BAB I
PENDAHULUAN

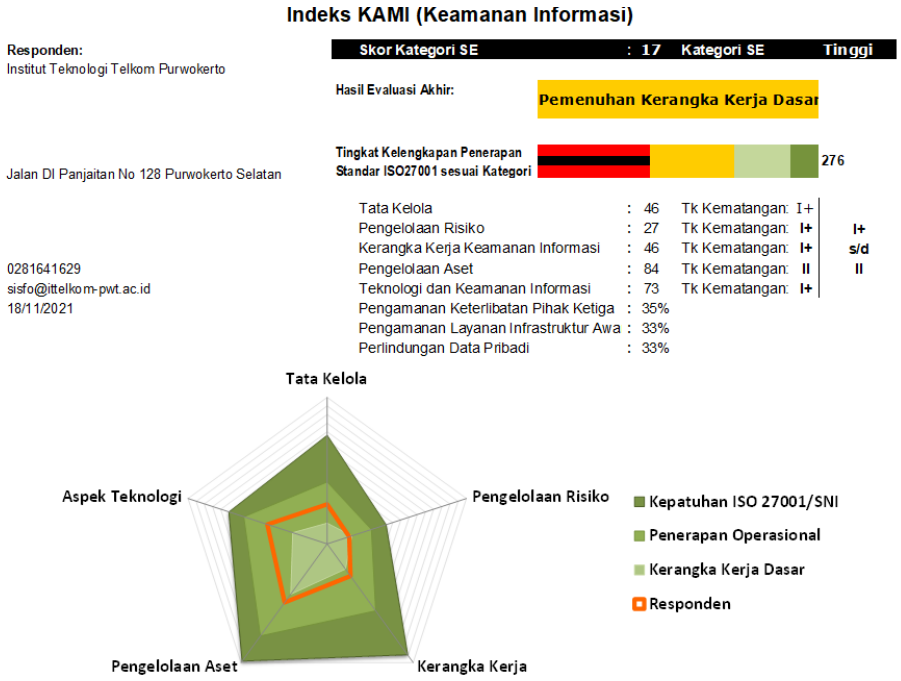
1.1. Latar Belakang Masalah

Di era globalisasi, pendidikan tergabung dalam salah satu sektor yang berkembang dan beradaptasi dengan munculnya berbagai teknologi. Kehadiran *website* dari sebuah instansi pendidikan menjadi penting karena dapat menjadi sumber informasi dan edukasi untuk para siswa dan masyarakat umum. Instansi perguruan tinggi adalah bagian dari organisasi yang mempercayakan informasi penting pada peralatan teknologi informasi. Layanan informasi tersebut tidak hanya diberikan pada civitas akademik lingkungan internal namun juga pada alumni dan masyarakat umum. Dalam upaya meningkatkan nilai pada instansi perguruan tinggi harus memiliki sumberdaya yang strategis [1].

Informasi merupakan salah satu sumber daya yang strategis menjadi syarat mutlak bagi instansi perguruan tinggi untuk melindungi keamanan informasi bedasarkan Klarifikasi Indeks Keamanan Informasi (KAMI) [2]. Informasi-informasi yang ditempatkan pada sebuah *website* harus dijaga dari berbagai ancaman, baik ancaman yang disebabkan oleh bencana alam hingga kejahatan teknologi informasi yang disebabkan oleh manusia, terutama dari oknum yang sengaja melakukan berbagai kerusakan terhadap informasi tersebut [3]. Sangat rentan bagi suatu instansi terserang *cyber*, tak sedikit instansi yang meras bukan sasaran para *hacker*. Penggunaan *websit*e sebagai sarana pemberi informasi. Institut Teknologi Telkom Purwokerto (ITTP) memiliki *website* yang berguna sebagai sarana penyimpanan data nilai tiap mahasiswa yang dikenal *dengan I-Gracias, Learning Management System* dan layanan Sistem dan Teknologi Informasi (STI) ITTP yang tidak luput dari serangan *cyber*.

