

**SKRIPSI**

**AUDIT KEAMANAN SISTEM INFORMASI BADAN  
AMIL ZAKAT NASIONAL KABUPATEN BENGKALIS  
MENGUNAKAN STANDAR ISO 27001**

*Sebagai salah satu syarat untuk menyelesaikan studi di  
Program Studi Sarjana Terapanan Keamanan Sistem Informasi  
Jurusan Teknik Informatika*



**Oleh:**

**MHD. AZIZI**

6404201015

**JURUSAN TEKNIK INFORMATIKA  
POLITEKNIK NEGERI BENGKALIS**

**2024**

**HALAMAN PENGESAHAN**  
**SKRIPSI**  
**AUDIT KEAMANAN SISTEM INFORMASI BADAN**  
**AMIL ZAKAT NASIONAL KABUPATEN BENGKALIS**  
**MENGGUNAKAN STANDAR ISO 27001**


**Oleh :**  
**MHD. AZIZI**  
**6404201015**

Telah diujikan dan dinyatakan lulus ujian skripsi pada tanggal 15 Maret 2024 oleh tim penguji Program Studi Sarjana Terapan Keamanan Sistem Informasi

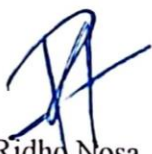
Pembimbing Utama

  
Kasmawi, M. Kom  
NIP. 197706072014041001

Bengkalis, 15 Maret 2024  
Anggota Tim Penguji

  
Darfani, M.Cs  
NIP. 198508122014041001

  
Rezki Kurniati, M. Kom  
NIP. 198306162018032001

  
M. Ridha Nosa, M. Kom  
NIP. 199109012022032006

Mengetahui,  
Ketua Jurusan Teknik Informatika



**KASMAWI, M. Kom**  
**NIP. 197706072014041001**

## PERNYATAAN KEASLIAN SKRIPSI

Saya Menyatakan dengan sesungguhnya bahwa Skripsi ini adalah asli hasil karya saya dan tidak terdapat karya yang pernah dilakukan untuk memperoleh gelar kesarjanaan di perguruan tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau dipublikasikan oleh orang lain, kecuali yang tertulis disebutkan sumbernya dalam naskah dan dalam daftar pustaka

Bengkalis, 15 Maret 2024



MHD. AZIZI

# **AUDIT KEAMANAN SISTEM INFORMASI BADAN AMIL ZAKAT NASIONAL KABUPATEN BENGKALIS MENGUNAKAN STANDAR ISO 27001**

Nama Mahasiswa : MHD. AZIZI  
NIM : 6404201015  
Dosen Pembimbing : Kasmawi, M. Kom

## **ABSTRAK**

Audit keamanan sistem informasi merupakan sebuah evaluasi menyeluruh terhadap infrastruktur IT dan kebijakan keamanan yang diterapkan oleh Badan Amil Zakat Nasional di Kabupaten Bengkalis. Audit ini dilakukan dengan merujuk pada standar ISO 27001, sebuah kerangka kerja internasional untuk manajemen keamanan informasi. Tujuan dari penelitian ini adalah untuk mengevaluasi sejauh mana Badan Amil Zakat Nasional Kabupaten Bengkalis mematuhi standar keamanan internasional, mengidentifikasi celah keamanan potensial, dan memberikan rekomendasi untuk meningkatkan keamanan sistem informasi mereka. Hasil audit menunjukkan bahwa Badan Amil Zakat Nasional Kabupaten Bengkalis telah mengimplementasikan sejumlah kontrol keamanan yang sesuai dengan standar ISO 27001, namun belum melibatkan dokumen formal yang terdokumentasi dengan jelas. Disarankan pada Badan Amil Zakat Nasional Kabupaten Bengkalis untuk membuat SOP/Prosedur tanggung jawab operasional, Perlindungan dari *Malware*, Cadangan (*Backup*), dan Pencatatan (*Logging*) dan Pemantauan. Gunanya adalah untuk menjamin kepatuhan organisasi terhadap standar ISO 27001 dengan mengatur langkah-langkah yang diperlukan untuk menerapkan kontrol keamanan, mengelola resiko, dan mematuhi kebijakan keamanan informasi.

*Kata kunci: Audit, Sistem, Informasi, Iso*

**AUDIT KEAMANAN SISTEM INFORMASI BADAN AMIL  
ZAKAT NASIONAL KABUPATEN BENGKALIS  
MENGUNAKAN STANDAR ISO 27001**

*Name of student* : MHD. AZIZI  
*Student ID Number* : 6404201015  
*Supervisor* :Kasmawi, M. Kom

***ABSTRACT***

*An information system security audit is a comprehensive evaluation of the IT infrastructure and security policies implemented by the National Amil Zakat Agency in Bengkalis Regency. This audit is conducted with reference to the ISO 27001 standard, an international framework for information security management. The purpose of this study is to evaluate the extent to which the National Amil Zakat Agency of Bengkalis Regency complies with international security standards, identify potential security gaps, and provide recommendations to improve the security of their information systems. The audit results show that the Bengkalis Regency National Amil Zakat Agency has implemented a number of security controls in accordance with the ISO 27001 standard, but has not involved formal, clearly documented documents. It is recommended that the Bengkalis Regency National Amil Zakat Agency create SOPs/Procedures for operational responsibility, Malware Protection, Backup, and Logging and Monitoring. The point is to ensure organizational compliance with the ISO 27001 standard by regulating the steps needed to implement security controls, manage risks, and comply with information security policies.*

*Keywords: Audit, System, Information, Iso*

## **KATA PENGANTAR**

Dengan rasa syukur yang mendalam, penulis mengucapkan terima kasih kepada Allah SWT atas limpahan rahmat dan karunia-Nya, sehingga skripsi ini dengan judul "Audit Keamanan Sistem Informasi Badan Amil Zakat Nasional Kabupaten Bengkalis Menggunakan Standar ISO 27001" dapat diselesaikan. Skripsi ini disusun sebagai salah satu syarat untuk memperoleh gelar Sarjana di Politeknik Negeri Bengkalis. Penulis menyadari bahwa proses penyusunan skripsi ini tidak lepas dari dukungan berbagai pihak. Oleh karena itu, penulis ingin menyampaikan rasa terima kasih yang sebesar-besarnya kepada

- Bapak Johny Custer, S.T, M.T selaku Direktur Politeknik Negeri BengkalisPak
- Kasmawi, M. Kom selaku dosen pembimbing yang telah memberikan arahan, bimbingan, dan motivasi yang sangat berharga selama proses penelitian dan penulisan skripsi ini.
- Seluruh Dosen Jurusan Teknik Informatika Politeknik Negeri Bengkalis yang telah mengajarkan banyak ilmu kepada penulis
- Badan Amil Zakat Nasional Kabupaten Bengkalis yang telah memberikan izin kepada peneliti untuk melakukan studi kasus audit sistem informasi ini
- Ibu dan ayah tercinta yang selalu memberikan doa, dukungan moral, dan materi yang tidak pernah putus.

Penulis menyadari bahwa skripsi ini masih memiliki kekurangan dan keterbatasan. Oleh karena itu, kritik dan saran yang membangun dari pembaca sangat diharapkan untuk perbaikan skripsi ini di masa depan. Semoga skripsi ini dapat bermanfaat bagi pembaca, khususnya dalam memahami penerapan standar ISO 27001 untuk meningkatkan keamanan sistem informasi pada Badan Amil Zakat Nasional Bengkalis.

Bengkalis, 15 Maret 2024

MHD. AZIZI

## DAFTAR ISI

	<b>Halaman</b>
<b>HALAMAN PENGESAHAN</b> .....	<b>i</b>
<b>HALAMAN PERNYATAAN</b> .....	<b>ii</b>
<b>ABSTRAK</b> .....	<b>iii</b>
<b>ABSTRACT</b> .....	<b>iv</b>
<b>KATA PENGANTAR</b> .....	<b>v</b>
<b>DAFTAR ISI</b> .....	<b>vi</b>
<b>DAFTAR GAMBAR</b> .....	<b>vii</b>
<b>DAFTAR TABEL</b> .....	<b>viii</b>
<b>BAB I PENDAHULUAN</b> .....	<b>1</b>
1.1 Latar Belakang .....	1
1.2 Permasalahan.....	2
1.3 Tujuan .....	2
1.4 Manfaat .....	2
1.5 Sistematika Penulisan .....	2
<b>BAB II KAJIAN PUSTAKA</b> .....	<b>4</b>
2.1 Deskripsi Permasalahan .....	4
2.2 Teori Penunjang .....	5
2.3 Penelitian Terkait .....	8
<b>BAB III DESKRIPSI SISTEM</b> .....	<b>13</b>
3.1 Deskripsi Solusi .....	13
3.2 Desain Sistem.....	15
<b>BAB IV EKSPERIMEN DAN HASIL</b> .....	<b>21</b>
4.1 Eksperimen.....	21
4.2 Hasil Eksperimen .....	34
<b>BAB V PENUTUP</b> .....	<b>42</b>
5.1 Kesimpulan .....	42
5.2 Saran.....	42
<b>DAFTAR PUSTAKA</b> .....	<b>43</b>

## DAFTAR GAMBAR

	<b>Halaman</b>
Gambar 3. 1 Desain Sistem.....	15
Gambar 3. 2 Lembar Pertanyaan Audit.....	17
Gambar 3. 3 Lembar Pertanyaan Audit.....	18
Gambar 4. 1 Lembar Kusioner.....	33
Gambar 4. 2 Lembar Kusioner.....	34
Gambar 4. 3 Lembar Kusioner.....	35
Gambar 4. 4 Panduan Pembayaran Zakat .....	36
Gambar 4. 5 Laporan Keuangan BAZNAS .....	37
Gambar 4. 6 Struktur organisasi BAZNAS.....	38
Gambar 4. 7 Dokumentasi Wawancara.....	39



## DAFTAR TABEL

	<b>Halaman</b>
Tabel 3. 1 <i>Maturity Level</i> .....	17
Tabel 3. 2 <i>Maturity Model</i> .....	19
Tabel 4. 1 A.12.1 Prosedur dan Tanggung Jawab Operasional .....	22
Tabel 4. 2 A.12.2 Perlindungan dari <i>Malware</i> .....	24
Tabel 4. 3 A.12.3 Cadangan ( <i>Backup</i> ) .....	26
Tabel 4. 4 A.12.4 Pencatatan ( <i>logging</i> ) dan Pemantauan .....	28
Tabel 4. 5 Rekapitulasi klausul keamanan sistem informasi pada BAZNAS Kabupaten Bengkalis .....	40

# **BAB I**

## **PENDAHULUAN**

### **1.1 Latar Belakang**

Badan Amil Zakat Nasional (BAZNAS) merupakan organisasi yang berperan dalam penghimpunan dan penyaluran zakat, infaq dan sedekah di Indonesia. BAZNAS Kabupaten Bengkalis adalah salah satu cabang atau perwakilan BAZNAS yang beroperasi di Kabupaten Bengkalis Provinsi Riau, Indonesia. Tugas utama BAZNAS adalah menghimpun dana dari masyarakat yang wajib menunaikan zakat, infaq dan sedekah, serta menjamin agar dana tersebut disalurkan ke pihak yang membutuhkan seperti fakir miskin, anak yatim piatu, dan orang-orang yang berada dalam keadaan sulit. BAZNAS Kabupaten Bengkalis memiliki sistem informasi yang digunakan untuk pengelolaan data donatur, untuk mengelola data penerima zakat, infaq dan sedekah, untuk mendistribusikan dana zakat kepada penerima manfaat sesuai dengan ketentuan dan peraturan yang berlaku dan lainnya. Dengan adanya sistem informasi ini maka perlu adanya Audit pada Sistem Informasi BAZNAS Kabupaten Bengkalis guna untuk mengidentifikasi dan mengevaluasi resiko keamanan yang mungkin terjadi dalam sistem informasi BAZNAS kabupaten bengkalis seperti ancaman dari pihak eksternal atau internal, kerentanan dalam infrastruktur TI, dan kelemahan dalam kebijakan keamanan.

