BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Di zaman modern saat ini, teknologi informasi berperan penting dalam membantu mempermudah pekerjaan manusia. Universitas Pendidikan Ganesha (Undiksha) merupakan salah satu lembaga penyelenggara pelayanan publik bidang pendidikan di Bali Utara yang menerapkan teknologi informasi dalam mendukung dan menjalankan sebagian besar proses bisnisnya. Unit Penunjang Akademik Teknologi, Informasi dan Komunikasi (UPA TIK) merupakan salah satu unit yang dimiliki oleh Universitas Pendidikan Ganesha (Undiksha) yang membantu melaksanakan seluruh kegiatan teknis di bidang teknologi informasi dan komunikasi (TIK) (Universitas Pendidikan Ganesha 2017).

UPA TIK memiliki 5 (lima) devisi yaitu devisi *Helpdesk* dan Dokumentasi, devisi Infrastuktur, Jaringan, dan Keamanan, devisi Manajemen Konten, devisi Pusat Data dan Informasi, devisi Sistem Informasi. Kelima devisi yang terdapat di UPA TIK memiliki peran dalam mendukung pelaksaan tugas dan fungsi dari UPA TIK. Tugas pokok UPA TIK adalah melaksanakan pengembangan, pengelolaan, dan pelayanan TIK, serta pengelolaan sistem informasi dan jaringan yang terdapat di Undiksha. Dalam melaksanakan tugasnya, UPA-TIK memiliki fungsi penyusunan rencana, program, dan anggaran UPA; pengembangan teknologi informasi dan komunikasi; pengelolaan teknologi informasi dan komunikasi; pemberian layanan di bidang teknologi informasi dan komunikasi; pengembangan dan pengelolaan sistem informasi; pengembangan dan pengelolaan jaringan; pemeliharaan dan perbaikan jaringan; dan pelaksanaan urusan tata usaha UPA.

Tugas dan fungsi yang dimiliki oleh UPA TIK secara tak langsung mengindikasikan bahwa UPA TIK merupakan tempat dimana seluruh aktivitas pertukaran, pengelolaan, dan penyimpanan informasi pada sistem terjadi, sehingga rentan terhadap munculnya ancaman keamanan informasi. Berdasarkan panduan yang dikeluarkan oleh Tim Direktorat Keamanan Informasi (Kominfo) dijelaskan bahwa

dalam penyelenggaraan tata kelola TIK oleh instansi penyelenggara pelayanan publik, aspek keamanan informasi memiliki peranan yang penting/krusial yang tidak bisa diabaikan karena dapat menyebabkan permasalahan di bagian keamanan informasi yang menyangkut kerahasiaan (confidentiality), keutuhan (integrity) dan ketersediaan (availability) sehingga menghambat kinerja tata kelola TIK secara keseluruhan (Direktorat Keamanan Informasi 2011).

Ancaman keamanan informasi (Information Security Threat) yang kemungkinan bisa terjadi yaitu serangan DoS, DDoS, Back Door, Sniffer, Spoofing, Phishing, Password Guessing, Brute Force, Software Exploitation, SQL Injection, Malware, dan serangan lainnya yang berisiko dapat merusak dan mengganggu kinerja dari sistem informasi.

Hasil wawancara dengan salah satu perwakilan dari divisi infrastruktur dan jaringan terkait serangan yang pernah terjadi adalah pihak luar pernah masuk dan mengubah tampilan website milik Undiksha dan adanya serangan DdoS. Seragan DdoS yang terjadi saat itu menyebabkan perangkat elektronik di UPA TIK sempat macet beberapa saat. Serangan terjadi karena pihak UPA TIK tidak mengetahui bahwa belum dilakukan update pada perangkat lunak seperti php, cms, wordpess yang digunakan oleh sistem sehingga pembobol menemukan celah untuk masuk. Melakukan pengukuran tingkat kematangan kemanan informasi merupakan upaya untuk menganalisis tingkat kesiapan keamanan informasi dan mencegah terjadinya serangan. Pengukuran ini dilakukan dengan tujuan memperoleh gambaran nyata terhadap kondisi keamanan informasi di UPA TIK.

Pencegahan terjadinya serangan siber di UPA TIK diawali dengan dengan cara melakukan pengukuran keamanan informasi dalam lingkup organisasi secara teratur. Pengukuran di lingkup organisasi ini dilakukan untuk mengetahui bagaimana kondisi terbaru terkait kesiapan pengamanan informasi di UPA TIK yang mempermudah dalam melakukan pengambilan keputusan yang dapat meningkatkan kesiapan pengamanan informasi karena alasan terjadinya serangan adalah akibat dari kelalaian pihak UPA TIK yang lupa melakukan update pada perangkat lunak. Sehingga, dengan dilakukannya pengukuran keamanan di lingkup organisasi secara teratur maka pihak

UPA TIK secara terjadwal akan tau kapan melakukan update tanpa harus terjadi serangan terlebih dahulu. Pengukuran keamanan informasi dapat dilakukan menggunakan beberapa *framework* yang sudah ada diantaranya COBIT, ISO/IEC, Indeks KAMI, dan lainnya. Pemilihan *framework* itu sendiri harus didasarkan pada kepentingan dan kondisi di instansi yang akan diukur keamanan informasinya.

