentang aset yang ada pada repository Perguruan Tinggi X, Kendala yang pernah dihadapi oleh pustakawan, maintenance dan pengendalian risiko yang ada

C. Metodologi Penelitian

Permasalahan penelitian ini akan diselesaikan dengan metode penelitian yang ditunjukkan pada diagram alir di bawah ini.



Gambar 1.1 Sumber: Peneliti

1. Pada tahap pemanfaatan, terlebih dahulu kita menentukan sasaran dan mengumpulkan data yaitu menganalisis objek penelitian.
2. Fase Tampilan Organisasi adalah fase pembuatan profil ancaman dengan mengidentifikasi aset yang penting bagi organisasi dan kebutuhan keamanannya.
3. Fase Technology View mengidentifikasi proses bisnis dan profil ancaman aset penting yang didukung oleh layanan teknologi informasi Digital Library College X.
4. Pada tahap identifikasi risiko dilakukan identifikasi risiko.Hal ini berarti melakukan penilaian risiko sesuai ISO 27001 dan menerapkan langkah-langkah mitigasi risiko, serta konsultasi bersama dengan perpustakaan digital perguruan tinggi.
5. Pada tahap ini dilakukan pengecekan apakah validasi yang telah selesai sesuai dengan kondisi eksisting Perpustakaan Universitas Digital.

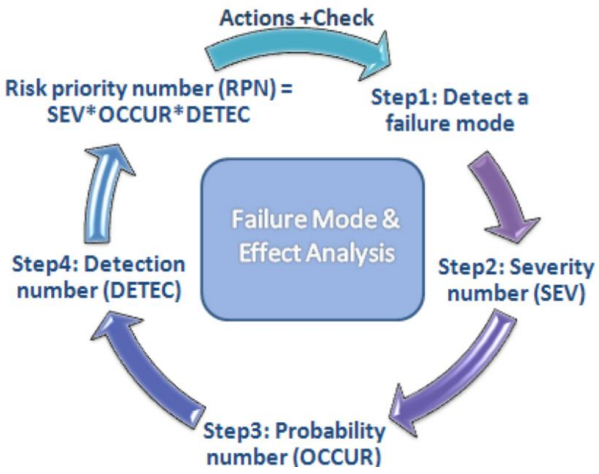
D. FMEA

Mode kegagalan dan analisis efek (FMEA) adalah metode menganalisis potensi kesalahan atau kegagalan dalam suatu sistem atau proses. Potensi kesalahan yang teridentifikasi diklasifikasikan menurut ukuran dan dampaknya terhadap proses. Tujuan FMEA adalah meminimalkan dan menghindari kesalahan dan kegagalan. FMEA mengidentifikasi tiga hal:

1. Penyebab kegagalan dari sistem, desain produk, serta proses selama siklus hidupnya
2. Efek dari kegagalan
3. Tingkat kekritisan efek dari suatu kegagalan.

Proses yang dilakukan dalam implementasi FMEA adalah mengukur kemungkinan terjadinya kesalahan atau kegagalan berdasarkan tiga komponen.

Di bawah ini adalah diagram alur langkah-langkah proses FMEA.



Gambar 1.2 FMEA

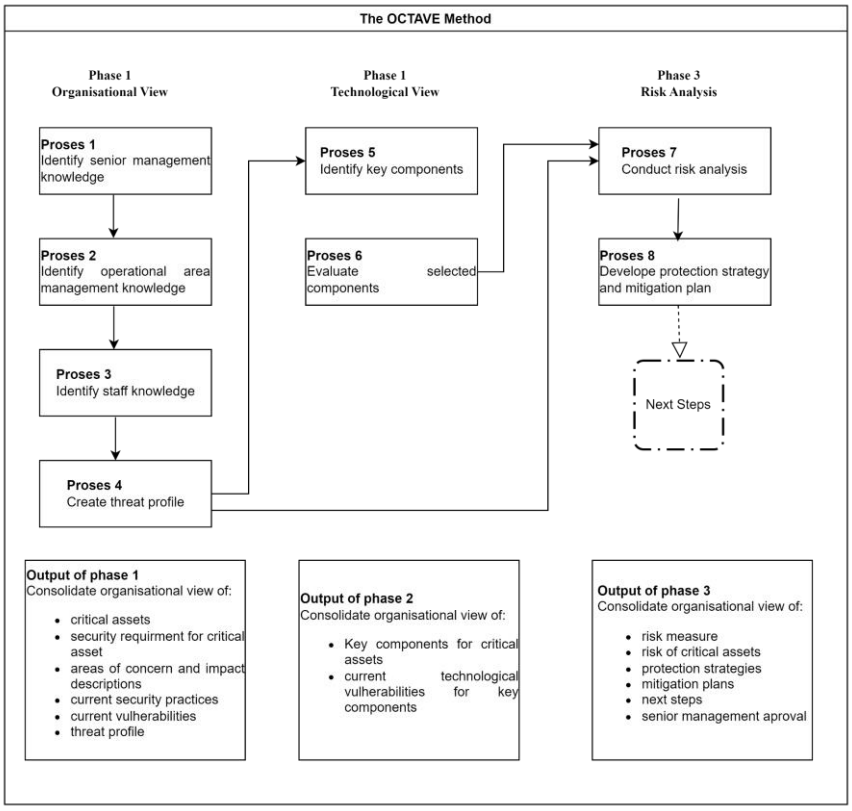
Komponen-komponen kegagalan tersebut adalah sebagai berikut.

1. **Severity Number atau SEV**(tingkat keparahan)/Impact Angka Keparahan atau SEV/Keparahan Dampak adalah ukuran numerik subjektif mengenai seberapa kuat persepsi pengguna terhadap dampak suatu kesalahan.
2. **Probability Number atau OCCUR**(tingkat kejadian)/Likelihood Angka Probabilitas atau OCCUR (Occurrence Rate)/Likelihood Occurrence rate adalah ukuran untuk memperkirakan probabilitas suatu kemungkinan penyebab terjadinya suatu risiko yang dapat mengarah pada mode kegagalan atau mengakibatkan hasil tertentu.
3. **Detection Number atau DETEC**(Deteksi)/Cause Pengukuran deteksi adalah perkiraan numerik subjektif dari pengendalian yang dirancang untuk mencegah atau mendeteksi penyebab kegagalan sebelum mencapai pelanggan.. (Ahdi Anshori & Reza Perdanakusuma, 2019)

E. Metode OCTAVE

OCTAVE adalah kerangka kerja yang memungkinkan organisasi untuk memahami, menilai, dan mengatasi risiko keamanan informasi dari perspektif organisasi.

Diagram berikut memberikan gambaran umum tentang metode OCTAVE, termasuk tahapan metode, proses, dan hasil dari setiap tahapan.



Gambar 1.3 Metode Octave

Fase 1: Build Asset-Based Threat Profiles Tim analisis mengidentifikasi aset-aset penting dan apa yang saat ini dilakukan untuk melindunginya.

Selanjutnya, persyaratan keamanan untuk setiap aset penting ditentukan.

Terakhir, untuk setiap aset penting, kerentanan organisasi terhadap praktik yang ada dan profil ancaman diidentifikasi.

Fase ini memiliki empat proses.

1. Proses 1: Identifikasi pengetahuan manajemen tingkat atas.
   Peserta dalam proses ini adalah manajer senior organisasi.
2. Proses 2: Verifikasi pengetahuan pengelolaan area operasional.
   Manajer departemen bisnis terlibat dalam proses ini.
3. Proses 3: Identifikasi pengetahuan karyawan.
   Karyawan organisasi terlibat dalam proses ini.Staf TI biasanya menghadiri lokakarya yang berbeda dari staf umum.
4. Proses 4: Membuat profil ancaman.
   Partisipan dalam proses ini adalah anggota tim analisis.

Fase 2: Identify Infrastructure Vulnerabilities Tim analisis mengidentifikasi titik akses jaringan dan kelas komponen TI yang terkait dengan setiap aset penting.

Tim kemudian menentukan seberapa tahan setiap kelas komponen terhadap serangan jaringan dan menentukan kerentanan teknis apa pun yang ditemukan pada aset penting selama fase penilaian organisasi.

Fase 2 juga disebut sebagai "pandangan teknologi" dari metode OCTAVE karena berfokus pada infrastruktur komputer organisasi.

Fase 2 juga disebut sebagai "pandangan teknologi" dari metode OCTAVE karena berfokus pada infrastruktur komputer organisasi.

a) Proses 5: *Identify Key Components*. Tim analitik dan beberapa karyawan TI terlibat dalam proses ini. Tujuan Proses 5 adalah memilih komponen infrastruktur yang akan diperiksa kerentanan teknisnya sebagai bagian dari Proses 6. Proses 5 terdiri dari dua aktivitas: mengidentifikasi kelas komponen utama dan mengidentifikasi komponen infrastruktur yang akan ditinjau. - Pemrosesan 6: Evaluasi komponen yang dipilih. Tim analitik dan beberapa karyawan TI terlibat dalam proses ini. Tujuan dari Proses 6 adalah untuk mengidentifikasi kelemahan teknis pada komponen infrastruktur yang diidentifikasi dalam Proses 5. Kelemahan teknis menunjukkan betapa rentannya infrastruktur komputer suatu organisasi.
b) Proses 6 terdiri dari dua kegiatan, yaitu Menjalankan alat penilaian kerentanan terhadap komponen infrastruktur tertentu, meninjau kerentanan teknologi, dan merangkum hasilnya.

