BAB II
LANDASAN TEORI

2.1 Dasar Teori

2.1.1 Keamanan Informasi

Keamanan informasi Menurut Sarno dan Iffano adalah suatu usaha untuk melindungi aset informasi terhadap ancaman dan risiko yang mungkin akan terjadi. sehingga keamanan informasi secara tidak langsung dapat menjamin kontinuitas bisnis, meminimalisir risiko-risiko yang akan terjadi terjadi, dan mengoptimalkan pengembalian investasi. semakin banyak informasi sebuah perusahaan yang disimpan, dikelola, dan dibagikan maka makin akan semakin besar kemungkinan terjadinya risiko kerusakan, kehilangan atau terekspos nya data perusahaan ke pihak luar yang tidak berkepentingan (sarno, & Iffano 2009. Basyarahil, 2017)

Keamanan informasi merupakan aspek penting dalam upaya sebuah organisasi untuk melindungi aset informasinya. Jenis keamanan informasi dapat dibagi menjadi beberapa bagian yaitu (Whitman & Mattord, 2013. Basyarahil, 2017) :

a. *Physical security* Merupakan keamanan yang berfokus pada strategi untuk melindungi pekerja atau anggota organisasi, aset fisik, dan tempat kerja dari berbagai ancaman yaitu berupa bahaya kebakaran, akses tanpa otorisasi dan bencana alam.
b. *Personal security* merupakan keamanan yang hampir sama dengan physical security dalam menjaga orang-orang dalam suatu perusahaan atau organisasi.
c. *Operational security* merupakan keamanan yang berfokus pada strategi untuk melindungi kemampuan perusahaan atau organisasi agar tidak terdapat gangguan dan hambatan saat bekerja.
d. *Communication security* merupakan keamanan yang bertujuan untuk melindungi media komunikasi, teknologi komunikasi beserta isinya,

dan kemampuan untuk menggunakan alat ini agar organisasi dapat mencapai tujuannya.

e. *Network Security* merupakan keamanan yang berfokus pada perlindungan peralatan jaringan dan organisasi, jaringan dan isinya, serta kemampuan untuk memanfaatkan jaringan tersebut dalam memenuhi fungsi komunikasi data organisasi tersebut.

Keamanan informasi juga memiliki tiga karakteristik penting yaitu:

a. *Confidentiality* (kerahasiaan) yaitu merupakan karakteristik yang menjadi pondasi utama dalam tiap-tiap kebijakan keamanan sistem informasi. *Confidentiality* adalah seperangkat aturan yang bertujuan untuk menentukan apakah sebuah subjek tertentu dapat mengakses ke objek tertentu lainnya. Karakteristik ini juga hanya bisa diakses oleh orang yang berwenang dan bisa menjamin kerahasiaan data yang dikirim, diterima dan disimpan.
b. *Integrity* (kepercayaan) adalah terpercayanya suatu informasi yang ada. yang mencakup data *integrity*. Keutuhan informasi dapat dikatakan utuh jika informasi belum dirubah atau masih orginal. Maksud dari perubahan adalah perubahan yang terjadi karena kesengajaan ataupun tidak.
c. *Availability* (ketersedian) merupakan ketersediaan sumber informasi saat diperlukan. Ketersediaan ini dapat dipengaruhi oleh faktor teknis, faktor alam, dan faktor manusia. akan tetapi umumnya manusia adalah faktor yang paling lemah diantara tiga faktor lainnya.

Dari Penjelasan diatas dapat ditarik kesimpulkan bahwa *confidentiality*, *integrity*, dan *availability* adalah karakteristik yang saling berhubungan dan harus dipenuhi untuk melindungi sebuah keamanan informasi. Berikut adalah gambaran dari hubungan antara ketiga karakteristik dapat dilihat pada gambar 2.1 berikut ini:

Gambar 2.1 karakteristik keamanan informasi

(sumber: https://dolphin.cmcglobal.com.vn/quan-li-tai-san-thong-tin-cua-doanh-nghiep/)