Keamanan informasi menjadi sangat penting. Karena informasi adalah aset penting bagi perusahaan, informasi membantu perusahaan membuat keputusan. Hanya pihak internal perusahaan dan pihak yang berwenang terhadap informasi yang dapat mengaksesnya. Keamanan berarti menghindari hal-hal yang berbahaya. Akibatnya, keamanan sistem informasi dapat didefinisikan sebagai peraturan yang digunakan untuk mencegah akses yang tidak sah ke sistem informasi.[1]

*International Organization For Standardization (ISO) 27001* adalah sebuah standar yang mengatur manajemen keamanan informasi, yang bertindak sebagai panduan untuk pembuatan kebijakan keamanan dan prosedur terdokumentasi,

serta sebagai dasar penilaian terhadap risiko. Standar ini merupakan spesifikasi dari kerangka kerja manajemen keamanan sistem informasi, yang memberikan pedoman umum bagi perusahaan dalam mencapai dan merespons tantangan yang berkaitan dengan manajemen keamanan informasi. Sebelumnya, standar yang digunakan dalam konteks keamanan sistem informasi adalah ISO 17799.[1]

## **1.2 Permasalahan**

Belum Pernah dilakukannya audit keamanan pada sistem informasi BAZNAS Kabupaten Bengkalis, oleh sebab itu perlu dilakukan penelitian audit guna untuk mengukur tingkat keamanan sistem informasi di BAZNAS Kabupaten Bengkalis menggunakan standar ISO 27001 sehingga dapat diketahui sejauh mana tingkat level kematangan sistem informasi di BAZNAS, hasil dari audit ini dapat menjadi dasar untuk memberikan rekomendasi dalam meningkatkan keamanan sistem informasi di BAZNAS.

## **1.3 Tujuan**

Tujuan dilakukan penelitian audit pada sistem informasi BAZNAS menggunakan standar ISO 27001 adalah untuk menilai keamanan pada sistem informasi BAZNAS untuk mengetahui seberapa nilai tingkat level keamanan sistem informasi BAZNAS jika dilakukan audit menggunakan standar ISO 27001.

## **1.4 Manfaat**

Diharapkan dapat memberikan rekomendasi untuk meningkatkan keamanan pada sistem informasi BAZNAS Kabupaten Bengkalis dan juga menambah pengetahuan mengenai standar ISO 27001.

## **1.5 Sistematika Penulisan**

Jelaskan tentang sistematika pembahasan dalam buku proyek akhir yang meliputi:

**Bab I    Pendahuluan**

Pada Bab 1 berisi latar belakang, permasalahan tujuan, manfaat, dan juga sistematika penulisan.

**Bab II   Kajian Pustaka**

Pada Bab II berisi tentang bagian-bagian penting yang ada pada kajian pustaka.

**Bab III  Desain Sistem**

Pada Bab III menjelaskan tentang tahapan alur sistem yang dilakukan untuk audit sistem informasi menggunakan standar ISO 27001.

**Bab IV  Eksperimen dan Hasil**

Pada Bab IV ini berisi tentang proses dan hasil dari kegiatan yang dilakukan selama penelitian Audit Sistem Informasi BAZNAS Kabupaten Bengkalis Menggunakan ISO 27001.

**Bab V    Penutup**

Pada Bab V berisi kesimpulan, hasil, dan saran penelitian.

## **BAB II**

### **KAJIAN PUSTAKA**

BAZNAS Kabupaten Bengkalis adalah salah satu cabang atau perwakilan BAZNAS yang beroperasi di Kabupaten Bengkalis Provinsi Riau, Indonesia. Tugas utama BAZNAS adalah menghimpun dana dari masyarakat yang wajib menunaikan zakat, infaq dan sedekah, serta menjamin agar dana tersebut disalurkan ke pihak yang membutuhkan seperti fakir miskin, anak yatim piatu, dan orang-orang yang berada dalam keadaan sulit. BAZNAS Kabupaten Bengkalis memiliki sistem informasi yang digunakan untuk pengelolaan data donatur, untuk mengelola data penerima zakat, infaq dan sedekah, untuk mendistribusikan dana zakat kepada penerima manfaat sesuai dengan ketentuan dan peraturan yang berlaku dan lainnya. Dengan adanya sistem informasi ini maka perlu adanya Audit pada Sistem Informasi BAZNAS Kabupaten Bengkalis guna untuk mengukur tingkat keamanan sistem informasi di BAZNAS Kabupaten Bengkalis menggunakan standar ISO 27001 sehingga dapat diketahui sejauh mana tingkat level kematangan sistem informasi di BAZNAS, hasil dari audit ini dapat menjadi dasar untuk memberikan rekomendasi dalam meningkatkan keamanan sistem informasi di BAZNAS.

#### **2.1 Deskripsi Permasalahan**

Dengan adanya sistem informasi ini maka perlu adanya Audit pada Sistem Informasi BAZNAS Kabupaten Bengkalis guna untuk mengukur tingkat keamanan sistem informasi di BAZNAS Kabupaten Bengkalis menggunakan standar ISO 27001 sehingga dapat diketahui sejauh mana tingkat level kematangan sistem informasi di BAZNAS, hasil dari audit ini dapat menjadi dasar untuk memberikan rekomendasi dalam meningkatkan keamanan sistem informasi di BAZNAS.

## **2.2 Teori Penunjang**

### **2.2.1 Audit Sistem Informasi**

Audit sistem informasi adalah bentuk pengawasan dan pengendalian yang melibatkan evaluasi menyeluruh terhadap infrastruktur teknologi. Proses audit ini dapat dilakukan secara terpisah atau sebagai bagian dari audit laporan keuangan. Tujuan inti dari audit sistem informasi adalah mengevaluasi apakah pengendalian yang diterapkan pada sistem informasi memberikan keyakinan yang memadai atas:

1. Perlindungan Aset Aset dalam teknologi informasi mencakup berbagai elemen seperti perangkat lunak, perangkat keras, fasilitas TI, dokumentasi sistem, personil, data-file, dan perangkat lainnya. Tujuan perlindungan aset ini adalah untuk menilai sejauh mana TI dapat memberikan jaminan atas ketersediaan, integritas, dan kerahasiaan informasi.
2. Integritas data merupakan prinsip fundamental dalam audit sistem informasi. Integritas data mengacu pada kondisi di mana data memiliki atribut kelengkapan, keaslian, akurasi, dan dapat dipercaya. Kehadiran integritas data sangat penting karena informasi yang tidak terganggu memungkinkan organisasi untuk memberikan gambaran yang akurat tentang entitasnya. Namun, penting untuk diingat bahwa menjaga integritas data tidaklah gratis. Ada biaya yang terkait dengan upaya tersebut, dan diharapkan bahwa manfaat yang diperoleh sebanding dengan biaya yang dikeluarkan.
3. Keandalan Sistem Informasi diukur dari sejauh mana sistem tersebut berhasil mencapai tujuan organisasi. Sebelum mengukur efektivitas sistem, penting untuk memahami kebutuhan pengguna dan karakteristik mereka.
4. Efisiensi sistem informasi dapat diukur dari seberapa efisien sumber daya yang digunakan, termasuk mesin, perangkat lunak, sarana komunikasi, dan tenaga kerja yang terlibat dalam pengoperasian sistem, untuk menghasilkan output sesuai dengan kebutuhan dengan menggunakan sumber daya seminimal mungkin.[1]

### **2.2.2 Keamanan Sistem Informasi**

Keamanan sistem informasi melibatkan upaya perlindungan terhadap informasi dari berbagai ancaman yang dapat timbul, termasuk serangan siber, kebocoran data, dan pelanggaran keamanan lainnya. Hal ini dilakukan untuk memastikan kelancaran operasional bisnis, menjaga kepercayaan pelanggan, mematuhi regulasi yang berlaku, serta menghindari kerugian finansial dan reputasi. Dengan mengimplementasikan keamanan sistem informasi yang efektif, perusahaan dapat meminimalkan risiko bisnis, meningkatkan produktivitas karyawan, serta memaksimalkan potensi pengembalian investasi dan peluang bisnis yang ada.[2]

### **2.2.3 ISO/IEC 27001**

ISO/IEC 27001 merupakan standar yang umum digunakan untuk menilai persyaratan dalam menerapkan keamanan sistem informasi. Dengan menggunakan ISO/IEC 27001, dapat memastikan perlindungan terhadap aspek-aspek penting dari keamanan informasi, seperti kerahasiaan, integritas, dan ketersediaan data. ISO 27001 merupakan kerangka kerja standar internasional yang mencakup berbagai standar terkait keamanan informasi. ISO 27001 memberikan panduan dalam penggunaan teknologi dan manajemen aset untuk membantu organisasi memastikan efektivitas keamanan informasi. Ini termasuk aspek-aspek seperti kontrol akses data yang berkelanjutan, menjaga kerahasiaan, dan memastikan integritas informasi yang dimiliki oleh organisasi.

