BAB I
PENDAHULUAN

1.1. Latar Belakang Masalah

Pelayanan publik memiliki peran yang krusial dalam menjamin kelangsungan serta kemajuan bangsa, masyarakat, dan negara. Pergeseran layanan administrasi organisasi dari semula sistem konvensional menjadi sistem berbasis teknologi informasi saat ini didorong oleh pertumbuhan teknologi informasi dan komunikasi. Beberapa negara bahkan hampir seluruhnya, penggunaan teknologi informasi dan komunikasi telah diterapkan secara bertahap untuk meningkatkan kualitas pelayanan publik, termasuk di Indonesia. Berbagai pemerintahan daerah di Indonesia melihat peluang untuk meningkatkan keterbukaan, efisiensi, dan demokrasi pemerintah dengan menyediakan layanan pemerintah berbasis teknologi tersebut.

Pemerintah Daerah Kabupaten XYZ berupaya meningkatkan standar pelayanan publik dan penyelenggaraan pemerintahan yang bertanggung jawab, efisien, bersih, dan transparan melalui sistem berbasis elektronik sebagai halnya tercantum dalam Peraturan Presiden No. 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE). Penyediaan *e-government* yang dikembangkan oleh Pemerintah Daerah Kabupaten XYZ adalah salah satunya dengan mengadakan *website* yang dapat diakses secara publik. Dengan adanya *website* saat ini diharapkan dapat memudahkan pemerintah untuk menyebarkan berbagai informasi dan layanan daerah kepada masyarakat dan sekitarnya.

Website Resmi Pemerintah Kabupaten XYZ merupakan salah satu sarana vital dalam menjalankan urusan pemerintahan daerah yang mana didalamnya terdapat instrumen dan aset penting berupa data dan informasi. Terlebih *website* ini bukan hanya dapat diakses oleh pengelola *website* saja, namun masyarakat juga dapat mengakses secara mudah. Dengan kemudahan akses yang diberikan, tidak menutup kemungkinan adanya orang-orang tidak bertanggung jawab yang sengaja memasukan virus atau melakukan serangan seperti *malware*, sehingga keamanan data menjadi sangat berisiko dari ancaman tersebut.

Berdasarkan hasil wawancara oleh peneliti dengan informan pertama yakni Kepala Bidang Pengembangan Informatika Dinas Komunikasi dan Informatika Kabupaten XYZ, *Website* Resmi Pemerintah Kabupaten XYZ pernah terjadi insiden yakni dalam bentuk *deface* pada tahun 2020 dan kembali terulang di tahun 2022. Insiden *deface* yang terjadi pada *website* atas ulah orang tidak bertanggung jawab yang mengubah tampilan dan menampilkan informasi yang tidak sesuai ini, selain berdampak pada keamanan dan kinerja sistem, ancaman tersebut juga mengakibatkan pengelola *website* yakni Dinas Komunikasi dan Informatika Kabupaten XYZ sendiri kehilangan kepercayaan dari pengguna karena data dan informasi yang ada sempat rusak dan bocor.

Kasus risiko dan kerentanan yang terjadi pada *Website* Resmi Pemerintah Kabupaten XYZ mengharuskan pengelola *website* untuk dapat menjaga keamanan informasi yang ada. Menjaga keamanan informasi berarti harus memahami bagaimana mengelola risiko dan menerima konsekuensi dari setiap ancaman yang mungkin muncul. Oleh karena itu, agar *Website* Resmi Pemerintah Kabupaten XYZ tidak mengalami ancaman risiko yang mengancam aset organisasi dan integritas data seperti kejadian *deface* berulang kali tersebut, maka pengelola *website* perlu melakukan antisipasi dengan mengidentifikasi dan mengukur tingkat risiko pada keamanan informasinya. *National Institute of Standard and Technology* (NIST) *Special Publication* (SP) 800-30 merupakan salah satu panduan yang dapat diterapkan untuk mengevaluasi seberapa baik manajemen risiko keamanan informasi dijalankan. Panduan ini telah distandarisasi oleh Pemerintah Pusat Amerika Serikat (US).

Berkaitan dengan latar belakang yang telah dijabarkan, maka peneliti tertarik untuk melakukan penelitian dengan judul "PENGUKURAN MANAJEMEN RISIKO KEAMANAN INFORMASI PADA WEBSITE RESMI PEMERINTAH KABUPATEN XYZ MENGGUNAKAN METODE NIST SP 800-30". Hasil penelitian ini diharapkan mampu menghasilkan pengukuran perencanaan strategis berbasis risiko untuk keamanan informasi dalam pengembangan *Website* Resmi Pemerintah Kabupaten XYZ.

