

ABSTRAK

Jantung dari setiap organisasi bisnis adalah teknologi informasi yang dimiliki, untuk itu keamanannya harus dapat dijaga. Di Indonesia mayoritas instansi penyelenggara pelayanan publik belum/sedang menyusun kerangka kerja keamanan informasi yang memenuhi standar ISO 27001. Salah satunya adalah PT INTI (Persero) Bandung. Beberapa kasus terkait keamanan informasi di perusahaan sering terjadi, oleh karena itu dilakukan audit untuk memperbaiki sistem manajemen keamanan informasi dalam perusahaan.

Jenis penelitian yang digunakan adalah penelitian terapan, dan penelitian ini termasuk penelitian kualitatif yang bersifat deskriptif. Teknik untuk mengambil data dan untuk validitas adalah dengan triangulasi teknik, dengan wawancara terstruktur dan pengambilan data lainnya dengan observasi, studi dokumen, dan foto-foto yang digunakan untuk uji validitas. Analisis dilakukan dengan mereduksi data yang didapat yang kemudian dianalisis dengan *work paper gap analysis* beserta diberikan rekomendasinya, dan kemudian dihitung tingkat *maturity level* untuk setiap *annex*-nya. Model *maturity level* yang digunakan adalah CMMI (*Capability Maturity Model Integration*).

Hasil penelitian menunjukkan nilai *maturity level* pada *annex 5* berada di level 0.43 (PASIF), *annex 7* berada di level 3 (PRO-AKTIF), *annex 9* berada di level 2.5 (AKTIF), *annex 9* berada di level 2.5 (AKTIF).

Keyword: Keamanan informasi, audit keamanan informasi, ISO 27001, *Gap Analysis*, *Maturity level*