*International Organization for Standardization (ISO) 27001* merupakan suatu standar yang memberikan pedoman terkait keamanan informasi dalam skala internasional. Standar ini menetapkan kerangka kerja yang membantu organisasi untuk mengelola risiko keamanan informasi dengan lebih efektif. Dengan menerapkan ISO 27001, organisasi dapat memastikan bahwa sistem informasi mereka terlindungi dengan baik dari ancaman yang ada. Ini melibatkan proses evaluasi risiko, penerapan kontrol keamanan yang sesuai, serta langkah-langkah pemantauan dan pembaruan secara terus-menerus. ISO 27001 tidak hanya menekankan pentingnya teknologi dalam menjaga keamanan informasi, tetapi

juga fokus pada manajemen aset informasi secara menyeluruh. Ini mencakup kebijakan, prosedur, dan praktik yang dirancang untuk memastikan kerahasiaan, integritas, dan ketersediaan informasi yang diolah oleh organisasi. Dengan menerapkan standar ini, organisasi dapat meningkatkan kepercayaan pelanggan, mengurangi risiko kehilangan data sensitif, dan meningkatkan efisiensi operasional secara keseluruhan.[3]

ISO 27001 menyertakan 11 klausul kontrol keamanan, 39 objektif kontrol, dan 133 kontrol keamanan. Berikut adalah sebelas klausul kontrol keamanan yang termasuk di dalamnya:

1. Kebijakan keamanan informasi
2. Organisasi keamanan informasi
3. Manajemen aset
4. Sumber daya manusia menyangkut keamanan informasi
5. Keamanan fisik dan lingkungan
6. Komunikasi dan manajemen operasi
7. Akses control
8. Pengadaan/akuisisi, pengembangan dan pemeliharaan sistem informasi
9. Pengelolaan insiden keamanan informasi
10. Manajemen kelangsungan usaha (business continuity management)
11. Kepatuhan

#### **2.2.4 Maturity Level**

Penilaian tingkat kematangan menggunakan *SSE-CMM*, yang merupakan *Capability Maturity Model (CMM)* untuk *System Security Engineering (SSE)*. *CMM* merupakan suatu kerangka kerja yang digunakan untuk mengembangkan proses, baik yang bersifat informal maupun formal, termasuk proses teknis. Dalam penilaian ini, pembobotan didasarkan pada penilaian risiko. Dalam konteks SMKI, risiko merujuk pada hasil audit dan penilaian tingkat kematangan dari setiap kontrol keamanan. Dalam proses penilaian, dokumen wawancara diperoleh dari prosedur pembuatan pertanyaan yang didasarkan pada pernyataan sebelumnya. Bukti-bukti dan temuan audit diperoleh melalui wawancara dengan



perusahaan. Setelah didapatkan bukti dan temuan audit tersebut, dilakukan evaluasi dan analisis untuk menentukan nilai tingkat kemampuan dari masing-masing kontrol keamanan.[4]

### **2.3 Penelitian Terkait**

Beberapa penelitian terkait yang relevan dengan penelitian ini yaitu sebagai berikut:

“Audit Keamanan Sistem Informasi Pada Data Center Menggunakan Standar SNI-ISO 27001” Hasil penelitian menunjukkan perlunya data dan dokumentasi terhadap evaluasi akhir tingkat kematangan dari proses audit guna mengurangi resiko ancaman terhadap sistem informasi yang ditimbulkan, sehingga permasalahan dapat ditanggulangi dengan melakukan upaya-upaya yang dapat meminimalisir kemungkinan resiko yang telah ditimbulkan. Tahapan-tahapan auditing telah dilakukan pada sistem informasi pada data center dengan menggunakan standar SNI-ISO 27001 menghasilkan tingkat kematangan masih pada level *“repeatable but intuitive”* yaitu masih memerlukan pengawasan lebih lanjut dalam pengelolaan dari sisi keamanan. Manajemen keamanan sistem informasi sangatlah penting bagi institusi Pemerintah Aceh dalam pengelolaan aset informasi yang mengacu pada sebuah standar. Hal ini akan bisa berdampak negatif dari keberlangsungan layanan informasi khususnya layanan surat elektronik (email) yang dikelola oleh Dinas Komunikasi, Informasi dan Persandian Aceh. Sehingga perlunya tata kelola manajemen yang baik sesuai standar nasional maupun internasional agar terciptanya pengelolaan yang baik terhadap layanan sistem informasi surat elektronik dengan melakukan proses audit internal terhadap pengelolaannya dari sisi keamanan fisik dan lingkungan dimana sistem informasi layanan surat elektronik kelola . Penelitian ini membahas tentang “Audit Keamanan Sistem Informasi Pada Data Center Menggunakan Standar SNI-ISO 27001.[2]

“Audit Keamanan Sistem Informasi Akademik Sekolah Tinggi Farmasi Bandung Berbasis Risiko Dengan Menggunakan Standar ISO 27001” Berdasarkan hasil analisis risiko dalam penelitian ini, ditentukan 16 kontrol

objektif dan 57 kontrol keamanan yang tersebar dalam 4 klausul ISO 27001. Dari hasil audit dapat disimpulkan bahwa nilai tingkat kematangan tata kelola keamanan sistem informasi STFB adalah 2,5 yang berarti tingkat keamanan masih berada pada level 2 *planned and tracked* (sudah direncanakan dan dilacak secara aktif) namun telah mendekati level 3 *well defined* (telah didefinisikan dengan baik. Dengan dilakukannya audit berbasis risiko dengan menggunakan standar ISO 27001 di Sekolah Tinggi Farmasi Bandung (STFB). ISO 27001 adalah standar yang biasa digunakan untuk mengaudit keamanan sistem informasi sebuah perusahaan dan digunakan untuk menghasilkan dokumen (temuan dan rekomendasi) yang merupakan hasil dari audit keamanan sistem informasi perusahaan tersebut. Selain itu hasil audit juga akan menggambarkan tingkat kematangan (*Maturity Level*), tingkat kelengkapan penerapan SNI ISO/IEC 27001:2009 dan peta area tata kelola keamanan sistem informasi di Sekolah Tinggi Farmasi Bandung (STFB) dengan menggunakan *Capability Maturity Model for Integration (CMMI)*. [5]

“Audit Keamanan Sistem Informasi Manajemen Akademik dan Kemahasiswaan Menggunakan SNI ISO/IEC 27001:2013” (Studi Kasus STMIK Mardira Indonesia) SNI ISO/IEC 27001:2013 sebagai standar untuk mengaudit keamanan sebuah sistem informasi dan digunakan sebagai acuan untuk menghasilkan dokumen (temuan dan rekomendasi) yang merupakan hasil audit keamanan sistem informasi SIMAK di STMIK Mardira Indonesia. Dari hasil penelitian teridentifikasi bahwa klausul yang digunakan adalah, Klausul 5 : Kebijakan Keamanan (*Security Policy*) saat ini kebijakan keamanan SIMAK masih belum sesuai, Klausul 7 : Manajemen Aset (*Asset Management*) masih belum sesuai untuk mencapai dan memelihara perlindungan yang sesuai terhadap aset organisasi dikarenakan belum adanya surat kebijakan tentang pengelolaan aset, Klausul 9 : Kontrol Akses (*Access Control*) agar tidak terjadi penyalahgunaan hak akses serta adanya prosedur pengendalian hak akses, Klausul 15 : Kepatuhan (*Compliance*) belum disesuaikan dengan peraturan akademik yang berlaku, serta waktu yang telah dijadwalkan pada kalender pendidikan juga aspek legal software yang digunakan. Pengamatan terhadap SIMAK bahwa dalam

proses pengoperasian sistem masih mengalami hambatan seperti adanya kebocoran data yang mengakibatkan kinerja lembaga terganggu, belum cukup pengamanan dan pengendalian untuk mengantisipasi bentuk kecurangan dan tindakan ilegal yang mengakibatkan kerugian besar bagi para pemilik informasi serta hak akses tidak terkontrol, sehingga sebuah sistem informasi yang digunakan haruslah memiliki tingkat keamanan informasi yang terjamin, meliputi keamanan database, *hardware*, *software* dan sumber daya manusia.[6]

“Audit Keamanan Sistem Informasi Berdasarkan Standar ISO 27001 Pada PT. BPR JATIM” Hasil audit tingkat kematangan nilai keseluruhan sebesar 2,90 yang berarti bahwa kontrol keamanan berada pada level 2 *planned and tracked*, namun sudah mendekati level 3 *well defined* yang merupakan level yang diharapkan oleh perusahaan, sehingga perlu adanya peningkatan kontrol keamanan yang telah direkomendasikan. Manajemen keamanan informasi sangat penting bagi kantor pusat PT. BPR JATIM, karena semua laporan yang berasal dari kantor cabang di seluruh Jawa Timur akan dikirim ke pusat setiap harinya dan keamanan jaringan dalam pengiriman data memungkinkan terjadinya resiko kehilangan data-data rahasia perusahaan. Sistem Core Banking beroperasi secara online menggunakan server di vendor. Namun kantor pusat tetap mendapatkan laporan rutin dari kantor cabang yang tetap harus memiliki *backup* dan *recovery* data server. Mengingat pentingnya informasi, maka keamanan informasi harus mencakup prosedur untuk manajemen aset, manajemen sumber daya manajemen aset, manajemen sumber daya manusia, keamanan fisik dan lingkungan, keamanan logis, keamanan operasional dan teknologi informasi dalam penanganan insiden keamanan informasi.[4]

“Audit Sistem Informasi Berbasis ISO 27001 di Era New Normal” Hasil penelitian ini mengindikasikan adanya *strength*, *weakness*, *opportunity*, dan *threat* dari penggunaan audit sistem informasi berbasis ISO 27001. Strategi yang dapat dilakukan audit sistem informasi berbasis ISO 27001 adalah dengan melakukan perluasan penggunaan audit sistem informasi berbasis ISO 27001 di era new normal. Keamanan sistem informasi merupakan prosedur pencegahan akses yang tidak sah, oleh karena itu perusahaan berupaya meningkatkan keamanan sistem

informasi dengan mengimplementasikan ISO 27001. Keamanan sistem informasi berguna untuk menjaga kerahasiaan, ketersediaan, dan integritas.[1]

“Analisis Keamanan Sistem Informasi Universitas X” Penelitian ini bertujuan untuk memberikan informasi indeks keamanan sistem informasi Universitas X dari tingkat kematangan maupun tingkat kesiapannya. Hasil analisis menunjukkan bahwa tingkat kematangan keamanan sistem informasi Universitas X mencapai tingkat I+ s/d II+ sehingga belum memenuhi standar ISO 27001/SNI sesuai dengan Standar Sistem Manajemen Keamanan Informasi (Standar SMKI). Tingkat kesiapan sistem informasi Universitas X berada pada tingkat kesiapan pemenuhan kerangka kerja dasar. Penelitian ini menggunakan pendekatan kualitatif dengan pengolahan data Indeks KAMI. Pengumpulan data dilakukan melalui kuesioner dan wawancara yang dilakukan untuk konfirmasi dari kuesioner. Responden / narasumber penelitian ini berasal dari Lembaga X yang mengelola sistem informasi Universitas X, berjumlah 3 orang partisipan.[7]

