BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi telah menimbulkan dampak terhadap bidang pendidikan (Aritonang dkk., 2018), salah satunya adalah pemanfaatan situs web dan jaringan internet yang menjadi bagian yang tak terpisahkan dalam lingkungan perguruan tinggi (Sulistyowati & Ginardi, 2018). Perguruan tinggi saat ini menjadi peneliti terdepan dalam mengadopsi teknologi (Singh dkk., 2016), tujuannya adalah untuk mengoptimalkan komunikasi dan manajemen informasi antara mahasiswa, dosen, dan staf administrasi (Riadi & Kurniawan, 2018). Meskipun akses yang semakin luas terhadap teknologi memberikan manfaat besar dalam proses pembelajaran, namun juga meningkatkan risiko keamanan informasi terhadap berbagai ancaman (Singh dkk., 2016). .

Bencana merupakan ancaman yang sulit diprediksi kapan akan terjadi (Rohman dkk., 2020). Risiko dari bencana tersebut selalu menyebabkan kerugian bagi keberlangsungan proses bisnis yang sedang berlangsung, dengan dampak yang bervariasi baik dalam jangka pendek maupun jangka panjang (Nasution, 2020). Menjaga keamanan informasi dari serangan *cyber* di dunia maya serta menjaga keamanan informasi dari kerentanan dan pelanggaran keamanan, seperti peretasan merupakan tantangan besar bagi perguruan tinggi dengan berbagai jenis pengguna, seperti mahasiswa, dosen, orang tua, staf kependidikan, dan masyarakat umum (Sulistyowati & Ginardi, 2018).

Potensi risiko dalam suatu organisasi dapat muncul dari beragam sumber, mencakup ancaman terhadap keamanan informasi, bencana eksternal seperti kebakaran, serta kerentanan internal seperti kegagalan perangkat keras, yang secara kolektif berpotensi mengganggu operasional dan memerlukan strategi mitigasi komprehensif (Ramadhintia & Bisma, 2021). Keberagaman risiko dapat menghasilkan konsekuensi yang signifikan, termasuk potensi hilangnya data krusial, baik melalui tindakan yang disengaja maupun kelalaian yang tidak diinginkan (Armadyana dkk., 2023). Data memiliki peran yang sangat penting dalam sistem informasi, karena data adalah salah satu komponen utama dari sistem informasi, bersama dengan perangkat keras, perangkat lunak, prosedur, jaringan, dan sumber daya manusia (Munadhiroh dkk., 2023).

Potensi risiko yang mungkin terjadi adalah gangguan konektivitas antara perangkat *client* dan server, yang dapat mengakibatkan terputusnya komunikasi data (Ramadhintia & Bisma, 2021). Hal ini menjadi semakin kritis ketika menyangkut informasi perusahaan yang bersifat sensitif dan *confidential* (Armadyana dkk., 2023). Selain itu, terdapat juga ancaman terhadap integritas perangkat lunak, di mana infeksi virus dapat menyebabkan malfungsi atau kegagalan sistem (Ramadhintia & Bisma, 2021). Mengingat hal tersebut, entitas bisnis, perlu memberikan perhatian khusus dan prioritas tinggi pada upaya perlindungan dan pengamanan aset informasi mereka dari berbagai bentuk ancaman yang mungkin timbul (Armadyana dkk., 2023). Untuk mengantisipasi potensi risiko, setiap organisasi perlu mengimplementasikan strategi preventif melalui perencanaan yang cermat atau tindakan mitigasi yang terstruktur, langkah-langkah

ini dirancang untuk menanggulangi kemungkinan terjadinya kesalahan atau kegagalan dalam operasional organisasi (Nurdin, 2024).

Manajemen risiko merupakan hal penting bagi sebuah organisasi, hal ini bertujuan untuk melindungi kerahasiaan data internal dan eksternal, serta menjaga reputasi guna mempertahankan kepercayaan publik (Nurdin, 2024). Untuk melindungi aset informasi, diperlukan pengelolaan yang efektif, salah satunya melalui penerapan manajemen risiko keamanan informasi yang sesuai dengan kebutuhan instansi (Saputra dkk., 2019). Implementasi manajemen risiko yang efektif bertujuan untuk menghasilkan pedoman keamanan informasi yang komprehensif serta solusi holistik guna meminimalkan potensi kerugian organisasi (Wijaya dkk., 2021).