Jika karakteristik sistem keamanan informasi dan prinsip dasar penyusunan program keamanan informasi sudah terpenuhi, maka akan terjamin dan terlindungi sumber daya informasi dari ancaman orang-orang yang tidak bertanggungjawab yang akan menyalah gunakan data dan informasi untuk kepentingan yang bisa merugikan sebuah organisasi atau perusahaan. (BPPTIK/Nika/Hary/hdn)

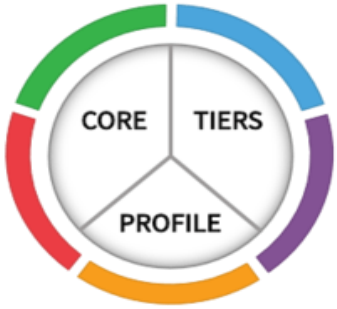
2.1.2 National Institute Standards of Technology (NIST) CyberSecurity Framework

National Institute Standards of Technology (NIST) CyberSecurity Framework merupakan kerangka kerja kebijakan panduan keamanan komputer yang pertama kali terbit pada bulan Februari 2014 tentang bagaimana organisasi sektor swasta di Amerika Serikat dapat menilai dan meningkatkan kemampuan untuk mencegah, mendeteksi, dan menangani serangan dari dunia maya. Untuk mengimplementasikan kerangka kerja NIST ini membutuhkan kerangka kerja lain karena sifatnya bergantung pada kerangka kerja yang lain. Kerangka kerja lain yang dapat digunakan adalah COBIT 5, ISO/IEC 27001, NIST SP. 800-53, CIS CSC dan ISA 62443.

Kerangka Keamanan Siber terdiri dari tiga komponen utama:

a. Inti Kerangka
b. Tingkat Implementasi
c. Profil

Gambar komponen utama cybersecurity framework dapat dilihat pada gambar 2.2 berikut ini.



Gambar 2.2 komponen utama Cybersecurity framework
(sumber:https://www.nist.gov/cyberframework/online-learning/components-framework)

1. *Framework Core* (Kerangka Inti)

Kerangka Inti menyediakan serangkaian kegiatan untuk mencapai cybersecurity dengan hasil yang spesifik, dan sebagai referensi contoh panduan untuk mencapai hasil tersebut. Kerangka inti bukanlah daftar periksa tindakan yang dilakukan akan tetapi menyajikan hasil keamanan siber terutama pada yang diidentifikasi oleh pemangku kepentingan berguna dalam mengelola risiko keamanan siber. Inti terdiri dari empat elemen yaitu: Fungsi, Kategori, subkategori, dan referensi informatif. Elemen inti dapat dilihat pada gambar 2.3 berikut ini (https://www.nist.gov/cyberframework/online-learning/components framework).

Gambar 2.3 Komponen framework Core
(sumber: Framework for Improving Critical Infrastructure Cybersecurity version 1.1,2018)

Elemen *Framework Core* bekerja sama sebagai berikut:

a. **Fungsi** yaitu mengontrol aktivitas keamanan siber dasar pada level tertingginya. Fungsi digunakan untuk Mengidentifikasi, Melindungi, Mendeteksi, Menanggapi, dan Memulihkan. Membantu organisasi untuk memanajemen risiko keamanan sibernya dengan mengatur informasi, memungkinkan keputusan manajemen risiko, menangani ancaman, dan meningkatkan dengan belajar dari aktivitas sebelumnya. Fungsi juga sejalan dengan metodologi yang ada untuk manajemen insiden serta membantu menampilkan dampak investasi dalam keamanan siber
b. **Kategori** adalah subdivisi dari suatu fungsi ke dalam kelompok hasil keamanan siber berkaitan erat dengan kebutuhan programatik dan aktivitas tertentu.
c. **Subkategori** adalah membagi Kategori lebih lanjut menjadi sebuah hasil khusus terkait teknis atau kegiatan manajemen. Memberikan serangkaian hasil meskipun tidak lengkap, akan tetapi membantu mendukung pencapaian hasil di setiap Kategori".
d. **Referensi Informatif** adalah bagian khusus dari standar, pedoman, dan praktik umum di antara bagian infrastruktur kritis yang menunjukkan metode untuk mencapai hasil yang berkaitan dengan setiap Subkategori. Referensi Informatif dipaparkan dalam Kerangka Inti tidak lengkap dan bersifat ilustratif.

