

DAFTAR ISI

	Halaman
DAFTAR ISI	viii
DAFTAR GAMBAR	xi
DAFTAR TABEL	xii
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	3
1.3 Tujuan Penelitian.....	3
1.4 Batasan Masalah.....	4
1.5 Manfaat Penelitian.....	4
1.6 Sistematika Penulisan.....	5
BAB II LANDASAN TEORI	6
2.1 Dasar Teori	6
2.1.1 Keamanan Informasi	6
2.1.2 National Institute Standards of Technology (NIST) CyberSecurity Framework	8
2.1.3 Capability Maturity Model Integration (CMMI)	12
2.1.4 Sistem Informasi Akademik Universitas Tanjungpura (SIKAD Untan)	16
2.2. Penelitian Terdahulu.....	17
BAB III METODOLOGI PENELITIAN	19
3.1 Kerangka Penelitian.....	19
BAB IV ANALISIS DAN PERANCANGAN	22
BAB V HASIL DAN PEMBAHASAN	239
5.1 Kuesioner.....	239
5.2 Penilaian Maturity level	239
5.2.1 Penilaian Maturity level subcategory ID.AM-1	239
5.2.2 Maturity level subcategory ID.AM-2	241
5.2.3 Maturity level subcategory ID.AM-3	242

5.2.4 Maturity level subcategory ID.AM-4	243
5.2.5 Maturity level subcategory ID.AM-5	244
5.2.6 Maturity level subcategory ID.AM-6	245
5.3.7 Maturity level subcategory ID.AM.....	247
5.2.8 Maturity level subcategory ID.RA-1	248
5.2.9 Maturity level subcategory ID.RA-2	250
5.2.10 Maturity level subcategory ID.RA-3	251
5.2.11 Maturity level subcategory ID.RA-4	253
5.2.12 Maturity level subcategory ID.RA-5	254
5.2.13 Maturity level subcategory ID.RA-6	255
5.2.14 Maturity level keseluruhan category ID.RA.....	257
5.3 Penilaian keseluruhan Maturity Level.....	258
5.3.1 Maturity level function identify	258
5.4 Rekomendasi	260
5.4.1 Rekomendasi Perbaiki Subcategory ID.AM-1 (perangkat dan sistem fisik dalam organisasi diinventarisasi).....	260
5.4.2 Rekomendasi Perbaiki Subcategory ID.AM-2 (Platform perangkat lunak dan aplikasi dalam organisasi diinventarisasi).....	261
5.4.3 Rekomendasi Perbaiki Subcategory ID.AM-3 (Komunikasi organisasi dan arus data dipetakan).	262
5.4.4 Rekomendasi Perbaiki Subcategory ID.AM-4 (Sistem informasi eksternal dikatalogkan)	264
5.4.5 Rekomendasi Perbaiki Subcategory ID.AM-5 (Sumber daya (perangkat keras, perangkat, data, waktu, personel, dan perangkat lunak) diprioritaskan berdasarkan klasifikasi, kekritisannya, dan nilai bisnisnya)	265
5.4.6 Rekomendasi Perbaiki Subcategory ID.AM-6 (Peran dan tanggung jawab keamanan siber untuk seluruh tenaga kerja dan pemangku kepentingan pihak ketiga (misalnya, pemasok, pelanggan, mitra) ditetapkan).....	267
5.4.7 Rekomendasi Perbaiki Subcategory ID.RA-1 (Kerentanan aset diidentifikasi dan didokumentasikan).....	269
5.4.8 Rekomendasi Perbaiki Subcategory ID.RA-2 (Ancaman siber intelijen diterima dari berbagai informasi di forum dan sumber).....	273

5.4.9 Rekomendasi Perbaiki Subcategory ID.RA-3 (Ancaman, baik internal maupun eksternal, diidentifikasi dan didokumentasikan).	274
5.4.10 Rekomendasi Perbaiki Subcategory ID.RA-4 (Potensi dampak bisnis dan kemungkinan diidentifikasi).	275
5.4.11 Rekomendasi Perbaiki Subcategory ID.RA-5 (Ancaman, kerentanan, kemungkinan, dan dampak digunakan untuk menentukan risiko).	277
5.4.12 Rekomendasi Perbaiki Subcategory ID.RA-6 (Respons risiko diidentifikasi dan diprioritaskan).	279
BAB VI PENUTUP	281
6.1 Kesimpulan.....	281
6.2 Saran.....	282
DAFTAR PUSTAKA	283
LAMPIRAN	286
Lampiran 1. Kuisisioner	286
Lampiran 2. Dokumentasi Kuisisioner	335