BAB I
PENDAHULUAN

1.1 LATAR BELAKANG

Kemajuan teknologi dan informasi yang saat ini berkembang pesat di berbagai bidang menawarkan banyak manfaat. Namun, teknologi dan informasi juga menghadirkan bahaya yang semakin besar bagi keamanan data. Di dunia modern, menjaga keamanan informasi merupakan bagian penting dari perkembangan jangka panjang bisnis TI mana pun (Obuh, 2023). Kerugian finansial dan juga penurunan produktifitas perusahaan merupakan suatu hal yang sangat krusial, hal tersebut disebabkan karena adanya kebocoran ataupun kegagalan sistem sehingga keamanan informasi sangat penting untuk keberlangsungan hidup organisasi. Kegagalan sistem dan kebocoran informasi biasanya berkaitan dengan perlindungan aset dan keamanan sehingga keamanan itu sangat penting. Pentingnya keamanan informasi tidak hanya terbatas pada aspek finansial dan operasional, tetapi juga reputasi dan kepercayaan publik. Kebocoran data atau informasi sensitif dapat merusak reputasi organisasi dan memicu hilangnya kepercayaan publik bahkan bisa terkena sanksi hukum.

Pengendalian sumber daya organisasi sangatlah penting. Salah satu pendekatan untuk mencapainya adalah melalui analisis, penilaian, dan pengurangan risiko, yang dikenal sebagai manajemen risiko keamanan informasi (Tutik et al., 2022). Berdasarkan Peraturan Pemerintah Indonesia Nomor 82 Tahun 2012, Pasal 13 mengatur tentang pemanfaatan sistem dan transaksi elektronik. Pasal ini menyatakan bahwa penanggung jawab sistem elektronik wajib mengelola risiko untuk menghindari kerugian atau kerusakan. Manajemen risiko meliputi analisis risiko dan pengembangan strategi mitigasi dan respons untuk mengatasi ancaman, gangguan, dan kesulitan dalam sistem elektronik yang dikelolanya. Sumber daya organisasi dapat mencakup manusia dan data yang berharga. UPA TIK merupakan cabang eksekutif teknis yang bekerja sama secara langsung dengan sistem informasi yang memanfaatkan teknologi informasi dan komunikasi.

Bencana atau risiko ini dapat muncul dalam berbagai cara. Bencana atau risiko ini dapat terjadi akibat siklus alam atau ancaman yang timbul dari peralatan dan tindakan individu, seperti pengguna (Rohman et al., 2020). Berdasarkan hasil wawancara dengan Sekretaris UPA TIK, belum ada kebijakan yang jelas mengenai keamanan informasi di UPA TIK. Manajemen risiko sangat penting untuk mengurangi kemungkinan terjadinya kegagalan sistem di Undiksha. UPA TIK Undiksha sendiri belum pernah melakukan manajemen risiko yang komprehensif sebelumnya sehingga masih perlu menerapkan manajemen risiko dengan menggunakan *framework* sehingga proses manajemen risiko yang dilakukan tidak sepenuhnya maksimal. Terlebih lagi, kejadian kerusakan alat karena dipinjam oleh mahasiswa dan kehilangan data yang pernah terjadi memberikan gambaran akan potensi risiko yang mengintai. Tanpa adanya kebijakan yang jelas, UPA TIK rentan terhadap kerugian yang lebih besar, baik dari segi keuangan maupun reputasi. Implementasi manajemen risiko menjadi krusial dalam mengidentifikasi ancaman dan kerentanan yang mungkin terjadi, serta merumuskan strategi mitigasi yang tepat guna mengurangi dampaknya. Dengan demikian, langkah-langkah konkret dalam menerapkan manajemen risiko menjadi suatu keharusan bagi UPA TIK untuk menjaga keamanan informasi secara efektif dan menghindari kerugian yang dapat terjadi di masa mendatang. Dengan kondisi UPA TIK saat ini, masih perlu ada perbaikan lebih baik dan pemantauan berkelanjutan terhadap isu-isu keamanan. UPA TIK juga memiliki rencana untuk meningkatkan keamanan dibidang infrastruktur sehingga keamanan informasi pada infrastruktur TI di UPA TIK penting dilakukan. Hal ini menjadi alasan utama untuk bisa mengelola risiko keamanan informasi pada infrastruktur dengan baik. Sangat penting untuk meningkatkan perlindungan sistem informasi, dengan mempertimbangkan berbagai ancaman seputar data (Eskaluspita, 2020). Oleh karena itu, sangat penting bagi perusahaan untuk menetapkan kriteria yang berfungsi sebagai panduan dalam menjaga aset berharga milik perusahaan atau lembaga.