Universitas Sangga Buana telah mengembangkan *website* induk (https://usbypkp.ac.id) yang dikelola oleh Biro Teknologi Informasi (IT) Sangga Buana. *Website* https://usbypkp.ac.id dapat diakses oleh seluruh pengguna dan terhubung dengan berbagai layanan *online* universitas, seperti Kuliah Online, Sistem Informasi Terintegrasi (Siforter), *Repository*, Pendaftaran Mahasiswa Baru (PMB) Sangga Buana, dan Jurnal. Namun demikian, Biro IT belum melaksanakan analisis risiko keamanan informasi terhadap *website* tersebut. Sehingga pihak universitas belum mengetahui sejauh mana kesiapan universitas dalam menghadapi ancaman-ancaman yang mungkin muncul saat risiko-risiko yang sebenarnya ada dan tidak dapat teridentifikasi dengan baik. Meningkatnya intensitas penggunaan antara sistem dan pengguna berbanding lurus dengan bertambahnya risiko kerusakan oleh pihak-pihak yang tidak memiliki tanggung jawab, kondisi tersebut

menciptakan tantangan baru dalam aspek keamanan yang perlu diantisipasi (Riadi & Kurniawan, 2018). Untuk menghindari peristiwa tersebut, dibutuhkan manajemen risiko yang mampu mengurangi kerusakan, seperti kerugian finansial, penurunan reputasi universitas, gangguan atau bahkan penghentian proses bisnis (Seta dkk., 2017).

Guna menjamin sistem tetap beroperasi sesuai kebutuhan dan fungsinya, diperlukan pengukuran kinerja melalui pemeriksaan berkala yang mengacu pada standar, sehingga pemeriksaan keamanan sistem informasi dapat terlaksana secara efektif dan terukur (Riadi & Kurniawan, 2018). Terdapat banyak kerangka kerja yang telah dikembangkan untuk mengatasi risiko-risiko yang mungkin dihadapi oleh sebuah organisasi (Rohman dkk., 2020). *OCTAVE* (*Operationally Critical Threat, Assets, and Vulnerability Evaluation*) merupakan salah satu metode yang diterapkan dalam manajemen dan analisis risiko teknologi informasi, yang mencakup kumpulan alat, teknik, dan metode untuk mengevaluasi dan merencanakan keamanan sistem informasi berdasarkan risiko (Jakaria dkk., 2013).

Beberapa penelitian terdahulu yang relevan dengan penelitian ini dengan hasil penelitian membuktikan bahwa *OCTAVE Allegro* membantu dalam mengetahui area dampak dan skala prioritas, mengidentifikasi risiko, memberikan rekomendasi tindakan mitigasi yang dapat dilakukan pada Universitas Advent Indonesia (Wagiu dkk., 2019). Adapun penelitian lain dengan hasil penelitian penilaian risiko menggunakan metode *OCTAVE Allegro* dapat membantu menemukan 5 dari 7 aset informasi yang dikelola oleh ICT Fakultas Ilmu Komputer Universitas Sriwijaya dianggap sebagai aset kritis. Dengan mengetahui penilaian risiko masing-masing

aset informasi, ICT Fakultas Ilmu Komputer Universitas Sriwijaya dapat membuat keputusan yang tepat dalam mengurangi risiko sesuai dengan kemungkinan-kemungkinan risiko yang dapat terjadi pada kemudian hari (Zulfia dkk., 2021). Selain itu, penelitian lain dengan hasil penelitiannya mengungkapkan bahwa SIAKAD STIQ Al-Lathiffiyah menghadapi 5 ancaman risiko. Dari ancaman tersebut, 4 risiko memerlukan tindakan mitigasi, sementara 1 risiko dapat diterima dengan pendekatan tindakan yang sesuai (Astuti dkk., 2023).

Berdasarkan penelitian terdahulu menunjukkan bahwa metode *OCTAVE Allegro* merupakan alat yang efektif dalam penilaian risiko keamanan informasi pada institusi pendidikan, dengan menerapkan metode ini, institusi dapat mengidentifikasi aset informasi yang bersifat kritis, menilai tingkat risiko, dan menentukan langkah-langkah yang tepat untuk mengurangi atau mengelola risiko tersebut. Oleh karena itu, peneliti akan melakukan penelitian dengan judul "Analisis Risiko Keamanan Informasi pada *Website* Universitas Sangga Buana Menggunakan Metode *OCTAVE Allegro*" dengan mengikuti standar manajemen keamanan informasi ISO/IEC 27001:2022. Penelitian ini diharapkan dapat memberikan kontribusi dalam meningkatkan keamanan informasi di lingkungan perguruan tinggi, khususnya di Universitas Sangga Buana.