Fase 3: *Develop Security Strategy and Plans* Dengan menganalisis informasi yang dikumpulkan, tim analitik mengidentifikasi risiko terhadap aset penting organisasi dan memutuskan apa yang harus dilakukan. Tim ini mengembangkan strategi perlindungan dan rencana mitigasi organisasi untuk mengatasi risiko yang teridentifikasi. Tim juga menentukan "langkah selanjutnya" yang perlu dilaksanakan dan memperoleh persetujuan dari manajemen senior mengenai hasil keseluruhan proses.

a) Proses 7: *Conduct Risk Analysis*. Para peserta dalam proses 7 adalah anggota tim analisis, tujuan dari proses ini adalah untuk mengidentifikasi dan menganalisis risiko terhadap aset kritis organisasi. Proses 7 meliputi tiga kegiatan, yaitu mengidentifikasi dampak Gambar 2.6 Fase Risk Analysis 32 dari ancaman

terhadap aset kritis, membuat kriteria evaluasi risiko, dan mengevaluasi dampak dari ancaman terhadap aset kritis. - Proses 8: Develop Protection Strategy.

b) Proses 8 mencakup dua workshop.Peserta lokakarya Proses 8 pertama mencakup anggota tim analisis dan beberapa anggota organisasi. Tujuan Proses 8 adalah mengembangkan strategi perlindungan organisasi, rencana mitigasi risiko untuk aset penting, dan daftar tindakan jangka pendek. (Ahdi Anshori & Reza Perdanakusuma, 2019)

F. Proses Manajemen Risiko ISO 27001 & 27002

ISO 27001 dan ISO 27002 adalah standar internasional yang berkaitan dengan manajemen keamanan informasi. ISO 27001 menetapkan persyaratan untuk suatu Sistem Manajemen Keamanan Informasi (ISMS), sementara ISO 27002 memberikan panduan dan rekomendasi untuk mengimplementasikan kontrol keamanan informasi dalam konteks ISMS. (Fadilla et al., n.d.; Sari et al., 2022)

Proses manajemen risiko dalam ISO 27001 dan 27002 melibatkan beberapa langkah yang umumnya terkait dengan identifikasi, evaluasi, pengelolaan, dan pemantauan risiko keamanan informasi(David Purba et al., 2018). Berikut adalah langkah-langkah utama dalam proses manajemen risiko ISO 27001 dan 27002:

1. **Identifikasi Risiko:**
   a. Identifikasi aset informasi: Identifikasi semua aset informasi yang dimiliki oleh organisasi, termasuk data, hardware, software, dan informasi lainnya yang kritis.
   b. Identifikasi ancaman dan kerentanan: Identifikasi potensi ancaman terhadap aset informasi dan identifikasi kerentanannya terhadap ancaman tersebut.
2. **Evaluasi Risiko:**
   a. Penilaian risiko: Mengukur dampak potensial dari ancaman terhadap aset dan menilai probabilitas terjadinya risiko tersebut.
   b. Penetapan risiko: Tentukan tingkat risiko yang dapat ditoleransi oleh organisasi
3. **Pengelolaan Risiko:**
   a. Pemilihan kontrol: Menetapkan kontrol keamanan informasi Tindakan yang tepat untuk mengurangi risiko ke tingkat yang dapat diterima.
   b. Implementasi kontrol: Menerapkan kontrol keamanan informasi yang dipilih untuk mengelola risiko.
   c. Dokumentasi kebijakan: Mendokumentasikan kebijakan keamanan informasi dan prosedur terkait.
4. **Pemantauan dan Pemeliharaan:**
   a. Pemantauan: Memantau efektivitas kontrol keamanan informasi dan kondisi risiko secara berkala.
   b. Pemeliharaan: Melakukan perubahan pada sistem dan prosedur jika diperlukan untuk memastikan keamanan informasi tetap sesuai dengan persyaratan ISO 27001 dan 27002.
5. **Perbaikan Berkelanjutan:**

a. Tinjauan Manajemen: Melakukan tinjauan manajemen untuk mengevaluasi kinerja ISMS dan membuat perbaikan berkelanjutan.
b. Perbaikan: Mengidentifikasi dan menerapkan perbaikan berkelanjutan untuk meningkatkan efektivitas ISMS.

Results and Discussion

1. Identifikasi Aset, Ancaman dan Dampak, kerentanan serta Potential Cause (sebagai Tambahan)

Ketika kerentanan ancaman terhadap aset informasi diidentifikasi dari situs web Repository Digital Library Universitas X, disebut sebagai penyebab potensial dari risiko yang terjadi.

terdapat aset web Repository Digital library yang berupa:

Tabel 2.1 Identifikasi Aset

Data /Informasi:	**Software :**	**Hardware :**	**People**
a) Tesis b) Perencanaan bisnis c) Skripsi d) KKP e) Produk dari profesi f) Niers g) Penelitian abdimas h) BKD Dosen Modul Pembelajaran i) PPT Pembelajaran Tujuannya untuk memudahkan mahasiswa dan civitas akademik untuk mengakses dimana dan kapanpun bisa mendapatkan bahan referensi yang dicari	a) Repository Digital Library Perguruan tinggi X Sifat dari software bukan open source, melainkan beli perguruan tinggi Y dengan harga Rp. 16.000.000 dan tidak bisa dikembangkan propertinya a) License yayasan Z Dimana pihak Biro IT yang membayarnya b) Domain web berlangganan dengan PT A Dan setiap bulan pihak yayasan Z dan hosting repository perguruan tinggi X adalah Biro IT. Jadi	a) Perangkat Komputer b) Perangkat Jaringan Internet c) Server database yang digunakan di central yang sama server system website yang lain. Yang mengelola semua biro IT dan sudah terjadwalkan setiap bulannya, persyaratan pada web repository digital library perguruan tinggi X, yang menggunakan standar SNI dan PERPUSNAS	a) Staff Administrasi b) Pustakawan c) Teknisi IT

	pihak perpustakaan serta staf yang ada tinggal memakai saja		

untuk ancaman dan dampak yang kemungkinan terjadi pada aset terbagi menjadi 4 bagian yaitu:

Tabel 2.2 Ancaman dan Dampak

Data /Informasi:	**Software :**	**Hardware :**	**People**
a) Pencurian identitas data diri dan informasi penting, b) Spam muncul di antara data member yang akan di verifikasi, (Spam Malware) c) Data Corrupt	a) Pengguna jahat dapat menyuntikkan JavaScript,VBS cript, ActiveX, HTML atau Flash ke dalam aplikasi yang rentan untuk menipu pengguna di untuk mengumpulkan data dari mereka. Penyerang dapat mencuri cookie sesi dan mengambil alih akun, meniru pengguna. Dimungkinkan juga untuk mengubah konten halaman yang disajikan kepada pengguna. b) Penyerang dapat memaksa pengguna aplikasi web untuk	a) Server lemot b) Hilangnya Pasokan Listrik c) Konektivitas internet Menurun d) Koneksi Terputus	a) Kesalahan penginputan dan penghapusan Data b) Kesalahan Penggunaan

	mengeksekusi tindakan yang dipilih penyerang. CSRF yang sukses Eksploitasi dapat membahayakan data dan operasi pengguna akhir jika terjadi pengguna normal. Jika pengguna akhir yang ditargetkan adalah administrator akun, ini dapat membahayakan seluruh aplikasi web. c) kemungkinan menerima hasil yang salah/tidak lengkap saat memindai server yang dilindungi oleh IPS/IDS/WAF. Juga, jika WAF mendeteksi sejumlah serangan yang berasal dari pemindai, alamat IP dapat diblokir setelah beberapa upaya d) Kemungkinan pengungkapan informasi: daftar direktori, nama		

	file brute forcing, file cadangan e) Dampaknya tergantung pada aplikasi web yang terpengaruh. f) Penyerang dapat mencoba menemukan kata sandi yang lemah dengan secara sistematis mencoba setiap kombinasi huruf yang mungkin, angka, dan simbol sampai menemukan satu kombinasi yang benar yang berfungsi g) pada versi Internet Explorer yang lebih lama dimungkinkan untuk mengeksekusi kode JavaScript arbitrer menggunakan fungsi expression() Internet Explorer. Penyerang juga dapat mengekstrak sumber halaman dan berpotensi mencuri token		

	CSRF menggunakan pemilih CSS h) Direktori ini dapat mengekspos informasi sensitif yang dapat membantu pengguna jahat untuk menyiapkan serangan yang lebih canggih. i) kemungkinan penolakan layanan j) masalah navigasi situs k) alamat email yang diposting di situs web dapat menarik spam l) kemungkinan pengungkapan informasi sensitif m) kemungkinan pengungkapan informasi sensitif		

untuk kerentanan atau vulnerability pada aset terbagi menjadi 4 bagian yaitu:

Tabel 2.3 Kerentanan aset

Data /Informasi:	**Software :**	**Hardware :**	**People**
a) Kesalahan penempatan hak akses	a) Script lintas situs (Medium)	a) Pertambahan memori yang cepat dalam	a) Pustakawan kurang teliti b) Pelatihan terkait

b) Kurang memperhatikan pentingnya antivirus c) Jaringan internet kurang stabil	b) Bentuk HTML tanpa Perlindungan CSRF (Medium) c) Web Application Firewall terdeteksi (Medium) d) Apache Mod_negotiation brute forcing nama file (low) e) Clickjacking: Header X-Frame-Options Hilang (low) f) Serangan menebak kata sandi halaman login (low) g) Kemungkinan penempatan jalur relative (low) h) Kemungkinan direktori sensitif(low) i) Waktu response lambat (low) j) Tautan rusak (low) k) Alamat email ditemukan (low) l) Pengungkapan versi server web halaman kesalahan (low) m) Input jenis kata sandi dengan pelengkapan	pemrosesan data b) Kerentanan terhadap voltase yang bervariasi hubungan arus pendek pada panel listrik, Supply listrik yang tidak stabil c) Kualitas jaringan yang kurang baik d) Efek bencana alam dan kejadian yang tidak terduga	teknologi informasi tidak cukup

	otomatis diaktifkan (low)		

dan potential cause yang terdapat pada aset terbagi menjadi 4 bagian yaitu:

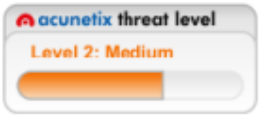
Data /Informasi:	**Software :**	**Hardware :**	**People**
a) Tidak ada penggunaan hak akses b) PC dan System terserang Virus c) Speed koneksi internet yang lemah dan tidak stabil	dari indeks A - M kurangnya keamanan pada web yang menyebabkan kerentanan aplikasi.	a) Kapasitas memori server yang sudah tidak memenuhi kebutuhan (Memory Full) b) Korsleting listrik, pemadaman listrik c) Gangguan jaringan pada provider d) Kerusakan pada infrastruktur jaringan	a) Kesalahan penginputan dan penghapusan data b) Kurangnya training prosedur penggunaan TI yang diberikan.

