

**TUGAS AKHIR**  
**MAGANG MBKM MANDIRI**  
**IMPLEMENTASI ISO 27001 DALAM PENGELOLAAN**  
**RISIKO KEAMANAN INFORMASI**  
**STUDI KASUS: *PENETRATION TESTING* DI INSTANSI XYZ**

**Diajukan untuk Memenuhi Persyaratan Kelulusan  
Program MBKM Mandiri**



**ANDREAN ARADYKA**

**NIM : 225411112**

**PROGRAM STUDI INFORMATIKA**  
**PROGRAM SARJANA**  
**FAKULTAS TEKNOLOGI INFORMASI**  
**UNIVERSITAS TEKNOLOGI DIGITAL INDONESIA**  
**YOGYAKARTA**

**2024**

**TUGAS AKHIR**  
**IMPLEMENTASI ISO 27001 DALAM PENGELOLAAN**  
**RISIKO KEAMANAN INFORMASI**  
**STUDI KASUS: *PENETRATION TESTING* DI INSTANSI XYZ**

**Diajukan sebagai salah satu syarat untuk menyelesaikan studi**



**Disusun Oleh**  
**ANDREAN ARADYKA**  
**NIM : 225411112**

**PROGRAM STUDI INFORMATIKA**  
**PROGRAM SARJANA**  
**FAKULTAS TEKNOLOGI INFORMASI**  
**UNIVERSITAS TEKNOLOGI DIGITAL INDONESIA**  
**YOGYAKARTA**  
**2024**

**HALAMAN PERSETUJUAN  
TUGAS AKHIR**

**Judul** : **Implementasi ISO 27001 dalam Pengelolaan Risiko  
Keamanan Informasi**  
**Studi Kasus: *Penetration Testing* di Instansi XYZ**

**Nama** : **Andrean Aradyka**

**NIM** : **225411112**

**Program Studi** : **Informatika**

**Program** : **Sarjana**

**Semester** : **Ganjil**

**Tahun Akademik** : **2024/2025**

Telah diperiksa dan disetujui untuk diujikan di hadapan  
Dewan Penguji Tugas Akhir

Yogyakarta, 3 September 2024

Dosen Pembimbing,



Dr. L.N. Harnaningrum, S.Si., M.T.

NIDN : 0513057101

**HALAMAN PENGESAHAN**

**TUGAS AKHIR**

**IMPLEMENTASI ISO 27001 OLEH PT SEKURITI SIBER INDONESIA  
DALAM PENGELOLAAN RISIKO KEAMANAN INFORMASI  
STUDI KASUS: PENETRATION TESTING DI INSTANSI XYZ**

Telah dipertahankan di depan Dewan Penguji Tugas Akhir dan dinyatakan diterima untuk memenuhi sebagian persyaratan guna memperoleh Gelar


**Sarjana Komputer  
Program Studi Informatika  
Fakultas Teknologi Informasi  
Universitas Teknologi Digital Indonesia  
Yogyakarta**

Yogyakarta, 3 September 2024

Dewan Penguji	NIDN	Tandatangan
1. M. Agung Nugroho, S.Kom., M.Kom. (Ketua)	0507078501	
2. Dr. L.N. Harnaningrum, S.Si., M.T. (Sekretaris)	0513057101	
3. Dini Fakta Sari, S.T., M.T.. (Anggota)	0507108401	

Mengetahui

Ketua Program Studi Informatika

  
Dini Fakta Sari, S.T., M.T.  
NPP : 121172

## **PERNYATAAN KEASLIAN TUGAS AKHIR**

Dengan ini saya menyatakan bahwa naskah tugas akhir ini belum pernah diajukan untuk memperoleh gelar Sarjana Komputer di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara sah diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Yogyakarta, 3 September 2024



Andrean Aradyka

NIM: 225411112

## INTISARI

PT Sekuriti Siber Indonesia merupakan perusahaan yang fokus pada keamanan sistem informasi, termasuk layanan penetration testing, security assessment, dan pendampingan audit ISO 27001. Proyek magang ini bertujuan mendukung Instansi XYZ dalam mempersiapkan audit ISO 27001.

Proses implementasi ISO 27001 meliputi penentuan ruang lingkup, evaluasi kesenjangan, penetration testing, audit internal, dan audit eksternal. Fokus laporan ini adalah pada penetration testing, yang digunakan untuk menemukan dan mengeksploitasi kerentanan sistem guna menilai keamanan informasi Instansi XYZ. Salah satu aspek penting dari ISO 27001 adalah pengendalian A.12.6.1, yang berfokus pada pengelolaan kerentanan teknis dengan tujuan memastikan bahwa kerentanan dalam sistem dan perangkat lunak ditangani secara tepat waktu untuk mengurangi risiko keamanan. Hasil pengujian, yang mencakup temuan, tingkat risiko, dan rekomendasi perbaikan, dipresentasikan untuk membantu Instansi XYZ mempersiapkan audit ISO 27001.

