BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil penelitian di Dinas Komunikasi dan Informatika (Diskominfo) Provinsi Daerah Istemewah Yogyakarta (DIY), dapat disimpulkan bahwa proses identifikasi aset informasi penting telah dilakukan melalui observasi menggunakan checklist kontrol, wawancara semi-terstruktur, serta analisis dokumen internal seperti *Risk Register*, *Statement of Applicability* (SoA), dan SOP keamanan informasi. Dari proses tersebut diperoleh daftar aset strategis yang mencakup data operasional, layanan publik, sistem aplikasi internal, infrastruktur jaringan dan server, serta dokumentasi ISMS. Identifikasi ini memastikan bahwa seluruh aset yang bernilai kritis terhadap keberlangsungan layanan publik dan reputasi organisasi telah terdokumentasi dengan baik sesuai prinsip ISO/IEC 27001:2022.

Selanjutnya, proses penilaian risiko keamanan informasi dilakukan dengan mengacu pada kerangka ISO 31000:2018 melalui analisis *Likelihood* dan *Impact*. Hasil penilaian menunjukkan terdapat lima risiko utama, dua di antaranya masuk kategori tinggi, yaitu kegagalan backup data dan rendahnya awareness pegawai baru, sementara tiga risiko lain berada pada kategori sedang, yaitu akses fisik ilegal, perubahan organisasi, dan tidak adanya evaluasi stakeholder. Penilaian ini kemudian menjadi dasar penyusunan strategi mitigasi, antara lain implementasi backup ganda, penguatan kontrol akses fisik, pembaruan dokumen peran dan tanggung jawab, serta program pelatihan dan evaluasi stakeholder, sehingga pengelolaan risiko dapat dilakukan secara terukur, terdokumentasi, dan sesuai standar ISO/IEC 27001:2022.

5.2 Saran

1. Untuk Praktik Organisasi
    a. Meningkatkan keamanan data dengan menerapkan sistem backup ganda (onsite dan offsite) serta melakukan *restore test* secara rutin.
    b. Memperkuat kesadaran pegawai melalui program *security induction training* untuk pegawai baru dan pelatihan berkala bagi seluruh staf.

c. Mengoptimalkan kontrol akses fisik ruang server dengan *double verification* (fingerlock dan kartu akses) serta pemantauan CCTV secara *real-time*.

2. Untuk Penelitian Selanjutnya
   a. Memperluas objek penelitian ke instansi atau organisasi lain untuk memperoleh gambaran komparatif penerapan ISMS.
   b. Menggunakan metode kuantitatif penuh dengan data historis insiden untuk menghasilkan perhitungan risiko yang lebih akurat.
   c. Melakukan kajian perbandingan dengan standar keamanan lain seperti NIST Cybersecurity Framework atau COBIT guna memperkaya perspektif pengelolaan risiko.