YAYASAN PERGURUAN CIKINI
INSTITUT SAINS DAN TEKNOLOGI NASIONAL
FAKULTAS SAINS DAN TEKNOLOGI INFORMASI

Jl. Moh. Kahfi II, Bhumi Srengseng Indah, Jagakarsa, Jakarta Selatan 12640
Telp. 021-7270090 (hunting), Fax. 021-7866955, hp: 081291030024
Email: fsti@istn.ac.id Website: www.istn.ac.id

SURAT PENUGASAN TENAGA PENDIDIK

Nomor : 204 / 03.1 – I / IX / 2022

SEMESTER *GANJIL*, TAHUN AKADEMIK 2022 / 2023

Nama	: Aryo Nur Utomo, ST.,M.Kom.	Status Pegawai	:	Edukatif Tetap	
NIK	: 01.121225	Program Studi	:	Sistem Informasi	
Jabatan Akademik	: Asiste Ahli				

Bidang	Perincian Kegiatan	Ruang/ Tempat	Jam/ Minggu	Kredit (sks)	Hari / Waktu
I PENDIDIKAN Dan PENGAJARAN	**MENGAJAR DI KELAS (KULIAH / RESPONSI DAN LABORATORIUM)**				
	1. Cloud Computing (SI)	A-1	1 Jam/Minggu	1	Senin / 08:00-09:40
	2. Sistem Pendukung Keputusan (SI)	D-2	1,5 Jam/Minggu	1,5	Selasa / 08:00-10:00
	3. Sistem Temu Kembali Informasi(SI)	E-4	1 Jam/Minggu		Senin /15:30-17:00
	4. IT Service Management (SI)	D-3	1 Jam/Minggu	1	Jum'at / 14:30-16:00
	5. Keamanan Sistem Informasi (SI)	E-1	1 Jam/Minggu	1	Rabu / 15:30-17:00
	6. Algoritma dan Pemrograman (TIF)	A-2	1 Jam/Minggu	1	Kamis / 08:00-09:40
	7. Analisis dan Perancangan Algoritma (TIF)	A-1	1 Jam/Minggu	1	Senin / 10.30-12.10
	8. Pemrograman Jaringan (Java/Python)	D-2	1,5 Jam/Minggu	1,5	Selasa / 14.41-15.40
	9. Pembelajaran Mesin (TIF)	E-1	1,5 Jam/Minggu	1,5	Rabu / 13.00-14.40
	10. Komputer Forensik (TIF)	A-2	1,5 Jam/Minggu	1,5	Jumat / 12.30-14.00
	11. Pengelolaan Layanan TI (ITSM) (TIF)	A-1	1 Jam/Minggu	1	Senin / 08.00-09.40
	12. Data Compress & Coding (PIGS)	A-2	1 Jam/Minggu		Selasa / 08.00-09.40
	13. Manajemen Proyek Perangkat Lunak	A-3	1,5 Jam/Minggu		Kamis / 10.00-11.30
	14. Menduduki Jabatan Struktural (Ka.Prodi TIF)		20 Jam/Minggu	3	
II PENELITIAN	Penulisan Karya Ilmiah			1	
III PENGABDIAN DAN MASYARAKAT	Pelatihan dan Penyuluhan				
IV UNSUR-UNSUR PENUNJANG	Berperan Serta Aktif dalam Pertemuan IlmiahSeminar				
	Jumlah Total			16	

Kepada yang bersangkutan akan diberikan gaji / honorarium sesuai dengan peraturan penggajian yang berlaku di Institut Sains Dan Teknologi Nasional
Penugasan ini berlaku dari tanggal 02 September 2022 sampai dengan tanggal 29 Februari 2023.

Jakarta, 30 September 2022
Dekan,

(Marhaeni, S.Kom.,M.Kom.)

Tembusan :
1. Direktur Akademik – ISTN
2. Direktur Non Akademik – ISTN
3. Ka. Biro Sumber Daya Manusia – ISTN
4. Kepala Program Studi Sistem Informasi
5. Arsip.