***Kata Kunci:*** Penetration Testing, ISO 27001, Keamanan Sistem Informasi, Audit Internal dan Eksternal, Manajemen Kerentanan.

## ***ABSTRACT***

*PT Sekuriti Siber Indonesia is a company that focuses on information system security, including services such as penetration testing, security assessment, and ISO 27001 audit assistance. This internship project aims to support XYZ Agency in preparing for the ISO 27001 audit.*

*The ISO 27001 implementation process includes defining the scope, gap analysis, penetration testing, internal audit, and external audit. The focus of this report is on penetration testing, which is used to identify and exploit system vulnerabilities to assess the information security of XYZ Agency. One of the critical aspects of ISO 27001 is control A.12.6.1, which focuses on managing technical vulnerabilities with the objective of ensuring that vulnerabilities in systems and software are addressed in a timely manner to reduce security risks. The testing results, which include findings, risk levels, and improvement recommendations, are presented to assist XYZ Agency in preparing for the ISO 27001 audit.*

***Keywords:*** *Penetration Testing, ISO 27001, Information System Security, Internal and External Audit, Vulnerability Management.*

## KATA PENGANTAR

Saya panjatkan puji dan syukur kepada Tuhan Yang Maha Esa atas rahmat dan karunia-Nya sehingga saya dapat menyelesaikan laporan magang ini dengan baik. Laporan ini didasarkan pada pengalaman selama magang di PT Sekuriti Siber Indonesia, sebuah perusahaan yang bergerak di bidang keamanan sistem informasi.

Magang ini bertujuan untuk membantu Instansi XYZ dalam mempersiapkan diri untuk lolos audit ISO 27001. Selama magang, saya terlibat dalam berbagai aktivitas yang mencakup kesepakatan ruang lingkup sertifikasi, gap assessment, penetration testing, audit internal, hingga persiapan untuk audit eksternal. Fokus utama dari laporan ini adalah melakukan penetration testing untuk mengidentifikasi dan mengeksploitasi kerentanan dalam sistem informasi Instansi XYZ, sebagai bagian dari persyaratan implementasi ISO 27001.

Saya menyadari bahwa laporan ini tidak akan tersusun tanpa dukungan dan bimbingan dari berbagai pihak. Oleh karena itu, saya ingin mengucapkan terima kasih kepada:

1. Ibu Dr. L.N. Harnaningrum, S.Si., M.T. di Universitas Teknologi Digital Indonesia, yang telah memberikan dukungan dan pengarahan dalam penyusunan laporan ini.
2. Bapak Nezim, selaku pembimbing magang di PT Sekuriti Siber Indonesia yang telah memberikan arahan dan ilmu yang sangat berharga.
3. Seluruh staf dan rekan kerja di PT Sekuriti Siber Indonesia yang telah membantu dan memberikan banyak pengalaman selama magang.
4. Keluarga dan teman-teman yang selalu memberikan dukungan dan doa.

Semoga laporan ini dapat memberikan manfaat dan wawasan bagi pembaca, serta menjadi sumbangsih yang berguna dalam bidang keamanan informasi, khususnya dalam proses sertifikasi ISO 27001. Saya menyadari bahwa laporan ini masih jauh dari sempurna, oleh karena itu kritik dan saran yang membangun sangat saya harapkan.

Akhir kata, saya berharap semoga laporan magang ini dapat memberikan kontribusi positif bagi pengembangan diri saya serta kemajuan bidang keamanan informasi di Indonesia.