Lima fungsi Inti Kerangka didefinisikan dibawah ini. Fungsi harus dilakukan secara bersamaan dan *kontinue* untuk membentuk budaya operasional yang menjawab dinamika risiko keamanan siber (Framework for Improving Critical Infrastructure Cybersecurity version 1.1,2018). Berikut gambar fungsi framework core dapat dilihat pada gambar 2.4 berikut ini.

Gambar 2.4 fungsi framework Core
(sumber: https://www.nist.gov/cyberframework/online-learning/five-functions)

a. **Identifikasi (Identify)**
   Dikembangkan pemahaman sebuah organisasi atau perusahaan untuk mengelola risiko keamanan siber yaitu seperti sistem, orang, aset, data, dan kemampuan. Aktivitas pada Fungsi Identifikasi adalah dasar untuk penggunaan kerangka yang efektif. Memahami konteks bisnis, sumber daya yang mendukung bahwa fungsi sangat penting, dan risiko keamanan siber yang memungkinkan organisasi untuk fokus dan memprioritaskan usahanya, sesuai dengan strategi manajemen risiko dan kebutuhan bisnisnya.

b. **Lindungi (Protect)**
   Dikembangkan dan diaplikasikan pengamanan yang sesuai untuk menjamin pengiriman jasa yang baik. Fungsi Lindungi mendukung kemampuan untuk membatasi atau menahan dampak potensi acaman keamanan siber.

c. Deteksi (Detect)
   Dikembangkan dan menerapkan kegiatan yang sesuai untuk mengidentifikasi terjadinya acaman keamanan siber. Fungsi Deteksi memungkinkan penemuan insiden keamanan siber secara tepat waktu.

d. Menanggapi (Respons)
   Mengembangkan dan menerapkan aktivitas yang sesuai untuk mengambil tindakan terkait insiden keamanan siber yang terdeteksi.

Fungsi Respons mendukung kemampuan untuk menampung dampak dari suatu potensi insiden keamanan siber.

e. Pulih (Recover)

Dikembangkan dan menerapkan aktivitas yang sesuai untuk memelihara rencana ketahanan dan untuk memulihkan kemampuan atau layanan apa pun yang terganggu karena keamanan siber. Fungsi Pemulihan mendukung pemulihan tepat waktu ke operasi normal untuk mengurangi dampak dari insiden keamanan siber

(sumber: https://www.nist.gov/cyberframework/online-learning/five-functions)

2.1.3 Capability Maturity Model Integration (CMMI)

Capability mature model integration (CMMI) ialah pendekatan yang bisa digunakan dalam mengembangkan *software* dan meningkatkan kualitas produk ataupun layanan pada sebuah organisasi. CMMI juga digunakan untuk meningkatkan proses (process improvement) dalam sebuah organisasi. Penerapan CMMI bertujuan untuk meningkatkan proses pengembangan dan perawatan *software* didalam sebuah organisasi.

Capability mature model integration (CMMI) mempunyai dua tahap representasi dalam usaha untuk melaksanakan perbaikan pada proses pengembangan perangkat lunak yang diterapkan oleh organisasi, ialah bertahap (staged) dan berkelanjutan (continuous). Perbedaan utama yang mendasari antara dua representasi ini merupakan bagaimana process area yang ada akan diorganisasikan serta direpresentasikan. Process area yang dimaksud merupakan hal- hal yang menjadi tujuan akhir difokuskan untuk diselesaikan. Kategori pemodelan ini membantu organisasi pengembang software dalam memutuskan strategi proses pengembangan perangkat lunak. Model ini akan memfasilitasi penentuan kemampuan untuk setiap tahapan proses dan mengidentifikasi masalah- masalah kritis yang harus secepatnya dibenahi.

