

## ABSTRAK

PT. XYZ merupakan perusahaan yang bergerak sebagai penyedia produk-produk elektronika industri dan prasarana serta infrastruktur yang luas. Dalam kegiatan operasionalnya, tentunya didukung Teknologi Informasi yang dapat meningkatkan nilai tambah dan daya saing perusahaan. PT. XYZ memiliki aset TI utama yang perlu dilindungi untuk menjaga fungsi hubungan dengan proses bisnis yang berjalan. Dalam perlindungan aset TI, perlu diketahui ancaman-ancaman yang mungkin terjadi dan menilai kontrol yang sudah ada untuk mengurangi dampak negatif dari risiko. PT. XYZ memiliki penerapan *risk assessment* dalam pengelolaan TI dan proses bisnis pada tiap divisi terkait. Akan tetapi, penerapan tersebut belum sepenuhnya menilai adanya ancaman pada aset TI dan menilai seberapa jauh kontrol yang sudah ada dapat mengurangi ancaman yang akan datang serta dampaknya. Maka dari itu, diperlukan implementasi dan penilaian *risk assessment* di PT. XYZ untuk menjaga fungsi TI dalam kegiatan operasionalnya.

Implementasi dan penilaian *risk assessment* terhadap infrastruktur TI dilakukan menggunakan *framework* COBIT 5 *for risk* yang difokuskan untuk melakukan pengelolaan/kontrol terhadap risiko TI. Penerapan *risk assessment* dilakukan dengan mengacu pada *risk scenario* dan *control objective* pada COBIT 5 *for risk*. Penelitian ini dilakukan dengan mengidentifikasi *risk scenario* pada aset TI berdasarkan penilaian kontrol yang ada dengan *control objective* pada COBIT 5 *for risk*, selanjutnya menentukan *risk treatment* yang disesuaikan dengan keputusan perusahaan sebagai kontrol untuk menjaga kemungkinan ancaman dan dampak yang terjadi.

Hasil pada penelitian ini berupa rekomendasi mengenai implementasi dan penilaian *risk assessment* berupa *risk potential* dan *risk treatment*, sehingga diharapkan implementasi dan penilaian *risk assessment* yang mengacu pada COBIT 5 *for risk* dapat diterapkan pada PT. XYZ dalam melakukan kontrol sebagai pengelolaan pada aset TI.

Kata Kunci: COBIT 5 *for risk*, *risk assessment*, *risk scenario*, *control objective*, *risk potential*, *risk treatment*