**TUGAS KEAMANAN JARINGAN**

**“PENERAPAN SISTEM KEAMANAN ISO 27002 PADA PERUSAHAAN GARUDA INDONESIA”**



**Disusun oleh :**

**Eka Saputra 14.11.0030/2014**

**Agung Prasetia 14.11.0042/2014**

**Iqbaluddin Syam Had 14.11.0082/2014**

**Fajar adde irawan 14.11.0086/2014**

**Imanudin Sholeh 14.11.0344/2014**

**SEKOLAH TINGGI MANAGEMEN INFORMATIKA DAN KOMPUTER**

**AMIKOM PURWOKERTO**

**PURWOKERTO**

**2014/2015**

1. *Introduction*

Garuda Indonesia adalah maskapai penerbangan nasional Indonesia yang terbang ke lebih dari 40 tujuan domestik dan 36 tujuan internasional. Garuda Indonesia meraih penghargaan sebagai Maskapai Penerbangan Regional Terbaik di Dunia yang diberikan oleh Skytrax. Terbang untuk pertama kalinya di tahun 1949, saat ini Garuda Indonesia membawa lebih dari 25 juta penumpang setiap tahunnya.

Untuk melindungi data – data perusahaan dibutuhkan sistem keamanan yang mampu mengamankan semua informasi termasuk data-data pegawai, pelanggan, data-data transaksi, pemesanan, dan data-data lainnya yang ada pada perusahaan tersebut. Sistem keamanan yang dipakai Garuda Indonesia adalah ISO 27002.

ISO / IEC 27002 sudah sangat populer dikalangan IT, standar yang diakui secara internasional dari praktek yang baik untuk keamanan informasi. ISO / IEC 27002 jejak sejarahnya kembali lebih dari 30 tahun untuk prekursor dari BS 7799.

1. *Evaluation*
2. *Interpretation*
3. *Summary*

Garuda Indonesia adalah maskapai penerbangan nasional Indonesia yang terbang ke lebih dari 40 tujuan domestik dan 36 tujuan internasional. Garuda Indonesia meraih penghargaan sebagai Maskapai Penerbangan Regional Terbaik di Dunia yang diberikan oleh Skytrax. Terbang untuk pertama kalinya di tahun 1949, saat ini Garuda Indonesia membawa lebih dari 25 juta penumpang setiap tahunnya.

Untuk melindungi data – data perusahaan dibutuhkan sistem keamanan yang mampu mengamankan semua informasi termasuk data-data pegawai, pelanggan, data-data transaksi, pemesanan, dan data-data lainnya yang ada pada perusahaan tersebut. Sistem keamanan yang dipakai Garuda Indonesia adalah ISO 27002.

ISO / IEC 27002 sudah sangat populer dikalangan IT, standar yang diakui secara internasional dari praktek yang baik untuk keamanan informasi. ISO / IEC 27002 jejak sejarahnya kembali lebih dari 30 tahun untuk prekursor dari BS 7799.

Seperti pemerintahan, keamanan informasi adalah topik yang luas dengan konsekuensi di seluruh bagian organisasi modern. Keamanan informasi, dan karenanya ISO / IEC 27002, adalah sangat relevan untuk semua jenis organisasi termasuk perusahaan komersial dari semua ukuran. Risiko keamanan informasi dan kontrol persyaratan tertentu dapat berbeda detail tetapi ada banyak kesamaan, misalnya sebagian besar organisasi harus mengatasi risiko keamanan informasi yang berkaitan dengan karyawan mereka ditambah kontraktor, konsultan dan pemasok eksternal layanan informasi.

ISO / IEC 27002:2005 menetapkan pedoman dan prinsip-prinsip umum untuk memulai, melaksanakan, memelihara, dan meningkatkan manajemen keamanan informasi dalam suatu organisasi. Tujuan diuraikan memberikan panduan umum tentang tujuan umum diterima manajemen keamanan informasi. ISO / IEC 27002:2005 berisi praktik terbaik dari tujuan pengendalian dan kontrol dalam bidang manajemen keamanan informasi.

Tujuan pengendalian dan kontrol dalam ISO / IEC 27002:2005 dimaksudkan untuk diterapkan untuk memenuhi persyaratan diidentifikasi oleh penilaian risiko. ISO / IEC 27002:2005 ini dimaksudkan sebagai dasar umum dan pedoman praktis untuk mengembangkan standar keamanan organisasi dan praktek manajemen keamanan yang efektif, dan untuk membantu membangun kepercayaan dalam kegiatan antar-organisasi. Banyak sistem informasi belum dirancang untuk menjadi aman. Keamanan yang dapat dicapai melalui cara-cara teknis terbatas, dan harus didukung oleh manajemen yang tepat dan prosedur. Mengidentifikasi yang mengontrol harus di tempat membutuhkan perencanaan yang matang dan perhatian terhadap detail. Manajemen keamanan informasi membutuhkan, sebagai minimum, partisipasi seluruh karyawan dalam organisasi. Hal ini juga mungkin memerlukan partisipasi dari pemegang saham, pemasok, pihak ketiga, pelanggan atau pihak eksternal lainnya. Saran spesialis dari organisasi luar mungkin juga diperlukan.