Pada repesentasi staged ini, suatu organisasi pengembang perangkat lunak melewati beberapa macam tahapan ataupun tingkatan dalam upayanya mencapai tingkat kematangan(maturity) yang tinggi. Tahapan ataupun tingkatan yang

dicapai oleh organisasi tersebut wajib bersifat kumulatif, yang artinya setiap tahapan ataupun tingakatan di atas harus bisa memenuhi tujuan- tujuan(golas) pada tahapan di bawahnya. Tingkatan(level) harus benar- benar dipenuhi oleh setiap organisasi pengembang secara bertahap. Tingkatan (level) ini dibagi menjadi 5 tahapan, ialah:

a. Initial (level 1)

Pada tingkat initial (level 1), sesuatu organisasi pengembang perangkat lunak disimulasikan sebagai ad hoc dan kondisinya kacau. Organisasi perngembang perangkat lunak yang cenderung tidak memiliki lingkungan yang tidak stabil untuk mendukung berjalannya proses pengembangan perankat lunak. Oleh karena itu, tingkat keberhasilan yang dihasilkan oleh organisasi pengembang memiliki ketergantungan terhadap keahlian dan kerja keras dari satu ataupun beberapa orang yang ada didalamnya. Pada tingkatan ini, meskipun nanti suatu organisasi pengembang dapat memberikan hasil akhir suatu produk ataupun jasa sesuai tujuan, akan tetapi tahap perencanaan yang telah dilakukan sebelumnya cenderung tidak dapat memenuhi harapan. Keberhasilan membuat produk/ sistem perangkat lunak tidak mempunyai sifat yang stabil.

b. Managed (level 2)

Pada tingkat managed (level 2), terdapat suatu kesepakatan dasar untuk prosedur bersumber pada kebijakan yang ada terhadap perencanaan kegiatan. Oleh karena itu, produk atau jasa yang dibuat dapat dijaga kualitasnya(quality control). Beberapa usaha yang dilakukan dalam melindungi kualitas produk ataupun jasa diantaranya ialah melakukan perencanaan kegiatan, pembagian tugas- tugas, memantau antara perencanaan yang dilakukan dengan penerapan di lapangan, melaksanakan tindakan apabila terdapat perubahan terhadap perencanaan, dan melaksanakan milestone atau pemantauan produk ataupun jasa pada suatu titik tertentu pada rangkaian kegiatan. Tidak hanya terdapat standardisasi prosedur dalam pengembangan suatu produk ataupun jasa, terdapat komitmen yang tercipta di antara para stakeholder.

c. Defined (level 3)

Pada tingkat defined (level 3), proses- proses sudah dikarakterisasi dan dipahami dengan baik, dan dipaparkan melalui standar, prosedur, tool, serta metode yang ada. Kumpulan proses standar dari organisasi, yang merupakan dasar dari tingkat kematangan 3, didirikan serta ditingkatkan seiring berjalannya waktu. Proses- proses standar ini digunakan untuk membangun konsistensi di dalam organisasi. Proyek membangun proses terdefinisi dengan mengacu kepada proses standar yang dimiliki oleh organisasi tersebut.

d. Quantitatively Managed (level 4)