DAFTAR HADIR PESERTA KULIAH MAHASISWA

GANJIL REGULER TAHUN 2022/2023

FAK / JURUSAN : Sistem Informasi S1 HARI/TANGGAL : Rabu

MATA KULIAH : Keamanan Sistem Informasi

KELAS /PESERTA : A / 5 JAM KULIAH : 15.30-17.00

KURIKULUM : 2018

DOSEN : Aryo Nur Utomo, ST.M.Kom. RUANG :

NO	NIM	NAMA MAHASISWA	TANGGAL PERTEMUAN								JUMLAH
			23/ 11	30/ 11	07/ 12	14/ 12	21/ 12	28/ 12	04/ 01	18/ 01	
1	16350012	Adityarachman Aziz Pradana	√	√	√	√	√	√	√	U	7
2	20350003	Anisa Qadri Kurniasih	√	√	√	√	√	√	√	U	7
3	20350004	Rizky Fauzi Ramadhan	√	√	√	√	√	√	√	U	7
4	20350006	Miftah Zaidan Falih	√	√	√	√	√	√	√	U	7
5	20350008	Muhammad Ibnu Afan Fuadi	√	√	√	√	√	√	√	U	7

Jakarta , ... Februari 2023

Dosen Pengajar

(Aryo Nur Utomo, S.T., M.Kom.)

BERITA ACARA PERKULIAHAN
(PRESENTASI KEHADIRAN DOSEN)
SEMESETER GANJIL TAHUN AKADEMIK 2022/2023
PROGRAM STUDI SISTEM INFORMASI S1 FSTI-ISTN

Mata Kuliah	:	Keamanan Sistem Informasi	Semester	:	355009
Dosen	:	Aryo Nur Utomo, ST, M.Kom	SKS	:	2
Hari	:	Rabu	Kelas	:	A
Jam	:	15:30-17:00	Ruang	:	B-2

No.	TANGGAL	MATERI KULIAH	JML MHS HADIR	TANDA TANGAN DOSEN
9.	23-November 2022	Risk Management #1 in Information Security.	5	
10.	30-November 2022	Risk Management #2 in Information Security.	5	
11.	7-Desember 2022	Planning to build Information Security system di sebuah organisasi.	5	
12.	14-Desember 2022	Security Technology.	5	
13.	21-Desember 2022	Physical Security.	5	
14.	28-Desember 2022	Implementing Security.	5	
15.	4-Januari 2023	Security IT & Attack.	5	
16.	18-Januari 2023	**UJIAN AKHIR SEMESTER (UAS)**	5	

DOSEN PENGAJAR

(Aryo Nur Utomo, ST. M.Kom)

DAFTAR NILAI

SEMESTER GANJIL REGULER TAHUN 2022/2023

Program Studi : Sistem Informasi S1
Matakuliah : Keamanan Sistem Informasi
Kelas / Peserta : A
Perkuliahan : Kampus ISTN Bumi Srengseng Indah
Dosen : B. Sumardiyono, ST, M.Kom.

No	NIM	N A M A	ABSEN	TUGAS	UTS	UAS	MODEL	PRESENTASI	NA	HURUF
			10%	30%	30%	30%	0%	0%		
1	16350012	**Adityarachman Aziz Pradana**	100	75	70	73	0	0	75.4	**A-**
2	20350003	**Anisa Qadri Kurniasih**	100	75	70	70	0	0	74.5	**B+**
3	20350004	**Rizky Fauzi Ramadhan**	100	75	70	67	0	0	73.6	**B+**
4	20350006	**Miftah Zaidan Falih**	100	75	70	74	0	0	75.7	**A-**
5	20350008	**Muhammad Ibnu Afan Fuadi**	100	75	70	70	0	0	74.5	**B+**

Rekapitulasi Nilai							
A	0	B+	3	C+	0	D+	0
A-	2	B	0	C	0	D	0
		B-	0	C-	0	E	0

Jakarta,20 February 2023

Dosen Pengajar

B. Sumardiyono, ST, M.Kom.

Information Security

4. Risk Management: Identifying and Assessing Risk

Oleh :

Ir. Aryo Nur Utomo, MKom

Tujuan instruksional

Setelah mengikuti bab ini, anda memiliki kemampuan berikut:

- Menentukan manajemen risiko dan perannya dalam SecSDLC tersebut.
- Memahami bagaimana risiko diidentifikasi.
- Menilai risiko berdasarkan kemungkinan terjadinya dan dampaknya terhadap organisasi.
- Pegangan untuk aspek dasar dari mendokumentasikan identifikasi risiko dan penilaian.