1.2 Identifikasi Masalah

Berdasarkan latar belakang yang telah diuraikan di atas, terdapat beberapa masalah yang telah diidentifikasi, yaitu:

1. Belum dilakukan analisis risiko keamanan informasi pada *website* Universitas Sangga Buana.
2. Terdapat potensi risiko keamanan informasi yang signifikan, yang memerlukan identifikasi, analisis, dan mitigasi secara komprehensif.

1.3 Rumusan Masalah

Merujuk pada identifikasi masalah yang telah dijelaskan sebelumnya, maka perumusan masalah dalam penelitian ini adalah:

1. Bagaimana hasil analisis risiko keamanan informasi pada *website* Universitas Sangga Buana menggunakan metode *OCTAVE Allegro* dengan pendekatan kualitatif?
2. Bagaimana hasil analisis risiko keamanan informasi pada *website* Universitas Sangga Buana menggunakan metode *OCTAVE Allegro* dengan pendekatan kuantitatif?

1.4 Batasan Masalah

Batasan masalah dalam penelitian ini adalah sebagai berikut:

1. Penelitian difokuskan pada *website* Universitas Sangga Buana.
2. Analisis risiko keamanan informasi menggunakan *OCTAVE Allegro*.
3. Sumber data untuk proses analisis risiko diperoleh dari narasumber, yaitu staf bidang IT dan populasi pada penelitian ini terdiri dari mahasiswa aktif Universitas Sangga Buana tahun masuk/angkatan 2020-2022.

1.5 Manfaat Penelitian

Penelitian ini diharapkan memberikan beberapa manfaat, antara lain:

1. Memberikan *feedback*/masukan terkait potensi ancaman risiko keamanan informasi pada *website* Univeristas Sangga Buana.
2. Memberikan kontribusi dengan dilakukannya analisis risiko keamanan informasi pada *website* Univeristas Sangga Buana.
3. Memberikan pemahaman tentang berbagai risiko yang berkaitan dengan keamanan informasi.

1.6 Tujuan Penelitian

Berdasarkan penjelasan di atas, tujuan dari dilakukannya penelitian ini yaitu:

1. Untuk mengetahui hasil analisis risiko keamanan informasi pada *website* Universitas Sangga Buana menggunakan metode *OCTAVE Allegro* dengan pendekatan kualitatif.
2. Untuk mengetahui hasil analisis risiko keamanan informasi pada *website* Universitas Sangga Buana menggunakan metode *OCTAVE Allegro* dengan pendekatan kuantitatif.

1.7 Sistematika Penulisan

Penelitian ini terdiri dari lima bagian utama yang disusun secara sistematis. Setiap bab memiliki konten yang saling berhubungan, membentuk suatu kerangka penelitian yang komprehensif dan terstruktur sebagai berikut:

BAB I PENDAHULUAN

Bab ini mencakup berbagai komponen penting yang mendasari penelitian. Di dalamnya terdapat penjelasan mengenai konteks permasalahan, pemetaan isu-isu terkait, perumusan pertanyaan penelitian, penetapan lingkup studi, sasaran yang

ingin dicapai, nilai guna dari penelitian ini, serta uraian tentang struktur penyajian laporan.

BAB II LANDASAN TEORI

Bab ini berisi teori-teori, penjelasn, tata cara, dan referensi penelitian yang berasal dari literatur akademis yang kredibel dan relevan dengan analisis risiko keamanan informasi.

BAB III OBJEK DAN METODE PENELITIAN

Bab ini menjelaskan objek penelitian yaitu *website* Universitas Sangga Buana, termasuk sejarah, visi misi, dan struktur organisasi. Bab ini juga menjelaskan metode penelitian yang digunakan.

BAB IV HASIL PENELITIAN DAN PEMBAHASAN

Bab ini menguraikan tahapan-tahapan yang ditempuh melalui proses pengambilan data di lapangan, pengujian hipotesis melalui analisis data, serta mengkaji hasil teuan empiris yang diperoleh dibandingkan dengan hasil penelitian terdahulu dan teori para ahli untuk mencapai tujuan penelitian.

BAB V KESIMPULAN DAN SARAN

Bab ini menyajikan ringkasan temuan utama dari studi yang tela dilakukan. Selain itu, bab ini juga memberikan rekomendasi untuk pengembangan penelitian di masa mendatang, mengidentifikasi area-area yang berpotensi untuk diteliti lebih lanjut.