BAB I
PENDAHULUAN

1.1. Latar Belakang

Transformasi digital telah membawa perubahan signifikan dalam tata kelola pemerintahan dan mendorong peningkatan efisiensi, transparansi, serta kualitas layanan publik. Dalam era pelayanan yang dituntut semakin cepat, akuntabel, dan berbasis data, pemanfaatan teknologi informasi menjadi pilar utama bagi instansi pemerintah. Perkembangan ini turut memengaruhi pengelolaan pendapatan daerah, di mana proses administrasi perpajakan beralih dari sistem manual menuju sistem digital yang lebih terintegrasi. Salah satu sistem yang berperan penting dalam digitalisasi pengelolaan pendapatan daerah adalah Sistem Manajemen Informasi Objek Pajak (SISMIOP). Sistem ini digunakan oleh Badan Pengelola Pendapatan, Keuangan, dan Aset Daerah (BPPKAD) untuk mendukung proses pendataan, penilaian, penetapan, pembayaran, hingga pelaporan Pajak Bumi dan Bangunan (PBB) (Kementerian Keuangan Republik Indonesia, 2017).

Sebagai sistem inti, SISMIOP mengelola informasi sensitif, seperti identitas wajib pajak, nilai objek pajak, serta histori pembayaran. Informasi tersebut merupakan aset strategis yang mendukung efektivitas pelayanan publik dan menjaga kepercayaan masyarakat. Oleh karena itu, perlindungan informasi melalui penerapan prinsip kerahasiaan, integritas, dan ketersediaan menjadi sangat penting. Semakin bernilai suatu informasi, semakin tinggi pula potensi risiko dan ancaman yang dapat muncul, baik dari serangan eksternal maupun penyalahgunaan internal. Keamanan informasi tidak hanya diperlukan untuk menjamin keberlangsungan layanan, tetapi juga menjadi fondasi dalam membangun tata kelola pemerintahan yang profesional dan berdaya saing (Maleh dkk., 2021).

Namun demikian, berbagai penelitian menunjukkan bahwa sebagian besar instansi pemerintah di Indonesia masih mengelola keamanan informasi secara ad-hoc, belum terstandarisasi, serta belum sepenuhnya berbasis pada manajemen risiko yang terstruktur (Ajoudanian & Aboutalebi, 2025). Kondisi ini menyebabkan organisasi kurang siap menghadapi ancaman siber yang semakin kompleks,

termasuk risiko penyalahgunaan akses internal, kerentanan aplikasi berbasis web, dan potensi kebocoran data. Kesenjangan tersebut menegaskan pentingnya evaluasi keamanan informasi secara komprehensif pada SISMIOP, mengingat perannya yang signifikan dalam pengelolaan pendapatan daerah.

Pemilihan BPPKAD Kabupaten Banjarnegara sebagai objek penelitian didasarkan pada kondisi SISMIOP yang telah beroperasi sejak tahun 2020 dan berperan sebagai sistem kritikal dalam pengelolaan data perpajakan daerah. Hingga saat ini, belum pernah dilakukan evaluasi keamanan informasi secara formal dan terstruktur, serta belum terdapat penerapan kontrol keamanan informasi yang terdokumentasi sebagai bagian dari tata kelola sistem informasi. Kondisi tersebut berpotensi menimbulkan risiko terhadap kerahasiaan, integritas, dan ketersediaan data pajak daerah yang bersifat sensitif. Karakteristik SISMIOP yang mengelola data wajib pajak, bernilai finansial, dan berdampak langsung pada pendapatan daerah menuntut pendekatan evaluasi yang tidak hanya bersifat deskriptif, tetapi juga kuantitatif dan berbasis tingkat kapabilitas.