“Evaluasi Keamanan Sistem Informasi PASDEAL Berdasarkan Indeks Keamanan Informasi (KAMI) ISO/IEC 27001:2013” Evaluasi dilakukan terhadap berbagai area yang menjadi target penerapan keamanan informasi berdasarkan standar ISO/IEC 27001:2013. Berdasarkan hasil penilaian indeks KAMI, diketahui bahwa Pasdeal mendapatkan skor 591 poin dari penerapan standar ISO 27001 dengan predikat cukup baik. Sistem informasi merupakan aset yang berharga bagi para pelaku bisnis, salah satunya yang bergerak di bidang e-commerce. Pasdeal merupakan distributor pulsa dan jasa server yang menerapkan sistem informasi *e-commerce*. Penggunaan sistem informasi dalam bidang penjualan atau perdagangan elektronik dinilai efisien karena telah menjadi platform media dan layanan serta kemampuan baru dan unik yang tidak ditemukan di dunia fisik. Faktor keamanan informasi merupakan aspek yang sangat penting untuk diperhatikan dalam mempertimbangkan kinerja tata kelola TIK. Untuk itu, sistem informasi memerlukan evaluasi keamanan informasi agar dapat mengetahui celah dan kekurangan keamanan informasi yang ada pada sistem informasi tersebut.[8]

“Audit Keamanan Sistem Informasi Akademik Stikes Jendral Achmad Yani Menggunakan SNI ISO/IEC 27001:2013” Hasil dari audit kepatuhan terhadap ISO/IEC 27001:2013 dengan rumus jumlah pertanyaan yang sesuai dengan penerapan ISO/IEC 27001:2013 dibagi dengan total jumlah soal yang diberikan pada auditee. Klausul keamanan sumber daya manusia dengan nilai 14,3 % , klausul keamanan kendali akses dengan nilai 33.3 % , klausul keamanan fisik dan lingkungan dengan nilai 46.6 % , klausul keamanan operasional dengan nilai 26.6 % , dan klausul keamanan komunikasi dengan nilai 66.6 % . Untuk melakukan perbaikan dilakukan perancangan kontrol keamanan sistem informasi akademik yang nilainya dibawah 50 % , dengan membuat kebijakan, prosedur dan formulir sehingga didapatkan kontrol keamanan yang lebih baik. Sistem informasi akademik yang ada di STIKES (Sekolah Tinggi Ilmu Kesehatan) telah diimplementasikan dan digunakan untuk memudahkan dalam mengelola akademik. Kurangnya kesadaran keamanan informasi pengguna, pengelolaan hak akses yang tepat, pemeliharaan keamanan jaringan, keamanan fisik dan operasional menyebabkan resiko terganggunya sistem informasi akademik oleh orang yang tidak bertanggung jawab. Untuk melihat kelemahan-kelemahan yang ada pada sistem informasi akademik harus dilakukan audit dengan menggunakan standar ISO/IEC 27001:2013.[9]

“Analisis Keamanan Sistem Informasi Penjualan Pada PT ARTA BOGA CEMERLANG Cabang Kediri Dengan Menggunakan Standar ISO 27001:2013” Hasilnya menunjukkan bahwa perusahaan memiliki kebijakan keamanan informasi yang mendukung penjualan, melindungi data pelanggan, mengelola aset informasi, mengatur akses sistem, dan menangani insiden keamanan. PT Arta Boga Cemerlang juga disarankan untuk mengadopsi standar global seperti ISO 27001:2013 dan memperbarui kebijakan dan prosedur keamanan informasi secara teratur. Dengan melakukan itu, perusahaan dapat menjaga kerahasiaan, integritas, dan ketersediaan data pelanggan, serta meningkatkan kepercayaan dan kepuasan pelanggan dalam proses penjualan.[10]

## **BAB III**

### **DESKRIPSI SISTEM**

#### **3.1 Deskripsi Solusi**

Deskripsi solusi dari keamanan sistem informasi di BAZNAS Kabupaten Bengkalis meliputi Penelitian Lapangan, Evaluasi Tingkat Keamanan Sistem Informasi, Standar ISO 27001, *Maturity Level*, Hasil Rekomendasi adalah sebagai berikut:

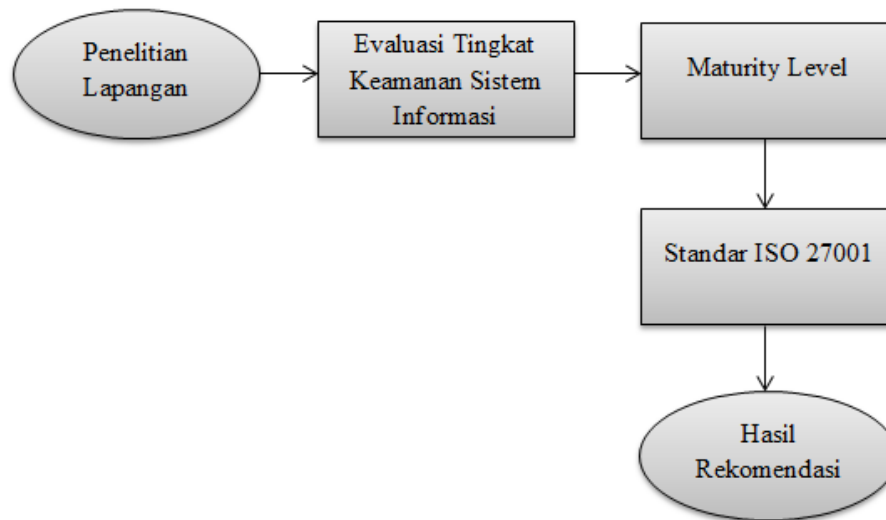
1. BAZNAS Kabupaten Bengkalis Sebagai sebuah lembaga yang mengelola zakat, BAZNAS harus menjaga keamanan data pribadi yang dimiliki. Umumnya data pribadi yang ada di sistem informasi BAZNAS termasuk Nama lengkap individu atau nama perusahaan, Nomor identitas pribadi, seperti Nomor Induk Kependudukan, Alamat tempat tinggal atau alamat perusahaan, Nomor telepon dan alamat email, Informasi keuangan, termasuk detail transaksi zakat.
2. Penelitian Lapangan: Penelitian lapangan merupakan langkah awal yang sangat penting dalam proses audit keamanan sistem informasi. auditor akan melakukan survei dan penelitian secara langsung di lingkungan Baznas. Auditor akan mengumpulkan data tentang sistem informasi yang digunakan, penelitian ini juga akan mencakup peninjauan terhadap kebijakan keamanan yang telah ditetapkan oleh BAZNAS, termasuk praktik pengelolaan risiko dan kepatuhan terhadap regulasi terkait.
3. Evaluasi Tingkat Keamanan Sistem Informasi: Evaluasi ini melibatkan analisis mendalam terhadap keamanan sistem informasi BAZNAS. Auditor akan menilai efektivitas dari kontrol keamanan yang telah diterapkan, serta mengidentifikasi potensi celah keamanan yang mungkin ada. Auditor akan memeriksa apakah kontrol keamanan tersebut memadai untuk melindungi data sensitif dan menjaga integritas sistem informasi.
4. Standar ISO 27001: Audit keamanan sistem informasi BAZNAS akan mengacu pada standar ISO 27001, yang merupakan kerangka kerja internasional untuk manajemen keamanan informasi. Auditor akan

mengevaluasi sejauh mana BAZNAS mematuhi persyaratan ISO 27001 dan apakah sistem keamanan mereka sudah sejalan dengan standar ini. Auditor akan memeriksa implementasi kontrol keamanan yang disarankan oleh standar ISO 27001, serta langkah-langkah yang diambil untuk memastikan keamanan informasi secara keseluruhan.

5. *Maturity Level*: Penilaian *maturity level* merupakan aspek penting dalam audit keamanan sistem informasi. Tim auditor akan menilai seberapa matang atau sejauh mana sistem keamanan informasi Baznas telah berkembang dan diintegrasikan dalam organisasi. Auditor akan mempertimbangkan faktor-faktor seperti kebijakan keamanan, proses operasional, pemantauan dan pengukuran kinerja keamanan, serta kesiapan organisasi dalam menghadapi ancaman keamanan yang kompleks.
6. Hasil Rekomendasi: Berdasarkan temuan dari penelitian, evaluasi, dan penilaian, tim auditor akan menyusun hasil rekomendasi. Rekomendasi ini akan mencakup saran-saran perbaikan yang dapat diimplementasikan oleh Baznas untuk meningkatkan keamanan sistem informasi mereka. Rekomendasi ini dapat berupa perbaikan kebijakan, peningkatan kontrol keamanan, pelatihan bagi staf, atau pengembangan infrastruktur IT. Setiap rekomendasi haruslah disusun secara spesifik, terukur, dapat dicapai, relevan, dan berbatas waktu.

### 3.2 Desain Sistem

Berikut adalah desain sistem dan penjelasan dari penelitian Audit Keamanan Sistem Informasi Baznas Kabupaten Bengkalis Menggunakan Standar ISO 27001:



**Gambar 3. 1** Desain Sistem

1. **Penelitian Lapangan:** Tahap awal dalam audit keamanan sistem informasi Baznas adalah melakukan penelitian lapangan secara menyeluruh. Ini melibatkan tim auditor yang melakukan survei langsung di lingkungan BAZNAS. Mengumpulkan data tentang infrastruktur IT, sistem informasi yang digunakan, serta proses bisnis yang terlibat. Tujuan dari penelitian ini adalah untuk mendapatkan pemahaman yang komprehensif tentang keadaan aktual keamanan sistem informasi BAZNAS.
2. **Evaluasi Tingkat Keamanan Sistem Informasi:** Evaluasi ini adalah langkah berikutnya setelah penelitian lapangan. Tim auditor akan menganalisis secara menyeluruh tingkat keamanan sistem informasi BAZNAS. Mereka akan menilai efektivitas dari kontrol keamanan yang telah diterapkan dan mengidentifikasi area-area yang memerlukan perbaikan. Evaluasi ini bertujuan untuk memastikan bahwa sistem informasi BAZNAS dapat melindungi data sensitif dan menjaga keandalan operasionalnya.