Yogyakarta, 16 Agustus 2024  
Penulis



## DAFTAR ISI

<b>HALAMAN SAMPUL.....</b>	<b>i</b>
<b>HALAMAN PERSETUJUAN.....</b>	<b>iii</b>
<b>HALAMAN PENGESAHAN.....</b>	<b>iv</b>
<b>PERNYATAAN KEASLIAN TUGAS AKHIR.....</b>	<b>v</b>
<b>INTISARI.....</b>	<b>vi</b>
<b>ABSTRACT.....</b>	<b>vii</b>
<b>KATA PENGANTAR.....</b>	<b>viii</b>
<b>DAFTAR ISI.....</b>	<b>ix</b>
<b>DAFTAR GAMBAR.....</b>	<b>xi</b>
<b>DAFTAR TABEL.....</b>	<b>xii</b>
<b>BAB I PENDAHULUAN.....</b>	<b>1</b>
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	2
1.3 Ruang Lingkup.....	2
1.3.1 Aplikasi XXDOC.....	2
1.3.2 Aplikasi KELHEBAT.....	2
1.3.3 Batasan Penelitian.....	2
1.3.4 Metodologi Pengujian.....	3
1.4 Tujuan Penelitian.....	3
1.5 Manfaat Penelitian.....	3
1.5.1 Manfaat Teoritis.....	3
1.5.2 Manfaat Praktis.....	4
<b>BAB 2 TINJAUAN PUSTAKA DAN DASAR TEORI.....</b>	<b>5</b>
2.1 Tinjauan Pustaka.....	5
2.1.1 ISO 27001 dan Technical Vulnerability Management (A.12.6.1).....	5
2.1.2 OWASP Top 10 dan OWASP API Security Top 10.....	5
2.1.3 Metode Greybox Testing.....	5
2.1.4 Keamanan Aplikasi Mobile.....	6
2.1.5 Implementasi Technical Vulnerability Management.....	6
2.2 Dasar Teori.....	6
2.2.1 ISO 27001 dan Technical Vulnerability Management.....	6
2.2.2 Penetration Testing dan Greybox Testing.....	6
2.2.3 OWASP Top 10 dan OWASP API Security Top 10.....	7
2.2.4 Keamanan Aplikasi Mobile.....	7
<b>BAB 3 METODE PENELITIAN.....</b>	<b>8</b>
3.1 Analisa Kebutuhan.....	8
3.1.1 Kebutuhan Fungsional.....	8
3.1.2 Kebutuhan Non-Fungsional.....	8
3.2 Rancangan.....	8

3.2.1 Alur Kerja.....	8
3.2.2 Diagram Alur (Workflow Diagram).....	12
<b>BAB 4 IMPLEMENTASI DAN PEMBAHASAN.....</b>	<b>13</b>
4.1 Implementasi.....	13
4.1.1 Alur Kerja.....	13
4.1.2 Pengujian pada Aplikasi Mobile XXDOC.....	16
4.1.3 Pengujian pada Aplikasi Web KELHEBAT.....	17
4.2 Hasil Temuan.....	19
4.2.1 Hasil Temuan pada Aplikasi Mobile XXDOC.....	19
4.2.2 Hasil Temuan pada Aplikasi Web KELHEBAT.....	21
<b>BAB 5 PENUTUP.....</b>	<b>25</b>
5.1 Kesimpulan.....	25
5.1.1 Pada Aplikasi Mobile XXDOC.....	25
5.1.2 Pada Aplikasi Web KELHEBAT.....	25
5.2 Saran.....	26
<b>DAFTAR PUSTAKA.....</b>	<b>27</b>
<b>LAMPIRAN.....</b>	<b>28</b>
2. Lampiran B — Log Activity Program MBKM UTDI.....	28

## DAFTAR GAMBAR

Gambar 3.1 Alur Kerja <i>Penetration Testing</i> .....	12
Gambar 4.1 Contoh Tabel <i>Gap Assessment</i> .....	14
Gambar 4.2 Tahap Dekompilasi APK dengan Apktool.....	16
Gambar 4.3 Hasil Dekompilasi APK dengan Apktool.....	17
Gambar 4.4 Hasil Log dari APK.....	17
Gambar 4.5 Hasil dari Intercept Request dan Response Aplikasi.....	18
Gambar 4.6 Perintah Memory Dump.....	20
Gambar 4.7 Direktori Penyimpanan File.....	21
Gambar 4.8 Halaman Login.....	22
Gambar 4.9 Tools Intercept Proxy.....	22
Gambar 4.10 Cross Site Scripting Reflected.....	24

## DAFTAR TABEL

Tabel 4.1 Celah aplikasi mobile XXDOC.....	19
Tabel 4.2 Celah aplikasi mobile XXDOC.....	19
Tabel 4.3 Celah aplikasi mobile XXDOC.....	20
Tabel 4.4 Celah aplikasi web KELHEBAT.....	21
Tabel 4.5 Celah aplikasi web KELHEBAT.....	22
Tabel 4.6 Celah aplikasi web KELHEBAT.....	24
Tabel A.1 Lampiran Kegiatan Minggu ke-1.....	28
Tabel A.2 Lampiran Kegiatan Minggu ke-2.....	28
Tabel A.3 Lampiran Kegiatan Minggu ke-3.....	28
Tabel A.4 Lampiran Kegiatan Minggu ke-4.....	28
Tabel A.5 Lampiran Kegiatan Minggu ke-5.....	29
Tabel A.6 Lampiran Kegiatan Minggu ke-6.....	29
Tabel A.7 Lampiran Kegiatan Minggu ke-7.....	29
Tabel A.8 Lampiran Kegiatan Minggu ke-8.....	29
Tabel A.9 Lampiran Kegiatan Minggu ke-9.....	30
Tabel A.10 Lampiran Kegiatan Minggu ke-10.....	30
Tabel A.11 Lampiran Kegiatan Minggu ke-11.....	30
Tabel A.12 Lampiran Kegiatan Minggu ke-12.....	30
Tabel A.13 Lampiran Kegiatan Minggu ke-13.....	31