Berdasarkan permasalahan tersebut, terdapat beberapa aspek utama yang menjadi dasar penelitian ini, yaitu belum diketahuinya tingkat kematangan keamanan informasi SISMIOP, belum teridentifikasinya kesenjangan antara kondisi aktual dan standar yang seharusnya, serta belum tersusunnya strategi peningkatan keamanan informasi yang berbasis kerangka kerja terintegrasi. Untuk menjawab permasalahan tersebut, diperlukan pendekatan manajerial dan teknis yang tidak hanya mengidentifikasi kelemahan kontrol keamanan, tetapi juga mampu memberikan arahan pengembangan keamanan secara berkelanjutan. Sistem Manajemen Keamanan Informasi (SMKI) menjadi kerangka kerja penting dalam mengelola keamanan informasi secara strategis, baik pada aspek tata kelola maupun manajemen keamanan informasi (ISACA Germany Chapter, 2016).

Berbagai kerangka kerja keamanan informasi, seperti ISO/IEC 27000 *series*, NIST *Cybersecurity Framework* (CSF), ISF, COSO, dan COBIT, telah banyak digunakan dalam meningkatkan tata kelola keamanan informasi. Namun, tidak terdapat satu *framework* pun yang mampu mencakup seluruh aspek tata kelola, kontrol teknis, dan evaluasi tingkat kematangan secara bersamaan. Oleh

karena itu, integrasi antar *framework* dinilai sebagai pendekatan yang lebih efektif dan komprehensif (Omoyiola, 2020; Herath dkk., 2023). Model kematangan keamanan informasi menjadi pendekatan yang efektif untuk mengevaluasi kondisi keamanan organisasi karena menyediakan skala penilaian yang terstruktur, konsisten, dan berbasis kapabilitas (Rabii dkk., 2020).

Dalam penelitian ini, tiga kerangka kerja dipilih karena memiliki karakteristik yang saling melengkapi, yaitu NIST CSF sebagai kerangka kerja strategis berbasis fungsi untuk pengelolaan risiko (Kwon dkk., 2020), ISO/IEC 27002 sebagai referensi kontrol teknis keamanan informasi berbasis risiko, (ISACA Germany Chapter, 2016), dan *Cybersecurity Capability Maturity Model* (C2M2) sebagai model evaluatif untuk menilai tingkat kapabilitas dan kematangan keamanan informasi secara progresif (Christopher dkk., 2014). Berdasarkan kebutuhan tersebut, penelitian ini merumuskan pertanyaan utama mengenai tingkat kematangan keamanan informasi SISMIOP, kesenjangan antara kondisi aktual dan tingkat kematangan yang ditargetkan, serta rekomendasi strategis yang dapat dirumuskan melalui integrasi ketiga kerangka kerja tersebut.

NIST CSF menyediakan struktur pengelolaan risiko melalui enam fungsi inti, yaitu *Govern*, *Identify*, *Protect*, *Detect*, *Respond*, dan *Recover*, yang relevan untuk sektor publik (National Institute of Standards and Technology, 2024). ISO/IEC 27002 menyediakan daftar kontrol keamanan yang konkret dan dapat dievaluasi secara langsung terhadap kebutuhan SISMIOP (ISO/IEC, 2022). Sementara itu, C2M2 digunakan karena menerapkan prinsip pemenuhan kapabilitas secara bertahap, di mana organisasi tidak dapat mencapai tingkat kematangan yang lebih tinggi apabila masih terdapat domain keamanan yang belum terpenuhi(U.S. Department Of Energy, 2022).

Penelitian ini dibatasi pada aspek keamanan informasi yang berkaitan dengan pengelolaan SISMIOP di lingkungan BPPKAD Kabupaten Banjarnegara. Evaluasi difokuskan pada penerapan kontrol keamanan informasi berdasarkan subkategori NIST CSF, kontrol ISO/IEC 27002, serta penilaian tingkat kematangan menggunakan C2M2 dengan mempertimbangkan aspek tata kelola (*governance*) dan manajemen keamanan informasi (*management*).