3. Standar *ISO 27001*: Audit keamanan sistem informasi BAZNAS didasarkan pada standar *ISO 27001*, sebuah kerangka kerja internasional untuk manajemen keamanan informasi. auditor akan menilai sejauh mana BAZNAS mematuhi persyaratan standar ini dan apakah sistem keamanan mereka sesuai dengan standar internasional tersebut. Hal ini membantu BAZNAS dalam memastikan bahwa sistem keamanan mereka memenuhi standar terkini dan terbaik dalam industri.
4. *Maturity Level*: Penilaian *maturity level* merupakan aspek penting dalam audit keamanan sistem informasi. Tim auditor akan mengevaluasi seberapa matang atau sejauh mana sistem keamanan informasi BAZNAS telah berkembang dan terintegrasi dalam organisasi. Mereka akan mempertimbangkan faktor-faktor seperti kebijakan keamanan, proses operasional, pemantauan kinerja keamanan, serta kesiapan Baznas dalam menghadapi ancaman keamanan yang semakin kompleks.
5. Hasil Rekomendasi: Berdasarkan temuan dari penelitian dan evaluasi, tim auditor akan menyusun hasil rekomendasi. Rekomendasi ini akan berisi saran-saran perbaikan yang dapat diimplementasikan oleh BAZNAS untuk meningkatkan keamanan sistem informasi mereka. Setiap rekomendasi akan dirancang untuk memperbaiki kelemahan yang ditemukan dalam audit, memastikan kepatuhan dengan standar keamanan yang relevan, dan meningkatkan kematangan sistem keamanan informasi secara keseluruhan.

Berikut adalah gambar lembar pertanyaan audit keamanan sistem informasi BAZNAS Kabupaten Bengkulu, yang terdiri dari 4 subklausul. Subklausul A.12.1 Prosedur dan Tanggung Jawab Operasional, A.12.2 Perlindungan dari Malware, A.12.3 Cadangan (*Backup*), A.12.4 Pencatatan (*logging*) dan Pemantauan:

**LEMBAR PERTANYAAN AUDIT ISO 27001**

Klausul A12 Keamanan Operasi

A.12.1 Prosedur dan Tanggung Jawab Operasional

Question	
1	Apakah prosedur operasional untuk mengelola sistem informasi sudah didokumentasikan?
2	Jika ada, apakah prosedur operasional tersebut tersedia untuk semua pengguna yang membutuhkan?
3	Apakah perubahan terhadap organisasi, proses bisnis, fasilitas pengolahan informasi dan sistem dapat mempengaruhi keamanan informasi?
4	Apakah perubahan yang terjadi dapat dikendalikan?
5	Apakah ada pemantauan penggunaan sumber daya untuk kebutuhan kapasitas dimasa mendatang?
6	Apakah ada langkah-langkah yang diambil untuk mengatur dan memastikan penggunaan sumberdaya sesuai kapasitas sistem yang dibutuhkan?
7	Apakah lingkungan pengembangan, pengujian, dan operasional harus dipisahkan untuk mengurangi resiko yang tidak sah pada lingkungan operasional?
8	apakah pemisahan lingkungan dilakukan secara efektif untuk menghindari gangguan tidak sah?

A.12.2 Perlindungan dari Malware

Question	
1	Apakah ada kendali deteksi, pencegahan, dan pemulihan untuk melindungi terhadap malware?
2	Apakah kendali tersebut sudah diimplementasikan dan melindungi pengguna dari serangan malware?
3	Apakah kendali yang diambil efektif dalam mendeteksi malware?
4	Apakah pengguna berperan penting dalam upaya pencegahan malware?

Gambar 3. 2 Lembar Pertanyaan Audit

A.12.3 Cadangan (*Backup*)

Question	
1	Apakah ada salinan cadangan informasi, perangkat lunak dan image sistem?
2	apakah salinan tersebut perlu diambil dan diuji secara berkala?
3	Apakah ada kebijakan mengenai salinan cadangan? Jika ada, apakah salinan cadangan tersebut sudah disetujui dan diterapkan?

A.12.4 Pencatatan (*Logging*) dan Pemantauan

Question	
1	Apakah ada pencatatan kejadian aktivitas pengguna, pengecualian, kegagalan dan kejadian keamanan informasi?
2	Apakah catatan kejadian sudah direkam dengan benar?
3	Apakah kejadian tersebut disimpan dan direview secara berkala?
4	Apakah ada pencatatan log dan informasi log yang harus dilindungi?
5	Apakah log harus dilindungi dari pemalsuan dan akses tidak berwenang?
6	Apakah ada langkah-langkah yang diambil untuk mencegah manipulasi atau modifikasi terhadap log sistem?
7	Apakah ada pencatatan aktivitas administrator sistem dan operator sistem?
8	Apakah pencatatan tersebut dilindungi dan direview secara berkala?
9	Apakah ada langkah yang diambil untuk memastikan administrator dan operator menjalankan tugas dengan baik?
10	Apakah ada penjamin bahwa waktu dari semua sistem pengelolaan informasi yang terkait dalam organisasi atau wilayah di sinkronkan ke sumber waktu acuan tunggal?
11	Apakah ada cara khusus untuk menentukan sinkronisasi waktu yang akurat di seluruh sistem?

Gambar 3. 3 Lembar Pertanyaan Audit

**Tabel 3. 1 Maturity Level**

<i>Maturity Index</i>	<i>Maturity Level</i>
0 – 0.49	0 – <i>Non Existent</i>
0.51 – 1.50	1 – <i>Initial/Adhoc</i>
1.51 – 2.50	2 – <i>Repeatable But Intutive</i>
2.51 – 3.50	3 – <i>Defined Process</i>
3.51 – 4.50	4 – <i>Managed and Measurable</i>
4.51 – 5.00	5 - <i>Optimized</i>

**Tabel 3. 2 Maturity Model**

<i>Level</i>	<i>Deskripsi</i>
0 ( <i>Non Existent</i> )	Belum adanya permasalahan yang harus diatasi. Perusahaan merasa tidak membutuhkan mekanisme proses keamanan. Sehingga tidak ada pengawasan sama sekali.
1 ( <i>Initial/ Ad Hoc</i> )	Sudah adanya bukti bahwa perusahaan mengetahui adanya permasalahan yang harus diatasi. Perusahaan sudah memiliki inisiatif untuk melakukan keamanan. Namun sifatnya masih non formal.
2 ( <i>Repeatable but Intuitive</i> )	Sudah adanya perencanaan, pengelolaan, dan implementasi sistem berbasis komputer yang lebih terarah. Perusahaan memiliki kebiasaan terpola untuk merencanakan keamanan yang dilakukan secara berulang namun belum melibatkan dokumen formal.
3 ( <i>Defined Process</i> )	Sudah memiliki proses keamanan yang sudah didokumentasikan dengan baik kemudian dikomunikasikan melalui pelatihan. Perusahaan juga menyadari perlunya proses keamanan sehingga adanya aturan yang menunjukkan untuk perusahaan secara rutin melakukan keamanan.
4 ( <i>Managed and Measurable</i> )	Sudah adanya proses komputerisasi dengan baik, pengembangan sistem sudah terarah dan dijalankan secara terorganisir. Proses keamanan sudah secara formal dilakukan dan secara terus menerus dievaluasi untuk meningkatkan layanan perusahaan.
5 ( <i>Optimised</i> )	Sudah mengikuti best practice yang ditandai dengan adanya proses otomatisasi pada sistem dengan metodologi yang tepat.

$$\text{Index Maturity} = \frac{\text{Jumlah pertanyaan yang dijawab}}{\text{jumlah pertanyaan klausul}} * 100\%$$

Berikut pada rumus diatas menjelaskan bagaimana cara untuk mengetahui tingkat kematangan klausul, yaitu dengan cara menjumlahkan score pertanyaan yang dijawab oleh responden, lalu dibagi dengan total pertanyaan. Dengan memakai rumus perhitungan klausul ini maka kita dapat mengetahui sejauh mana level tingkat kematangan dari sistem informasi BAZNAS Kabupaten Bengkalis.

## **BAB IV**

### **EKSPERIMEN DAN HASIL**

#### **4.1 Eksperimen**

*International Organization for Standardization (ISO) 27001* adalah standar internasional yang mengatur sistem manajemen keamanan informasi (*Information Security Management System/ISMS*). Standar ini dirancang untuk membantu organisasi atau perusahaan dalam mengelola risiko keamanan informasi dengan cara sistematis dan terstruktur. ISO 27001 mencakup kontrol yang berupa kebijakan, proses, prosedur, struktur organisasi, dan fungsi-fungsi infrastruktur TI. Tujuan dari ISO 27001 adalah untuk memastikan organisasi memiliki kontrol yang tepat terkait keamanan informasi, menunjukkan tata kelola yang baik dalam penanganan dan pengamanan informasi, dan memberikan mekanisme untuk mengukur berhasil atau tidaknya kontrol pengamanan. ISO 27001 juga memberikan panduan untuk organisasi atau perusahaan untuk mengatur dan mengelola risiko keamanan informasi. Standar ini mencakup aspek-aspek yang penting seperti kontrol akses, kontrol perangkat lunak, kontrol data, kontrol fisik, kontrol operasi, kontrol perangkat lunak, kontrol perangkat lunak, kontrol perangkat lunak, dan kontrol perangkat lunak. ISO 27001 juga menyediakan langkah-langkah untuk mengukur dan mengendalikan risiko keamanan informasi, serta mengatur tata kelola untuk mengelola keamanan informasi dalam organisasi.

ISO 27001 juga menyediakan langkah-langkah untuk mengukur dan mengendalikan risiko keamanan informasi, serta mengatur tata kelola untuk mengelola keamanan informasi dalam organisasi. Standar ini memiliki berbagai keuntungan, seperti mengurangi risiko keamanan informasi, memperbaiki tata kelola, memperjelas tata kelola, memperjelas tata kelola, memperjelas tata kelola, dan memperjelas tata kelola. ISO 27001 juga memiliki sertifikasi, yang memungkinkan organisasi atau perusahaan untuk memperoleh sertifikat ISO 27001 jika mereka memenuhi persyaratan standar ini. Sertifikasi ini dapat membantu organisasi atau perusahaan memperjelas tata kelola keamanan

informasi, memperjelas tata kelola keamanan informasi, dan memperjelas tata kelola keamanan informasi. ISO/IEC 27001 mempunyai 14 klausul kontrol keamana 35 objektif kontrol dan 144 kontrol.