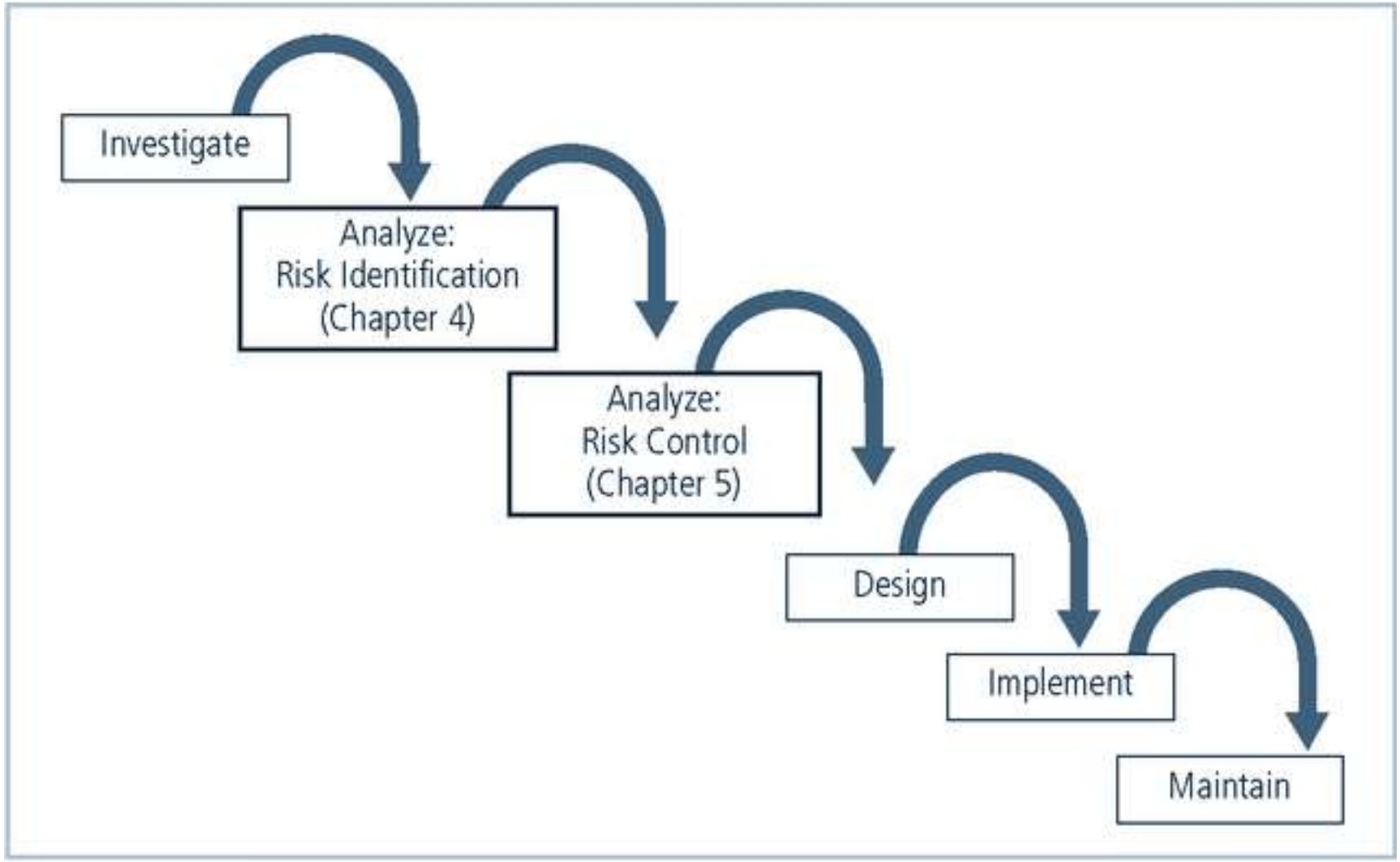

FIGURE 4-1 Risk Management and the SecSDLC

Manajemen Risiko

- “Jika Anda mengenal musuh dan mengenal diri sendiri, Anda tidak perlu takut hasil dari ratusan pertempuran.
- Jika Anda mengenal diri sendiri, tapi bukan musuh, untuk setiap kemenangan yang diperoleh, Anda juga akan menderita kekalahan.
- Jika Anda tidak tahu akan musuh maupun diri sendiri, Anda akan menyerah dalam setiap pertempuran.”