Operational, Critically Critical Threat, Asset, and Vulnerability Evaluation-Small (OCTAVE-S) adalah kerangka berbasis kerja untuk mengenali risiko teknologi informasi. Kerangka kerja OCTAVE-S digunakan untuk melakukan penilaian, memeriksa, dan menerapkan strategi berdasarkan tingkat risiko

keamanan dari berbagai perspektif dalam suatu organisasi (C. Alberts et al., 2005). OCTAVE-S dapat berguna dalam penilaian risiko dengan mengidentifikasi aset teknologi informasi utama bagi organisasi. OCTAVE-S dapat mendeteksi kelemahan dan bahaya yang terkait dengan sumber daya TI ini dan mampu menilai potensi konsekuensi jika bahaya ini terwujud (Moteff, 2005). Pendekatan OCTAVE-S dirancang untuk perusahaan dengan jumlah karyawan maksimal 100 orang. Dengan mempertimbangkan situasi terkini di UPA ICT Undiksha, OCTAVE-S tampaknya merupakan pendekatan yang tepat untuk organisasi kecil. Dari perspektif teknis, OCTAVE-S sangat sesuai dengan analisis ini, karena disesuaikan dengan lingkungan teknologi unik UPA ICT Undiksha. Hal ini memudahkan penilaian risiko keamanan informasi berdasarkan infrastruktur, aplikasi, dan persyaratan teknis UPA TIK. OCTAVE-S menyediakan kerangka kerja yang mendorong penggunaan sumber daya internal UPA ICT Undiksha secara efektif. Hal ini termasuk memanfaatkan personel, perangkat, dan teknologi yang ada untuk melakukan penilaian risiko keamanan informasi. Dari segi manajemen, OCTAVE-S membantu UPA TIK Undiksha dalam menetapkan prioritas dan mengelola risiko keamanan informasi. Dengan memahami tingkat risiko yang terkait dengan infrastruktur TI, UPA TIK dapat mengalokasikan sumber daya secara efektif untuk mengurangi risiko yang paling kritis. Penggunaan OCTAVE-S sebagai kerangka kerja yang digunakan dalam pebelitian ini memungkinkan UPA TIK yang belum memiiki kebijakan keamanan informasi untuk memulai proses evaluasi risiko dari awal dengan pendekatan yang sistematis dan terukur. Saat ini, UPA ICT belum memiliki kebijakan keamanan informasi. Namun, OCTAVE-S dapat digunakan untuk membuat kerangka kerja keamanan yang disesuaikan dengan kebutuhan dan konteks organisasi. Penerapan OCTAVE-S dalam penelitian ini akan membantu mengenali, mengukur, dan mengelola risiko keamanan informasi secara lebih efisien, selain mendukung pengambilan keputusan yang lebih efektif.

Di Indonesia, Indeks KAMI, yang terkait dengan Keamanan Informasi, digunakan untuk menilai penerapan standar SNI ISO 27001:2009 dan manajemen keamanan informasi. Indeks ini berguna untuk menentukan tingkat pengembangan dan ketahanan di bidang ini (BSSN, 2021). Indeks KAMI mengukur kesiapan