Berikut data hasil penelitian yang terdiri dari uji keamanan klausul yang digunakan:

#### A.12 Keamanan Operasi

**Tabel 4. 1** A.12.1 Prosedur dan Tanggung Jawab Operasional

Pertanyaan	Jawaban	Skor	Maturity
Apakah prosedur operasional untuk mengelola sistem informasi sudah didokumentasikan?	Iya, sudah	3	<i>(Defined Process)</i> Sudah memiliki proses keamanan yang sudah didokumentasikan dengan baik kemudian dikomunikasikan melalui pelatihan. Perusahaan juga menyadari perlunya proses keamanan sehingga adanya aturan yang menunjukkan untuk perusahaan secara rutin melakukan keamanan.
Jika ada, apakah prosedur operasional tersebut tersedia untuk semua pengguna yang membutuhkan?	Tersedia, contohnya tatacara pembayaran zakat online di BAZNAS tersedia pada halaman website	3	<i>(Defined Process)</i> Sudah memiliki proses keamanan yang sudah didokumentasikan dengan baik kemudian dikomunikasikan melalui pelatihan. Perusahaan juga menyadari perlunya proses keamanan sehingga adanya aturan yang menunjukkan untuk perusahaan secara rutin melakukan keamanan.

Apakah perubahan terhadap organisasi, proses bisnis, fasilitas pengolahan informasi dan sistem dapat mempengaruhi keamanan informasi?	Iya	2	<i>(Repeatable but Intuitive)</i> Sudah adanya perencanaan, pengelolaan, dan implementasi sistem berbasis komputer yang lebih terarah. Perusahaan memiliki kebiasaan terpolat untuk merencanakan keamanan yang dilakukan secara berulang namun belum melibatkan dokumen formal.
Apakah perubahan yang terjadi dapat dikendalikan?	Iya	2	<i>(Repeatable but Intuitive)</i> Sudah adanya perencanaan, pengelolaan, dan implementasi sistem berbasis komputer yang lebih terarah. Perusahaan memiliki kebiasaan terpolat untuk merencanakan keamanan yang dilakukan secara berulang namun belum melibatkan dokumen formal.
Apakah ada pemantauan penggunaan sumber daya untuk kebutuhan kapasitas dimasa mendatang?	Belum ada	0	<i>(Non Existent)</i> Belum adanya permasalahan yang harus diatasi. Perusahaan merasa tidak membutuhkan mekanisme proses keamanan. Sehingga tidak ada pengawasan sama sekali.
Apakah ada langkah-langkah yang diambil untuk mengatur dan memastikan penggunaan sumberdaya sesuai kapasitas sistem yang dibutuhkan?	Melakukan analisa terkait kebutuhan sistem	2	<i>(Repeatable but Intuitive)</i> Sudah adanya perencanaan, pengelolaan, dan implementasi sistem berbasis komputer yang lebih terarah. Perusahaan memiliki kebiasaan terpolat untuk merencanakan keamanan



			yang dilakukan secara berulang namun belum melibatkan dokumen formal.
Apakah lingkungan pengembangan, pengujian, dan operasional harus dipisahkan untuk mengurangi resiko yang tidak sah pada lingkungan operasional?	Harusnya iya	2	<i>(Repeatable but Intuitive)</i> Sudah adanya perencanaan, pengelolaan, dan implementasi sistem berbasis komputer yang lebih terarah. Perusahaan memiliki kebiasaan terpola untuk merencanakan keamanan yang dilakukan secara berulang namun belum melibatkan dokumen formal.
apakah pemisahan lingkungan dilakukan secara efektif untuk menghindari gangguan tidak sah?	Untuk sekarang belum ada dilakukan	0	<i>(Non Existent)</i> Belum adanya permasalahan yang harus diatasi. Perusahaan merasa tidak membutuhkan mekanisme proses keamanan. Sehingga tidak ada pengawasan sama sekali.
<b>Score Maturity</b>	<b>1,75</b>		
<b>Index</b>	<b><i>Repeatable but Intuitive</i></b>		

Dari hasil pengujian klausul A.12 Keamanan Operasi Prosedur dan Tanggung Jawab Operasional, dapat kita ketahui bahwa jumlah kebijakan keamanan operasi memiliki indeks maturity level **1,75** berikut rumus untuk mencari score maturity

$$\text{Index Maturity} = \frac{14}{8} * 100\%$$

8

Hasil penjumlahan untuk score pertanyaan yang dijawab ialah 14 kemudian di bagi dengan 8. 8 ialah banyaknya jumlah pertanyaan klausul maka dapatlah hasilnya **1,75** kemudian di kali 100% untuk mengalikan hasil pembagian dengan

100% cukup mengalikan hasil pembagian dengan 1 atau 100\* dalam bentuk desimal yaitu 1. Langkah ini tidak akan mengubah nilai dari hasil pembagian sebelumnya, karena mengalikan dengan satu akan mendapatkan nilai yang sama.

**Tabel 4. 2** A.12.2 Perlindungan dari Malware

<b>Pertanyaan</b>	<b>Jawaban</b>	<b>Skor</b>	<b>Maturity</b>
Apakah ada kendali deteksi, pencegahan, dan pemulihan untuk melindungi terhadap malware?	Ada	2	<i>(Repeatable But Intutive)</i> Sudah adanya perencanaan, pengelolaan, dan implementasi sistem berbasis komputer yang lebih terarah. Perusahaan memiliki kebiasaan terpola untuk merencanakan keamanan yang dilakukan secara berulang namun belum melibatkan dokumen formal.
Apakah kendali tersebut sudah diimplementasikan dan melindungi pengguna dari serangan malware?	Iya, kendali yang sudah diterapkan berupa pemasangan anti virus	2	<i>(Repeatable But Intutive)</i> Sudah adanya perencanaan, pengelolaan, dan implementasi sistem berbasis komputer yang lebih terarah. Perusahaan memiliki kebiasaan terpola untuk merencanakan keamanan yang dilakukan secara berulang namun belum melibatkan dokumen formal.
Apakah kendali yang diambil efektif dalam mendeteksi malware?	Untuk sekarang efektif, karena belum pernah terjadinya serangan dari	2	<i>(Repeatable But Intutive)</i> Sudah adanya perencanaan, pengelolaan, dan implementasi sistem berbasis komputer yang lebih terarah. Perusahaan

	malware		memiliki kebiasaan terpola untuk merencanakan keamanan yang dilakukan secara berulang namun belum melibatkan dokumen formal.
Apakah pengguna berperan penting dalam upaya pencegahan malware	Iya	2	<i>(Repeatable But Intutive)</i> Sudah adanya perencanaan, pengelolaan, dan implementasi sistem berbasis komputer yang lebih terarah. Perusahaan memiliki kebiasaan terpola untuk merencanakan keamanan yang dilakukan secara berulang namun belum melibatkan dokumen formal.
<b>Score Maturity</b>	<b>2</b>		
<b>Index</b>	<b><i>Repeatable But Intutive</i></b>		

Dari hasil pengujian subklausul Perlindungan dari Malwere dapat kita ketahui bahwa jumlah kebijakan kemanan informasi memiliki maturity indeks sejumlah 2 berikut rumus untuk mencari score maturitynya

$$\text{Index Maturity} = \frac{8}{4} * 100\%$$

Hasil penjumlahan untuk score pertanyaan yang dijawab ialah 8 kemudian di bagi dengan 4. 4 ialah banyaknya jumlah pertanyaan klausul maka dapatlah hasilnya **2** kemudian di kali 100% untuk mengalikan hasil pembagian dengan 100% cukup mengalikan hasil pembagian dengan 1 atau 100\* dalam bentuk desimal yaitu 1. Langkah ini tidak akan mengubah nilai dari hasil pembagian sebelumnya, karena mengalikan dengan satu akan mendapatkan nilai yang sama.

Tabel 4. 3 A.12.3 Cadangan (*Backup*)

Pertanyaan	Jawaban	Skor	Maturity
Apakah ada salinan cadangan informasi, perangkat lunak dan image sistem?	Ada, contohnya seperti laporan keuangan pada BAZNAS	3	<i>(Defined Process)</i> Sudah memiliki proses keamanan yang sudah didokumentasikan dengan baik kemudian dikomunikasikan melalui pelatihan. Perusahaan juga menyadari perlunya proses keamanan sehingga adanya aturan yang menunjukkan untuk perusahaan secara rutin melakukan keamanan.
apakah salinan tersebut perlu diambil dan diuji secara berkala?	Perlu	2	<i>(Repeatable but Intuitive)</i> Sudah adanya perencanaan, pengelolaan, dan implementasi sistem berbasis komputer yang lebih terarah. Perusahaan memiliki kebiasaan terpola untuk merencanakan keamanan yang dilakukan secara berulang namun belum melibatkan dokumen formal.
Apakah ada kebijakan mengenai salinan cadangan? Jika ada, apakah salinan cadangan tersebut sudah disetujui dan diterapkan?	Belum ada	0	<i>(Non Existent)</i> Belum adanya permasalahan yang harus diatasi. Perusahaan merasa tidak membutuhkan mekanisme proses keamanan. Sehingga tidak ada pengawasan sama sekali.

<b>Score Maturity</b>	<b>1,66</b>
<b>Index</b>	<b>Repeatable But Intutive</b>

Dari hasil pengujian subklausul Cadangan (*Backup*) dapat diketahui bahwa jumlah kebijakan keamanan informasi memiliki maturity indeks sejumlah 1,66 berikut rumus untuk mencari score maturitynya

$$\text{Maturity Level} = \frac{5}{3} * 100\%$$

Hasil penjumlahan untuk score pertanyaan yang dijawab ialah 5 kemudian di bagi dengan 4. 4 ialah banyaknya jumlah pertanyaan klausul maka dapatlah hasilnya **1,66** kemudian di kali 100% untuk mengalikan hasil pembagian dengan 100% cukup mengalikan hasil pembagian dengan 1 atau 100\* dalam bentuk desimal yaitu 1. Langkah ini tidak akan mengubah nilai dari hasil pembagian sebelumnya, karena mengalikan dengan satu akan mendapatkan nilai yang sama.