Hasil dari Test Vulnerability website digital library perguruan tinggi X menggunakan tools Acunetix :

Scan details

Scan information	
Start time	28/11/2022 21:49:40
Finish time	29/11/2022 08:20:05
Scan time	10 hours, 30 minutes
Profile	Default
Server information	
Responsive	True
Server banner	cloudflare
Server OS	Unknown
Server technologies	PHP

Threat level



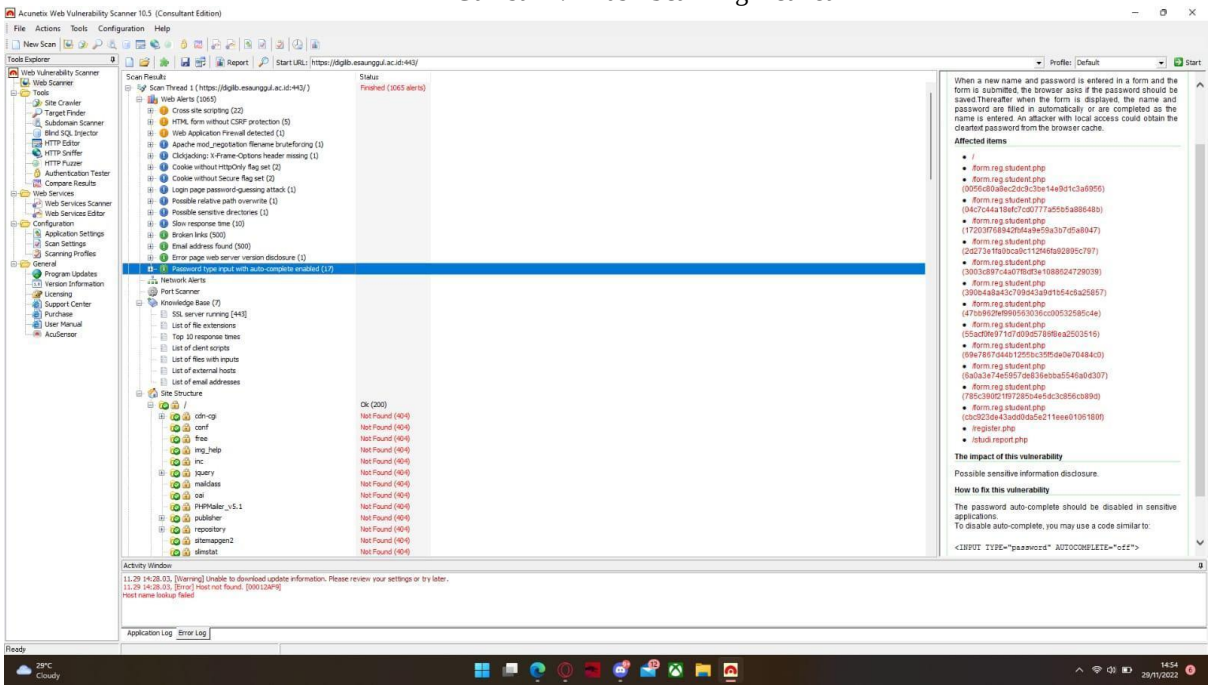
Acunetix Threat Level 2

One or more medium-severity type vulnerabilities have been discovered by the scanner. You should investigate each of these vulnerabilities to ensure they will not escalate to more severe problems.

Alerts distribution

Total alerts found	1065
High	0
Medium	28
Low	19
Informational	1018

Gambar 2.1 Hasil Scanning Acunetix



Gambar 2.2 Hasil Scanning Acunetix

2. Identifikasi Risiko

Sebelum memasuki tahapan penilaian risiko, terlebih dahulu akan diidentifikasi risiko yang dapat mengancam keamanan informasi aset informasi di situs web Perpustakaan Digital Universitas X. Risiko yang dimaksudkan adalah kejadian yang memiliki kemungkinan besar terjadi, bahkan sering terjadi, karena hal-hal yang berasal dari lingkungan eksternal dan internal perusahaan, seperti bencana alam, gangguan sosial dan fasilitas umum, dan operasi Tabel berikut menunjukkan identifikasi risiko.

Tabel 2.4 Identifikasi Risiko

Aset web Repository Digital Library	Potential cause	Risiko
Data /Informasi: a) Tesis b) Perencanaan bisnis c) Skripsi d) KKP e) Produk dari profesi f) Niers g) Penelitian abdimas h) BKD Dosen i) Modul Pembelajaran j) PPT Pembelajaran	a) Tidak ada penggunaan hak akses b) PC dan System terserang Virus c) Speed koneksi internet yang lemah dan tidak stabil	a) Mudah di Hack b) Human atau Technician error c) Network failure

Tujuannya untuk memudahkan mahasiswa dan civitas akademik untuk mengakses dimana dan kapanpun bisa mendapatkan bahan referensi yang dicari		
Software a) Repository Digital Library Perguruan tinggi X, Sifat dari software bukan open source, melainkan beli perguruan tinggi Y dengan harga Rp. 16.000.000 dan tidak bisa dikembangkan propertinya b) License yayasan Z, Dimana pihak Biro IT yang membayarnya c) Domain web berlangganan dengan PT A. Dan setiap bulan pihak yayasan Z dan hosting repository perguruan tinggi X adalah Biro IT. Jadi pihak perpustakaan serta staf yang ada tinggal memakai saja	a) Indeks A - M kurangnya keamanan pada web yang menyebabkan kerentanan aplikasi.	b) Software Failure c) Serangan Hacker d) Pencurian media tau informasi penting
Hardware : a) Perangkat Komputer b) Perangkat Jaringan Internet c) Server database yang digunakan di central yang sama server system website yang lain. Yang mengelola semua biro IT dan sudah terjadwalkan setiap bulannya, persyaratan pada web repository digital library perguruan tinggi X, yang menggunakan standar SNI dan PERPUSNAS	a) Kapasitas memori server yang sudah tidak memenuhi kebutuhan (Memory Full) b) Korsleting listrik, pemadaman listrik c) Gangguan jaringan pada provider d) Kerusakan pada infrastruktur jaringan	a) Memory Penuh b) Kebakaran c) Network Failure d) Network Failure
People	a) Kesalahan penginputan dan penghapusan data b) Kurangnya training prosedur penggunaan TI yang diberikan.	a) Human atau Technician Error

1. **Penilaian Risiko (Assessment Risiko) Menggunakan Metode FMEA (Failure Mode effect analysis)**

   Pada langkah ini, tingkat severity, occurance, dan detection ditentukan dengan memberikan deskripsi lebih lanjut tentang risiko yang telah diidentifikasi. Nilai severity, occurance, dan detection yang dihasilkan dari proses ini digunakan untuk menghitung RPN (Risk Priority Number) parameter dari tingkat severity, occurrence, dan detection.

   - Penjelasan: Dengan menentukan tingkat bahaya yang akan terjadi pada output yang dihasilkan, tahapan pertama dalam metode FMEA adalah keseriusan atau tingkat bahaya.

Tabel 2.5 nilai severity

Rating	Kriteria
1	Negligible severity (Pengaruh buruk yang dapat diabaikan). Pengaruh ini tidak berdampak pada kualitas produk.
2	Mild severity (Pengaruh buruk yang ringan). Efek yang ditimbulkan akan bersifat ringan, konsumen tidak merasakan penurunan kualitas produk.
3	
4	Moderate severity (pengaruh buruk yang moderate). Konsumen merasakan penurunan kualitas produk, namun masih dalam batas wajar.
5	
6	
7	High severity (Pengaruh buruk yang tinggi). Konsumen merasakan penurunan kualitas yang wajar.
8	
9	Potential severity (Pengaruh buruk yang sangat tinggi). Efek yang ditimbulkan sangat berpengaruh terhadap kualitas produk sehingga konsumen akan menolaknya
10	

   - Penjelasan : Occurrence atau frekuensi/tingkat kejadian, yaitu pada tahapan ini akan diukur frekuensi atau tingkat kejadian tersebut dan dari penyebab tersebut akan menghasilkan kegagalan.
     Tabel Nilai Occurrence :

Tabel 2.6 Nilai Occurance

Rating	Rata-Rata Kegagalan	Degree
1	0,01/1000 Produk	Remote
2	0,1/1000 Produk	Low
3	0,5/1000 Produk	
4	1/1000 Produk	Moderate
5	2/1000 Produk	
6	5/1000 Produk	
7	10/1000 Produk	High
8	20/1000 Produk	
9	50/1000 Produk	Very High
10	100 / 1000 Produk	

- Penjelasan : Detectability atau kemudahan untuk dapat dideteksi, yaitu parameter yang digunakan untuk mengetahui atau mendeteksi penyebab potensial yang menyebabkan terjadinya kegagalan.

Tabel 2.7 Nilai Detectability

Rating	Kriteria	Berdasarkan Frekuensi Kejadian
1	Metode Pencegahan sangat efektif. Tidak ada kesempatan penyebab mungkin muncul	0,01/1000 Produk
2	Kemungkinan penyebab terjadi sangat rendah	0,1/1000 Produk

3		0,5/1000 Produk
4	Kemungkinan penyebab terjadi bersifat moderat. Metode pencegahan kadang memungkinkan penyebab itu terjadi	1/1000 Produk
5		2/1000 Produk
6		5/1000 Produk
7	Kemungkinan penyebab terjadi masih tinggi. Metode pencegahan kurang efektif. Penyebab masih berulang kembali.	10/1000 Produk
8		20/1000 Produk
9	Kemungkinan penyebab terjadi masih tinggi. Metode pencegahan tidak efektif. Penyebab masih berulang kembali	50/1000 Produk
10		100 / 1000 Produk

Berikut merupakan tabel penilaian risiko:

Tabel 2.8 Penilaian Risiko

Risiko	**Potential Cause**	**SEV (parah)**	**OCC (terjadinya)**	**DEC (deteksi)**	**RPN (nomor prioritas risiko)**	**LEVEL**
Kurangnya hak akses pengguna dan kelemahan sistem	Tidak ada penggunaan hak akses	6	3	5	72	Low
	PC dan System terserang Virus	5	4	3	60	Low
	Speed koneksi internet yang lemah dan tidak stabil	4	3	3	36	Very Low

Software Failure	Indeks A - M kurangnya keamanan pada web yang menyebabkan kerentanan aplikasi.	6	4	5	120	Medium
Hardware Failure	Kapasitas memori server yang sudah tidak memenuhi kebutuhan (Memory Full)	6	4	4	96	Low
	Korsleting listrik, pemadaman listrik	9	3	4	108	Medium
	Gangguan jaringan pada provider	4	3	3	36	Very Low
	Kerusakan pada infrastruktur jaringan	5	4	4	80	Low
Human atau Technician Error	Kesalahan penginputan dan penghapusan data	6	4	4	96	Low
	Kurangnya training prosedur penggunaan TI yang diberikan	5	3	4	60	Low

4. Mitigasi Risiko

Setelah melakukan identifikasi aset kritis, identifikasi risiko dan penilaian risiko selanjutnya adalah melakukan mitigasi terhadap risiko tersebut. Mitigasi dilakukan dengan menggunakan standar ISO 27001 dan 27002 dan disk Dari hasil identifikasi dan

penilaian risiko maka berikut beberapa kontrol objektif dari standar ISO/IEC 27001 dan 27002 yang direkomendasikan untuk penanganan risiko-risiko yang telah diidentifikasi tersebut adalah :

