ABSTRAK

Di era yang terus berkembang ini, organisasi dihadapkan pada tantangan yang semakin kompleks dalam mengelola keamanan informasi mereka. Penggunaan satu standar atau *framewor*k manajemen kemanan dianggap masih kurang optimal karena tidak ada satu solusi yang mencakup keseluruhan organisasi. Karena itu, ada kebutuhan untuk menjabarkan aktifitas yang mengintegrasikan manajemen kemanan informasi berdasarkan standar dan *framework* yang ada. Penelitian ini bertujuan untuk memberikan gambaran mengenai penerapan aktifitas manajemen keamanan pada empat organisasi berdasarkan integrasi ISO 27001, NIST CSF, dan CIS Control V8 yang pengumpulan datanya dilakukan dengan melakukan wawancara pada narasumber di setiap organisasi. Organisasi A yang bergerak di sektor informatika memiliki tingkat penerapan manajemen keamanan yang baik dengan skor 3.3. Sementara itu, Organisasi B di sektor kebudayaan hanya mencapai skor 1.9 dengan kategori cukup. Organisasi C dalam sektor kesehatan juga berada di level cukup dengan skor 2.5. Disisi lain, Organisasi D yang berada di sektor pendidikan menunjukkan hasil memuaskan dengan skor tertinggi, yaitu 4.8. Dengan penilaian penerapan maanjemen keamanan yang telah dilakukan, organisasi dapat melakukan perbaikan yang sesuai dengan cakupan organisasi. Pertama, pada Organisasi A dan Organisasi C. Kedua organisasi ini direkomendasikan untuk menerapkan pendekatan '*Defense in depth'*, yang melibatkan pengimplementasian keamanan berlapis. Sementara untuk Organisasi B dapat fokus pada *"Information Security*", hal ini berkaitan dengan tujuan penggunaan jaringan komputer pada organisasi tersebut. Disisi lain organisasi D yang dinilai telah sangat baik dalam penerapan manajemen keamanannya dapat melakukan perbaikan pada aktifitas preventif pada organisasi.

Kata kunci – manajemen keamanan, standar, kerangka kerja, penilaian, ISO 27001, NIST CSF, CIS Control V8.