

ABSTRAK

Dinas Komunikasi dan Informatika Kabupaten Bantul memiliki peran strategis sebagai pengelola infrastruktur TIK, pusat data, dan penyelenggara Sistem Pemerintahan Berbasis Elektronik (SPBE). Namun, seiring dengan masifnya digitalisasi, ancaman siber seperti *web defacement*, *phishing*, hingga kebocoran data penduduk menjadi tantangan nyata yang terus terjadi berulang dan berisiko melumpuhkan operasional pemerintahan serta merusak kepercayaan masyarakat. Meskipun telah menerapkan standar ISO/IEC 27001 selama tiga tahun terakhir, instansi belum pernah melakukan peninjauan keamanan berkala melalui proses penilaian risiko yang terstruktur dan rinci guna menghadapi dinamika ancaman siber terbaru.

Penelitian ini bertujuan untuk melakukan penilaian risiko keamanan informasi secara komprehensif menggunakan kerangka kerja NIST SP 800-30 Rev. 1 dan merumuskan rekomendasi kontrol keamanan berdasarkan katalog NIST SP 800-53 Rev. 5. Metodologi penelitian menggunakan pendekatan *threat-oriented* yang bersifat proaktif, dengan fokus pada identifikasi ancaman sebelum mengevaluasi kerentanan sistem. Data diperoleh melalui observasi lapangan, studi dokumen pada *incident log*, serta wawancara dan diskusi anggota tim manajemen risiko Diskominfo Kab. Bantul guna memahami konteks operasional dan teknis. Tahapan penelitian dilaksanakan secara sistematis meliputi proses pembingkaihan risiko (*framing*), pelaksanaan penilaian risiko (*assessing*), hingga penentuan strategi respons risiko (*responding*).

Hasil penelitian berhasil mengidentifikasi 49 peristiwa ancaman (18 *adversarial* dan 31 *non-adversarial*), 52 celah kerentanan, serta 7 kondisi predisposisi. Profil risiko di Diskominfo Kab. Bantul didominasi oleh tingkat Sangat Rendah hingga Rendah, yang mencerminkan kematangan kontrol eksisting implementasi ISO 27001. Temuan kritis menunjukkan bahwa ancaman *phishing* menjadi satu-satunya risiko tingkat Sedang dan prioritas mitigasi utama karena dipicu oleh rendahnya kesadaran keamanan pengguna serta absennya mekanisme *Multi-Factor Authentication* (MFA). Berdasarkan hasil penilaian, ditetapkan strategi respons berupa 40 risiko dimitigasi dan 9 risiko diterima. Mitigasi risiko dirumuskan melalui pemilihan 18 keluarga kontrol NIST SP 800-53 (*Moderate Baseline*) dengan fokus dominan pada kelompok *System and Information Integrity* (SI), *Contingency Planning* (CP), *Access Control* (AC), dan *System and Communications Protection* (SC).

Dengan demikian, hasil penelitian ini menunjukkan bahwa penggunaan NIST SP 800-53 mampu memberikan panduan operasional yang lebih granular sebagai pelengkap standar ISO 27001 dalam melindungi aset digital daerah. Rekomendasi kontrol yang dihasilkan telah divalidasi oleh pihak instansi dan dinyatakan relevan serta cocok untuk diimplementasikan. Penelitian ini menyarankan instansi untuk segera menerapkan mekanisme MFA, memperkuat kesadaran keamanan pegawai, serta memperkuat dokumen *Business Continuity Plan* (BCP) guna menjamin kontinuitas layanan publik di Pemerintah Kabupaten Bantul.

Kata Kunci: penilaian risiko, keamanan informasi, NIST SP 800-30, NIST SP 800-53, SPBE, Diskominfo Kab. Bantul.

ABSTRACT

The Communications and Information Technology Office (Diskominfo) of Bantul Regency plays a strategic role as the manager of ICT infrastructure, the data center, and the organizer of the Electronic-Based Government System (SPBE). However, along with massive digitalization, cyber threats such as web defacement, phishing, and resident data leaks have become real challenges that recur frequently, risking government operations and damaging public trust. Although the agency has implemented ISO/IEC 27001 for the past three years, it has never conducted a structured and detailed periodic security review through a risk assessment process to face the latest dynamic cyber threats.

This research aims to conduct a comprehensive information security risk assessment using the NIST SP 800-30 Rev. 1 framework and to formulate security control recommendations based on the NIST SP 800-53 Rev. 5 catalog. The methodology uses a proactive threat-oriented approach, focusing on identifying threats before evaluating system vulnerabilities. Data were obtained through field observations, document studies of incident logs, as well as interviews with members of the Diskominfo Bantul risk management team to understand the technical and operational context. The research stages were implemented systematically, covering risk framing, risk assessing, and risk responding processes.

The results successfully identified 49 threat events (18 adversarial and 31 non-adversarial), 52 vulnerabilities, and 7 predisposing conditions. The risk profile at Diskominfo Bantul is dominated by Very Low to Low levels, reflecting the maturity of existing controls from the ISO 27001 implementation. A critical finding shows that phishing is the only Medium-level risk and the top mitigation priority, triggered by low user security awareness and the absence of Multi-Factor Authentication (MFA) mechanisms. Based on the assessment results, a response strategy was established where 40 risks are mitigated and 9 risks are accepted. Risk mitigation was formulated by selecting 18 NIST SP 800-53 control families (Moderate Baseline), with a dominant focus on the System and Information Integrity (SI), Contingency Planning (CP), Access Control (AC), and System and Communications Protection (SC) groups.

In conclusion, this research demonstrates that the NIST SP 800-53 catalog provides more granular operational guidance as a complement to the ISO 27001 standard in protecting regional digital assets. The resulting control recommendations have been validated by the agency and declared relevant and suitable for implementation. This research suggests that the agency immediately implement MFA mechanisms, strengthen employee security awareness, and develop a tested Business Continuity Plan (BCP) to ensure public service continuity within the Bantul Regency Government environment.

Keywords: risk assessment, information security, NIST SP 800-30, NIST SP 800-53, SPBE, Diskominfo Kab. Bantul.