1.2. Rumusan Masalah

Berdasarkan uraian latar belakang di atas, rumusan masalah adalah sebagai berikut:

1. Bagaimana mengidentifikasi risiko keamanan informasi menggunakan metode NIST SP 800-30 pada *Website* Resmi Pemerintah Kabupaten XYZ?
2. Sejauhmana tingkat risiko yang dihasilkan *Website* Resmi Pemerintah Kabupaten XYZ?
3. Bagaimana menentukan respon dan rekomendasi yang digunakan untuk mengurangi risiko pada *Website* Resmi Pemerintah Kabupaten XYZ?

1.3. Batasan Masalah

Berikut ini adalah batasan dari penelitian agar tetap berada dalam pokok permasalahan yang dirumuskan:

1. Penelitian dilaksanakan di Dinas Komunikasi dan Informatika Kabupaten XYZ sebagai pengelola *Website* Resmi Pemerintah Kabupaten XYZ.
2. Penelitian ini hanya membahas mengenai pengukuran tingkat risiko pada bagian keamanan informasi *Website* Resmi Pemerintah Kabupaten XYZ.
3. Metode yang digunakan untuk mengukur manajemen risiko adalah metode atau *framework* NIST SP 800-30.

1.4. Tujuan dan Manfaat Penelitian

1.4.1. Tujuan Penelitian

Berdasarkan rumusan masalah yang dijabarkan sebelumnya, penelitian dilaksanakan dengan tujuan:

1. Mengidentifikasi risiko munculnya keamanan informasi pada *Website* Resmi Pemerintah Kabupaten XYZ menggunakan metode NIST SP 800-30.

2. Mengetahui hasil pengukuran untuk memetakan, membangun alternatif manajemen risiko, dan memantau serta mengendalikan penanganan risiko terhadap aset pendukung *Website* Resmi Pemerintah Kabupaten XYZ.
3. Memberikan rekomendasi kepada pengelola dan manajemen *Website* Resmi Pemerintah Kabupaten XYZ tentang manajemen risiko keamanan informasi.

1.4.2. Manfaat Penelitian

Manfaat dari penelitian ini diharapkan dapat:

1. Menghasilkan pengukuran tingkat risiko keamanan informasi pada *Website* Resmi Pemerintah Kabupaten XYZ yang dikelola oleh Pemerintah Daerah Kabupaten XYZ.
2. Membantu Pemerintah Daerah Kabupaten XYZ dalam meningkatkan keamanan informasi.
3. Dapat dijadikan referensi bagi peneliti lainnya untuk mengevaluasi manajemen risiko keamanan informasi pada suatu organisasi.

1.5. Luaran Penelitian

Luaran pada penelitian ini berupa:

1. Dokumentasi hasil pengukuran tingkat risiko dan rekomendasi kontrol keamanan informasi pada *Website* Resmi Pemerintah Kabupaten XYZ sesuai panduan NIST SP 800-30.
2. Artikel ilmiah yang dipublikasikan di jurnal ilmiah terakreditasi.

1.6. Sistematika Penulisan

Adapun susunan pengaturan penyusunan tugas akhir supaya dapat memberikan kemudahan informasi bagi pembaca dengan dibagi menjadi beberapa bagian yakni sebagai berikut:

BAB 1 PENDAHULUAN

Latar belakang penelitian, rumusan masalah, batasan masalah, tujuan dan manfaat penelitian, luaran penelitian, serta sistematika penulisan semuanya diuraikan secara ringkas dan jelas dalam bab ini.

BAB 2 TINJAUAN PUSTAKA

Pada bab ini berisikan jurnal penelitian yang terkait. Selain itu juga, bab ini menguraikan teori yang merinci seperti konsep, metode, model, algoritma, teknik, prosedur, dan definisi yang terkait dengan permasalahan yang mendasari penelitian.

BAB 3 METODOLOGI PENELITIAN

Langkah-langkah yang diterapkan selama penelitian dijelaskan dalam bab ini bersama dengan waktu dan lokasi penelitian serta metodologi yang digunakan. Langkah-langkah ini kemudian digunakan untuk mengatasi masalah yang sudah ada untuk memenuhi tujuan sebuah penelitian.

BAB 4 HASIL DAN PEMBAHASAN

Hasil penelitian disajikan dalam bab ini berupa data yang didapat berdasarkan tahapan atau metode yang telah digunukan selama penelitian sehingga menghasilkan luaran yang diharapkan.

BAB 5 PENUTUP

Bab ini merupakan bab penutup dari penulisan dan merupakan bab terakhir yang berisi kesimpulan dari analisis temuan penelitian serta menawarkan gagasan bagaimana penelitian ini dapat dikembangkan lebih lanjut.

DAFTAR PUSTAKA

LAMPIRAN