

DAFTAR ISI

ABSTRAK	i
<i>ABSTRACT</i>	ii
HALAMAN PENGESAHAN.....	iii
HALAMAN PERNYATAAN ORISINALITAS.....	iv
KATA PENGANTAR	v
Daftar Isi.....	i
Daftar Gambar.....	iv
Daftar Tabel	v
Daftar Lampiran	vii
Daftar Istilah.....	viii
Daftar Singkatan.....	ix
Bab I Pendahuluan	1
I.1. Latar Belakang	1
I.2. Perumusan Masalah.....	3
I.3. Tujuan Penelitian.....	3
I.4. Batasan Penelitian	4
I.5. Manfaat Penelitian.....	4
Bab II Tinjauan Pustaka	5
II.1. Penelitian Terdahulu.....	5
II.2. Landasan Teori	8
II.2.1. Keamanan Sistem Informasi	8
II.2.2. Teknologi Informasi.....	9
II.2.3. Pengelolaan Risiko.....	10
II.2.4. ISO/IEC 27005:2022.....	10

II.2.5.	Sistem Manajemen Keamanan Informasi	12
II.2.6.	ISO/IEC 27002:2022.....	13
II.3.	Alasan Pemilihan Teori, Kerangka Kerja, atau Mekanisme	13
Bab III	Metodologi Penelitian.....	15
III.1.	Kerangka Berpikir (Opsional)	15
III.2.	Sistematika Penyelesaian Masalah	16
III.3.	Pengumpulan Data.....	20
III.4.	Pengolahan Data atau Pengembangan Produk / Artifak.....	21
III.4.1.	<i>Risk Profile</i>	21
III.4.2.	Asessmen Risiko	22
III.4.3.	<i>Gap Analysis</i>	22
Bab IV	PENGUMPULAN DAN ANALISIS DATA	23
IV.1.	Deskripsi Objek Penelitian	23
IV.1.1.	Visi dan Misi PT Dago Endah.....	24
IV.1.2.	Struktur Organisasi PT Dago Endah	24
IV.2.	Penetapan Konteks.....	25
IV.2.1.	Kriteria Likelihood	25
IV.2.2.	Kriteria Dampak	26
IV.2.3.	<i>Risk Response</i>	27
Bab V	PENILAIAN RISIKO DAN USULAN REKOMENDASI	30
V.1.	Identifikasi Risiko	30
V.1.1.	Identifikasi Aset	30
V.1.2.	Identifikasi Ancaman Terhadap Aset.....	33
V.1.3.	Temuan Kontrol ISO/IEC 27002:2022 Pada Perusahaan	39
V.2.	Potensi Ancaman berdasarkan kontrol ISO/IEC 27002:2022 yang belum terpenuhi.....	43

V.2.1.	Pemilihan Prioritas Ancaman.....	51
V.2.2.	Identifikasi Ancaman Utama	51
V.2.3.	Pengelompokan Ancaman terhadap Aset TI.....	53
V.2.4.	Ancaman terhadap Aset Utama.....	53
V.2.5.	Ancaman terhadap Aset Pendukung	54
V.2.6.	Justifikasi Kontrol Eksisting Ancaman Utama	56
V.3.	Evaluasi Risiko.....	58
V.4.1.	Evaluasi Risiko Untuk Aset Utama	58
V.4.2.	Evaluasi Risiko Untuk Aset Pendukung <i>Hardware</i>	61
V.4.3.	Evaluasi Risiko untuk Aset Pendukung <i>Network</i>	63
V.4.4.	Evaluasi Risiko untuk Aset Pendukung Aset <i>Software</i>	65
V.4.	Pengendalian Risiko	68
V.5.	Rekomendasi Untuk Pengendalian Risiko	71
V.6.1.	Rekomendasi <i>Technology</i> Untuk Serangan <i>Malware</i>	71
V.6.2.	Rekomendasi Kebijakan Sanksi dan Pelanggaran	72
V.6.3.	Rekomendasi Keamanan Informasi dan Penggunaan Internet.....	74
V.6.4.	Rekomendasi Kebijakan Pengendalian Keamanan DoS.....	77
V.6.5.	Rekomendasi Pemusnahan Dokumen dan Data.....	79
V.6.6.	Rekomendasi <i>Technology</i> Sistem <i>Overload</i>	81
V.6.7.	Rekomendasi Prosedur Pelaporan Insiden.....	83
Bab VI	KESIMPULAN DAN SARAN	85
V.1.	Kesimpulan.....	85
V.2.	Saran.....	85
Daftar Pustaka		87