  (Sun Tzu)

Kenali Diri Sendiri

- Pertama, kita harus mengidentifikasi, menguji, dan memahami informasi, dan sistem yang saat ini terpasang.
- Dalam rangka untuk melindungi aset kita, didefinisikan di sini sebagai informasi dan sistem yang menggunakan, menyimpan, dan mengirimkan informasi tsb, intinya kita harus memahami segala sesuatu tentang informasi.
- Setelah kita telah meneliti aspek-aspek, kita kemudian dapat mengkaji apa yang sudah kita lakukan untuk melindungi informasi dan sistem dari ancaman.

Kenali Diri Musuh

- Kaitan kpd keamanan informasi ini berarti mengidentifikasi, memeriksa, dan memahami ancaman yang paling langsung mempengaruhi organisasi dan keamanan aset informasi organisasi kita.
- Kita kemudian dapat menggunakan pemahaman/informasi yang kita dapat tentang aspek-aspek tsb untuk membuat daftar prioritas ancaman menurut kepentingan organisasi.

Akuntabilitas Manajemen Risiko

- Ini adalah tanggung jawab dari masing-masing komunitas yang berkepentingan untuk mengelola risiko; setiap masyarakat memiliki peran untuk memainkan:
  - Keamanan Informasi – yang terbaik memahami ancaman[2] dan serangan[2] yang menyebabkan risiko kepada organisasi.
  - Manajemen dan Pengguna - berperan dalam deteksi dini dan memproses respon - mereka juga memastikan pengalokasian sumber daya yang cukup.
  - Teknologi Informasi - harus membantu dalam membangun sistem yang *secure* dan operasional mereka aman.

Akuntabilitas Manajemen Risiko

- Ketiga komunitas (Keamanan Informasi, Manajemen & Pengguna, Teknologi Informasi) juga harus:
  - Mengevaluasi pengendalian risiko.
  - Menentukan pilihan-pilihan pengendalian mana yang berbiaya efektif.
  - Membantu dalam mendapatkan atau memasang pengendalian yang diperlukan.
  - Pastikan bahwa pengendalian tetap efektif.

Proses Manajemen Risiko

- Manajemen menginventarisasi aset.
- Ancaman[2] dan kerentanan[2] berbahaya yang berhasil diidentifikasi dari inventarisasi aset harus ditinjau dan diverifikasi secara lengkap dan terkini.
- Potensi kendali dan strategi mitigasi harus ditinjau untuk melengkapinya.
- Efektivitas biaya setiap pengendalian harus ditinjau juga, dan keputusan tentang pemakaian kendali ditinjau pula.
- Selanjutnya, manajer dari semua tingkatan bertanggung jawab pada jadwal yang dibuat untuk memastikan efektivitas setiap pengendalian yang sedang berlangsung dapat dijalankan.

Identifikasi Risiko

- Sebuah strategi manajemen risiko menyebut untuk “mengenali diri sendiri” dengan mengidentifikasi, mengklasifikasi, dan memprioritaskan aset[2] informasi dari organisasi.
- Aset tsb adalah target dari berbagai ancaman dan agen ancaman dan tujuan kita adalah untuk melindungi mereka dari ancaman.
- Selanjutnya mengidentifikasi ancaman:
  - Menilai keadaan dan men-*setting* setiap aset informasi.
  - Identifikasi kerentanan dan mulai mencari kontrol yang dapat digunakan untuk mengelola risiko.

Identifikasi Aset dan Penaksiran Nilai

- Ini proses berulang-ulang dimulai dengan identifikasi aset, termasuk semua unsur-unsur sistem organisasi: orang, prosedur, data dan informasi, perangkat lunak, perangkat keras, dan elemen jaringan.
- Kemudian, kita mengelompokkan dan mengkategorikan aset, menambahkan detail[2] sejalan ketika kita menggali lebih dalam saat analisis.

TABLE 4-1 Categorizing the Components of an Information System

Traditional system components	SecSDLC and risk management system components	
People	Employees	Trusted employees Other staff
	Nonemployees	People at trusted organizations Strangers
Procedures	Procedures	IT and business standard procedures IT and business sensitive procedures
Data	Information	Transmission Processing Storage
Software	Software	Applications Operating systems Security components
Hardware	System devices and peripherals	Systems and peripherals Security devices
	Networking components	Intranet components Internet or DMZ components

Identifikasi Aset Hardware, Software dan Network

- Dengan *tools* otomatis kadang-kadang dapat mengungkap unsur-unsur sistem yang membentuk perangkat keras, perangkat lunak, dan komponen jaringan.
- Setelah dibuat, daftar inventaris harus disimpan saat ini, seringkali melalui alat yang secara berkala me-*refresh* data.

