

BAB I

PENDAHULUAN

1.1 Latar Belakang

Keamanan informasi merupakan aspek penting dalam era digital saat ini, di mana informasi dianggap sebagai aset berharga bagi setiap organisasi. Ancaman terhadap keamanan informasi dapat datang dari berbagai sumber, baik internal maupun eksternal yang dapat mengakibatkan kerugian yang signifikan dalam hal finansial, reputasi, maupun operasional (Muahidin, Kusriani, dan Nasiri 2022). Pentingnya menjaga keamanan informasi semakin dirasakan oleh individu maupun organisasi, mengingat informasi sangat mudah dicuri atau disalah gunakan oleh pihak yang tidak bertanggung jawab (Elan dkk. 2023).

Ancaman terhadap keamanan informasi terus berkembang seiring dengan kemajuan teknologi, baik berasal dari individu, organisasi, mekanisme, atau kejadian yang berpotensi merusak atau menyalahgunakan sumber daya informasi milik suatu perusahaan atau organisasi (Ramadhani 2018). Melindungi keamanan informasi menjadi hal krusial bagi instansi pemerintah yang memiliki tanggung jawab besar dalam menjaga kerahasiaan data, membangun kepercayaan masyarakat, serta memenuhi ketentuan regulasi yang berlaku.

Contoh nyata ancaman terhadap keamanan informasi di instansi pemerintah adalah serangan *ransomware* pada Pusat Data Nasional (PDN) pada tahun 2024. Serangan ini menyebabkan gangguan pada sistem PDN selama hampir tiga hari, berdampak besar pada berbagai layanan publik, serta bocornya data pribadi warga negara Indonesia. Kerugian yang ditimbulkan dari insiden ini berpotensi

menimbulkan dampak yang lebih lanjut bagi korban kebocoran data pribadi, yang dapat mengalami kerugian signifikan (Somomoeljono 2024). Kejadian ini menegaskan pentingnya evaluasi keamanan informasi yang berkelanjutan untuk memperkuat perlindungan data, mengidentifikasi celah, serta mencegah ancaman serupa di masa depan.

Evaluasi keamanan informasi menjadi langkah penting yang perlu dilakukan oleh setiap instansi pemerintah termasuk Dinas PUTRLH Tasikmalaya. Dinas PUTRLH Tasikmalaya, yang merupakan instansi pengelola berbagai data strategis, memerlukan evaluasi secara berkala untuk mengukur keamanan informasinya dari ancaman yang dapat mengganggu operasional maupun pelayanan publik. Salah satu cara untuk mengukur tingkat keamanan informasi adalah dengan menggunakan Indeks KAMI (Keamanan Informasi), yang dirancang untuk menilai tingkat kesiapan dan kematangan kerangka kerja keamanan informasi berdasarkan standar ISO 27001 (Juliharta 2019).

Beberapa penelitian telah membuktikan efektivitas Indeks KAMI dalam evaluasi keamanan informasi. (Khusna dan Sugiantoro 2023) mencatat bahwa UPT-PSI Universitas Muria Kudus memiliki tingkat kematangan *Tinggi* dengan skor 480. Sebaliknya, Diskominfo Kota XYZ memperoleh skor 418 dan dikategorikan *Tidak Layak* (Ferdiansyah, Subektiningsih, dan Indrayani 2019). (Khamil, Arya, dan Susila 2022) juga melaporkan bahwa meskipun skor Sistem Elektronik Diskominfo Gianyar *Tinggi*, tingkat kematangan hanya pada level I–II+, sehingga belum layak. (Azmi dkk. 2024) menunjukkan bahwa SMK XYZ memperoleh skor 314 dengan status *Tidak Layak*. Hasil-hasil tersebut menunjukkan

bahwa instansi pemerintah maupun pendidikan masih menghadapi tantangan serius dalam pengelolaan keamanan informasi.