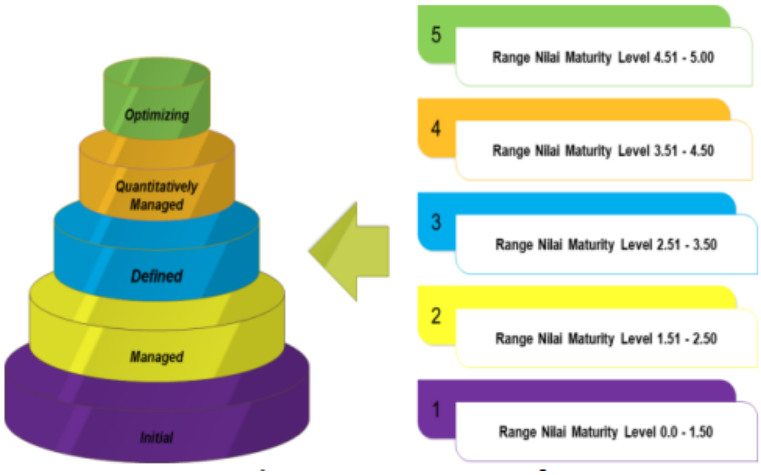
Pada tingkat quantitatively managed (level 4), organisasi serta proyek membangun tujuan kuantitatif untuk kualitas dan kinerja proses, serta menggunakannya sebagai kriteria dalam pengelolaan proses. Tujuan kuantitatif didasarkan pada kebutuhan pelanggan, pengguna akhir, organisasi, serta pihak yang mengimplementasi proses. Kualitas dan kinerja proses dipahami dalam istilah- istilah statistik dan dikelola sepanjang waktu penggunaan proses. Untuk subproses yang terpilih, pengukuran detil akan kinerja proses dikumpulkan serta dianalisa secara statistik. Pengukuran kualitas dan kinerja proses dimasukkan ke dalam penyimpanan pengukuran organisasi untuk menunjang proses pengambilan keputusan yang bersumber pada fakta. Penyebab khusus dari variasi proses diidentifikasi serta, apabila tepat, sumbernya dikoreksi untuk menghindari kejadian lagi di lain waktu.

e. Optimizing (level 5)

Pada tingkat optimizing (level 5), suatu organisasi secara berkesinambungan meningkatkan proses- prosesnya bersumber pada pengertian kuantitatif hendak penyebab- penyebab umum dari variasi proses. Tingkat kematangan 5 mengkonsentrasikan kepada peningkatan secara berkesinambungan akan kinerja proses melalui proses inkremental serta inovatif, dan juga peningkatan secara teknologi. Tujuan peningkatan proses secara kuantitatif untuk organisasi dibangun, diperbaiki secara berkesinambungan untuk mengatasi tujuan bisnis yang dinamis, serta

digunakan sebagai kriteria dalam mengelola peningkatan proses. Akibat-akibat dari peningkatan proses yang diterapkan diukur serta dievaluasi secara bertentangan terhadap tujuan peningkatan proses kuantitatif. Baik proses terdefinisi maupun kumpulan proses standar organisasi merupakan tujuan dari kegiatan peningkatan yang bisa diukur (Syafitri, 2016)

Adapun nilai indeks pada maturity level CMMI dapat dilihat pada gambar 2.5 dan tabel 2.1 berikut ini.