  Bisa menggunakan *network/asset management tool*

Identifikasi Aset Hardware, Software dan Network

- Atribut apa dari setiap aset informasi harus dilacak?
- Ketika memutuskan mana aset informasi untuk dilacak, pertimbangkan memasukkan atribut aset:
  - Name
  - IP address
  - MAC address
  - Tipe elemen
  - Serial number
  - Nama pabrikan
  - Manufacturer's model number or part number
  - Software version, update revision, or FCO (First Class Object) number
  - Lokasi fisik
  - Lokasi logik
  - Entiti yg mengendalikan

Identifikasi Aset People, Procedures, dan Data

- Berbeda dengan hardware dan elemen software yang bersifat *tangible* yang sudah dijelaskan, maka sumber daya manusia, dokumentasi (prosedur), dan aset data informasi tidak mudah ditemukan dan didokumentasikan.
- Aset ini harus diidentifikasi, dijelaskan, dan dievaluasi oleh orang menggunakan pengetahuan, pengalaman, dan penghakiman (menilai baik & buruk).
- Sejalan ketika elemen ini diidentifikasi, mereka juga harus dicatat ke dalam beberapa proses penanganan data yang dapat diandalkan (mis, database).

Informasi untuk aset Orang

- Untuk Orang:
  - Nama posisi/nomor/id - coba untuk hindari nama[2] sebutan untuk mengidentifikasi posisi, peran, atau fungsi (mis, Divisi Audit Internal mungkin diberi sebutan Divisi-13 untuk menunjukkan ke-angkerannya).
  - Supervisor
  - Tingkat pengetahuan sekuriti
  - Keahlian khusus

Informasi untuk aset Prosedur

- Untuk Prosedur:
  - Deskripsi
  - Tujuan dibuat
  - Elemen[2] apa yang terkait dengan itu
  - Dimana ia disimpan untuk referensi
  - Dimana ia disimpan untuk tujuan update

Informasi untuk aset Data

- Untuk Data:
  - Klasifikasi
  - Pemilik / Pembuat / Manager
  - Ukuran struktur data
  - Struktur data yang digunakan – sekuensial, relasional
  - Online atau offline
  - Dimana lokasinya
  - Prosedur backup yang digunakan

Klasifikasi Aset Informasi

- Kebanyakan organisasi telah memiliki skema klasifikasi untuk aset[2]nya.
- Contoh dari klasifikasi itu adalah:
  - Data rahasia *(confidential data)*
  - Data internal (*internal data*)
  - Data publik (*public data*)
- Organisasi informal mungkin harus mengorganisir diri untuk membuat model klasifikasi data bisa yang digunakan.
- Sisi lain dari skema klasifikasi data adalah struktur izin keamanan bagi personel.

Penilaian Aset Informasi

- Setiap aset dikategorisasi.
- Pertanyaan[2] yang membantu dalam membuat kriteria yang digunakan untuk penilaian aset:
  - Aset informasi mana yang paling kritis agar organisasi berjalan sukses?
  - Aset informasi mana yang menghasilkan penghasilan (uang) paling besar?
  - Aset informasi mana yang menghasilkan keuntungan (uang, image, kepercayaan, dll) paling besar?
  - Aset informasi mana yang akan memakan biaya paling besar untuk menggantinya.
  - aset informasi mana yang akan memakan biaya paling besar untuk memproteksinya?
  - Aset informasi mana yang akan menjadi paling memalukan atau menyebabkan kewajiban (membayar kompensasi) terbesar jika terungkap?

System Name: SLS E-Commerce
Date Evaluated: February 2003
Evaluated By: D. Jones

Information assets	Data classification	Impact to profitability
Information Transmitted:		
EDI Document Set 1 —Logistics BOL to outsourcer (outbound)	Confidential	High
EDI Document Set 2—Supplier orders (Outbound)	Confidential	High
EDI Document Set 2—Supplier fulfillment advice (inbound)	Confidential	Medium
Customer order via SSL (inbound)	Confidential	Critical
Customer service Request via e-mail (inbound)	Private	Medium
DMZ Assets:		
Edge Router	Public	Critical
Web server #1—home page and core site	Public	Critical
Web server #2—Application server	Private	Critical

Notes: BOL: Bill of Lading:
DMZ: Demilitarized Zone
EDI: Electronic Data Interchange
SSL: Secure Sockets Layer

FIGURE 4-3 Example Worksheet for the Asset Identification of Information Systems

Penilaian Aset Informasi

- Buat bobot untuk setiap kategori didasarkan pada jawaban[2] pertanyaan diatas.