Tabel 2.9 Mitigasi Risiko

Aset (Risiko)	**Penyebab Risiko**	**Evaluasi dampak risiko**
Data /Informasi: a) Tesis b) Perencanaan bisnis c) Skripsi d) KKP e) Produk dari profesi f) Niers g) Penelitian abdimas h) BKD Dosen i) Modul Pembelajaran j) PPT Pembelajaran Tujuannya untuk memudahkan mahasiswa dan civitas akademik untuk mengakses dimana dan kapanpun bisa mendapatkan bahan referensi yang dicari Risiko: Kurangnya hak akses pengguna dan kelemahan sistem	a) Tidak ada penggunaan hak akses b) PC dan System terserang Virus c) Speed koneksi internet yang lemah dan tidak stabil	a) Pencurian identitas data diri dan informasi penting b) Spam muncul di antara data member yang akan di verifikasi, (Spam Malware) c) Data Corrupt
Software a) Repository Digital Library Perguruan tinggi X, Sifat dari software bukan open source, melainkan beli perguruan tinggi Y dengan harga Rp. 16.000.000 dan tidak bisa dikembangkan propertinya b) License yayasan Z, Dimana pihak Biro IT yang membayarnya c) Domain web berlangganan dengan PT A. Dan setiap bulan	A - M kurangnya keamanan pada web yang menyebabkan kerentanan aplikasi.	a) Pengguna jahat dapat menyuntikkan JavaScript,VBScript, ActiveX, HTML atau Flash ke dalam aplikasi yang rentan untuk menipu pengguna di untuk mengumpulkan data dari mereka. Penyerang dapat mencuri cookie sesi dan mengambil alih akun, meniru pengguna. Dimungkinkan juga untuk mengubah konten halaman yang disajikan kepada pengguna.

pihak yayasan Z dan hosting repository perguruan tinggi X adalah Biro IT. Jadi pihak perpustakaan serta staf yang ada tinggal memakai saja Risiko: Software Failure		b) Penyerang dapat memaksa pengguna aplikasi web untuk mengeksekusi tindakan yang dipilih penyerang. CSRF yang sukses Eksploitasi dapat membahayakan data dan operasi pengguna akhir jika terjadi pengguna normal. Jika pengguna akhir yang ditargetkan adalah administrator akun, ini dapat membahayakan seluruh aplikasi web. c) Kemungkinan menerima hasil yang salah/tidak lengkap saat memindai server yang dilindungi oleh IPS/IDS/WAF. Selain itu, jika WAF mendeteksi sejumlah serangan yang berasal dari pemindai, alamat IP dapat diblokir setelah beberapa upaya d) Kemungkinan pengungkapan informasi: daftar direktori, nama file brute forcing, file cadangan e) Dampaknya tergantung pada aplikasi web yang terpengaruh. f) Penyerang dapat mencoba menemukan kata sandi yang lemah dengan secara sistematis mencoba setiap kombinasi huruf

		yang mungkin, angka, dan simbol sampai menemukan satu kombinasi yang benar yang berfungsi g) pada versi Internet Explorer yang lebih lama dimungkinkan untuk mengeksekusi kode JavaScript arbitrer menggunakan fungsi expression() Internet Explorer. Penyerang juga dapat mengekstrak sumber halaman dan berpotensi mencuri token CSRF menggunakan pemilih CSS h) Direktori ini dapat mengekspos informasi sensitif yang dapat membantu pengguna jahat untuk menyiapkan serangan yang lebih canggih. i) kemungkinan penolakan layanan j) masalah navigasi situs k) alamat email yang diposting di situs web dapat menarik spam l) kemungkinan pengungkapan informasi sensitif m) kemungkinan pengungkapan informasi sensitif
Hardware : a) Perangkat Komputer	a) Kapasitas memori server yang sudah tidak memenuhi kebutuhan (Memory Full	a) Server lemot b) Hilangnya Pasokan Listrik

b) Perangkat Jaringan Internet c) Server database yang digunakan di central yang sama server system website yang lain. Yang mengelola semua biro IT dan sudah terjadwalkan setiap bulannya, persyaratan pada web repository digital library perguruan tinggi X, yang menggunakan standar SNI dan PERPUSNAS Risiko: hardware failure	b) Korsleting listrik, pemadaman listrik c) Gangguan jaringan pada provider d) Kerusakan pada infrastruktur jaringan	c) Konektivitas internet Menurun d) Koneksi Terputus
People Risiko: Human atau Technician Error	a) Kesalahan penginputan dan penghapusan data b) Kurangnya training prosedur penggunaan TI yang diberikan	a) Kesalahan penginputan dan penghapusan Data b) Kesalahan Penggunaan

Tabel 2.10 Tindakan Mitigasi risiko ISO27001 dan 27002

Tindakan Mitigasi risiko berdasarkan ISO 27001 & 27002			
Aset	**Kontrol**	**Sub Kontrol**	**Keterangan**
Data /Informasi: k) Tesis l) Perencanaan bisnis m) Skripsi n) KKP o) Produk dari profesi p) Niers q) Penelitian abdimas r) BKD Dosen s) Modul Pembelajaran	Penggunaan javascript,DHTML dan Ajax yang tidak kompatibel dengan semua browser akan berakibat fatal untuk validasi form dan penggunaan javascript untuk menu. Begitu pula dengan penggunaan DHTML dan Ajax, jika tidak di tes terlebih dahulu atau pemrograman didalamnya tidak	Secure HTTP atau yang disebut dengan HTTPS dan sertifikasi SSL memiliki keamanan enkripsi data bisa diketahui dengan alamat situs yang diawali dengan *https*. Selain itu, keamanan juga bisa dilihat dengan adanya logo gembok di kiri atas sebelah tautan situs.	a) Organisasi menetapkan kebijakan mengenai monitoring aset teknologi informasi b) Monitoring dilakukan secara berkala untuk memastikan aset teknologi

t) PPT Pembelajaran Tujuannya untuk memudahkan mahasiswa dan civitas akademik untuk mengakses dimana dan kapanpun bisa mendapatkan bahan referensi yang dicari	mendukung untuk diakses di semua browser juga akan berakibat fatal.		
b) Repository Digital Library Perguruan tinggi X Sifat dari software bukan open source, melainkan beli perguruan tinggi Y dengan harga Rp. 16.000.000 dan tidak bisa dikembangkan propertinya c) License yayasan Z Dimana pihak Biro IT yang membayarnya d) Domain web berlangganan dengan PT A Dan setiap bulan pihak yayasan Z dan hosting repository perguruan tinggi X adalah Biro IT. Jadi pihak perpustakaan serta staf yang ada tinggal memakai saja	Tempatkan infrastruktur baik software maupun perangkat jaringan yang aman jauh dari kemungkinan banjir dan menyiapkan perencanaan penyediaan cadangan infrastruktur baik software maupun perangkat.	Menyediakan OWASP Apps Security Verification Standard (ASVS), firewall, VPN, antispam, content filtering dan lapisan keamanan jaringan yang up to date untuk melindungi data sensitif seperti data mahasiswa	a) Organisasi menetapkan kebijakan mengenai monitoring aset teknologi informasi b) Monitoring dilakukan secara berkala untuk memastikan aset teknologi
Hardware : Perangkat Komputer Perangkat Jaringan Internet	Membuat jadwal, melakukan pengecekan data dan back up data secara berkala	Menyediakan genset dan harus memperbaiki sistem regenerasi genset, hendaklah bagian IT terlebih dahulu menyalakan genset, karena	a) Organisasi menetapkan kebijakan mengenai monitoring aset teknologi informasi b) Monitoring dilakukan secara berkala untuk

Server database yang digunakan di central yang sama server system website yang lain. Yang mengelola semua biro IT dan sudah terjadwalkan setiap bulannya, persyaratan pada web repository digital library perguruan tinggi X, yang menggunakan standar SNI dan PERPUSNAS		topangan daya sangat mempengaruhi proses bisnis	memastikan aset teknologi
People	Database Management System (DBMS) seperti (MySQL, PostgreSQL, Oracle, Ms SQL Server) perguruan tinggi dapat dengan mudah mengakses dan menyimpan data informasi.	a) Organisasi menetapkan kebijakan mengenai monitoring aset teknologi informasi b) Monitoring dilakukan secara berkala untuk memastikan aset teknologi	Database Management System (DBMS) seperti (MySQL, PostgreSQL, Oracle, Ms SQL Server) perguruan tinggi dapat dengan mudah mengakses dan menyimpan data informasi.

5. Analisis Kontrol Saat ini Pada Web Repository Digital Library Perguruan Tinggi X

Berdasarkan data yang didapat pada saat wawancara sesi 1 dan 2 terdapat analisis kontrol saat ini yang ada pada web repository digital library Perguruan Tinggi X :

Tabel 2.11 Analisis Kontrol

Jenis Kontrol	Keterangan : Sudah Diterapkan
Maintenance untuk web repository digital library Perguruan Tinggi X	Sudah dilakukan oleh BTIK
Maintenance pada Hardware	Sudah dilakukan oleh BTIK

Keamanan Sistem dari jenis virus, data corrupt	Sudah dilakukan oleh BTIK (Masih bisa ditangani)
Sosialisasi dalam penggunaan web Repository Digital Library Perguruan Tinggi X	Sudah dilakukan sosialisasi untuk para karyawan dan pengguna

6. Penentuan Likelihood

Setiap potensi risiko diukur dan diklasifikasikan berdasarkan dua kriteria utama, yaitu kemungkinan (likelihood) dan dampak (impact) yang mungkin terjadi. Likelihood risiko dikelompokkan ke dalam 3 kategori, seperti Tinggi (High), Sedang (Medium), dan Rendah (Low). Tingkat High, menunjukkan bahwa risiko memiliki kemungkinan yang tinggi untuk terjadi, sedangkan semakin mendekati tingkat Low, menunjukkan bahwa kemungkinan terjadinya risiko menjadi sangat kecil untuk terjadi. Sama halnya dengan dampak, risiko dapat dinilai sebagai memiliki dampak besar, sedang, dan kecil tergantung pada potensi konsekuensi yang timbul.

Penilaian likelihood:

Skill Level Bagaimana keahlian dari kelompok pengguna.

- KR01 Kesalahan penempatan hak akses (2): Staff atau manajemen memiliki pemahaman dan kemampuan untuk mengelola hak akses dengan baik, sehingga tingkat kemungkinan rendah.
- KR02 Kurang memperhatikan pentingnya antivirus (5): Staff atau manajemen dianggap kurang memiliki pemahaman dan kemampuan untuk memahami pentingnya antivirus, sehingga tingkat kemungkinan tinggi.
- KR03 Jaringan internet kurang stabil (3): Staff atau manajemen memiliki pemahaman namun mungkin memiliki keterbatasan kemampuan dalam menangani masalah jaringan, sehingga tingkat kemungkinan cukup terkendali.
- KR04 Script lintas situs (2): Kemungkinan rendah karena staff atau manajemen memiliki pemahaman dan kemampuan untuk mengelola risiko terkait script lintas situs.
- KR05 Bentuk HTML tanpa Perlindungan CSRF (4): Tingkat kemungkinan cukup tinggi karena risiko ini memerlukan pemahaman dan keterampilan teknis yang baik untuk diatasi.
- KR06 Web Application Firewall terdeteksi (3): Kemungkinan cukup terkendali karena staff atau manajemen memiliki pemahaman dan kemampuan teknis.
- KR07 Apache Mod_negotiation brute forcing nama file (2): Risiko ini memiliki kemungkinan rendah karena staff atau manajemen dapat mengelola konfigurasi Apache dengan baik.
- KR08 Cookie tanpa bendera Aman disetel (1): Kemungkinan sangat rendah karena staff atau manajemen memiliki pemahaman dan kemampuan untuk mengatasi risiko ini.