Berdasarkan hasil investigasi dan analisis awal, menurut Bapak Yudha Saintika, S.T., M.T.I. selaku Kepala Bagian STI ITTP mengkonfirmasi bahwa *website* ITTP telah disusupi oleh *malware* yang termasuk kedalam jenis *Web Shell* dimana *malware* ini merupakan jenis *malware* yang secara khusus memudahkan

pelaku kriminal dalam mengontrol *website* yang berhasil diambil alih pelaku. Tercatat setiap harinya *website* ITTP menerima ribuan serangan secara terus menerus, baik yang dilakukan secara otomatis oleh robot maupun berdalangkan manusia. Salah satu serangan tersebut berhasil masuk dan menginfeksi *website* ITTP dengan berbagai macam *malware* berbahaya. *Malware* ini mampu masuk dan menginfeksi targetnya dengan berbagai cara seperti serangan *bruteforce* atau lebih dikenal pembobolan sistem keamanan ke halaman login *dashboard wordpress* yang tidak dilindungi sehingga dapat membobol *password website*, ekspoloitasi terhadap celah keamanan pada *wordpress* yang tidak diperbarui, dan kesalahan konfigurasi pada sistem.



(Lampiran 3) Gambar 1. 1 Nilai Indeks KAMI ITTP Triwulan ke-4 2021[4].

Pada Gambar 1.1 menampilkan Dashboard dari hasil *assessment* STI ITTP yang telah melakukan *assessment* pada bulan November 2021. Berdasarkan hasil *assessment* KAMI Institut Teknologi Telkom Purwokerto pada Triwulan ke-4 2021 antara bagian Sistem dan Teknologi Informasi (STI) ITTP dengan Unit Digital Transformation Yayasan Pendidikan Telkom pada hari Rabu tanggal 8 Desember 2021 dapat disimpulkan bahwa hasil evaluasi akhir tingkat kesiapan indeks KAMI ITTP adalah rendah.

(Lampiran 4) Tabel 1. 1 Nilai Tiap Area Keamanan Informasi ITTP pada Triwulan ke-4 2021[4].

Area Keamanan Informasi	Nilai ITTP	Nilai Referensi (SE Tinggi)	Rekomendasi Perbaikan
Tata Kelola	46	>72	ITTP perlu segera menyusun dan menetapkan: 1. Kebijakan Keamanan Informasi, 2. Kebijakan Keamanan Infrastruktur, 3. Pedoman Pengujian Keamanan Aplikasi, dan 4. Kebijakan Penanggulangan Insiden Keamanan Informasi yang menyangkut pelanggaran hukum pidana atau perdata. Selain itu, ITTP perlu melakukan: 1. Pemisahan dokumen Manual Mutu dengan Kebijakan Keamanan Informasi menjadi dua dokumen yang berbeda. 2. Penyelarasan nomor bab pada dokumen Manual Mutu dengan nomor klausul ISO 27001
Pengelolaan Resiko	27	>54	ITTP perlu untuk segera menerapkan secara menyeluruh 1. Pedoman Pengelolaan Risiko yang bersifat teknis di bagian STI (bukan strategis di institusi), 2. Risk assessment berdasarkan pedoman poin 1, dan 3. DRP untuk meningkatkan Keamanan Informasi
Kerangka Kerja Keamanan Informasi	46	>96	ITTP perlu segera Menyusun dan menetapkan: 1. Kebijakan Keamanan Infrastruktur, 2. Pedoman Rencana Pemulihan Bencana IT, dan 3. Pedoman Pengelolaan Keberlangsungan Bisnis.
Pengelolaan Data	84	>132	ITTP perlu segera menyusun: 1. Prosedur Pengendalian Informasi Terdistribusi, 2. Manajemen Konfigurasi, dan

Area Keamanan Informasi	Nilai ITTP	Nilai Referensi (SE Tinggi)	Rekomendasi Perbaikan
			3. Proses Manajemen Perubahan
Pengelolaan Aset	73	>102	ITTP perlu segera Menyusun dan menetapkan: 1. Pedoman Kebijakan Pengamanan Infrastruktur, 2. Laporan post moreterm analysis, dan 3. Laporan Penetration Test Aplikasi,
Teknologi dan Keamanan Informasi	276	>456	*Keterangan: >273 Pemenuhan Kerngka Kerja Dasar, >456 Cukup Baik, >584 Baik

Berdasarkan hasil evaluasi KAMI ITTP pada Triwulan ke-4 2021 rincian nilai dan rekomendasi perbaikan pada area keamanan pengelolaan risiko memiliki nilai 27 dari >54 nilai referensi dengan rekomendasi perbaikan untuk menerapakan pedoman pengelolaan risiko yang bersifat teknis di bagian STI. Selain itu, rekomendasi lainya adalah dibutuhkannya rancangan *Disaster Recovery Plan* untuk meningkatkan indeks KAMI[5]. Berdasarkan permasalahan diatas guna menyusun perencanaan penanganan bencana pada KAMI STI ITTP maka akan dilakukan penelitan dengan judul **"Penyusunan Disaster Recovery Plan Menggunakan Pendekatan Nist 800-34 (Studi Kasus: Bagian Sistem Dan Teknologi Informasi ITTP)"**.