Beberapa penelitian sebelumnya menunjukkan bahwa Indeks KAMI efektif dalam menilai kesiapan keamanan informasi berdasarkan standar ISO 27001. Kelebihan penelitian tersebut mengungkap pemahaman mendalam mengenai risiko dan ancaman yang dihadapi instansi pemerintah. Sebagian besar penelitian belum menyertakan analisis lebih lanjut terkait strategi keamanan informasi yang dapat digunakan untuk mengatasi risiko-risiko tersebut secara komprehensif. Penelitian sebelumnya cenderung kurang menekankan pentingnya strategi perbaikan untuk meningkatkan tingkat kematangan keamanan informasi. Gap lainnya terlihat dalam kurangnya pemanfaatan pendekatan manajerial yang terintegrasi, seperti pendekatan *Ward and Peppard*, untuk merancang langkah-langkah peningkatan keamanan informasi yang relevan.

Berdasarkan latar belakang yang telah dijelaskan, penelitian ini akan melakukan pengujian terhadap tingkat kematangan keamanan informasi Dinas PUTRLH Tasikmalaya menggunakan Indeks KAMI 5.0 dan pendekatan strategi *Ward and Peppard*. Penelitian ini bertujuan untuk mengevaluasi kesiapan dan pengelolaan keamanan informasi di instansi tersebut, serta merancang rekomendasi dan usulan perbaikan yang relevan dengan menggunakan metode *Ward and Peppard* berdasarkan hasil evaluasi Indeks KAMI.

1.2 Rumusan Masalah

Berdasarkan uraian latar belakang, maka rumusan masalah dalam penelitian ini sebagai berikut :

- a. Bagaimana tingkat kematangan keamanan informasi di Dinas PUTRLH Tasikmalaya berdasarkan evaluasi menggunakan Indeks KAMI 5.0?
- b. Bagaimana rekomendasi perbaikan yang dapat diusulkan untuk meningkatkan keamanan informasi di Dinas PUTRLH Tasikmalaya berdasarkan hasil evaluasi Indeks KAMI 5.0 dan analisis *Ward and Peppard* ?

1.3 Tujuan Penelitian

Tujuan dari penelitian ini adalah:

- a. Menilai kondisi keamanan informasi di Dinas PUTRLH Tasikmalaya melalui evaluasi menggunakan Indeks KAMI 5.0 untuk menentukan tingkat kematangan sistem keamanan informasi yang ada.
- b. Memberikan rekomendasi perbaikan yang relevan untuk meningkatkan sistem keamanan informasi di Dinas PUTRLH Tasikmalaya, berdasarkan hasil evaluasi Indeks KAMI 5.0 dan analisis *Ward and Peppard*.

1.4 Manfaat Penelitian

- a. Memberikan kontribusi bagi Dinas PUTRLH Tasikmalaya dalam memahami posisi kematangan keamanan informasinya serta langkah-langkah peningkatan yang perlu dilakukan.

- b. Menjadi referensi bagi penelitian atau implementasi serupa yang ingin menggabungkan pendekatan Indeks KAMI dan *Ward and Peppard* dalam evaluasi keamanan informasi.

1.5 Batasan Masalah

Batasan masalah yang ditentukan dalam penelitian ini adalah sebagai berikut:

- a. Penelitian ini hanya berfokus pada evaluasi keamanan informasi di Dinas PUTRLH Tasikmalaya dan tidak mencakup instansi lain atau organisasi di luar dinas tersebut.
- b. Evaluasi dilakukan menggunakan Indeks KAMI 5.0 untuk mengukur tingkat kematangan keamanan informasi dan pendekatan *Ward and Peppard* untuk analisis kekuatan serta kelemahan sistem yang ada.
- c. Data yang dianalisis terbatas pada informasi yang tersedia dalam periode penelitian.
- d. Fokus evaluasi mencakup aspek kebijakan, prosedur, dan praktik keamanan informasi yang diterapkan di Dinas PUTRLH Tasikmalaya.
- e. Data penelitian diperoleh dari dokumen internal, wawancara dengan staf terkait, dan observasi langsung.