Gambar 2.5 *Maturity Level*

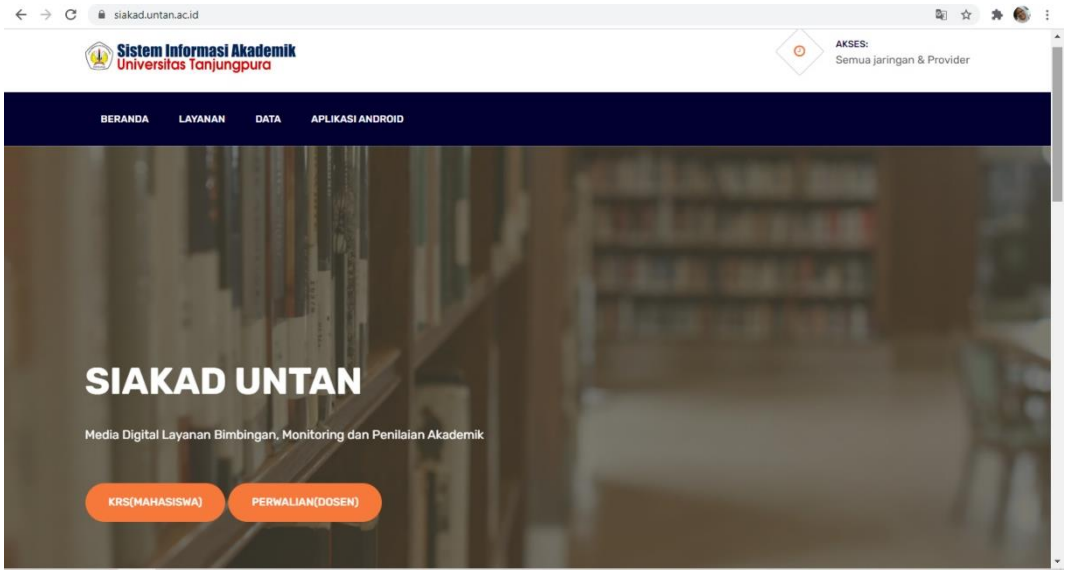
Tabel 2. 1 indeks *maturity Level*

No	Rentang Nilai	*Maturity Level*
1.	0.0 -1.50	*Initial*
2.	1.51-2-50	*Managed*
3.	2.51-3.50	*defined*
4.	3.51-4.50	*Quantitatively managed*
5.	4.51-5.00	*Optimizing*

Pada tabel rentang skala indeks *maturity level* mempunyai rentang nilai yang menyatakan bahwa tingkat kematangan *initial* memiliki nilai 0.0 -1.50, tingkat kematangan *Managed* memiliki nilai 1.51-2-50, tingkat kematangan *defined* memiliki nilai 2.51-3.50, tingkat kematangan *Quantitatively managed* 3.51-4.50, dan tingkat kematangan *Optimizing* 4.51-5.00 (Umar dkk, 2019).

2.1.4 Sistem Informasi Akademik Universitas Tanjungpura (SIAKAD Untan)

Sistem Informasi Akademik Universitas tanjungpura merupakan suatu sistem yang dirancang untuk mempermudah perkuliahan dalam kegiatan akademik. sistem ini dirancang untuk memenuhi kebutuhan dalam mengelola data akademik mahasiswa menggunakan teknologi komputer secara menyeluruh. Dengan begitu, kegiatan akademik dapat dikelola dengan baik. Pada SIAKAD untan terdapat dua level login yang pertama login sebagai mahasiswa dan yang kedua login sebagai dosen. Didalam SIAKAD Untan terdapat berbagai layananan seperti grafik akademik untuk melihat perkembangan akademik mahasiswa setiap semester, pengisian rencana studi, melihat hasil studi, transkrip nilai, bimbingan, E-learning, jadwal perkuliahan, history pembayaran semester, cetak KTM, dan cuti kuliah. Salah satu manfaat dari SIAKAD Untan adalah memudahkan mahasiswa dalam mendapatkan informasi yang dibutuhkan secara secepat. SIAKAD Untan dapat diakses melalui https://siakad.untan.ac.id/ . Tampilan dari SIAKAD Untan dapat dilihat pada gambar 2.6 berikut ini:



Gambar 2.6 SIAKAD Untan
(sumber : https://siakad.untan.ac.id/)

2.2. Penelitian Terdahulu

Peneliti serupa yang menganalisis tentang tingkat kematangan keamanan informasi telah banyak dilakukan sebelumya. Adapun daftar penelitian-penelitian terdahulu yang juga mengangkat topik serupa dapat dilihat pada tabel 2.2 berikut ini.

