

**ANALISIS KESESUAIAN PT XYZ TERHADAP STANDAR
ISO 27001:2022 DALAM MENGATASI ANCAMAN
PENCURIAN DATA MENGGUNAKAN METODE DECISION
TREE**

SKRIPSI SARJANA SISTEM INFORMASI

Karya Ilmiah sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer

Oleh:

Duhan Maulana Artline

217006516037



**PROGRAM STUDI SISTEM INFORMASI
FAKULTAS TEKNOLOGI KOMUNIKASI DAN INFORMATIKA
UNIVERSITAS NASIONAL**

2025

**ANALISIS KESESUAIAN PT XYZ TERHADAP STANDAR
ISO 27001:2022 DALAM MENGATASI ANCAMAN
PENCURIAN DATA MENGGUNAKAN METODE DECISION
TREE**

SKRIPSI SARJANA SISTEM INFORMASI

Karya Ilmiah sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer

Oleh:

Duhan Maulana Artline

217006516037



**PROGRAM STUDI SISTEM INFORMASI
FAKULTAS TEKNOLOGI KOMUNIKASI DAN INFORMATIKA
UNIVERSITAS NASIONAL**

2025

HALAMAN PENGESAHAN TUGAS AKHIR

Analisis Kesesuaian PT XYZ Terhadap Standar ISO 27001:2022
Dalam Mengatasi Ancaman Pencurian Data Menggunakan
Metode Decision Tree



Dosen Pembimbing

(Moch. Firmansyah, S.Kom., M.Kom.)

PERNYATAAN KEASLIAN TUGAS AKHIR

Saya menyatakan dengan sesungguhnya bahwa Tugas Akhir dengan judul :

Analisis Kesesuaian PT XYZ Terhadap Standar ISO 27001:2022

Dalam Mengatasi Ancaman Pencurian Data Menggunakan

Metode Decision Tree

Yang dibuat untuk melengkapi salah satu persyaratan menjadi Sarjana Komputer pada Program Studi Sistem Informasi Fakultas Teknologi Komunikasi dan Informatika Universitas Nasional, sebagaimana yang saya ketahui adalah bukan merupakan tiruan atau publikasi dari Tugas Akhir yang pernah diajukan atau dipakai untuk mendapatkan gelar di lingkungan Universitas Nasional maupun perguruan tinggi atau instansi lainnya, kecuali pada bagian – bagian tertentu yang menjadi sumber informasi atau acuan yang dicantumkan sebagaimana mestinya.

Jakarta, 02-09-2025



Duhan Maulana Artline

217006516037

LEMBAR PERSETUJUAN REVIEW AKHIR

Tugas Akhir dengan judul :

Analisis Kesesuaian PT XYZ Terhadap Standar ISO 27001:2022

Dalam Mengatasi Ancaman Pencurian Data

Menggunakan Metode Decision Tree

Dibuat untuk melengkapi salah satu persyaratan menjadi Sarjana Komputer pada Program Studi Sistem Informasi, Fakultas Teknologi Komunikasi dan Informatika Universitas Nasional. Tugas Akhir ini diujikan pada Sidang Review Akhir Semester Genap 2024-2025 pada tanggal 02 September Tahun 2025

Dosen Pembimbing 1

Moch. Firmansyah, S.Kom.,

M.Kom.

050022014

Ketua Program Studi

Dr. L. Andrianingsih, S.Kom.,

MMSI.

0303097902

LEMBAR PERSETUJUAN JUDUL YANG TIDAK ATAU YANG DIREVISI

Nama : Duhan Maulana Artline

NPM : 217006516037

Fakultas/Akademi : Fakultas Teknologi Komunikasi dan Informatika

Program Studi : Sistem Informasi

Tanggal Sidang : 27 Agustus 2025

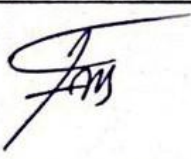
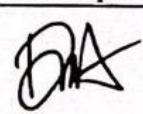
JUDUL DALAM BAHASA INDONESIA :

Analisis Kesesuaian PT XYZ Terhadap Standar ISO 27001:2022 Dalam Mengatasi
Ancaman Pencurian Data Menggunakan Metode Decision Tree

