BAB V KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil evaluasi penerapan keamanan informasi pada SIMRS Rumah Sakit XYZ, diperoleh kesimpulan sebagai berikut:

1. Kondisi aktual dan tingkat kematangan penerapan keamanan informasi pada SIMRS Rumah Sakit XYZ menunjukkan bahwa rumah sakit telah memiliki kebijakan, prosedur, pembagian tanggung jawab, dan pengamanan teknis yang mendukung pengelolaan SIMRS. Pengendalian yang telah diterapkan meliputi pembatasan hak akses berdasarkan peran, autentikasi pengguna, pencatatan aktivitas sistem, pencadangan data, penggunaan antivirus dan firewall, pemantauan server dan jaringan, pemisahan jaringan operasional dan jaringan tamu, serta pengamanan ruang server. Berdasarkan penilaian terhadap 53 kontrol terpilih, diperoleh total nilai aktual sebesar 159 dari nilai maksimum 265 dengan rata-rata *maturity level* sebesar 3,00. Nilai tersebut menempatkan penerapan keamanan informasi SIMRS pada Level 3 atau kategori Terdefinisi dan Konsisten. *Organizational Controls* memperoleh rata-rata 3,23, *People Controls* dan *Physical Controls* masing-masing 3,00, sedangkan *Technological Controls* memperoleh rata-rata 2,75. Hasil tersebut menunjukkan bahwa sebagian besar kontrol telah memiliki dasar formal dan diterapkan dalam kegiatan operasional, tetapi penerapannya belum seluruhnya didukung pemantauan, pengukuran, pengujian, dan evaluasi efektivitas secara berkala.
2. Hasil analisis kesenjangan antara kondisi aktual dan target Level 4 atau Terkelola dan Terukur menunjukkan total nilai target sebesar 212 dan nilai aktual sebesar 159, sehingga diperoleh total kesenjangan sebesar 53. Kesenjangan terbesar terdapat pada *Technological Controls* sebesar 25, diikuti *Organizational Controls* sebesar 17, *Physical Controls* sebesar 6, dan *People Controls* sebesar 5. Penilaian risiko terhadap kontrol yang memiliki kesenjangan menghasilkan tiga risiko tinggi, empat risiko sedang, dan enam risiko rendah. Risiko tinggi mencakup pengamanan perangkat dan pengelolaan kerentanan, kepatuhan pengguna terhadap *clear desk* dan *clear screen*, serta kesiapan penanganan insiden. Risiko sedang berkaitan dengan keamanan jaringan, pemulihan data dan layanan, perlindungan data, serta pengelolaan akun. Hasil tersebut menunjukkan bahwa peningkatan perlu diprioritaskan pada kontrol yang belum diterapkan secara

merata, belum diuji secara berkala, atau belum didukung pencatatan dan evaluasi yang konsisten.

3. Rekomendasi perbaikan disusun secara bertahap berdasarkan tingkat risiko, kondisi operasional, keterbatasan personel, dan dukungan anggaran Unit SIMRS. Prioritas perbaikan mencakup pemerataan antivirus dan pembaruan keamanan, pemeriksaan kerentanan, penerapan penguncian layar otomatis, evaluasi kepatuhan dan kesadaran pengguna, pemusatan pencatatan, penutupan, dan evaluasi insiden, simulasi penanganan insiden, pengujian keamanan jaringan, pengujian pemulihan data dan perpindahan layanan ke fasilitas cadangan, penguatan perlindungan data, serta penyempurnaan prosedur manajemen hak akses yang telah tersedia dan pengelolaan akses pihak ketiga. Sebagai dokumen pendukung, penelitian menghasilkan lima rancangan SOP, yaitu Rancangan SOP Pengelolaan Kerentanan dan Pembaruan Keamanan SIMRS, Rancangan SOP Evaluasi Kepatuhan dan Kesadaran Pengguna terhadap Keamanan SIMRS, Rancangan SOP Pencatatan, Penutupan, dan Evaluasi Insiden Keamanan Informasi SIMRS, Rancangan SOP Pengujian Pemulihan Data dan Layanan SIMRS, serta Rancangan SOP Pengelolaan Akses dan Kerahasiaan Pihak Ketiga pada SIMRS. Rekomendasi dan rancangan SOP tersebut disusun sebagai bahan pertimbangan bagi Unit SIMRS untuk meningkatkan penerapan keamanan informasi menuju kondisi yang lebih terpantau, terukur, dan dievaluasi secara berkala.

5.2 Saran

Berdasarkan hasil penelitian, beberapa saran yang dapat diberikan adalah sebagai berikut:

1. Rumah Sakit XYZ disarankan memprioritaskan perbaikan pada area dengan risiko tinggi, yaitu pengamanan perangkat dan pengelolaan kerentanan, kepatuhan pengguna terhadap penerapan clear desk dan clear screen, serta kesiapan penanganan insiden keamanan informasi. Pelaksanaannya perlu dimasukkan ke dalam program kerja dan anggaran pengembangan SIMRS serta dilakukan secara bertahap sesuai prioritas risiko, kebutuhan operasional, dan kapasitas personel yang tersedia.
2. Unit SIMRS disarankan menggunakan lima rancangan SOP yang dihasilkan dalam penelitian sebagai bahan penyempurnaan pengelolaan keamanan informasi. Pelaksanaan setiap prosedur perlu didukung formulir, daftar pemeriksaan, register, atau laporan hasil kegiatan agar penerapannya dapat ditelusuri, dipantau, dan dievaluasi secara berkala.

3. Unit SIMRS disarankan memperkuat pengamanan teknis secara bertahap dengan memastikan antivirus dan pembaruan keamanan diterapkan pada seluruh perangkat yang mengakses SIMRS, melakukan pemeriksaan kerentanan, mengaktifkan penguncian layar otomatis, serta meninjau akun dengan kewenangan khusus. Pengujian pemulihan data, server cadangan, dan jalur internet cadangan juga perlu dilakukan secara terjadwal dengan menetapkan target waktu pemulihan layanan dan batas kehilangan data yang dapat diterima.
4. Rumah Sakit XYZ dan Unit SIMRS disarankan meningkatkan pencatatan dan evaluasi terhadap pengelolaan vendor, akses ruang server, perubahan sistem, aktivitas log, inventaris aset, dan dokumen keamanan informasi. Perjanjian dengan vendor perlu memuat ketentuan kerahasiaan, keamanan data, pembatasan akses, dan pelaporan insiden. Setiap perubahan sistem dan pemberian akses kepada pihak luar juga perlu disertai persetujuan, pencatatan kegiatan, pemeriksaan hasil pekerjaan, dan penghentian akses setelah pekerjaan selesai.
5. Penelitian selanjutnya disarankan memperluas evaluasi terhadap kontrol Annex A ISO/IEC 27001:2022 yang belum termasuk dalam penelitian ini atau menggunakan pedoman keamanan informasi yang lebih khusus untuk sektor kesehatan. Penelitian berikutnya juga dapat menambahkan pengujian teknis, seperti vulnerability assessment dan penetration testing, setelah memperoleh izin resmi dari organisasi, sehingga kondisi keamanan aplikasi, server, jaringan, konfigurasi, perlindungan data, dan efektivitas kontrol teknis dapat dinilai secara lebih mendalam.