

# **BAB I PENDAHULUAN**

## **I.1 Latar Belakang**

Risiko merupakan faktor hal yang tidak bisa dihindari oleh suatu perusahaan. Perusahaan tanpa adanya persiapan yang matang akan berdampak fatal bahkan dapat merugikan perusahaan itu sendiri. Dalam dunia teknologi informasi, tidak dapat dipungkiri bahwa ada banyak faktor yang memiliki potensi untuk menjadi risiko bagi perusahaan. Maka dari itu, diperlukan langkah-langkah untuk mendeteksi risiko baik di dalam maupun di luar perusahaan, yang mengharuskan adanya sistem untuk menemukan risiko tersebut, sehingga penerapan manajemen risiko pada suatu perusahaan harus dilakukan. (Putra & Soewito, 2023).

Manajemen risiko merupakan suatu sistem menyeluruh yang melibatkan kebijakan, prosedur, dan praktik untuk mengidentifikasi, menilai, mengendalikan serta meminimalkan eksposur organisasi terhadap risiko dengan tujuan untuk meningkatkan nilai perusahaan (Zainal Putra dkk., 2017). Manajemen risiko memiliki proses mengidentifikasi risiko, menilai besarannya dan mengambil langkah yang tepat untuk mengurangi risiko ke tingkat yang dapat diterima oleh suatu perusahaan (Putra & Soewito, 2023). Manajemen risiko berguna bagi perusahaan agar dapat mengambil langkah-langkah yang tepat untuk meminimalkan dampak yang terjadi. Dengan menerapkan manajemen risiko, perusahaan dapat memberikan pengaruh yang signifikan terhadap kinerjanya. Dalam dunia Teknologi Informasi (TI) yang penuh ketidakpastian, manajemen risiko membantu perusahaan mengantisipasi, mengelola, dan merespons risiko dengan cara yang meminimalkan potensi kerugian dan memaksimalkan peluang.

PT XYZ adalah perusahaan yang berfokus kepada pemeliharaan dan perbaikan pesawat atau *Maintenance, Repair, dan Operation* (MRO). Selain fokusnya kepada MRO pesawat, PT XYZ juga memiliki unit IT dalam menunjang bisnis perusahaan. Teknologi Informasi sangat dibutuhkan dalam mendukung rencana jangka panjang perusahaan. Dalam mendukung rencana jangka panjang perusahaan, pastinya rencana yang sudah disiapkan tidak selalu berjalan dengan

lancar sesuai harapan. Maka dari itu, penerapan manajemen risiko pada unit IT di PT XYZ harus diterapkan untuk mendukung kelancaran rencana jangka panjang yang diharapkan.

PT XYZ sebenarnya sudah memiliki divisi yang berfokus pada pengelolaan risiko, yaitu unit *Enterprise Risk Management* (ERM). Unit ERM bertugas mengelola risiko secara umum di perusahaan. Divisi *Innovation & IT Project Management* menyatakan bahwa teknologi informasi merupakan hal yang sangat penting untuk mendukung bisnis perusahaan, namun masalah sering muncul karena belum adanya pendekatan khusus untuk mengelola risiko di unit IT. Ini bisa menyebabkan risiko-risiko TI tidak terkelola dengan baik dan mengganggu operasional perusahaan. Untuk mengatasinya, penelitian ini dilakukan untuk mengevaluasi potensi risiko yang mungkin muncul dalam operasional unit IT PT XYZ serta menyusun rekomendasi untuk penerapan manajemen risiko yang efektif. Dengan demikian, diharapkan unit IT PT XYZ dapat mendukung kelancaran rencana jangka panjang perusahaan dan mengurangi dampak negatif dari berbagai risiko yang mungkin terjadi.

Dalam penelitian ini akan menggunakan *framework* ISO 27005 sebagai standar dalam mengelola risiko. ISO 27005 mencakup langkah-langkah dalam menganalisis risiko keamanan informasi, yang diimplementasikan dalam manajemen risiko TI secara menyeluruh, sesuai dengan kebutuhan unit IT PT XYZ. Selain ISO 27005, penelitian ini juga akan mengimplementasikan *framework* COBIT 2019. Selain itu, penelitian ini juga menerapkan *framework* COBIT 2019 untuk menyediakan panduan dalam menentukan kontrol bagi risiko yang memerlukan penanganan. Untuk memperkuat rekomendasi, kontrol tambahan berdasarkan standar NIST SP 800-53 akan digunakan, terutama untuk *risk profile Logical Attack*. COBIT 2019 juga digunakan untuk identifikasi risiko pada penelitian ini yang diadopsi pada *Figure 2.7—Risk Profile Design Factor (IT Risk Categories)*. Selain *framework* yang digunakan, dalam penelitian ini akan melakukan penyebaran kuesioner serta wawancara untuk mengumpulkan data. Penyebaran kuesioner akan memberikan data untuk digunakan dalam penilaian

risiko, sedangkan wawancara akan dilakukan untuk mengevaluasi data yang didapatkan dari kuesioner. Dengan menerapkan ISO 27005, COBIT 2019, dan NIST SP 800-53, penelitian ini diharapkan dapat memberikan pandangan mendalam mengenai risiko TI yang mungkin dihadapi oleh PT XYZ.