organisasi untuk menerapkan keamanan informasi, berdasarkan standar SNI ISO 27001. Dokumen ini membahas topik-topik seperti kontrol keamanan informasi, identifikasi dan manajemen risiko, pengembangan sistem keamanan informasi, manajemen aset TI, dan elemen teknologi yang terkait dengan keamanan informasi. Indeks KAMI tidak secara khusus dirancang untuk memeriksa manajemen risiko dan hanya menyediakan data tentang status kesiapan keamanan informasi. Dokumen ini menerapkan standar ISO 27001:2022, yang dikenal sebagai ISMS, untuk menawarkan rekomendasi tentang cara mengurangi risiko. Standar ini merupakan standar global untuk Sistem Manajemen Keamanan Informasi. ISMS menggunakan metode manajemen risiko untuk melindungi sumber daya organisasi (Obuh, 2023). Selain itu, ISO 27001 memberikan pengakuan internasional untuk implementasi ISMS melalui sertifikat yang disebut sertifikasi Sistem Manajemen Keamanan Informasi (ISMS) Setiawan dalam Sarno (2009). ISO 27001:2022 digunakan sebagai acuan mitigasi berdasarkan dengan klausul objektif yang diharapkan mampu mengelola dan mengendalikan risiko keamanan informasi perusahaan atau instansi, yang mencakup kerahasiaan, ketersediaan, dan integritas, OCTAVE-S dapat membantu untuk mengidentifikasi ancaman yang berkaitan dengan TI dengan 3 fase yang ada pada OCTAVE-S. Ada beberapa aspek utama yang perlu dipertimbangkan saat memilih ISO 27001. Kriteria ini dapat disesuaikan untuk memenuhi kebutuhan, tujuan, persyaratan keamanan, prosedur bisnis, jumlah karyawan, dan skala organisasi perusahaan.

Berdasarkan latar belakang, maka dari itu peneliti mengambil judul penelitian "Analisis Manajen Risiko Keamanan Informasi menggunakan *Framework* OCTAVE-S dan ISO 27001:2022". Penelitian ini diharapkan dapat menghasilkan temuan tentang manajemen risiko dan penilaian risiko dengan rekomendasi yang diberikan berdasarkan kontrol yang disesuaikan dengan ancaman dan organisasi

1.2 RUMUSAN MASALAH

Berdasarkan informasi yang diberikan di atas, pertanyaan-pertanyaan berikut dapat diajukan dalam penelitian ini:

1. Bagaimana proses dan hasil analisis manajemen risiko menggunakan *Framework* OCTAVE-S pada UPA TIK Undiksha?

2. Bagaimana rekomendasi yang dihasilkan dari temuan-temuan analisis yang dilakukan mengacu pada standar ISO 27001:2022?

1.3 TUJUAN PENELITIAN

Adapun tujuan dari penelitian ini adalah sebagai berikut:

1. Mengetahui proses dan hasil analisis manajemen risiko menggunakan Framework OCTAVE-S.
2. Memberikan rekomendasi berdasarkan analisis temuan-temuan yang mengacu pada standar ISO 27001:2022 dan mendokumentasikan hasil temuan.

1.4 RUANG LINGKUP PENELITIAN

Berdasarkan sejarah permasalahan, penelitian ini bertujuan untuk menyempurnakan hasil penelitian. Ruang lingkup penelitian disajikan di bawah ini:

1. Analisis ini berfokus pada penilaian risiko yang terkait dengan infrastruktur teknologi di UPA TIK Undiksha.
2. Informasi yang digunakan berasal dari wawancara dan observasi yang dilakukan.
3. Temuan dan saran penelitian ini berkaitan dengan manajemen risiko keamanan, dengan mengacu pada standar ISO 27001:2022.

1.5 MANFAAT PENELITIAN

Hasil penelitian ini menekankan pentingnya tugas penelitian. Diharapkan penelitian ini akan memberikan informasi dan wawasan yang berharga. Oleh karena itu, menurut penjelasan mereka, karya ini berpotensi memberikan manfaat baik secara teori maupun praktik. Berikut ini adalah beberapa manfaat yang diharapkan:

1.5.1 Manfaat Teoritis

a. Melakukan identifikasi dan peninjauan manajemen risiko saat ini, menggunakan teori dan pelajaran yang dipelajari.
b. Gambaran umum tentang manajemen teknologi informasi yang tepat dapat diberikan kepada organisasi.

1.5.2 Manfaat Praktis

a. Membantu organisasi dalam menilai status keamanan terkini sistem informasi mereka, serta memberikan ringkasan langkah-langkah yang akan datang untuk memperkuat keamanan.
b. Temuan penelitian dan analisis yang dilakukan dalam studi ini dapat digunakan oleh organisasi untuk mengembangkan kebijakan masa depan, khususnya yang terkait dengan sistem manajemen keamanan informasi.