  Faktor mana yang paling penting bagi organisasi?

  (faktor paling penting punya bobot paling besar, dst)

- Setelah setiap pertanyaan dibobot, kemudian hitung (beri nilai) setiap aset menurut kepentingan.

- List aset[2] menurut kepentingan menggunakan lembar kerja analisis faktor tertimbang. (hasil ini akan terurut berdasar nilai akhir tertimbang untuk dianalisis).

TABLE 4-2 Example of a Weighted Factor Analysis Worksheet

Information asset	Criteria 1: impact to revenue	Criteria 2: impact to profitability	Criteria 3: public image impact	Weighted score
Criterion Weight (1-100) Must total 100	30	40	30	
EDI Document Set 1—Logistics BOL to outsourcer (outbound)	0.8 30x0,8= 24	0.9 40x0,9= 36	0.5 30x0,5=1 5	75 = 24+36+15
EDI Document Set 2—Supplier orders (outbound)	0.8	0.9	0.6	78
EDI Document Set 2—Supplier fulfillment advice (inbound)	0.4	0.5	0.3	41
Customer order via SSL (inbound)	1.0	1.0	1.0	100
Customer service request via e-mail (inbound)	0.4	0.4	0.9	55

Notes: EDI: Electronic Data Interchange
SSL: Secure Sockets Layer

Klasifikasi Data & Pengelolaan

- Berbagai skema klasifikasi digunakan oleh organisasi perusahaan dan militer.
- Pemilik informasi bertanggungjawab untuk mengklasifikasi aset informasi yang menjadi tanggungjawabnya.
- Pemilik informasi harus meninjau klasifikasi informasi secara berkala.
- Militer menggunakan lima-level skema klasifikasi tetapi kebanyakan organisasi tidak memerlukan level detail klasifikasi seperti yang digunakan oleh militer atau badan negara (federal).

Contoh:
skema militer = Unclassified, Sensitive But Unclassified (i.e., For Official Use Only), Confidential, Secret, and Top Secret.
skema organisasi = Public, For official use only, Sensitive, Classified.

Security Clearances

- Sisi lain dari skema klasifikasi data adalah struktur izin keamanan personil.
- Setiap data user dalam organisasi dikenakan level otorisasi tunggal yang menandakan level klasifikasi.
- Sebelum seseorang diijinkan akses ke set data tertentu, ia harus mengetahui dan memenuhi persyaratan.
- Level proteksi ekstra ini menjamin informasi yang rahasia (*confidentiality*) benar-benar terjaga.

Pengelolaan Klasifikasi Data

- Termasuk penyimpan, distribusi, pemindahan, dan penghancuran dari informasi berklasifikasi.
  - Harus secara jelas ditandai.
  - Ketika disimpan, ia harus tidak tersedia untuk orang yang tidak berotorisasi.
  - Ketika dipindahkan harus tidak menyolok (tersembunyi), seperti ditaruh didalam koper atau map yang aman.
- Kebijakan meja bersih mensyaratkan semua informasi disimpan didalam tempat penyimpannya setiap akhir hari.
- Perawatan yang tepat harus diambil untuk menghancurkan setiap salinan yang tidak dibutuhkan lagi.
- Pencuri informasi yang mengais di tempat sampah dapat membuktikan bahwa organisasi tidak profesional (memalukan).

Identifikasi Ancaman

- Setiap ancaman diidentifikasi sejauh memiliki potensi untuk menyerang salah satu aset yang dilindungi.
- Hal ini dengan cepat akan menjadi lebih kompleks dan menambah beban/kesulitan untuk perencanaannya.
- Untuk membuat bagian ini menjadi proses yang terkendali, setiap langkah dalam identifikasi ancaman dan proses identifikasi kerentanan dikelola secara terpisah, dan kemudian dikoordinasikan pada akhir proses.