Tabel 2. 2 Penelitian Terdahulu

1	Judul	Evaluasi Tingkat Kematangan Keamanan Infromasi Pada Sistem Informasi Manajemen Universitas Cokroaminoto Palopo
	Tahun	2018
	Penlis	Erfina, Ema Utami, Andi Sunyoto
	Deskripsi	Penelitian ini bertujuan untuk mengetahui tingkat kematangan keamanan informasi pada sistem informasi Universitas Cokroaminoto Palopo agar dapat mengevaluasi, mengimplementasikan dan memelihara keamanan informasi diperusahaan berdasarkan best practice dalam pengamanan informasi
	Metode	ISO/IEC 27001
	Hasil	Nilai tingkat kematangan SIMUNCP berada pada level = 1,48 yaitu initial-adhoc yang berarti bahwa SIMUNCP secara umum telah mengetahui masalah yang harus diatasi, namun tidak terdapat proses standar dalam aktivitas tersebut, pendekatan yang digunakan cenderung dilakukan secara individu atau perkasus, dengan kata lain pendekatan proses sistem informasi pada SIMUNCP tidak terorganisasi
2	Judul	Pengukuran Tingkat Kematangan Layanan IT dengan CMMI
	Tahun	2019
	Penlis	Desi Arisandy, Rudi, Salsalina Br Sembiring
	Deskripsi	Penelitian ini bertujuan mengukur sejauh mana tingkat kematangan layanan TI yang telah diimplementasikan diperguruan tinggi XYZ
	Metode	*Capability Maturity Model Integration* (CMMI)
	Hasil	Berdasarkan hasil penelitian yang telah dilakukan, tingkat kematangan layanan TI Universitas xyz masih berada pada level 1 *(initial)* dimana proses layanan berjalan secara ad-hoc dan kacau, serta keberhasilkan organisasi masih berasal dari kompetensi perorangan.
3	Judul	Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks KAMI berdasarkan ISO/IEC 27001:2013 pada politeknik ilmu pelayaran Semarang
	Tahun	2019
	Penlis	Desy Dwi Prasetyowati, Indra Gamayanto, sasono wibowo, suharnawi
	Deskripsi	Penelitian ini bertujuan untuk melakukan evaluasi terhadap tingkat keamanan informasi yang terdapat pada PIP
	Metode	Indeks KAMI berdasarkan ISO/IEC 27001:2013

Tabel 2. 3 Penelitian Terdahulu (Lanjutan)

	Hasil	Hasil yang didapatkan adalah untuk sistem elektronik menghasilkan score 20, tingkat kelengkapan informasi sebesar 238. Dilihat dari hasil bahwa masih rendahnya tingkat keamanan dan disini dibutuhkan tingkat keamanan yang lebih tinggi lagi.
4	Judul	Evaluasi Tingkat Kesiapan Keamanan Informasi pada Lembaga Pendidikan Menggunakan Indeks KAMI 4.0
	Tahun	2019
	Penlis	Pramudhita Ferdiansyah, Subektiningsih, Rini Indrayani
	Deskripsi	Penelitian ini dilakukan untuk mengukur tingkat kesiapan kematangan dan kelengkapan keamanan infromasi pada UPTD xyz dikarenakan banyaknya data informasi yang terdapat pada UPTD XYZ dalam menangani pelayanan publik.
	Metode	INDEKS KAMI 4.0
	Hasil	Hasil yang didapatkan dari evaluasi untuk kebutuhan sistem elektronik sebesar 20, sedangkan tingkat kelengkapan informasi mendapatkan skor 245. Dari hasil tersebut dapat disimpulkan bahwa tingkat keamanan informasi masih sangat rendah dan diperlukan perbaikan sistem keamanan informasi dengan bekerja sama dengan pengembang keamanan informasi dari pihak ketiga

Pada Penelitian terdahulu dan penelitian yang akan dilakukan sama-sama bertujuan untuk mengetahui tingkat kematangan keamanan informasi pada sebuah organisasi. Akan tetapi pada penelitian terdahulu terdapat beberapa framework yang digunakan untuk melakukan penilaian tingkat kematangan pada sebuah organisasi yaitu menggunakan Indeks KAMI berdasarkan ISO/IEC 27001, dan juga CMMI. Sedangkan pada penelitian yang akan dilakukan menggunakan NIST *Cybersecurity Framework* dan CMMI. ISO /IEC 27001 dan NIST sama-sama merupakan framework dari tata kelola TI hanya saja terdapat perbedaan pada ruang lingkupnya, ISO/IEC 27001 membahas tentang apa saja yang harus dilakukan oleh perusahaan dalam mengimplementasikan konsep-konsep keamanan informasi sedangkan NIST lebih membahas tentang bagaimana cara meningkatkan kualitas perusahaan dengan manajemen tingkat risiko yang seminimal mungkin. Penelitian yang akan dilakukan mengadopsi framework CMMI pada penelitian sebelumnya untuk penilaian tingkat kematangannya yang akan dikombinasikan dengan NIST *Cybersecurity Framework* untuk framework tata kelola TI dalam menganalisis risiko.