**Tabel 4. 4** A.12.4 Pencatatan (*logging*) dan Pemantauan

<b>Pertanyaan</b>	<b>Jawaban</b>	<b>Skor</b>	<b>Maturity</b>
Apakah ada pencatatan kejadian aktivitas pengguna, pengecualian, kegagalan dan kejadian keamanan informasi?	Iya, ada	2	<i>(Repeatable but Intuitive)</i> Sudah adanya perencanaan, pengelolaan, dan implementasi sistem berbasis komputer yang lebih terarah. Perusahaan memiliki kebiasaan terpola untuk merencanakan keamanan yang dilakukan secara berulang namun belum melibatkan dokumen formal.
Apakah catatan kejadian sudah direkam dengan benar?	Belum terlalu	1	<i>(Initial/ Ad Hoc)</i> Sudah adanya bukti bahwa perusahaan mengetahui adanya permasalahan yang harus diatasi. Perusahaan sudah memiliki inisiatif untuk

			melakukan keamanan. Namun sifatnya masih non formal.
Apakah kejadian tersebut disimpan dan direview secara berkala?	Hanya disimpan, untuk review secara berkala belum	1	<i>(Initial/ Ad Hoc)</i> Sudah adanya bukti bahwa perusahaan mengetahui adanya permasalahan yang harus diatasi. Perusahaan sudah memiliki inisiatif untuk melakukan keamanan. Namun sifatnya masih non formal.
Apakah ada pencatatan log dan informasi log yang harus dilindungi?	Iya, contohnya data pribadi seperti alamat, nomor hp, dll	2	<i>(Repeatable but Intuitive)</i> Sudah adanya perencanaan, pengelolaan, dan implementasi sistem berbasis komputer yang lebih terarah. Perusahaan memiliki kebiasaan terpola untuk merencanakan keamanan yang dilakukan secara berulang namun belum melibatkan dokumen formal.
apakah log harus dilindungi dari pemalsuan dan akses tidak berwenang?	Iya harus	2	<i>(Repeatable but Intuitive)</i> Sudah adanya perencanaan, pengelolaan, dan implementasi sistem berbasis komputer yang lebih terarah. Perusahaan memiliki kebiasaan terpola untuk merencanakan keamanan yang dilakukan secara berulang namun belum melibatkan dokumen formal.
Apakah ada langkah-langkah yang diambil untuk mencegah	Ada, melakukan penghapusan log	2	<i>(Repeatable But Intuitive)</i> Sudah adanya perencanaan,

manipulasi atau modifikasi terhadap log sistem?	secara berkala		pengelolaan, dan implementasi sistem berbasis komputer yang lebih terarah. Perusahaan memiliki kebiasaan terpola untuk merencanakan keamanan yang dilakukan secara berulang namun belum melibatkan dokumen formal.
Apakah ada pencatatan aktivitas administrator sistem dan operator sistem?	Ada	2	<i>(Repeatable But Intutive)</i> Sudah adanya perencanaan, pengelolaan, dan implementasi sistem berbasis komputer yang lebih terarah. Perusahaan memiliki kebiasaan terpola untuk merencanakan keamanan yang dilakukan secara berulang namun belum melibatkan dokumen formal.
Apakah pencatatan tersebut dilindungi dan direview secara berkala?	Iya, untuk meninjau lebih lanjut aktivitas administrator dan operator sistem	2	<i>(Repeatable But Intutive)</i> Sudah adanya perencanaan, pengelolaan, dan implementasi sistem berbasis komputer yang lebih terarah. Perusahaan memiliki kebiasaan terpola untuk merencanakan keamanan yang dilakukan secara berulang namun belum melibatkan dokumen formal.
Apakah ada langkah yang diambil untuk memastikan	Ada, target capaian dan	2	<i>(Repeatable But Intutive)</i> Sudah adanya perencanaan,

administrator dan operator menjalankan tugas dengan baik?	penilaian terhadap administrator dan operator		pengelolaan, dan implementasi sistem berbasis komputer yang lebih terarah. Perusahaan memiliki kebiasaan terpola untuk merencanakan keamanan yang dilakukan secara berulang namun belum melibatkan dokumen formal.
Apakah ada penjamin bahwa waktu dari semua sistem pengelolaan informasi yang terkait dalam organisasi atau wilayah di sinkronkan ke sumber waktu acuan tunggal?	Tidak ada, waktu universal	1	<i>(Initial/ Ad Hoc)</i> Sudah adanya bukti bahwa perusahaan mengetahui adanya permasalahan yang harus diatasi. Perusahaan sudah memiliki inisiatif untuk melakukan keamanan. Namun sifatnya masih non formal.
Apakah ada cara khusus untuk menentukan sinkronisasi waktu yang akurat di seluruh sistem?	ada, menggunakan waktu server bersama	2	<i>(Repeatable but Intuitive)</i> Sudah adanya perencanaan, pengelolaan, dan implementasi sistem berbasis komputer yang lebih terarah. Perusahaan memiliki kebiasaan terpola untuk merencanakan keamanan yang dilakukan secara berulang namun belum melibatkan dokumen formal.
<b>Score Maturity</b>	<b>1,72</b>		
<b>Index</b>	<b><i>Repeatable But Intutive</i></b>		

Dari hasil pengujian subklausul Pencatatan (*Logging*) dan Pemantauan dapat diketahui jumlah kebijakan keamanan informasi memiliki maturity indeks sejumlah **1,72** berikut rumus untuk mencari score maturitynya



$$\text{Maturity Level} = \frac{19}{11} * 100\%$$

Hasil penjumlahan untuk score pertanyaan yang dijawab ialah 19 kemudian di bagi dengan 11. 11 ialah banyaknya jumlah pertanyaan klausul maka dapatlah hasilnya **1,72** kemudian di kali 100% untuk mengalikan hasil pembagian dengan 100% cukup mengalikan hasil pembagian dengan 1 atau 100\* dalam bentuk desimal yaitu 1. Langkah ini tidak akan mengubah nilai dari hasil pembagian sebelumnya, karena mengalikan dengan satu akan mendapatkan nilai yang sama.

Berikut adalah gambar lembar kusioner pertanyaan Audit Keamanan Sistem Informasi pada Badan Amil Zakat Nasional Kabupaten Bengkalis:

**LEMBAR PERTANYAAN AUDIT ISO 27001**

Responden :Zulkarnain Bagas, M. Sos

Jabatan :Kepala bagian SDM dan umum

Klausul A12 Keamanan Operasi

A. 12.1 Prosedur dan Tanggung Jawab Operasional

QUESTION	ANSWER
Apakah prosedur operasional untuk mengelola sistem informasi sudah didokumentasikan?	Iya, sudah
Jika ada, apakah prosedur operasional tersebut tersedia untuk semua pengguna yang membutuhkan?	tersedia contohnya tata cara Pembayaran Zakat online di Baznas tersedia pada halaman website
Apakah perubahan terhadap organisasi, proses bisnis, fasilitas pengolahan informasi dan sistem dapat mempengaruhi keamanan informasi?	Iya
Apakah perubahan yang terjadi dapat dikendalikan?	Iya
Apakah ada pemantauan penggunaan sumber daya untuk kebutuhan kapasitas dimasa mendatang?	Belum ada
Apakah ada langkah-langkah yang diambil untuk mengatur dan memastikan penggunaan sumberdaya sesuai kapasitas sistem yang dibutuhkan?	Melakukan analisa terkait Kebutuhan sistem
Apakah lingkungan pengembangan, pengujian, dan operasional harus dipisahkan untuk mengurangi resiko yang tidak sah pada lingkungan operasional?	harusnya iya
apakah pemisahan lingkungan dilakukan secara efektif untuk menghindari gangguan tidak sah?	Untuk sekarang belum ada di lakukan

Gambar 4. 1 Lembar Kusioner

A.12.4 Pencatatan (logging) dan Pemantauan

QUESTION	ANSWER
Apakah ada pencatatan kejadian aktivitas pengguna, pengecualian, kegagalan dan kejadian keamanan informasi?	Iya, ada
Apakah catatan kejadian sudah direkam dengan benar?	Belum tentu
Apakah kejadian tersebut disimpan dan direview secara berkala?	hanya disimpan, untuk review secara berkala belum
Apakah ada pencatatan log dan informasi log yang harus dilindungi?	Iya, contohnya data pribadi seperti alamat, nohp, dll.
apakah log harus dilindungi dari pemalsuan dan akses tidak berwenang?	Iya, harus
Apakah ada langkah-langkah yang diambil untuk mencegah manipulasi atau modifikasi terhadap log sistem?	Ada, melakukan penghapusan log secara berkala
Apakah ada pencatatan aktivitas administrator sistem dan operator sistem?	Ada
Apakah pencatatan tersebut dilindungi dan direview secara berkala?	Iya, untuk menjaga lebih lanjut aktivitas administrator dan operator sistem
Apakah ada langkah yang diambil untuk memastikan administrator dan operator menjalankan tugas dengan baik?	ada, target Capaian dan Penilaian terhadap administrator dan operator
Apakah ada penjamin bahwa waktu dari semua sistem pengelolaan informasi yang terkait dalam organisasi atau wilayah di sinkronkan ke sumber waktu acuan tunggal?	Tidak ada, waktu universal
Apakah ada cara khusus untuk menentukan sinkronisasi waktu yang akurat di seluruh sistem?	ada, menggunakan waktu server bersama

Gambar 4. 2 Lembar Kusioner

A.12.2 Perlindungan dari Malware



QUESTION	ANSWER
Apakah ada kendali deteksi, pencegahan, dan pemulihan untuk melindungi terhadap malware?	Iya, ada
Apakah kendali tersebut sudah diimplementasikan dan melindungi pengguna dari serangan malware?	Iya, kendali yang sudah diterapkan berupa pemasangan anti virus
Apakah kendali yang diambil efektif dalam mendeteksi malware?	Untuk sekarang efektif, karena belum pernah terjadinya serangan dari malware
Apakah pengguna berperan penting dalam upaya pencegahan malware	Iya

A.12.3 Cadangan (Backup)

QUESTION	ANSWER
Apakah ada salinan cadangan informasi, perangkat lunak dan image sistem?	Ada, contohnya seperti laporan keuangan pada Bazznas
apakah salinan tersebut perlu diambil dan diuji secara berkala?	Perlu
Apakah ada kebijakan mengenai salinan cadangan? Jika ada, apakah salinan cadangan tersebut sudah disetujui dan diterapkan?	Belum ada



Gambar 4. 3 Lembar Kusioner


Berikut adalah panduan pembayaran pada sistem informasi Badan Amil Zakat Nasional Kabupaten Bengkalis:


7.		<b>820.31.08001</b> (Rekening Infak Dan Sedekah (Bank Riau Kepri Syariah)) A.n BAZNAS Infak Bengkalis)	<b>SALIN</b>
8.		<b>7106469991</b> (Rekening Infak Dan Sedekah (Bank Syariah Indonesia) A.n BAZNAS Infak Bengkalis)	<b>SALIN</b>






**Panduan Pembayaran:**

1. Pilih **Bank** yang dikehendaki lalu **Salin Nomor Rekening**
2. Lakukan proses Transfer dari ATM, M-banking, i-banking, SMS-banking, dan atau teller bank.
3. Simpan bukti transfer dan lakukan konfirmasi melalui

**Niat Menunaikan Zakat** 

نَوَيْتُ أَنْ أُخْرِجَ زَكَاةَ مَالِي فَرَضًا لِلَّهِ تَعَالَى 

 **REKENING ZAKAT**     **KONFIMASI ZAKAT**     **BAYAR ZAKAT ONLINE**     **E-PROPOSAL (COMING SOON)**     **KALKULATOR ZAKAT**

Gambar 4. 4 Panduan Pembayaran Zakat

Berikut ini adalah dokumentasi laporan keuangan Badan Amil Zakat Nasional Kabupaten Bengkalis:

Uraian	Catatan No.	2022	2021
<b>BAZNAS KABUPATEN BENGKALIS</b>			
<b>Laporan Perubahan Dana</b>			
<b>Untuk Tahun yang Berakhir Pada Tanggal 31 Des 2022 dan 31 Des 2021</b>			
<b>DANA INFAK KHUSUS &amp; SOSIAL</b>			
<b>KEAGAMAAN LAINNYA</b>	2.f.3.k.		
<b>Penerimaan Dana Infak Khusus &amp; Sosial</b>			
<b>Keagamaan Lainnya</b>			
Penerimaan Infak Dunia Islam		-	-
Penerimaan Infak Khusus		22.627.800	53.340.000
Penerimaan Fidyah		14.010.000	4.350.000
<b>Jumlah Penerimaan DIKSKL</b>		<b>36.637.800</b>	<b>57.690.000</b>
<b>Penyaluran Dana Infak Khusus &amp; Sosial</b>			
<b>Keagamaan Lainnya</b>			
Penyaluran Infak Dunia Islam		-	-
Penyaluran Infak Khusus		57.683.000	7.700.000
<b>Jumlah Penyaluran DIKSKL</b>		<b>57.683.000</b>	<b>7.700.000</b>
<b>Surplus (Defisit) Dana Infak Khusus &amp; Sosial Keagamaan Lainnya</b>		<b>(21.045.200)</b>	<b>49.990.000</b>
<b>Saldo Awal Dana Infak Khusus &amp; Sosial Keagamaan Lainnya</b>		<b>56.884.892</b>	<b>6.894.892</b>
<b>Saldo Akhir Dana Infak Khusus &amp; Sosial Keagamaan Lainnya</b>		<b>35.839.692</b>	<b>56.884.892</b>

Bengkalis, 09 Maret 2023

  
**Ismail S.Sos**  
 Ketua

Gambar 4. 5 Laporan Keuangan BAZNAS

Berikut ini adalah gambar struktur organisasi BAZNAS Kabupaten Bengkulu:



Gambar 4. 6 Struktur organisasi BAZNAS

Berikut adalah bukti dokumentasi wawancara audit sistem informasi BAZNAS Kabupaten Bengkalis:



Gambar 4. 7 Dokumentasi Wawancara



## 4.2 Hasil Eksperimen

Dari keseluruhan hasil perhitungan klausul yang diperoleh dari proses wawancara, dapat direkapitulasi hasil uji keamanan pada sistem informasi BAZNAS Kabupaten Bengkalis sebagai berikut:

**Tabel 4. 5** Rekapitulasi klausul keamanan sistem informasi pada BAZNAS Kabupaten Bengkalis

Rekapitulasi Klausul	Score Maturity
A.12.1 Prosedur dan Tanggung Jawab Operasional	1,75
A.12.2 Perlindungan dari Malware	2
A.12.3 Cadangan ( <i>Backup</i> )	1,66
A.12.4 Pencatatan ( <i>logging</i> ) dan Pemantauan	1,72
<b>Rata-Rata</b>	<b>1,78</b>

Dari hasil perhitungan klausul dan subklausul penelitian, maka diketahui untuk klausul Prosedur dan Tanggung Jawab Operasional skor maturitynya sebesar 1,75 untuk subklausul Perlindungan dari malware mendapat skor 2, untuk subklausul Cadangan (*Backup*) 1,66 dan untuk subklausul Pencatatan (*logging*) dan Pemantauan skornya 2. Setelah dilakukan penjumlahan pada skor maturity dan dibagi dengan banyaknya jumlah klausul maka dapatlah hasil rata-rata sebesar 1,78 ini berarti dapat dikatakan *Repeatable But Intutive*, Yang artinya sudah adanya perencanaan, pengelolaan, dan implementasi sistem berbasis komputer yang lebih terarah. Perusahaan memiliki kebiasaan terpola untuk merencanakan keamanan yang dilakukan secara berulang namun belum melibatkan dokumen formal yang terdokumentasi dengan jelas. Disarankan pada BAZNAS Kabupaten Bengkalis untuk membuat SOP/Prosedur tanggung jawab operasional, Perlindungan dari Malware, Cadangan (*Backup*), dan Pencatatan (*Logging*) dan Pemantauan. Kegunaan dibuatnya kebijakan tersebut adalah sebagai berikut:

- Prosedur dan tanggung jawab operasional gunanya ialah untuk menjamin kepatuhan organisasi terhadap standar *ISO 27001* dengan mengatur

langkah-langkah yang diperlukan untuk menerapkan kontrol keamanan, mengelola resiko, dan mematuhi kebijakan keamanan informasi.

- Perlindungan dari malware gunanya ialah untuk menyediakan panduan dan prosedur yang terstruktur bagi anggota organisasi untuk mencegah, mendeteksi, dan menanggapi serangan dari malware.
- Cadangan (Backup) SOP ini juga diperlukan untuk mematuhi persyaratan regulasi atau kepatuhan dan juga digunakan sebagai alat pelatihan untuk mengajarkan karyawan tentang pentingnya cadangan data dan cara yang benar untuk melaksanakan prosedur cadangan data yang aman dan efektif.
- SOP logging dan Pemantauan membantu organisasi mematuhi persyaratan regulasi dan kepatuhan yang berlaku dalam menjaga catatan keamanan dan privasi pada sistem informasi.

## **BAB V**

### **PENUTUP**

#### **5.1 Kesimpulan**

Dari hasil audit dari keamanan sistem informasi BAZNAS Kabupaten Bengkalis menggunakan standar ISO/IEC 27001 khususnya menggunakan klausul A12 Keamanan Operasional dapat disimpulkan bahwa pengukuran tingkat keamanan sistem informasi BAZNAS dikategorikan *Repeatable But Intuitive* dengan persentase **1,78** yang berarti Sudah adanya perencanaan, pengelolaan, dan implementasi sistem berbasis komputer yang lebih terarah. Perusahaan memiliki kebiasaan terpolat untuk merencanakan keamanan yang dilakukan secara berulang namun belum melibatkan dokumen formal atau terdokumentasi dengan jelas.

#### **5.2 Saran**

Berdasarkan hasil dari penelitian yang telah dilakukan, disarankan untuk melakukan evaluasi yang sistematis dan terencana terhadap pengembangan sistem, dan juga membuat SOP/Prosedur terkait tanggung jawab operasional, Perlindungan dari Malware, Cadangan (Backup) dan Pencatatan (Logging) dan Pemantauan untuk meningkatkan keamanan informasi BAZNAS Kabupaten Bengkalis ke level yang lebih tinggi (level 3 atau level 4). Untuk memastikan peningkatan kinerja sistem, evaluasi harus dilakukan secara berkala dan teratur guna meningkatkan tingkat kematangan ISO 27001 pada sistem informasi BAZNAS Kabupaten Bengkalis, terutama pada aspek prosedur dan tanggung jawab operasional, perlindungan terhadap malware, pencadangan (*backup*), pencatatan (*logging*), dan pemantauan. Selain itu, disarankan juga untuk melibatkan pelatihan dan peningkatan kesadaran bagi personel terkait.

## DAFTAR PUSTAKA

- [1] C. V. Febiolla and D. Setiawaty, "Audit Sistem Informasi Berbasis ISO 27001 Di Era New Normal," *Pros. ASIC 2020*, vol. 1, no. 1, pp. 1–23, 2020.
- [2] Syafrinal and Agusrijar, "Audit Keamanan Sistem Informasi Pada Data Center Menggunakan Standar SNI-ISO 27001," *Audit Keamanan Sist. Inf. Pada Data Cent. Menggunakan Standar SNI-ISO*, vol. 4, no. September, p. 581, 2020, [Online]. Available: <http://ejurnal.tunasbangsa.ac.id/index.php/jsakti/article/view/250>
- [3] R. Febriawan, "Peran Sistem Manajemen Keamanan Informasi ( SMKI ) Berstandar ISO 27001 Untuk Meningkatkan Keamanan Informasi (Sebuah Studi Literatur)," *ResearchGate*, no. November, p. 2, 2020.
- [4] J. Sistem Informasi, S. Tinggi Manajemen Komputer, and T. Komputer Surabaya, "Fine Ermana 2) Haryanto Tanuwijaya 3) Ignatius Adrian Mastan," pp. 1–8.
- [5] M. Ikhsan, E. Darwiyanto, and D. D. J. Suwawi, "Audit Keamanan Sistem Informasi Akademik Sekolah Tinggi Farmasi Bandung Berbasis Risiko dengan Menggunakan Standar ISO 27001," *e-Proceeding Eng.*, vol. 3, no. 3, p. 5222, 2016.
- [6] H. Wahyudi, A. Zulianto, A. Maulana, S. Mardira Indonesia, and U. Langlangbuana, "Audit Keamanan Sistem Informasi Manajemen Akademik dan Kemahasiswaan Menggunakan SNI ISO/IEC 27001:2013 Studi Kasus STMIK Mardira Indonesia," *J. Comput. Bisnis*, vol. Vol. 14 No, no. 1, pp. 40–46, 2020.
- [7] G. K. Dewi, "Analisis Keamanan Sistem Informasi Universitas X," *ABIS Account. Bus. Inf. Syst. J.*, vol. 9, no. 1, 2021, doi: 10.22146/abis.v9i1.64235.
- [8] Y. D. Wijaya, "Evaluasi Kemananan Sistem Informasi Pasdeal Berdasarkan Indeks Keamanan Informasi (Kami) Iso/Iec 27001:2013," *J. Sist. Inf. dan Inform.*, vol. 4, no. 2, pp. 115–130, 2021, doi:

10.47080/simika.v4i2.1178.

- [9] M. Hendayun, A. Zulianto, S. Sekolah, and T. Ilmu, “Audit Keamanan Sistem Informasi Akademik Stikes Jendral Achmad Yani Menggunakan SNI ISO / IEC 27001 : 2013 Abstraksi Pendahuluan,” *ISSN 2548-8082 / E-ISSN 2615-6350 Vol.3 No.2 Ed. 2019 Jurnal PRODUKTIF | 25 Audit*, vol. 3, no. 2, pp. 25–35, 2019.
- [10] E. Wicaksono, M. A. S. Anam, R. A. Bimantara, and R. Permatasari, “Analisis Keamanan Sistem Informasi Penjualan Pada Pt Arta Boga Cemerlang Cabang Kediri Dengan Menggunakan Standar Iso 27001:2013,” *Pros. Semin. Nas. Teknol. dan Sist. Inf.*, vol. 3, no. 1, pp. 344–353, 2023, doi: 10.33005/sitasi.v3i1.361.