JUDUL DALAM BAHASA INGGRIS :

Analysis of PT XYZ's Compliance with ISO 27001:2022 Standards in Overcoming the
Threat of Data Theft Using the Decision Tree Method

TANDA TANGAN DAN TANGGAL

Pembimbing 1	Ka. Prodi	Mahasiswa
TGL : 02 September 2025	TGL : 02 September 2025	TGL : 02 September 2025
	 Dr. b. Anasugus, M.Mi	 Duhan Maulana A

KATA PENGANTAR

Puji dan syukur penulis panjatkan kepada Tuhan Yang Maha Esa yang telah memberikan rahmat dan karunianya sehingga penulis dapat menyelesaikan skripsi dengan judul **“ANALISIS KESESUAIAN PT XYZ TERHADAP STANDAR ISO 27001:2022 DALAM MENGATASI ANCAMAN PENCURIAN DATA MENGGUNAKAN METODE DECISION TREE”** sebagai salah satu syarat kelulusan Program Studi Sarjana Sistem Informasi dari Fakultas Teknologi Komunikasi dan Informatika.

Penelitian dan penulisan skripsi ini tidak terlepas dari bantuan berbagai pihak, oleh karena itu penulis menyampaikan banyak terima kasih terutama kepada dosen pembimbing Tugas Akhir, Moch. Firmansyah, S.Kom., M.Kom. yang telah meluangkan banyak waktu, tenaga, pikiran, bimbingan, arahan, motivasi serta memaklumi segala kekurangan penulis selama penelitian tugas akhir dan penyusunan skripsi. Penulis juga mengucapkan banyak terima kasih kepada :

1. Keluarga tercinta yang selalu memberikan doa, dukungan, dan semangat yang tiada henti.
2. Dr. Drs. El Amry Bernawi Putera, M.A, selaku Rektor Universitas Nasional yang telah memberikan kesempatan kepada penulis untuk mengikuti perkuliahan pada Program S1 Sistem Informasi.
3. Terima kasih kepada Dr. Agung Triayudi, S.Kom., M.Kom selaku dekan FTKI dan Andrianingsih, S.Kom., MMSI selaku kaprodi Sistem Informasi.
4. Seluruh dosen pengajar di Program Studi Sistem Informasi Fakultas Teknologi Komunikasi dan Informatika maupun dosen dari Program Studi lain yang memberikan banyak ilmu.
5. Teman-teman dekat selama menempuh masa perkuliahan yaitu Ammar, Jessica, Lia dan Raffli yang telah menemani dalam proses belajar terutama selama masa penulisan tugas akhir.

6. Teman-teman tim Tabulator UNAS FEST 2023 yaitu Wuri, Ferin, dan Jepplin yang telah memberikan dukungan selama masa terakhir dalam perkuliahan serta dalam masa melaksanakan tugas akhir.
7. Teman-temang magang MSIB Kampus Merdeka x LinkAja, yaitu Ferdi, Vina, dan Rafael yang telah memberikan banyak dukungan dan hiburan selama proses magang higgsa saat masa penulisan tugas akhir.
8. Gerald selaku senior di AWDA yang telah menemani dan membantu diskusi selama proses dalam pembuatan web pada penulisan akhir serta sebagai motivator dalam proses adulting.
9. Tim IT GRC yaitu Mbak Qori, Mas Farchan, Mas Oji dan Mbak Lintang yang telah membantu dalam proses memahami konsep ISO 27001 selama proses magang berlangsung.

