ABSTRAK

Kemanan informasi menjadi perhatian bagi *cloud service provider* (CSP) dan penilaian risiko menjadi penting untuk dapat menumbuhkan kepercayaan pelanggan karena dengan adanya penilaian risiko yang sistematis dan terstruktur akan dapat memastikan kemanan informasi organisasi. ISO 27005:2018 adalah metode yang populer, namun tidak mendetail menyediakan pendekatan kuantitatif penilaian risiko, sehingga perlu didukung dengan NIST SP 800-30. Integrasi kedua metode tersebut telah teruji sesuai untuk digunakan pada organisasi profit dan non-profit. Dikarenakan CSP merupakan organisasi profit, maka penelitian ini akan berfokus untuk menguji kesesuaian integrasi NIST SP 800-30 dan ISO 27005:2018 pada CSP. Integrasi NIST SP 800-30 dan ISO 27005:2018 tidak dapat memberikan rekomendasi kontrol, maka pada penelitian ini dirujuk standar kontrol keamanan NIST SP 800-53.

Penelitian ini akan berfokus untuk menguji kesesuaian implementasi integrasi NIST SP 800-30 dengan dukungan ISO 27005, untuk menilai risiko pada SIAKAD *cloud service* melalui tahap identifikasi aset, identifikasi ancaman, identifikasi kerentanan dan kondisi predisposisi, penetapan likelihood & impact, dan penetapan risiko. Hasil yang akan didapatkan adalah *risk register* dan rekomendasi kontrol yang disusun dengan didasarkan pada pemetaan hasil penilaian risiko dengan standar keamanan dan privasi, NIST SP 800-53. Pengujian hipotesa akan dilakukan pada tahap pengkomunikasian dan validasi hasil yang melibatkan stakeholder terkait. Studi kasus yang digunakan adalah layanan SIAKAD *cloud* ABC, yang dimiliki CSP PT. XYZ.

Integrasi ISO 27005:2018 dan NIST SP 800-30 terbukti sesuai diimplementasikan pada CSP untuk membantu proses penilaian risiko, sebagai dasar pelaksanaan manajemen risiko dan kontrol keamanan informasi berkelanjutan. Hasil penilaian risiko yang dilakukan mengindikasikan bahwa layanan ABC, memiliki 125 risiko bernilai Rendah, 108 bernilai Sedang, 46 bernilai Tinggi, 15 Sangat Tinggi, dan 12 lainnya bernilai Sangat Rendah. Berdasarkan risk register yang diperoleh, dan analisa pemetaan terhadap NIST SP 800-53 yang dilakukan, dari 20 kelompok kontrol keamanan dan privasi, 18 diantaranya relevan diimplementasikan pada layanan ABC, PT. XYZ.

Kata kunci: Penilaian Risiko, NIST SP 800-30, ISO 27005, NIST SP 800-53, Kontrol Keamanan dan Privasi