Dengan belum tersedianya model evaluasi kematangan keamanan informasi yang mengintegrasikan NIST CSF, ISO/IEC 27002, dan C2M2 pada sektor publik di Indonesia, khususnya pada SISMIOP, penelitian ini diharapkan mampu memberikan instrumen evaluasi yang terukur serta rekomendasi strategis yang relevan. Pendekatan terintegrasi ini diperlukan karena data yang dikelola bersifat kritis, lintas fungsi, berdampak strategis, dan menuntut hasil evaluasi kuantitatif berbasis kapabilitas, sehingga satu kerangka kerja saja tidak cukup untuk menggambarkan kondisi keamanan informasi secara utuh.

1.2. Tujuan Penelitian

Tujuan dari penelitian ini untuk:

1. Mengidentifikasi tingkat kematangan keamanan informasi pada Sistem Manajemen Informasi Objek Pajak Bumi dan Bangunan (SISMIOP) berdasarkan kondisi aktual organisasi.
2. Menganalisis kesenjangan antara tingkat kematangan keamanan informasi aktual dengan tingkat kematangan yang ditargetkan.
3. Merumuskan rekomendasi strategis peningkatan keamanan informasi yang terstruktur dan berbasis standar.
4. Menyusun model evaluasi kematangan keamanan informasi berbasis integrasi NIST CSF, ISO/IEC 27002, dan C2M2 mendukung peningkatan kapabilitas keamanan informasi SISMIOP.

Untuk mencapai tujuan tersebut, penelitian ini diawali dengan penentuan profil organisasi menggunakan NIST CSF. Selanjutnya, subkategori NIST CSF dipetakan dengan kontrol keamanan ISO/IEC 27002 sebagai dasar penyusunan indikator penilaian. Tingkat kematangan keamanan informasi kemudian diukur dan dievaluasi menggunakan skala indikator C2M2 guna memperoleh gambaran kapabilitas keamanan informasi SISMIOP secara terstruktur dan kuantitatif.

1.3. Manfaat Penelitian

Penelitian ini memberikan manfaat dalam menyediakan evaluasi tingkat kematangan (*maturity level*) keamanan informasi pada Sistem Manajemen Informasi Objek Pajak Bumi dan Bangunan (SISMIOP), sehingga menghasilkan pemahaman yang komprehensif mengenai kondisi keamanan informasi saat ini

serta area yang memerlukan peningkatan. Hasil evaluasi tersebut menjadi dasar bagi BPPKAD Kabupaten Banjarnegara dalam pengambilan keputusan strategis untuk memperbaiki, memperkuat, dan mengembangkan sistem keamanan informasi secara lebih terukur, optimal, dan berkelanjutan guna mendukung efektivitas pengelolaan pendapatan daerah.

Selain itu, hasil penelitian ini memberikan kontribusi bagi pemerintah daerah dalam membangun dan meningkatkan kepercayaan publik terhadap layanan perpajakan berbasis digital. Transparansi dalam pengelolaan keamanan informasi serta tersedianya rekomendasi strategis yang disusun berdasarkan standar internasional menunjukkan komitmen organisasi dalam melindungi hak dan kepentingan wajib pajak. Bagi wajib pajak, peningkatan kematangan keamanan informasi pada SISMIOP memberikan rasa aman dan keandalan dalam memanfaatkan layanan Pajak Bumi dan Bangunan secara digital, sehingga berpotensi mendorong peningkatan kepatuhan wajib pajak serta pemanfaatan layanan elektronik secara lebih optimal.

Dari sisi akademik, penelitian ini berkontribusi terhadap pengembangan pengetahuan melalui penyusunan instrumen evaluasi tingkat kematangan keamanan informasi yang mengintegrasikan NIST *Cybersecurity Framework* (CSF), ISO/IEC 27002, dan *Cybersecurity Capability Maturity Model* (C2M2). Integrasi ketiga kerangka kerja tersebut menghasilkan model evaluasi kematangan keamanan informasi yang bersifat komprehensif dan berpotensi diterapkan pada sektor publik di Indonesia, khususnya pada sistem informasi pemerintah yang mengelola data sensitif dan bernilai strategis.