Akhir kata, semoga Tuhan Yang Maha Esa memberikan kebaikan dan bantuan yang telah diberikan dengan hal lebih baik. Penulis mengharapkan kritik dan saran yang bersifat membangun dan semoga skripsi ini dapat memberikan manfaat di bidang Sistem Informasi.
Jakarta,



02 September 2025

Penulis

ABSTRAK

PT XYZ merupakan perusahaan jasa keuangan, menghadapi bahaya pencurian data yang signifikan. Tujuan dari penelitian ini adalah untuk mengevaluasi kesesuaian PT XYZ dengan standar ISO 27001:2022, mengukur tingkat kesiapan (maturity level) untuk mencegah ancaman pencurian data, dan menemukan kontrol keamanan yang paling efektif menggunakan metode Decision Tree. Penelitian ini menggunakan metode campuran, baik kualitatif maupun kuantitatif, dan menggunakan kerangka kerja siklus Plan-Do-Check-Act (PDCA) untuk mengevaluasi proses, melakukan analisis tingkat kesiapan untuk mengukur kesiapan. Hasil penelitian menunjukkan bahwa tingkat kematangan PT XYZ secara keseluruhan mencapai 96%, yang termasuk dalam kategori "Optimasi". Analisis PDCA juga menunjukkan bahwa Sistem Manajemen Keamanan Informasi (SMKI) beroperasi dengan baik dan konsisten. Selain itu, berdasarkan analisis Decision Tree ID3, Pengendalian Organisasi (Organizational controls) dengan nilai kontribusi 0,342 dan "Pengendalian Teknologi" (Technological controls) dengan nilai kontribusi 0,235 merupakan faktor yang paling penting dalam kesiapan perusahaan untuk menghindari pencurian data. Kesimpulannya, PT XYZ sangat siap untuk menghadapi ancaman pencurian data. Tata kelola organisasi dan kontrol teknologi adalah bagian penting dari membangun sistem keamanan data yang baik.

Kata kunci: ISO 27001:2022, Keamanan Informasi, Tingkat Kematangan, Decision Tree, Pencurian Data, PDCA

ABSTRACT

PT XYZ is a financial services company, facing significant data theft dangers. The purpose of this study is to evaluate PT XYZ's compliance with ISO 27001:2022 standards, measure the maturity level to prevent the threat of data theft, and find the most effective security controls using the Decision Tree method. This study used mixed methods, both qualitative and quantitative, and used the Plan-Do-Check-Act (PDCA) cycle framework to evaluate the process, conduct an analysis of the level of readiness to measure the case. The results showed that the overall maturity rate of PT XYZ reached 96%, which is included in the category of "Optimization". The PDCA analysis also shows that the Information Security Management System (SMKI) operates well and consistently. In addition, based on Decision Tree ID3 analysis, Organizational controls with a contribution value of 0.342 and "Technological controls" with a contribution value of 0.235 are the most important factors in the company's readiness to avoid data theft. In conclusion, PT XYZ is very prepared to face the threat of data theft. Organizational governance and technology control are essential parts of building a good data security system.

Keywords: ISO 27001:2022, Information Security, Maturity Level, Decision Tree, Data Theft, PDCA

DAFTAR ISI

HALAMAN PENGESAHAN TUGAS AKHIR	iii
PERNYATAAN KEASLIAN TUGAS AKHIR	iv
LEMBAR PERSETUJUAN REVIEW AKHIR.....	v
LEMBAR PERSETUJUAN JUDUL YANG TIDAK ATAU YANG DIREVISI ..	vi
KATA PENGANTAR.....	vii
ABSTRAK	ix
ABSTRACT.....	x
DAFTAR ISI	xi
DAFTAR GAMBAR	xiv
DAFTAR TABEL.....	xv
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	5
1.3 Tujuan Masalah	5
1.4 Batasan Masalah.....	5
1.5 Kontribusi Penelitian.....	6
BAB II TINJAUAN PUSTAKA	9
2.1 Studi Literatur.....	9
2.2 Landasan Teori.....	15
2.2.1 Teknologi Informasi.....	15
2.2.2 Keamanan Informasi.....	16
2.2.3 Kejahatan Siber (<i>Cybercrime</i>)	16
2.2.4 ISO 27001	16
2.2.5 Audit Sistem Informasi	17
2.2.6 Siklus PDCA.....	17
2.2.7 Algoritma <i>Decision Tree</i> atau ID3	18
2.2.8 Firebase Studio	18
2.2.9 Node.js	19
2.2.10 Javascript	19
2.2.11 Vue	19