1.2.Perumusan Masalah

Berdasarkan dari uraian latar belakang pada penelitian in, berikut adalah masalah yang telah dirumuskan:

1. Indeks KAMI di Institut Teknologi Telkom Purwokerto masih rendah.
2. Pada area Keamanan Informasi bagian pengelolaan risiko mendapat rekomendasi perbaikan pembuatan DRP untuk meningkatkan keamanan informasi.

3. Adanya serangan terhadap *website* ITTP berupa pembobolan sistem keamanan pada halaman *login dashboard wordpress*.

1.3.Pertanyaan Penelitian

Berdasarkan latar belakang dan perumusan masalah disusun pertanyaan penelitian sebagai berikut:

"Bagaimana menyusun dokumen *Disaster Recovery Plan* menggunakan pendekatan *NIST 800-34* untuk menghasilkan strategi *recovery* berupa dokumen *DRP* yang terverifikasi dan tervalidasi?"

1.4.Batasan Masalah

Untuk membatasi penelitian agar fokus dan terarah, maka diperlukan ruang lingkup sebagai berikut:

1. Fokus penelitian ini dilakukan di bagian Sistem informasi Bagian Sistem dan Teknologi Informasi Institut Teknologi Telkom Purwokerto.
2. Difokuskan pada kerangka kerja yang digunakan dalam perancangan *Disaster Recovery Plan* adalah Evaluasi Indeks KAMI Institut Teknologi Telkom Purwokerto (ITTP) Triwulan ke-4 Tahun 2021.
3. Penelitian ini menghasilkan dokumen *Disaster Recovery Plan* berupa strategi *recovery* yang dihasilkan melalui *Risk Assessment* pada bagian Sistem Informasi bagian STI Institut Teknologi Telkom Purwokerto.

1.5.Tujuan Penelitian

Menghasilkan rancanangan untuk penanggulangan bencana alam dan non-alam yang memungkinkan terjadi, berupa dokumen *Disaster Recovery Plan* untuk menjalankan proses vital dan meminimalisir kerugian pada Sistem Informasi di Institut Teknologi Telkom Purwokerto.

1.6.Manfaat Penelitian

Manfaat penelitian dibagi menjadi dua yaitu manfaat teoritis adalah yang didapatkan subyek. Sedangkan manfaat praktis adalah manfaat yang didapatkan penulis dari penelitian ini. Adapun manfaat teoritis dan praktis yang didapatkan dari penelitian ini yaitu antara lain sebagai berikut.

1.6.1 Manfaat Teoritis

1. Memperkecil kerugian waktu dan meningkatkan produktivitas dalam menerapkan proses kritis pada bagian Sistem Informasi bagian STI Institut Teknologi Telkom Purwokerto dengan pelaksanaan prosedur recovery yang cepat.
2. Meningkatkan strategi terutama pada keamaanan Sistem Informasi Bagian STI Institut Teknologi Telkom Purwokerto setelah adanya *Disaster Recovery Plan*.
3. Bagian STI Institut Teknologi Telkom Purwokerto mendapat arahan terkait penanganan bencana yang dapat timbul menggunakan *Disaster Recovery Plan*.
4. Sebagai masukan untuk bagian STI Institut Teknologi Telkom Purwokerto dalam meningkatkan keamanan informasi.

1.6.2 Manfaat Praktis

1. Menambah pengalaman dalam melakukan penelitian.
2. Hasil penelitian ini diharapkan dapat memberikan sumbangan pemikiran maupun sebagai masukan pagi penelitian lain.
3. Mengimplementasikan teori dan ilmu yang telah didapatkan selama dalam perkuliahan dalam bidang keamanan informasi serta mempelajari menganalisa tiap data mentah dan data aset bagian STI yang dibutuhkan dalam menyusun strategi *recovery*.