TABLE 4-3 Threats to Information Security

Threat	Example
Act of human error or failure	Accidents, employee mistakes
Compromises to intellectual property	Piracy, copyright infringement
Deliberate acts of espionage or trespass	Unauthorized access and data collection
Deliberate acts of information extortion	Blackmail for information disclosure
Deliberate acts of sabotage or vandalism	Destruction of systems or information
Deliberate acts of theft	Illegal confiscation of equipment or information
Deliberate software attacks	Viruses, worms, macros, denial of service
Forces of nature	Fire, flood, earthquake, lightning
Quality of service deviations from service providers	Power and WAN quality of service issues
Technical hardware failures or errors	Equipment failure
Technical software failures or errors	Bugs, code problems, unknown loopholes
Technological obsolescence	Antiquated or outdated technologies

Mengidentifikasi dan Memprioritaskan Ancaman

- Setiap ancaman harus diperiksa lebih lanjut untuk menilai potensi dampak nya ke organisasi - ini disebut sebagai penilaian ancaman.
- Untuk membingkai diskusi dari penilaian ancaman, korelasikan setiap ancaman dengan beberapa pertanyaan berikut:
  - Ancaman mana yang jika hadir akan membahayakan kepada aset[2] organisasi dalam lingkungan tertentu?
  - Ancaman mana yang mewakili situasi paling berbahaya ke informasi dari organisasi?
  - Berapa biaya yang harus dikeluarkan untuk memulihkan saat sebuah serangan berhasil?
  - Manakah dari ancaman[2] tersebut yang akan membutuhkan pengeluaran terbesar untuk mencegah?

Identifikasi Kerentanan

- Kami sekarang menghadapi tantangan meninjau masing-masing aset informasi untuk setiap ancaman yang dihadapinya dan membuat daftar dari kerentanan yang tetap berisiko untuk organisasi.
- Kerentanan adalah jalan khusus yang mana agen^2 ancaman dapat memanfaatkannya untuk menyerang aset informasi.

TABLE 4-4 Vulnerability assessment of a hypothetical DMZ router

Threat	Possible vulnerabilities
Deliberate software attacks	▪ Internet protocol is vulnerable to denial of service ▪ Outsider IP fingerprinting activities can reveal sensitive information unless suitable controls are implemented
Act of human error or failure	▪ Employees or contractors may cause outage if configuration errors are made
Technical software failures or errors	▪ Vendor-supplied routing software could fail and cause an outage
Technical hardware failures or errors	▪ Hardware can fail and cause an outage ▪ Power system failures are always possible
Quality of service deviations from service providers	▪ Unless suitable electrical power conditioning is provided, failure is probable over time
Deliberate acts of espionage or trespass	▪ This information asset has little intrinsic value, but other assets protected by this device could be attacked if it compromised
Deliberate theft	▪ This information asset has little intrinsic value, but other assets protected by this device could be attacked if it is compromised
Deliberate acts of sabotage or vandalism	▪ Internet protocol is vulnerable to denial of service ▪ This devise may be subject to defacement or cache poisoning
Technological obsolescence	▪ If this asset is not reviewed and periodically updated, it may fall too far behind its vendor support model to be kept in service
Forces of nature	▪ All information assets in the organization are subject to forces of nature, unless suitable controls are provided
Compromises to intellectual property	▪ This information asset has little intrinsic value, but other assets protected by this device could be attacked if it is compromised
Deliberate acts of information extortion	▪ This information asset has little intrinsic value, but other assets protected by this device could be attacked if it is compromised

Identifikasi Kerentanan

- Periksa bagaimana setiap ancaman yang mungkin atau yang mungkin bisa dilakukan dan daftarkan aset organisasi dan kerentanannya.
- Proses bekerja baik ketika kelompok orang dengan berbagai latar belakang dalam organisasi bekerja iteratif dalam serangkaian sesi brainstorming.
- Pada akhir dari proses, sebuah informasi aset / daftar kerentanan harus dihasilkan
  - Daftar ini adalah titik mula untuk langkah selanjutnya, yaitu penilaian risiko.

Penilaian Risiko

- Kita dapat menentukan risiko relatif untuk setiap kerentanan melalui sebuah proses yang disebut penilaian risiko.
- Penilaian risiko memberikan peringkat risiko atau skor untuk setiap aset informasi spesifik, berguna dalam mengukur risiko relatif terhadap masing-masing aset informasi yang mungkin rentan dan nantinya membuat peringkat komparatif dalam proses pengendalian risiko.