2.2.12 GitHub	19
BAB III METODE PENELITIAN.....	20
3.1 Tahapan Penelitian.....	20
3.2 Pendekatan Penelitian.....	24
3.3 Tempat dan Waktu Penelitian	24
3.3.1 Tempat Penelitian.....	24
3.3.2 Waktu Penelitian	25
3.4 Rancangan atau Desain Penelitian	25
3.5 Teknik Pengumpulan Data (<i>Penentuan Indikator Maturity</i>).....	25
3.6 Teknik Analisis Data.....	27
BAB IV PEMBAHASAN.....	32
4.1 Hasil Perhitungan Maturity Level	32
4.1.1 Analisis Perhitungan Maturity Level Department IT Governance	32
4.1.2 Analisis Perhitungan Maturity Level Departement Risk Management	43
4.1.3 Analisis Perhitungan Maturity Level Departement Internal Audit	53
4.1.4 Analisis Perhitungan Maturity Level Departement Human Capital	60
4.1.5 Analisis Perhitungan Maturity Level Departement Compliance	72
4.1.6 Analisis Perhitungan Maturity Level Departement Legal	75
4.1.7 Analisis Perhitungan Maturity Level Departement General Services ..	78
4.1.8 Analisis Perhitungan Maturity Level Departement IT Security	81
4.1.9 Analisis Perhitungan Maturity Level Departement IT Operation.....	90
4.1.10 Analisis Perhitungan Maturity Level Departement IT Development .	99
4.2 Analisis PDCA (<i>Plan-Do-Check-Act</i>)	106
4.3 Analisis Decision Tree.....	108
4.3.1 Dataset	108
4.3.2 Hasil Pohon Keputusan.....	109
4.4 Dashboard Audit.....	111
4.4.1 Menu Beranda.....	111
4.4.2 Menu Pengaturan Kategori	112
4.4.3 Menu Pengaturan Kuesioner.....	115
4.4.4 Menu Isi Kuesioner.....	116
BAB V KESIMPULAN	117

5.1 Kesimpulan.....	117
5.2 Saran	118
DAFTAR PUSTAKA	120
LAMPIRAN.....	123



DAFTAR GAMBAR

Gambar 3.1 Tahapan Penelitian.....	20
Gambar 3.2 Analisis PDCA	29
Gambar 4.1 Dataset	108
Gambar 4.2 Hasil Pohon Keputusan.....	109
Gambar 4.3 Feature Importance	110
Gambar 4.4 Dashboard Audit	111
Gambar 4.5 Menu Beranda.....	112
Gambar 4.6 Pengaturan Direktorat.....	112
Gambar 4.7 Pengaturan Klausul.....	113
Gambar 4.8 Pengaturan Sub-klausul	113
Gambar 4.9 Pengaturan Annex.....	114
Gambar 4.10 Pengaturan Kontrol.....	114
Gambar 4.11 Pengaturan Skor	115
Gambar 4.12 Menu Pengaturan Kuesioner.....	115
Gambar 4.13 Menu Isi Kuesioner	116