- KR09 Serangan menebak kata sandi halaman login (2): Kemungkinan rendah karena staff atau manajemen dapat mengambil tindakan untuk mengurangi risiko serangan ini.
- KR10 Kemungkinan penimpaan jalur relative (2): Kemungkinan rendah karena staff atau manajemen dapat mengelola konfigurasi dengan baik.
- KR11 Kemungkinan direktori sensitive (1): Kemungkinan sangat rendah karena staff atau manajemen dapat mengelola hak akses dengan baik.
- KR12 Waktu response lambat (1): Risiko ini memiliki kemungkinan sangat rendah karena staff atau manajemen dapat mengelola performa sistem dengan baik.
- KR13 Tautan rusak (2): Kemungkinan rendah karena staff atau manajemen dapat melakukan pemantauan dan pemeliharaan tautan.
- KR14 Alamat email ditemukan (2): Risiko ini memiliki kemungkinan rendah karena staff atau manajemen dapat mengelola informasi sensitif dengan baik.
- KR15 Pengungkapan versi server web halaman kesalahan (1): Kemungkinan sangat rendah karena staff atau manajemen dapat mengelola konfigurasi server dengan baik.
- KR16 Input jenis kata sandi dengan pelengkapan otomatis diaktifkan (2): Kemungkinan rendah karena staff atau manajemen dapat mengelola konfigurasi dengan baik.
- KR17 Kerentanan terhadap voltase yang bervariasi hubungan arus pendek pada panel listrik, Supply listrik yang tidak stabil (5): Kemungkinan tinggi karena risiko ini dapat dipengaruhi oleh faktor eksternal yang sulit dikendalikan.
- KR18 Pertambahan memori yang cepat dalam pemrosesan data (4): Risiko ini memiliki kemungkinan cukup tinggi karena pertambahan memori bisa terjadi dengan cepat.
- KR19 Kualitas jaringan yang kurang baik (2): Risiko ini memiliki kemungkinan cukup tinggi karena kualitas jaringan dapat dipengaruhi oleh faktor luar.
- KR20 Efek bencana alam dan kejadian-yang tidak terduga (5): Kemungkinan tinggi karena bencana alam dan kejadian tidak terduga sulit diprediksi dan dikendalikan.
- KR21 Pustakawan kurang teliti (5): Risiko ini memiliki kemungkinan tinggi karena perilaku pustakawan dapat bervariasi dan sulit untuk dikendalikan.
- KR22 Pelatihan terkait teknologi informasi tidak cukup (3): Kemungkinan cukup tinggi karena tingkat pelatihan dapat bervariasi dan sulit dikendalikan.

Penilaian impact:
Loss of Confidentiality Seberapa banyak hal pribadi perusahaan jatuh ke tangan umum, dan seberapa sensitive hal tersebut.

- KR01 Kesalahan penempatan hak akses (1): Dampak rendah karena kesalahan penempatan hak akses mungkin hanya memberikan akses terhadap informasi yang tidak sangat sensitif.

- KR08 Cookie tanpa bendera Aman disetel (2): Dampak sedang karena cookie tanpa tanda aman dapat mengakibatkan akses tidak sah ke informasi yang lebih sensitif.

Loss of Integrity Seberapa banyak hal yang tidak sesuai dengan kenyataan, seberapa parah rusaknya

- KR11 Kemungkinan direktori sensitive (1): Dampak rendah karena penyalahgunaan hak akses terhadap direktori yang sensitif mungkin hanya memengaruhi sebagian kecil informasi.
- KR12 Waktu response lambat (1): Dampak rendah karena keterlambatan dalam merespon mungkin tidak langsung mengancam integritas data.

Loss of Availability Seberapa banyak layanan IT yang hilang dan seberapa vitalkah hal tersebut.

- KR03 Jaringan internet kurang stabil (2): Dampak sedang karena ketidakstabilan jaringan dapat mengganggu akses dan ketersediaan layanan.
- KR06 Web Application Firewall terdeteksi (3): Dampak cukup tinggi karena deteksi firewall dapat mempengaruhi ketersediaan aplikasi.
- KR07 Apache Mod_negotiation brute forcing nama file (2): Dampak sedang karena serangan brute forcing dapat mempengaruhi ketersediaan server.
- KR09 Serangan menebak kata sandi halaman login (1): Dampak rendah karena serangan ini mungkin tidak signifikan mengancam ketersediaan sistem.
- KR10 Kemungkinan penimpaan jalur relative (2): Dampak sedang karena penimpaan jalur dapat mempengaruhi ketersediaan fungsi-fungsi tertentu.
- KR13 Tautan rusak (1): Dampak rendah karena tautan rusak mungkin hanya memengaruhi sebagian kecil pengguna.
- KR14 Alamat email ditemukan (1): Dampak rendah karena informasi alamat email mungkin tidak sangat kritis untuk ketersediaan sistem.
- KR15 Pengungkapan versi server web halaman kesalahan (1): Dampak rendah karena pengungkapan versi server mungkin tidak langsung mengancam ketersediaan sistem.
- KR16 Input jenis kata sandi dengan pelengkapan otomatis diaktifkan (1): Dampak rendah karena ini hanya memengaruhi sebagian kecil pengguna.
- KR17 Kerentanan terhadap voltase yang bervariasi hubungan arus pendek pada panel listrik, Supply listrik yang tidak stabil (5): Dampak tinggi karena gangguan pasokan listrik dapat mengakibatkan kegagalan sistem yang kritis.
- KR18 Pertambahan memori yang cepat dalam pemrosesan data (3): Dampak sedang karena pertambahan memori dapat mempengaruhi ketersediaan sumber daya sistem.
- KR19 Kualitas jaringan yang kurang baik (4): Dampak cukup tinggi karena kualitas jaringan yang buruk dapat memengaruhi ketersediaan layanan.
- KR20 Efek bencana alam dan kejadian-yang tidak terduga (5): Dampak tinggi karena bencana alam dapat menyebabkan kerusakan fisik pada perangkat keras dan fasilitas.
- KR21 Pustakawan kurang teliti (4): Dampak tinggi karena kurangnya kehati-hatian dapat mengancam integritas dan ketersediaan informasi.

- KR22 Pelatihan terkait teknologi informasi tidak cukup (1): Dampak rendah karena kurangnya pelatihan mungkin tidak langsung memengaruhi ketersediaan sistem.

Dalam mengevaluasi kemungkinan (likelihood) dan dampak (impact) dari setiap risiko, diperlukan kriteria yang dapat menjadi panduan dalam penilaian tersebut. Kriteria tersebut artinya kemungkinan penyebab terjadinya risiko.

Tabel 2.12 Impact

Jenis Aset	ID	Kemungkinan Risiko (KR)	Likelihood	Impact
Aset Data/Informasi	KR01	Kesalahan penempatan hak akses	2	1
	KR02	Kurang memperhatikan pentingnya antivirus	5	5
	KR03	Jaringan internet kurang stabil	3	2
Aset Software	KR04	Script lintas situs	2	3
	KR05	Bentuk HTML tanpa Perlindungan CSRF	4	5
	KR06	Web Application Firewall terdeteksi	3	3
	KR07	Apache Mod_negotiation brute forcing nama file	2	2
	KR08	Cookie tanpa bendera Aman disetel	1	2
	KR09	Serangan menebak kata sandi halaman login	2	1
	KR10	Kemungkinan penimpaan jalur relative	2	2
	KR11	Kemungkinan direktori sensitive	1	1
	KR12	Waktu response lambat	1	1
	KR13	Tautan rusak	2	1
	KR14	Alamat email ditemukan	2	1
	KR15	Pengungkapan versi server web	1	1

		halaman kesalahan		
	KR16	Input jenis kata sandi dengan pelengkapan otomatis diaktifkan	2	1
Aset Hardware	KR17	Kerentanan terhadap voltase yang bervariasi hubungan arus pendek pada panel listrik, Supply listrik yang tidak stabil	5	5
	KR18	Pertambahan memori yang cepat dalam pemrosesan data	4	3
	KR19	Kualitas jaringan yang kurang baik	2	4
	KR20	Efek bencana alam dan kejadian-yang tidak terduga	5	5
Aset People	KR21	Pustakawan kurang teliti	5	4
	KR22	Pelatihan terkait teknologi informasi tidak cukup	3	1

Setelah melakukan penghitungan, maka diperoleh nilai akhir dari setiap risiko selanjutnya, mengidentifikasi level likelihood dari masing-masing risiko untuk menentukan sejauh mana kemungkinan terjadinya risiko tersebut.

Tabel 2.13 Likelihood

Overall risk security				
Impact	HIGH	Medium	High	Critical
	MEDIUM	KR03 KR04 KR19 KR22		
	LOW	KR01 KR07 KR08 KR09 KR10 KR11 KR12 KR13 KR14 KR15	KR02 KR05 KR17 KR18 KR20 KR21	

		KR16		
		LOW	MEDIUM	HIGH
	Likelihood			

7. Rekomendasi Kontrol Secara Keseluruhan

A. KR01 (Kesalahan penempatan Hak Akses) – Aset Data/Informasi

- Sisi organisasi : Keamanan akses pihak ketiga (4.2) dengan menerapkan proses untuk menganalisis risiko koneksi pihak ketiga dan menerapkan standar keamanan khusus untuk memerangi risiko koneksi pihak ketiga.
- Sisi keamanan : Memantau Akses dan penggunaan sistem (9.7) dengan menerapkan jejak audit yang mencatat pengecualian dan peristiwa terkait keamanan yang menghasilkan dan memelihara untuk membantu penyelidikan di masa mendatang dan dalam kontrol akses.
- Sisi hukum : Kepatuhan terhadap persyaratan hukum (12.1) Menerapkan standar untuk memastikan bahwa semua persyaratan undang-undang, peraturan, dan kontrak yang relevan secara khusus ditentukan dan didokumentasikan untuk setiap sistem informasi

B. KR02 (Kurang Memperhatikan Pentingnya Antivirus) – Aset Data/Informasi

- Sisi organisasi : Forum keamanan informasi manajemen (4.1) membentuk komite perusahaan atau organisasi untuk mengawasi keamanan informasi, mengembangkan dan menerapkan pernyataan misi organisasi keamanan informasi, terutama dalam menerapkan antivirus
- Sisi keamanan : Persyaratan keamanan sistem (10.1) menerapkan standar untuk memastikan bahwa analisis persyaratan keamanan merupakan bagian dari tahap analisis persyaratan dari setiap proyek pengembangan, terutama dalam pemilihan antivirus untuk aplikasi yang digunakan.
- Sisi hukum : Tinjauan kebijakan keamanan dan kepatuhan teknis (12.2) Menerapkan standar untuk memastikan bahwa semua area dalam organisasi dipertimbangkan untuk tinjauan rutin guna memastikan kepatuhan terhadap kebijakan dan standar keamanan terutama dalam memilih antivirus
- Sisi teknik : Menerapkan atau memasang antivirus pada setiap perangkat, guna untuk meminimalisir terjadinya virus yang masuk yang berbahaya untuk keamanan informasi

C. KR03 (Jaringan Internet Kurang Stabil) – Aset Data/Informasi

- Sisi organisasi : kontrol akses jaringan (9.4) menerapkan prosedur untuk memastikan bahwa layanan jaringan dan komputer yang dapat diakses

oleh pengguna individu atau dari terminal tertentu konsisten dengan kebijakan kontrol akses bisnis.

