# DAFTAR ISTILAH

| | | |
|---|---|---|
| ISO/IEC 27005:2022 | : | Standar internasional yang memberikan panduan dalam manajemen risiko keamanan informasi, mendukung implementasi ISO/IEC 27001. |
| Diskominfo | : | Dinas Komunikasi dan Informatika; instansi pemerintah daerah yang bertanggung jawab atas pengelolaan teknologi informasi dan komunikasi. |
| CIA (*Confidentiality, Integrity, Availability*) | : | Prinsip dasar keamanan informasi: menjaga kerahasiaan, integritas, dan ketersediaan informasi. |
| *Risk Assessment* | : | Proses sistematis untuk mengidentifikasi, menganalisis, dan mengevaluasi risiko. |
| *Risk Identification* | : | Tahapan dalam manajemen risiko untuk mengidentifikasi aset, ancaman, kerentanan, dan potensi insiden. |
| *Risk Analysis* | : | Proses untuk memahami sifat risiko dan menentukan tingkat risiko berdasarkan kemungkinan dan dampaknya. |
| *Risk Evaluation* | : | Proses membandingkan tingkat risiko dengan kriteria penerimaan risiko untuk menentukan prioritas penanganannya. |
| *Risk Treatment* | : | Proses pemilihan dan implementasi kontrol untuk mengurangi, mengalihkan, menerima, atau menghindari risiko. |
| *Likelihood* | : | Ukuran probabilitas atau frekuensi terjadinya suatu risiko. |
| *Impact* | : | Besarnya konsekuensi atau kerugian yang ditimbulkan oleh risiko terhadap organisasi. |
| *Risk Mitigation* | : | Strategi untuk mengurangi kemungkinan atau dampak dari suatu risiko. |
| *Risk Accept* | : | Keputusan untuk menerima suatu risiko karena berada dalam batas toleransi organisasi. |
| *Risk Avoid* | : | Strategi untuk menghindari aktivitas yang menyebabkan risiko. |
| *Risk Transfer* | : | Strategi untuk mengalihkan risiko kepada pihak ketiga, seperti menggunakan asuransi atau kontrak. |
| Aset Informasi | : | Segala bentuk data, sistem, perangkat, atau layanan yang memiliki nilai bagi organisasi dan perlu dilindungi. |
| Ancaman (*Threat*) | : | Potensi kejadian yang dapat menyebabkan kerusakan terhadap aset informasi, seperti serangan siber, kesalahan manusia, atau bencana alam. |
| Kerentanan (*Vulnerability*) | : | Kelemahan dalam sistem, proses, atau kontrol yang dapat dieksploitasi oleh ancaman. |
| *Residual Risk* | : | Risiko yang tersisa setelah kontrol diterapkan. |
| *Risk Appetite* | : | Tingkat risiko yang dapat diterima oleh organisasi dalam mengejar tujuan bisnisnya. |

| | | |
|---|---|---|
| *Stakeholder* | : | Pihak-pihak yang berkepentingan dan terlibat dalam proses manajemen risiko, baik internal maupun eksternal. |
| Divisi XYZ | : | Divisi fiktif dalam Diskominfo Provinsi Jawa Barat yang menjadi fokus penelitian untuk analisis risiko keamanan informasi. |
| *Risk Register* | : | Dokumen yang memuat daftar risiko yang telah diidentifikasi, termasuk deskripsi, tingkat risiko, dan perlakuannya. |