Definisi Risiko

***Risk Management**

-Manajemen risiko adalah suatu proses yang berarti perlindungan dan kontrol yang dirancang dan diimplementasikan.

-Manajemen risiko adalah proses menemukan dan menilai risiko terhadap operasi organisasi dan menentukan bagaimana risiko tersebut dapat dikendalikan atau dikurangi.

Analisis risiko adalah identifikasi dan penilaian tingkat risiko dalam organisasi.

***Risk Identification**

Risiko dimulai dengan proses pemeriksaan diri.

Pada tahap ini, manajer mengidentifikasi aset informasi organisasi, mengelompokkan dan mengkategorikan mereka ke dalam kelompok yang berguna, dan memprioritaskan mereka dengan kepentingan mereka secara keseluruhan.

***Risk Assessment**

Menilai risiko relatif untuk setiap kerentanan dicapai melalui proses yang disebut penilaian risiko.

Penilaian risiko menetapkan peringkat risiko atau skor untuk setiap kerentanan tertentu.

IIS dan Perekrutan Karyawan

Information Security Professional Credentials

*$(ISC)^2$ Certifications
*ISACA Certifications
*Global Information Assurance Certification (GIAC)
*Security Certified Program (SCP)
*Security+
*Certified Computer Examiner (CCE)

Employment Policies and Practices

*Hiring
*Contracts and Employment
*Security as Part of Performance Evaluation
*Termination Issues
*Personnel Security Practices
*Security of Personnel and Personal Data
*Security Considerations for Nonemployees

Firewall

Perangkat yang mencegah jenis informasi tertentu yang bergerak antara dunia luar, yang dikenal sebagai jaringan tidak dipercaya (misalnya, internet) dan dunia dalam, yang dikenal sebagai jaringan terpercaya.

Firewall mungkin sistem komputer yang terpisah, layanan yang berjalan pada router atau server yang ada, atau jaringan terpisah yang berisi sejumlah perangkat pendukung.

Best Security Practice

Upaya keamanan yang menyeimbangkan kebutuhan untuk akses informasi dengan kebutuhan untuk perlindungan yang memadai sekaligus menunjukkan tanggung jawab fiskal.

Risiko dan strategi kontrol waktu

Ketika tim manajemen umum organisasi menentukan bahwa risiko dari ancaman keamanan informasi menciptakan kerugian kompetitif, memberdayakan teknologi informasi dan komunitas keamanan informasi yang menarik untuk mengendalikan risiko tersebut.

Tim harus memilih salah satu dari empat strategi dasar untuk mengendalikan risiko yang timbul dari kerentanan ini.

Avoidance: Menerapkan perlindungan yang menghilangkan atau mengurangi risiko yang tidak terkendali yang tersisa

Transference: Pergeseran risiko ke daerah lain atau entitas luar

Mitigation: Mengurangi dampak harus penyerang berhasil mengeksploitasi kerentanan

Acceptance: Memahami dan mengakui konsekuensi risiko tanpa ada kontrol atau upaya mitigasi

Plan	Description	Example	When deployed	Timeframe
Incident Response (IR) Plan	Actions an organization takes during incidents (attacks)	• List of steps to be taken during disaster • Intelligence gathering • Information analysis	As incident or disaster unfolds	Immediate and real-time reaction
Disaster Recovery (DR) Plan	• Preparations for recovery should a disaster occur • Strategies to limit losses before and during disaster • Step-by-step instructions to regain normalcy	• Procedures for the recovery of lost data • Procedures for the reestablishment of lost services • Shutdown procedures to protect systems and data	Immediately after the incident is labeled a disaster	Short-term recovery
Business Continuity (BC) Plan	Steps to ensure continuation of the overall business when the scale of a disaster exceeds the DRP's ability to quickly restore operations	• Preparation steps for activation of secondary data centers • Establishment of a hot site in a remote location	Immediately after the disaster is determined to affect the continued operations of the organization	Long-term organization

Kalkulasi CBA (Cost Benefit Analysis)

*Kriteria yang paling umum digunakan ketika mengevaluasi sebuah proyek yang mengimplementasikan kontrol keamanan informasi dan perlindungan adalah kelayakan ekonomi.

*Akal sehat menyatakan bahwa organisasi tidak harus menghabiskan lebih banyak untuk melindungi aset yang bernilai. Proses pengambilan keputusan disebut analisis biaya-manfaat (CBA) atau studi kelayakan ekonomi.

*Biaya, item yang mempengaruhi biaya kontrol atau menjaga: biaya pengembangan, biaya pelatihan, biaya pelaksanaan, biaya jasa, const pemeliharaan.

*Manfaat adalah nilai organisasi menggunakan kontrol untuk mencegah kerugian yang terkait dengan kerentanan tertentu.

*Penilaian aset adalah proses yang memberikan nilai keuangan atau layak untuk setiap aset informasi.