DAFTAR TABEL

Tabel 2.1 Studi Literatur.....	9
Tabel 4.1 Hasil Analisis Maturity Level IT Governance	32
Tabel 4.2 Clause 4. Context of the organization.....	32
Tabel 4.3 Clause 6. Planning	35
Tabel 4.4 Clause 8. Operation	36
Tabel 4.5 Annex 5.12 Classification of information	38
Tabel 4.6 Annex Labelling of information	39
Tabel 4.7 Annex 5.14 Information transfer	40
Tabel 4.8 Annex 5.15 Access control	41
Tabel 4.9 Annex 5.18 Access rights	41
Tabel 4.10 Annex 5.35 Independent review of information security	42
Tabel 4.11 Annex 5.36 Compliance with policies, rules and standards for information security.....	43
Tabel 4.12 Hasil Analisis Maturity Level Risk Management.....	44
Tabel 4.13 Clause 6.1 Actions to address risks and opportunities.....	45
Tabel 4.14 Clause 6.1.2 Information security risk assessment.....	46
Tabel 4.15 Clause 6.1.3 Information security risk treatment.....	47
Tabel 4.16 Clause 8.2 Information security risk assessment.....	49
Tabel 4.17 Clause 8.3 Information security risk treatment.....	49
Tabel 4.18 Annex 5.24 Information security incident management planning and preparation	51
Tabel 4.19 Annex 5.29 Information security during disruption	52
Tabel 4.20 Annex 5.30 ICT readiness for business continuity	53
Tabel 4.21 Hasil Analisis Maturity Level Internal Audit.....	54
Tabel 4.22 Clause 9.1 Monitoring, measurement, analysis and evaluation.....	55
Tabel 4.23 Clause 9.2 Internal audit.....	57
Tabel 4.24 Clause 10.1 Continual improvement	59
Tabel 4.25 Hasil Analisis Maturity Level Human Capital.....	60
Tabel 4.26 Clause 7.1 Resources.....	61
Tabel 4.27 Clause 7.2 Competence	62
Tabel 4.28 Clause 7.3 Awareness	63
Tabel 4.29 Annex 6.1 Screening.....	64
Tabel 4.30 Annex 6.2 Terms and conditions of employment	65
Tabel 4.31 Annex 6.3 Information security awareness, education and training.....	66
Tabel 4.32 Annex 6.4 Disciplinary process.....	67
Tabel 4.33 Annex 6.5 Responsibilities after termination or change of employment.....	68
Tabel 4.34 Annex 6.6 Confidentiality or non-disclosure agreements	69
Tabel 4.35 Annex 6.7 Remote working.....	70
Tabel 4.36 Annex 6.8 Information security event reporting.....	71
Tabel 4.37 Annex 5.31 Legal, statutory, regulatory and contractual requirements	72

Tabel 4.38 Annex 5.34 Privacy and protection of personal identifiable information (PII)	73
Tabel 4.39 Annex 5.36 Compliance with policies, rules and standards for information security	74
Tabel 4.40 Annex 5.19 Information security in supplier relationships	75
Tabel 4.41 Annex 5.20 Addressing information security within supplier agreements	76
Tabel 4.42 Annex Monitoring, review and change management of supplier services	77
Tabel 4.43 Annex 7.2 Physical entry	78
Tabel 4.44 Annex 7.4 Physical security monitoring	80
Tabel 4.45 Annex 7.7 Clear desk and clear screen	80
Tabel 4.46 Hasil Analisis Maturity Level IT Security	81
Tabel 4.47 Annex 5.7 Threat Intelligence	82
Tabel 4.48 Annex 5.24 Information security incident management planning and preparation	83
Tabel 4.49 Annex Assessment and decision on information security events	84
Tabel 4.50 Annex 5.26 Response to information security incidents	84
Tabel 4.51 Annex 8.7 Protection against malware	86
Tabel 4.52 Annex 8.8 Management of technical vulnerabilities	86
Tabel 4.53 Annex 8.12 Data leakage prevention	87
Tabel 4.54 Annex 8.16 Monitoring activities	88
Tabel 4.55 Annex 8.23 Web Filtering	89
Tabel 4.56 Annex 8.24 Use of cryptography	90
Tabel 4.57 Hasil Analisis Maturity Level IT Operation	90
Tabel 4.58 Annex 5.9 Inventory of information and other associated assets	91
Tabel 4.59 Annex 5.11 Return of assets	92
Tabel 4.60 Annex 8.1 User end point devices	93
Tabel 4.61 Annex 8.3 Information access restriction	94
Tabel 4.62 Annex 8.5 Secure authentication	95
Tabel 4.63 Annex 8.9 Configuration management	96
Tabel 4.64 Annex 8.10 Information deletion	97
Tabel 4.65 Annex 8.13 Information backup	98
Tabel 4.66 Annex 8.19 Installation of software on operational systems	99
Tabel 4.67 Annex 8.4 Access to source code	100
Tabel 4.68 Annex 8.25 Secure development life cycle	101
Tabel 4.69 Annex 8.26 Application security requirements	102
Tabel 4.70 Annex 8.27 Secure system architecture and engineering principles	103
Tabel 4.71 Annex 8.29 Security testing in development and acceptance	104
Tabel 4.72 Annex 8.31 Separation of development, test and production environments	105
Tabel 4.73 Hasil Analisis Maturity Level PT XYZ	105