- Sisi keamanan : keamanan dalam kontrak outsourcing (4.3) pastikan persyaratan keamanan pemilik informasi telah dibahas dalam kontrak antara pemilik dan organisasi outsourcing. Terutama dalam keamanan jaringan internet.
- Sisi hukum: Kepatuhan terhadap persyaratan hukum (12.1) Menerapkan standar untuk memastikan bahwa semua persyaratan undang-undang, peraturan, dan kontrak yang relevan secara khusus ditentukan dan didokumentasikan untuk setiap sistem informasi.
- Sisi teknik : Menerapkan atau mengupgrade jaringan internet agar stabil ketika digunakan oleh pengguna

D. KR04 (Script Lintas Situs) dimana kerentanan keamanan yang memungkinkan penyerang menempatkan script sisi klien ke halaman web (pemalsuan permintaan lintas situs) – Aset Software
   - Sisi organisasi : kontrol akses jaringan (9.4) menerapkan prosedur untuk memastikan bahwa layanan jaringan dan komputer yang dapat diakses oleh pengguna individu atau dari terminal tertentu konsisten dengan kebijakan kontrol akses bisnis.
   - Sisi keamanan : Persyaratan keamanan sistem (10.1) menerapkan standar untuk memastikan bahwa analisis persyaratan keamanan merupakan bagian dari tahap analisis persyaratan dari setiap proyek pengembangan, terutama dalam keamanan informasi pada proses pengembangan.
   - Sisi hukum: Kepatuhan terhadap persyaratan hukum (12.1) Menerapkan standar untuk memastikan bahwa semua persyaratan undang-undang, peraturan, dan kontrak yang relevan secara khusus ditentukan dan didokumentasikan untuk setiap sistem informasi.
   - Sisi teknik : memeriksa kembali script yang ada agar meminimalisir kerentanan keamanan yang memungkinkan penyerang menempatkan script sisi klien ke halaman web atau aplikasi yang ada.
E. KR05 (Bentuk HTML Tanpa Perlindungan CSRF) – Aset Software
   - Sisi organisasi : Forum keamanan informasi manajemen (4.1) membentuk komite perusahaan atau organisasi untuk mengawasi keamanan informasi, mengembangkan dan menerapkan pernyataan misi organisasi keamanan informasi, terutama dalam menerapkan antivirus.
   - Sisi keamanan : Persyaratan keamanan sistem (10.1) menerapkan standar untuk memastikan bahwa analisis persyaratan keamanan merupakan bagian dari tahap analisis persyaratan dari setiap proyek pengembangan, terutama dalam keamanan informasi pada proses pengembangan.
   - Sisi hukum: Kepatuhan terhadap persyaratan hukum (12.1) Menerapkan standar untuk memastikan bahwa semua persyaratan undang-undang,

peraturan, dan kontrak yang relevan secara khusus ditentukan dan didokumentasikan untuk setiap sistem informasi.

- Sisi teknik: hal ini bisa dicegah dengan cara yang pertama, keluar dari aplikasi web setelah selesai menggunakannya, hapus browser cookie secara berkala, yang kemungkinan akan meminimalisir serangan pemalsuan permintaan lintas situs by CSRF.

F. KR06 (Web Application Firewall Terdeteksi) – Aset Software
   - Sisi organisasi : Keamanan Akses Pihak ketiga (4.2) dengan menerapkan kebijakan keamanan informasi, mengembangkan dan menerapkan pernyataan misi organisasi keamanan informasi
   - Sisi keamanan : Memantau akses dan penggunaan sistem (9,7) menerapkan jejak audit yang mencatat pengecualian dan peristiwa terkait keamanan yang menciptakan dan memelihara penyelidikan dimasa mendatang dalam kontrol akses.
   - Sisi hukum: Kepatuhan terhadap persyaratan hukum (12.1) Menerapkan standar untuk memastikan bahwa semua persyaratan undang-undang, peraturan, dan kontrak yang relevan secara khusus ditentukan dan didokumentasikan untuk setiap sistem informasi.
   - Sisi teknik : memastikan bahwa firewall dinonaktifkan sebelum menginstall firewall pihak ketiga, yang kemudian langsung di cek status nya sudah aktif atau belum.

G. KR07 (Apache MOD Negotiation Bruteforcing Nama File) – Aset Software
   - Sisi organisasi : Forum keamanan informasi manajemen (4.1) membentuk komite perusahaan atau organisasi untuk mengawasi keamanan informasi, mengembangkan dan menerapkan pernyataan misi organisasi keamanan informasi, terutama dalam menerapkan antivirus.
   - Sisi keamanan : Persyaratan keamanan sistem (10.1) menerapkan standar untuk memastikan bahwa analisis persyaratan keamanan merupakan bagian dari tahap analisis persyaratan dari setiap proyek pengembangan, terutama dalam keamanan informasi pada proses pengembangan.
   - Sisi hukum: Kepatuhan terhadap persyaratan hukum (12.1) Menerapkan standar untuk memastikan bahwa semua persyaratan undang-undang, peraturan, dan kontrak yang relevan secara khusus ditentukan dan didokumentasikan untuk setiap sistem informasi.
   - Sisi Teknik : Buka file httpd.conf. · Langkah 2 – Ganti beberapa atribut. Langkah 3 – Buka file httpd-ssl.conf.

H. KR08 (ClickJacking : Header X-Frame-Options Hilang) – Aset Software
   - Sisi Organisasi : Memantau Akses dan penggunaan sistem (9.7) menerapkan jejak audit yang mencatat pengecualian dan peristiwa terkait keamanan yang menciptakan dan memelihara penyelidikan di masa mendatang dalam kontrol akses.
   - Sisi hukum : Tinjauan kebijakan keamanan dan kepatuhan teknis (12.2) Menerapkan standar untuk memastikan bahwa semua area dalam

organisasi dipertimbangkan untuk tinjauan rutin guna memastikan kepatuhan terhadap kebijakan dan standar keamanan terutama dalam memilih antivirus.

- Sisi Keamanan : Persyaratan keamanan sistem (10.1) menerapkan standar untuk memastikan bahwa analisis persyaratan keamanan merupakan bagian dari tahap analisis persyaratan dari setiap proyek pengembangan, terutama dalam pemilihan antivirus untuk aplikasi yang digunakan.
- Sisi Teknik : Mengamankan website dari clickjacking dengan menggunakan X-Frame Options. X-Frame-Options merupakan sebuah header program yang berfungsi sebagai pencegahan terhadap tindakan jahat clickjacking pada situs web.

I. KR09 (Cookie Tanpat Set Bendera HTTPOnly) – Aset Software
   - Sisi Organisasi : Klasifikasi Informasi (5.2) Menerapkan standar untuk klasifikasi keamanan dan tingkat perlindungan yang diperlukan untuk aset informasi
   - Sisi Teknik : dengan cara Gunakan Cookie Khusus HTTP memungkinkan Proksi Aplikasi untuk menyertakan bendera HTTPOnly di header response HTTP. Bendera ini memberikan manfaat keamanan tambahan, misalnya, mencegah skrip pihak klien (CSS) menyalin atau memodifikasi cookie.

J. KR10 (Cookie Tanpa Bendera Aman Disetel) – Aset Software
   - Sisi organisasi : keamanan dalam kontrak outsourcing (4.3) pastikan persyaratan keamanan pemilik informasi telah dibahas dalam kontrak antara pemilik dan organisasi outsourcing.
   - Sisi keamanan : keamanan file sistem (10.4) menerapkan standar untuk melakukan control keta tatas implementasi perangkat lunak pada sistem operasional.
   - Sisi hukum: Tinjauan kebijakan keamanan dan kepatuhan teknis (12.2) Menerapkan standar untuk memastikan bahwa semua area dalam organisasi dipertimbangkan untuk tinjauan rutin guna memastikan kepatuhan terhadap kebijakan dan standar keamanan.
   - Sisi teknik : menambahkan bendera Aman ke cookie melalui koneksi terenkripsi mengurangi terkena pencurian cookie melalui penyadapan

K. KR11 (Serangan Menebak Kata sandi Halaman Login) – Aset Software
   - Sisi organisasi : tanggung jawab pengguna (9.3) menyelenggarakan pelatihan pengguna untuk memastikan pengguna diberikan pemahaman dan praktek keamanan yang baik dalam menggunakan kata sandi.
   - Sisi keamanan : Kriptografi (10.3) Menerapkan kebijakan dan standar pengguna control kriptografi, termasuk pengelolaan kunci enkripsi, dan implementasi yang efektif.
   - Sisi hukum: Kepatuhan terhadap persyaratan hukum (12.1) Menerapkan standar untuk memastikan bahwa semua persyaratan undang-undang,

peraturan, dan kontrak yang relevan secara khusus ditentukan dan didokumentasikan untuk setiap sistem informasi.

- Sisi teknik : mengkombinasikan password huruf, angka, dan simbol, serta variasi huruf kapital. Selain itu, bekali perangkat keamanan seperti Imunify360 dan melakukan penggantian URL login dapat meminimalisir risiko situs menjadi target serangan brute force (meretas password).

