

Mochamad Hiqaf Dimas Putranda, 2018. Identifikasi Tingkat Resiko Menggunakan ISO 27005 Pada Perangkat Keras Jaringan Di Bank Jatim Kantor Pusat Surabaya. Skripsi ini dibawah bimbingan Endah Purwanti, S.Si, M.Kom. dan Dr. Rimuljo Hendradi, S.Si, M.Si. Program Studi S1 Sistem Informasi. Fakultas Sains dan Teknologi, Universitas Airlangga.

ABSTRAK

Proses identifikasi tingkat resiko pada perangkat keras jaringan pada umumnya difokuskan pada pengukuran suatu ancaman tunggal tanpa mempertimbangkan akibat yang mungkin terjadi dari suatu ancaman terhadap aset yang disebabkan oleh ancaman dari tereksplotasinya aset yang lain. Bank Jatim merupakan sebuah perusahaan keuangan yang memiliki jaringan yang cukup luas, yang menghubungkan beberapa kantor cabang di beberapa kota di Jawa Timur. Penerapan sistem keamanan jaringan merupakan langkah perlindungan terhadap ancaman yang mungkin terjadi guna mempertahankan layanan bisnis dan operasional perusahaan.

Langkah-langkah proses identifikasi resiko dalam penelitian ini, mengacu kepada tahapan-tahapan dalam manajemen resiko berdasarkan ISO 27005:2008. Untuk melakukan proses identifikasi resiko dan ancaman terhadap masing-masing aset jaringan maka digunakan *IT Baseline Protection* sebagai studi pustaka. Proses untuk memprioritaskan resiko menggunakan metode perhitungan FMEA (*Fault Mode Effect Analysis*). Hasil dari perhitungan FMEA (*Fault Mode Effect Analysis*) adalah berupa total nilai RPN (*Risk Priority Number*) yang dihasilkan dari penentuan skala *severity*, *occurance*, dan *detection*. Nilai RPN (*Risk Priority Number*) yang tertinggi pada resiko yang terdapat pada suatu aset jaringan mengartikan bahwa resiko tersebut perlu segera ditangani oleh perusahaan karena memiliki dampak yang cukup besar jika ditinjau dari skala yang *severity*, *occurance*, dan *detection* ditentukan.

Kata Kunci — **ISO 27005, Manajemen Resiko, Fault Mode Effect Analysis, Risk Priority Number, IT Baseline Protection, Aset Jaringan**

Mochamad Hiqaf Dimas Putranda, 2018. Identifikasi Tingkat Resiko Menggunakan ISO 27005 Pada Perangkat Keras Jaringan Di Bank Jatim Kantor Pusat Surabaya. Skripsi ini dibawah bimbingan Endah Purwanti, S.Si, M.Kom. dan Dr. Rimuljo Hendradi, S.Si, M.Si. Program Studi S1 Sistem Informasi. Fakultas Sains dan Teknologi, Universitas Airlangga.

ABSTRACT

The process of identifying the degree of risk on network hardware is generally focused on measuring a single threat without considering the possible consequences of a threat to the asset caused by the threat of exploiting another asset. Bank Jatim is a financial company that has a wide network, which connects several branch offices in several cities in East Java. Implementation of network security system is a protective measure against possible threats to maintain business services and company operations.

The steps of risk identification process in this study, refer to the stages in risk management based on ISO 27005: 2008. To perform the process of identifying risks and threats against each network asset then used IT Baseline Protection as a literature study. Process to prioritize risk using FMEA (Fault Mode Effect Analysis) calculation method. The result of calculation of FMEA (Fault Mode Effect Analysis) is the total value of RPN (Risk Priority Number) resulting from determination of severity, occurrence, and detection scale. The highest RPN (Risk Priority Number) value at risk in a network asset means that the risk needs to be handled immediately by the company because it has considerable impact when viewed from the severity, occurrence, and detection scale.

Keywords — ISO 27005, Risk Management, Fault Mode Effect Analysis, Risk Priority Number, IT Baseline Protection, Network Asset