## **I.2 Perumusan Masalah**

Berdasarkan latar belakang di atas, maka rumusan masalah yang diangkat adalah sebagai berikut:

- a. Bagaimana identifikasi risiko TI dengan menggunakan COBIT 2019.
- b. Bagaimana pengelolaan risiko berdasarkan penerapan *framework* ISO 27005.
- c. Apa rekomendasi dan kontrol berdasarkan COBIT 2019 dan NIST SP 800-53 untuk mengatasi risiko yang teridentifikasi.

## **I.3 Tujuan Penelitian**

Berdasarkan perumusan masalah tersebut, Adapun tujuan penelitian sebagai berikut:

- a. Mengidentifikasi risiko TI menggunakan *framework* COBIT 2019.
- b. Melakukan pengelolaan risiko berdasarkan penerapan *framework* ISO 27005 untuk risiko yang mungkin muncul dalam unit IT.
- c. Memberikan rekomendasi dan kontrol risiko berdasarkan COBIT 2019 dan NIST SP 800-53 untuk risiko yang teridentifikasi.

## **I.4 Batasan Penelitian**

Berikut merupakan batasan masalah dari penelitian ini:

- a. Penelitian ini memiliki batasan dalam tahap *risk assessment* dan *risk treatment* yang menggunakan *framework* ISO 27005.
- b. Penelitian ini akan berfokus kepada identifikasi risiko yang diadopsi dari COBIT 2019 *Design Guide, Figure 2.7—Risk Profile Design Factor (IT Risk Categories)* yang berfokus kepada *risk profile Logical Attacks*,

*Program and Projects Lifecycle Management, Software Adoption/Usage Problems, dan Unauthorized Actions.*

- c. Penelitian ini tidak mencakup tahapan *monitoring* dan *review* terkait implementasi kontrol dan rekomendasi yang diberikan.
- d. Penelitian ini hanya fokus pada unit IT.

## **I.5 Manfaat Penelitian**

Manfaat penelitian ini:

1. Bagi PT XYZ, penelitian ini bermanfaat untuk memberikan wawasan yang baik kepada pihak PT XYZ mengenai pengelolaan manajemen risiko TI yang baik.
2. Bagi Penulis, penelitian ini bermanfaat untuk memperluas pemahaman mengenai Manajemen Risiko Teknologi Informasi, khususnya dalam konteks pengelolaan manajemen risiko TI.

## **I.6 Sistematika Penulisan**

Penelitian ini diuraikan dengan sistematika penulisan sebagai berikut:

### **Bab I Pendahuluan**

Pada bab ini berisi uraian mengenai konteks permasalahan, latar belakang penelitian, perumusan masalah, tujuan penelitian, batasan penelitian, manfaat penelitian, dan sistematika penulisan.

### **Bab II Tinjauan Pustaka**

Bab ini berisi literatur yang relevan dengan masalah yang diteliti, membahas hasil penelitian sebelumnya, serta menjelaskan teori terkait manajemen risiko dan kerangka kerja ISO 27005.

### **Bab III Metodologi Penelitian**

Pada bab ini berisi mengenai konseptual model, pengumpulan dan pengolahan data, metode yang dipilih, serta rencana dari alur penelitian yang dilakukan.

**Bab IV Pengumpulan dan Analisis Data**

Pada bab ini berisi tentang proses pengumpulan, pengolahan serta proses analisis data yang dipergunakan sebagai bahan terhadap penelitian yang sudah dilakukan.

**Bab V Rekomendasi dan Kontrol**

Pada bab ini akan menjelaskan kontrol yang telah ditetapkan untuk setiap item yang diidentifikasi, serta memberikan rekomendasi untuk mengatasi masalah yang terjadi.

**Bab VI Kesimpulan dan Saran**

Pada bab ini dijelaskan kesimpulan dari penelitian yang dilakukan serta jawaban dari pertanyaan penelitian yang disajikan di pendahuluan.