L. KR12 (Kemungkinan Penimpaan Jalur Relative) – Aset Software

- Sisi organisasi : Keamanan akses pihak ketiga (4.2) Menerapkan proses untuk menganalisis risiko koneksi pihak ketiga dan menerapkan standar keamanan khusus untuk menerangi risiko koneksi pihak ketiga.
- Sisi keamanan : Kontrol akses sistem operasi (9.5) Menerapkan standar untuk identifikasi terminal otomatis untuk mengautentikasi koneksi ke lokasi tertentu.
- Sisi hukum: Kepatuhan terhadap persyaratan hukum (12.1) Menerapkan standar untuk memastikan bahwa semua persyaratan undang-undang, peraturan, dan kontrak yang relevan secara khusus ditentukan dan didokumentasikan untuk setiap sistem informasi.
- Sisi teknik : mengaktifkan traceability (keterbacaan), mengaplikasikan keamanan di seluruh lapisan, mengotomatiskan praktik terbaik keamanan, dan melindungi data baik in-transit maupun at rest

M. KR13 (Kemungkinan direktori sensitive) – Aset Software

- Sisi organisasi : Keamanan akses pihak ketiga (4.2) Menerapkan proses untuk menganalisis risiko koneksi pihak ketiga dan menerapkan standar keamanan khusus untuk menerangi risiko koneksi pihak ketiga.
- Sisi keamanan : Kriptografi (10.3) Menerapkan kebijakan dan standar pengguna control kriptografi, termasuk pengelolaan kunci enkripsi, dan implementasi yang efektif.
- Sisi hukum: Tinjauan kebijakan keamanan dan kepatuhan teknis (12.2) Menerapkan standar untuk memastikan bahwa semua area dalam organisasi dipertimbangkan untuk tinjauan rutin guna memastikan kepatuhan terhadap kebijakan dan standar keamanan.
- Sisi teknik : Menonaktifkan indeks direktori atau menyertakan file index.html yang kosong dapat mencegah bocornya isi file dalam direktori melalui file log.

N. KR14 (Waktu response lambat) – Aset Software

- Sisi organisasi : Kontrol akses jaringan (9.4) menerapkan prosedur untuk memastikan bahwa layanan jaringan dan komputer yang dapat diakses oleh pengguna individu atau dari terminal tertentu konsisten dengan kebijakan kontrol akses bisnis.
- Sisi keamanan : Keamanan dalam lingkungan pengembangan dan dukungan (10.5) Menerapkan standar dan prosedur untuk proses manajemen perubahan.

- Sisi hukum: Tinjauan kebijakan keamanan dan kepatuhan teknis (12.2) Menerapkan standar untuk memastikan bahwa semua area dalam organisasi dipertimbangkan untuk tinjauan rutin guna memastikan kepatuhan terhadap kebijakan dan standar keamanan.
- Sisi teknik : mengupgrade spesifikasi hosting ketingkat yang lebih tinggi sehingga permintaan pengunjung semua bisa dipenuhi

O. KR15 (Tautan rusak) – Aset Software
- Sisi organisasi : Kontrol akses jaringan (9.4) menerapkan prosedur untuk memastikan bahwa layanan jaringan dan komputer yang dapat diakses oleh pengguna individu atau dari terminal tertentu konsisten dengan kebijakan kontrol akses bisnis.
- Sisi keamanan : Keamanan dalam sistem aplikasi (10.2) Mengimplementasikan standar untuk memverifikasi keabsahan dan kesesuaian data yang dimasukkan ke dalam sistem aplikasi.
- Sisi hukum: Tinjauan kebijakan keamanan dan kepatuhan teknis (12.2) Menerapkan standar untuk memastikan bahwa semua area dalam organisasi dipertimbangkan untuk tinjauan rutin guna memastikan kepatuhan terhadap kebijakan dan standar keamanan.
- Sisi teknik : menggunakan Google Search Console untuk mendeteksi tautan yang rusak dan laporan Kesalahan Perayapan memungkinkan melihat semua halaman lalu memungkinkan memperbaiki tautan 404 ke Google.

P. KR16 (Alamat email ditemukan) – Aset Software
- Sisi organisasi : penilaian risiko (2) melakukan penilaian yang akurat dan menyeluruh atau potensi risiko dan kerentanan terhadap kerahasiaan, integritas, dan ketersediaan sumber daya informasi.
- Sisi keamanan : manajemen akses pengguna (9.2) menerapkan prosedur untuk pendaftaran pengguna dan akses deregistrasi ke semua layanan TI multiguna.
- Sisi hukum: Tinjauan kebijakan keamanan dan kepatuhan teknis (12.2) Menerapkan standar untuk memastikan bahwa semua area dalam organisasi dipertimbangkan untuk tinjauan rutin guna memastikan kepatuhan terhadap kebijakan dan standar keamanan.
- Sisi teknik : memperbarui sistem dapat mengakibatkan kesalahan sinkronisasi dan masalah lain yang berpotensi menyebabkan kehilangan sebagian email.

Q. KR17 (Pengungkapan versi server web halaman kesalahan) – Aset Software
- Sisi organisasi : penilaian risiko (2) melakukan penilaian yang akurat dan menyeluruh atau potensi risiko dan kerentanan terhadap kerahasiaan, integritas, dan ketersediaan sumber daya informasi.
- Sisi keamanan : Keamanan dalam sistem aplikasi (10.2) Mengimplementasikan standar untuk memverifikasi keabsahan dan kesesuaian data yang dimasukkan ke dalam sistem aplikasi..

- Sisi hukum: Tinjauan kebijakan keamanan dan kepatuhan teknis (12.2) Menerapkan standar untuk memastikan bahwa semua area dalam organisasi dipertimbangkan untuk tinjauan rutin guna memastikan kepatuhan terhadap kebijakan dan standar keamanan.
- Sisi teknik : melakukan redirect 301 atau redirect 302 agar kesalahan seperti 404 bisa dihindari

R. KR18 (Input jenis kata sandi dengan pelengkapan otomatis diaktifkan) – Aset Software
   - Sisi organisasi : Keamanan akses pihak ketiga (4.2) Menerapkan proses untuk menganalisis risiko koneksi pihak ketiga dan menerapkan standar keamanan khusus untuk menerangi risiko koneksi pihak ketiga.
   - Sisi keamanan : Kriptografi (10.3) Menerapkan kebijakan dan standar pengguna control kriptografi, termasuk pengelolaan kunci enkripsi, dan implementasi yang efektif.
   - Sisi hukum: Tinjauan kebijakan keamanan dan kepatuhan teknis (12.2) Menerapkan standar untuk memastikan bahwa semua area dalam organisasi dipertimbangkan untuk tinjauan rutin guna memastikan kepatuhan terhadap kebijakan dan standar keamanan.
   - Sisi teknik : otomatis membuat bidang teks username tidak menampilkan kata-kata yang sebelumnya diketik dalam drop down karena tidak ada atribut seperti nama, id untuk kolom input maka ia tidak akan mengirim parameter tambahan juga.

S. KR19 (Kerentanan terhadap fluktuasi voltase dan potensi hubungan arus pendek pada panel listrik, serta ketidakstabilan pasokan listrik.) – Aset Hardware
   - Sisi organisasi : kontrol akses jaringan (9.4) menerapkan prosedur untuk memastikan bahwa layanan jaringan dan komputer yang dapat diakses oleh pengguna individu atau dari terminal tertentu konsisten dengan kebijakan kontrol akses bisnis.
   - Sisi keamanan : Keamanan dalam lingkungan pengembangan dan dukungan (10.5) Menerapkan standar dan prosedur untuk proses manajemen perubahan.
   - Sisi Hukum: Tinjauan kebijakan keamanan dan kepatuhan teknis (12.2) Menerapkan standar untuk memastikan bahwa semua area dalam organisasi dipertimbangkan untuk tinjauan rutin guna memastikan kepatuhan terhadap kebijakan dan standar keamanan.
   - Sisiteknik : memiliki cadangan listrik yang memadai sehingga kendala server down bisa dihindari.

T. KR20 (Pertambahan memori yang cepat dalam pemrosesan data) – Aset Hardware
   - Sisi organisasi : penilaian risiko (2) melakukan penilaian yang akurat dan menyeluruh atau potensi risiko dan kerentanan terhadap kerahasiaan, integritas, dan ketersediaan sumber daya informasi.

- Sisi keamanan : Keamanan dalam lingkungan pengembangan dan dukungan (10.5) Menerapkan standar dan prosedur untuk proses manajemen perubahan.
- Sisi hukum: Tinjauan kebijakan keamanan dan kepatuhan teknis (12.2) Menerapkan standar untuk memastikan bahwa semua area dalam organisasi dipertimbangkan untuk tinjauan rutin guna memastikan kepatuhan terhadap kebijakan dan standar keamanan.
- Sisi teknik : mengupgrade spesifikasi memori ketingkat yang lebih tinggi sehingga permintaan pengunjung semua bisa cepat diproses.

U. KR21 (Kualitas jaringan yang kurang baik) – Aset Hardware
- Sisi organisasi : keamanan dalam kontrak outsourcing (4.3) pastikan persyaratan keamanan pemilik informasi telah dibahas dalam kontrak antara pemilik dan organisasi outsourcing.
- Sisi keamanan : Keamanan dalam lingkungan pengembangan dan dukungan (10.5) Menerapkan standar dan prosedur untuk proses manajemen perubahan.
- Sisi hukum: Tinjauan kebijakan keamanan dan kepatuhan teknis (12.2) Menerapkan standar untuk memastikan bahwa semua area dalam organisasi dipertimbangkan untuk tinjauan rutin guna memastikan kepatuhan terhadap kebijakan dan standar keamanan.
- Sisi teknik : Menginstal plugin cache untuk mengurangi penggunaan bandwidth dan meningkatkan kecepatan proses loading.

V. KR22 (Efek bencana alam dan kejadian-yang tidak terduga) – Aset Hardware
- Sisi organisasi : klasifikasi informasi (5.2) menerapkan standar untuk klasifikasi keamanan dan tingkat perlindungan yang diperlukan untuk aset informasi.
- Sisi keamanan : Memantau Akses dan penggunaan sistem (9.7) menerapkan jejak audit yang mencatat pengecualian dan peristiwa keamanan yang dihasilkan dan dipelihara untuk mendukung penyelidikan di masa depan.
- Sisi hukum: Tinjauan kebijakan keamanan dan kepatuhan teknis (12.2) Menerapkan standar untuk memastikan bahwa semua area dalam organisasi dipertimbangkan untuk tinjauan rutin guna memastikan kepatuhan terhadap kebijakan dan standar keamanan.
- Sisi teknik : Hot DRC merupakan tipe solusi bencana dengan cara mengatur operasional bisnis secepat mungkin menggunakan koneksi yang sudah dipasang dan tersedia di lokasi server DRC sehingga data bisnis atau perusahaan terus di backup secara berkelanjutan.

W. KR23 (Pustakawan kurang teliti) – Aset People
- Sisi organisasi : Forum keamanan informasi manajemen (4.1) membentuk komite perusahaan atau organisasi untuk mengawasi keamanan informasi, mengembangkan dan menerapkan pernyataan misi organisasi keamanan informasi.