Pengantar Penilaian Risiko

- Perkiraan Identifikasi Faktor Risiko
  - Kemungkinan, kemungkinan potensi kerentanan dimanfaatkan (skala 0.1 s/d 1.0).
  - Nilai aset[2] informasi, (skala 1 s/d 100, dgn 100 adalah aset yg paling utk misi kritis).
  - Prosentase risiko dimitigasi (diatasi), estimasi prosentase kerentanan dapat dikontrol.
  - Ketidakpastian, tdk mungkin mengetahui semuanya dari setiap kerentanan, kapan kejadiannya, seberapa besar dampaknya. Tetapkan sebuah faktor kedalam persamaan untuk menentukan estimasi sebagai informasi ketidakpastian (faktor asumsi).

Penentuan Risiko

Untuk tujuan penilaian risiko relatif :

risiko =

kemungkinan terjadinya kerentanan

kali

nilai (atau dampak)

minus

prosentase risiko yang sudah bisa dikendalikan

plus

sebuah elemen/faktor ketidakpastian

Identifikasi Kemungkinan Pengendalian

- Untuk setiap ancaman dan kerentanannya yang terkait yang memiliki risiko residual (sisa), buat daftar awal dari ide[2] pengendaliannya.
- Residual risk adalah risiko yang tetap ada pada aset informasi bahkan setelah kontrol yang direncanakan telah diterapkan.

Kontrol Akses

- Salah satu aplikasi dari kontrol berada di area kontrol akses.
- Kontrol akses adalah semua kontrol yang secara khusus mencatat/mendaftar tempat[2] yg dikunjungi dari seorang user kedalam sebuah area terotorisasi dari organisasi.
- Ada beberapa pendekatan untuk mengendalikan akses.
- Kontrol akses dapat berupa
  - Diskresioner (kebebasan menentukan kebijakan)
  - Mandatory
  - nonDiskresioner

Jenis-jenis dari Kontrol Akses

- Discretionary Access Controls (DAC) adalah diimplementasikan pada kebijaksanaan (diskresi) atau pilihan pengguna data.
- Mandatory Access Controls (MACs) adalah disusun dan dikoordinasikan dengan skema klasifikasi data, dan diperlukan.
- Nondiscretionary Controls adalah mereka ditentukan oleh otoritas sentral dalam organisasi dan dapat didasarkan pada peran individu (Peran Berbasis Kontrol) atau set tertentu dari tugas atau tugas individu yg diberikan (Task-Based Controls) atau dapat didasarkan pada daftar tertentu dipeliharakan pada subyek atau obyek.

Lattice-based Control (Kontrol berdasar-kisi)

- Tipe lain dari akses nondiscretionary adalah kontrol berbasis-kisi, di mana struktur kisi (atau matriks) dibuat mengandung subjek dan objek, dan batas-batas yang berhubungan dengan masing-masing pasangan yang dikandung.
- Ini menentukan level akses setiap subjek harus setiap objek.
- Dalam kontrol berbasis-kisi, kolom atribut[2] yang berhubungan dengan objek tertentu adalah disebut sebagai daftar kontrol akses atau ACL.
- Baris dari atribut[2] yang berhubungan dengan subjek tertentu (seperti pengguna) adalah disebut sebagai tabel kemampuan.

Mendokumentasikan Hasil Penilaian Risiko

- Tujuan dari proses ini adalah untuk mengidentifikasi aset informasi dari organisasi yang memiliki kerentanan tertentu dan membuat daftar nya, diperingkat untuk fokus pada mereka yang membutuhkan perlindungan yang paling pertama.
- Dalam mempersiapkan daftar ini kita lakukan dgn mengumpulkan dan memperbaharui informasi faktual mengenai aset, ancaman yang mereka hadapi, dan kerentanan mereka alami.
- Kita juga harus mengumpulkan beberapa informasi mengenai kontrol yang sudah di implementasi.

Pengantar Penilaian Risiko

- Proses yang telah anda kembangkan untuk identifikasi risiko harus mencakup untuk tujuan apa laporan dibuat, siapa yang bertanggung jawab untuk mempersiapkan laporan, dan yang meninjau mereka.
- Nantinya bahwa worksheet kerentanan peringkat risiko adalah dokumen kerja awal untuk langkah berikutnya dalam proses manajemen risiko: menilai dan mengendalikan risiko.

TABLE 4-6 Risk Identification and Assessment Deliverables

Deliverable	Purpose
Information asset classification worksheet	Assembles information about information assets and their impact on or value to the organization
Weighted criteria analysis worksheet	Assigns ranked value or impact weight to each information asset
Ranked vulnerability risk worksheet	Assigns ranked value of risk rating for each uncontrolled asset-vulnerability pair

Terimakasih