Framework yang akan dimanfaatkan dalam pengukuran kondisi keamanan informasi di UPA TIK yaitu Indeks KAMI. Dibandingkan dengan Cobit, Indeks KAMI dipilih karena pengukuran pada Indeks KAMI adalah mengukur tingkat kesiapan keamanan infrormasi untuk organisasi yang lebih condong ke kategori audit keamanan informasi sedangkan Cobit lebih ke bagian tata kelola keamanan informasi. Alasan lain yang memperkuat dipilihnya Indeks KAMI juga terletak pada Cobit itu sendiri yang merupakan *framework* yang dibuat oleh lembaga ISACA sedangkan status UPA TIK yang merupakan unit di bawah Undiksha yang merupakan instansi pemerintah, sehingga perlu mengikuti ketentuan langsung dari pusat karena lembar penilaian Indeks KAMI dibuat langsung oleh Badan Siber dan Sandi Negara (BSSN) Indonesia dan telah bersesuaian dengan Peraturan Presiden No. 95 Tahun 2018 tentang SPBE yang menyatakan setiap instansi juga harus menerapkan keamanan SPBE di mana ketentuan terkait standar dan prosedurnya diatur oleh lembaga yang bertanggung jawab atas hal tersebut yaitu BSSN dan Peraturan BSSN Nomor 8 Tahun 2020 pasal 9 dan pasal 12 menyatakan instansi wajib menerapkan SNI ISO/IEC 27001. Penerapan SNI ISO/IEC 27001 dapat dilakukan dengan melakukan penilaian menggunakan Indeks KAMI.

Indeks KAMI merupakan alat bantu yang disusun oleh BSSN pada tahun 2008 dalam upaya mencegah terjadinya serangan siber di lingkup organisasi. Indeks KAMI memiliki peran yang penting sebagai acuan yang digunakan di nasional dalam membantu instansi untuk melakukan indetifikasi tingkat kesiapan pengamanan informasi melalui penyajian data kelengkapan dan kematangan kerangka kerja kepada ketua instansi. Indeks KAMI saat ini sudah berada di versi 4.2 yang merupakan penyempurnaan dari versi sebelumnya dengan adanya revisi formulasi dan redaksional pada *Chart Dashboard*. Indeks KAMI versi 4.2 terdapat 7 (tujuh) area pokok yang akan

dilakukan evaluasi. Ketujuh area evaluasi tersebut telah disesuaikan dengan aspek yang terdapat dalam ISO/IEC 27001, area tersebut diantaranya meliputi : kategori sistem elektronik, tata kelola keamanan informasi, pengelolaan risiko keamanan informasi, kerangka kerja keamanan informasi, pengelolaan aset informasi, teknologi dan keamanan informasi, dan yang terakhir adalah suplemen yang mencakup keterlibatan pihak ke-3 terhadap instansi terkait dengan pengamanan layanan *cloud* dan perlindungan data pribadi.

Berdasarkan penjelasan yang dipaparkan, peneliti melakukan penelitian pengukuran keamanan informasi di UPA TIK Undiksha. Penelitian dilakukan guna memberikan gambaran terkait kondisi kesiapan pengamanan informasi yang dimiliki oleh UPA TIK saat ini dan rekomendasi yang sesuai untuk meningkatkan kesiapan dan kematangan pengamanan informasi menggunakan alat bantu berupa Indeks KAMI versi 4.2.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang sudah dipaparkan diatas, maka rumusan masalah penelitian ini adalah :

1. Bagaimana hasil pengukuran menggunakan Indeks KAMI 4.2 di UPA TIK Universitas Pendidikan Ganesha?
2. Bagaimana usulan rekomendasi dalam upaya meningkatkan keamanan informasi di UPA TIK Universitas Pendidikan Ganesha?

1.3 Ruang Lingkup Penelitian

Ruang lingkup penelitian yang menjadi fokus dalam pembuatan penelitian ini meliputi hal-hal berikut:

1. Penelitian dilaksanakan pada UPA TIK Unviersitas Pendidikan Ganesha dengan periode pengambilan data dari tahun 2022-2024 yang meliputi devisi sistem informasi, devisi pusat data dan informasi, devisi infrastruktur jaringan den keamanan, serta devisi *helpdesk* dan dokumentasi.
2. Penelitian hanya berfokus pada pertanyaan area evaluasi Indeks KAMI Versi 4.2

3. Hasil akhir dari penelitian ini berupa pembuatan rekomendasi menggunakan analisis SWOT yang masih dalam ruang lingkup Indeks KAMI sebagai alat bantu yang digunakan pada penelitian

1.4 Tujuan Penelitian

Penelitian ini dilakukan guna mencapai tujuan sebagai berikut :

1. Mengetahui hasil pengukuran menggunakan indeks KAMI 4.2 di UPA TIK Universitas Pendidikan Ganesha
2. Memberikan usulan rekomendasi untuk meningkatkan maupun mempertahankan keamanan informasi di UPA TIK Universitas Pendidikan Ganesha

1.5 Manfaat Penelitian

Manfaat praktis yang akan didapat dari dilaksanakannya penelitian adalah sebagai berikut :

1. Bagi Pihak UPA TIK

   Penelitian yang telah disusun ini diharapkan dapat memberikan informasi berupa gambaran terkait kematangan dan kesiapan kerangka kerja keamanan informasi serta rekomendasi perbaikannya pada UPA TIK Universitas Pendidikan Ganesha yang mana gambaran dan rekomendasi tersebut bisa dijadikan pertimbangan dalam meningkatkan kesiapan instansi dalam melakukan pengamanan informasi.
2. Bagi Peneliti

   Penelitian diharapkan mampu memperluas pengetahuan dan meningkatkan pemahaman peneliti tentang keamanan informasi pada instansi pelayanan publik serta menambah pengalaman peneliti dalam penerapan ilmu SI/TI yang telah dipelajari selama kuliah.