- Sisi keamanan : control akses aplikasi (9.6) menerapkan prosedur untuk membatasi akses ke data dan fungsi sistem aplikasi sesuai kebijakan akses yang telah ditetapkan berdasarkan kebutuhan yang ada.
- Sisi hukum: Tinjauan kebijakan keamanan dan kepatuhan teknis (12.2) menerapkan standar untuk memastikan bahwa semua area dalam organisasi dipertimbangkan untuk tinjauan rutin guna memastikan kepatuhan terhadap kebijakan dan standar keamanan.
- Sisi teknik : melaksanakan pelatihan pustakawan untuk memastikan kompetensi dan praktik keamanan web berjalan dengan baik.

X. KR24 (Pelatihan terkait teknologi informasi tidak cukup) – Aset People

- Sisi organisasi : Forum keamanan informasi manajemen (4.1) membentuk komite perusahaan atau organisasi untuk mengawasi keamanan informasi, mengembangkan dan menerapkan pernyataan misi organisasi keamanan informasi.
- Sisi keamanan : Persyaratan keamanan sistem (10.1) menerapkan standar untuk memastikan bahwa analisis persyaratan keamanan merupakan bagian dari tahap analisis persyaratan dari setiap proyek pengembangan.
- Sisi hukum: Tinjauan kebijakan keamanan dan kepatuhan teknis (12.2) Menerapkan standar untuk memastikan bahwa semua area dalam organisasi dipertimbangkan untuk tinjauan rutin guna memastikan kepatuhan terhadap kebijakan dan standar keamanan.
- Sisi teknik : pemilihan SDM yang memiliki kompetensi TIK sehingga mampu menjalani praktik keamanan informasi

Kesimpulan

Dalam studi kasus penelitian ini yaitu pada web repository digital library perguruan tinggi X untuk menganalisis keamanan risiko dan mengidentifikasi potensi kerentanan dan ancaman yang dapat membahayakan kerahasiaan, integritas, dan ketersediaan aset digital yang tersimpan di dalam repository dengan menggunakan bantuan tools Acunetix kita bisa mengetahui kerentanan yang ada pada web repository dan untuk mitigasi risiko pada web repository digital library penelitian ini menggunakan standar framework ISO/IEC 27001 dan 27002 dengan menghasilkan tindakan mitigasi risiko yang harus dilakukan terhadap aset-aset yang ada pada web repository digital library seperti perguruan tinggi harus menetapkan kebijakan mengenai monitoring aset teknologi informasi, Monitoring dilakukan secara berkala untuk memastikan aset teknologi, untuk pengelolaan Database Management System (DBMS) seperti (MySQL, PostgreSQL, Oracle, Ms SQL Server) perguruan tinggi dapat dengan mudah mengakses dan menyimpan data informasi, dengan begitu perguruan tinggi dapat menerapkan rekomendasi dari penelitian yang sudah dilakukan pada pembahasan sebelumnya, jadi pengguna bisa dengan aman untuk menggunakan web repository digital library tanpa khawatir dengan keamanan informasinya.

Keterbatasan dalam penelitian ini adalah beberapa informasi yang belum dapat peneliti cantumkan karena bersifat rahasia untuk bisnis dari perguruan tinggi, jadi peneliti melakukan analisis dengan informasi yang bisa di publikasi, serta waktu yang peneliti gunakan cukup memakan waktu yang singkat sedangkan peneliti harus menganalisis secara detail mengenai web repository digital library perguruan tinggi X, jadi ada kemungkinan hasil tidak sesuai dengan harapan. Rekomendasi untuk penelitian selanjutnya, Upaya penelitian di masa depan dapat mengeksplorasi tantangan implementasi praktis dan faktor keberhasilan yang dihadapi oleh organisasi, terutama di sektor perguruan tinggi, ketika mengimplementasi/mengadopsi ISO/IEC 27001 dan 27002.

Referensi

Ahdi Anshori, F., & Reza Perdanakusuma, A. (2019). *Perencanaan Keamanan Informasi Berdasarkan Analisis Risiko Teknologi Informasi Menggunakan Metode OCTAVE dan ISO 27001 (Studi Kasus Bidang IT Kepolisian Daerah Banten)* (Vol. 3, Issue 2). http://j-ptiik.ub.ac.id

Ala, A. I. (2023). Penerapan IT Security Awareness Standar Keamanan ISO 27001 Di BPJS Ketenagakerjaan Kantor Cabang Purwakarta. *Jurnal Media Infotama*, *19*(1), 103–110.

Arifky Nanda Prasetya. (2019). *SISTEM REKOMENDASI PENILAIAN RISIKO KEAMANAN INFORMASI INFRASTRUKTUR TI DENGAN METODE RULE BASED REASONING DAN ISO27002:2013*. https://repository.uin-suska.ac.id/19925/

Candiwan, C., & Priyadi, Y. (n.d.). *Analysis of Information Security Audit Using at IT Division-X Company, In Bandung, Indonesia*. https://doi.org/10.13140/RG.2.1.1483.3044

David Purba, A., Ketut, I., Purnawan, A., Agus, P., & Pratama, E. (2018). Audit Keamanan TI Menggunakan Standar ISO/IEC 27002 dengan COBIT 5. *MERPATI*, *6*(DESEMBER).

Disterer, G. (2023). ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Jurnal Ilmiah Ekonomi Manajemen Akuntansi Dan Bisnis*, *2*(1), 119–125.

Fadilla, I., Sartika1, N., & Bisma2, R. (n.d.). Perancangan Sistem Informasi Manajemen Risiko berdasarkan ISO 27001:2013 (Sistem Manajemen Keamanan Informasi). *JEISBI*, *02*, 2021.

Fahrurozi, M, Tarigan, SA, Tanjung, MA, & ... (2020). The Use of ISO/IEC 27005: 2018 for Strengthening Information Security Management (A Case Study at Data and Information Center of Ministry of Defence). 2020 12th …, ieeexplore.ieee.org, <https://ieeexplore.ieee.org/abstract/document/9271748/>

Firdani, A., & Reza Perdanakusuma, A. (2019). *Perencanaan Pengelolaan Keamanan Informasi Berbasis ISO 27001 menggunakan Indeks KAMI Studi Kasus: Dinas Komunikasi dan Informatika Kabupaten Rembang* (Vol. 3, Issue 6). http://j-ptiik.ub.ac.id

Febrianto, F, & Sensuse, DI (2017). Evaluasi keamanan informasi menggunakan ISO/IEC 27002: studi kasus pada Stimik Tunas Bangsa Banjarnegara. Jurnal Ilmiah Infokam, amikjtc.com, <http://amikjtc.com/jurnal/index.php/jurnal/article/view/127>

Hermawan, W. (2019). Perancangan Manajemen Risiko Keamanan Informasi pada Penyelenggara Sertifikasi Elektronik (PSrE). *Jurnal Telekomunikasi Dan Komputer*, *9*(2), 129. https://doi.org/10.22441/incomtech.v9i2.6474

Mahersmi, B. L., Muqtadiroh, F. A., & Hidayanto, B. C. (2016). ANALISIS RISIKO KEAMANAN INFORMASI DENGAN MENGGUNAKAN METODE OCTAVE DAN KONTROL ISO 27001 PADA DISHUBKOMINFO KABUPATEN TULUNGAGUNG. *Seminar Nasional Sistem Informasi Indonesia*.

Nancylia, M, Mudjtabar, EK, Sutikno, S, & ... (2014). The measurement design of information security management system. 2014 8th …, ieeexplore.ieee.org, <https://ieeexplore.ieee.org/abstract/document/7065914/>

Putra, A. A., Nurhayati, O. D., & Windasari, I. P. (2016). Perencanaan dan implementasi information security management system menggunakan framework ISO/IEC 20071. *Jurnal Teknologi Dan Sistem Komputer*, *4*(1).

Putra, IMM, & Mutijarsa, K (2021). Designing information security risk management on bali regional police command center based on ISO 27005. 2021 3rd East Indonesia Conference …, ieeexplore.ieee.org, <https://ieeexplore.ieee.org/abstract/document/9431865/>

Risqi, A., & Nasution, S. (2021). Identifikasi Permasalahan Penelitian. In *ALACRITY : Journal Of Education* (Vol. 1, Issue 2). http://lpppipublishing.com/index.php/alacrity

Sari, M. K., Saintika, Y., & Prabowo, W. A. (2022). Penyusunan Manajemen Risiko Keamanan Informasi Dengan Standar ISO 27001 Studi Kasus Institut Teknologi Telkom Purwokerto. *Jurnal Sistem Dan Teknologi Informasi (JustIN)*, *10*(4), 423. https://doi.org/10.26418/justin.v10i4.48977

Sejati, DP Audit Security Information on Parts of Multimedia New Based on Standards Iso 27002: 2005 in Radio of the Republic of Indonesia Surabaya. neliti.com, <https://www.neliti.com/publications/448845/audit-security-information-on-parts-of-multimedia-new-based-on-standards-iso-270>

Sihwi, SW, Andriyanto, F, & ... (2016). An expert system for risk assessment of information system security based on ISO 27002. 2016 IEEE International …, ieeexplore.ieee.org, <https://ieeexplore.ieee.org/abstract/document/7802992/>

Soesanto, E, Kurniasih, F, Mutiara, P, & ... (2023). Sistem manajemen keamanan informasi dengan standar ISO/IEC 27001 dan ISO/ICE 27002 pada PT Jasa Marga. Co-Creation: Jurnal …, jurnal.arkainstitute.co.id, <https://jurnal.arkainstitute.co.id/index.php/co-creation/article/view/700>

Soesanto, E., Kurniasih, F., Mutiara, P., & Afifi, S. T. (2023). Sistem manajemen keamanan informasi dengan standar ISO/IEC 27001 dan ISO/ICE 27002 pada PT Jasa Marga. *Jurnal Ilmiah Ekonomi Manajemen Akuntansi Dan Bisnis*, *1*(4), 169–179. https://jurnal.arkainstitute.co.id/index.php/co-creation/index

Sukmaji, M, Yasirandi, R, & ... (2021). Information security policy and SOP as the access control document of PT. Jui Shin Indonesia Using ISO/IEC 27002: 2013. Jurnal Pilar Nusa …, ejournal.nusamandiri.ac.id, <https://ejournal.nusamandiri.ac.id/index.php/pilar/article/view/2282>

Wicaksono, B. B., & Papilaya, F. S. (2018). EVALUASI KEAMANAN INFORMASI BERDASARKAN ISO/IEC 27002: 2013 INFORMATION SECURITY MANAGEMENT SYSTEM (STUDI KASUS PERUSAHAAN XYZ). *Jurnal Teknologi Informasi*, 1–24.