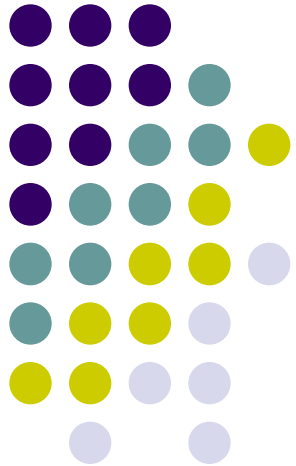
ISO 27001:2005 Information Security Management Systems

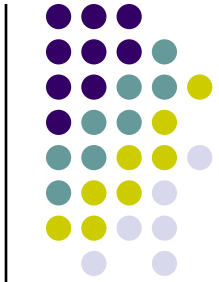
Arrianto Mukti Wibowo, M.Sc., CISA
amwibowo@cs.ui.ac.id



Additional topic:

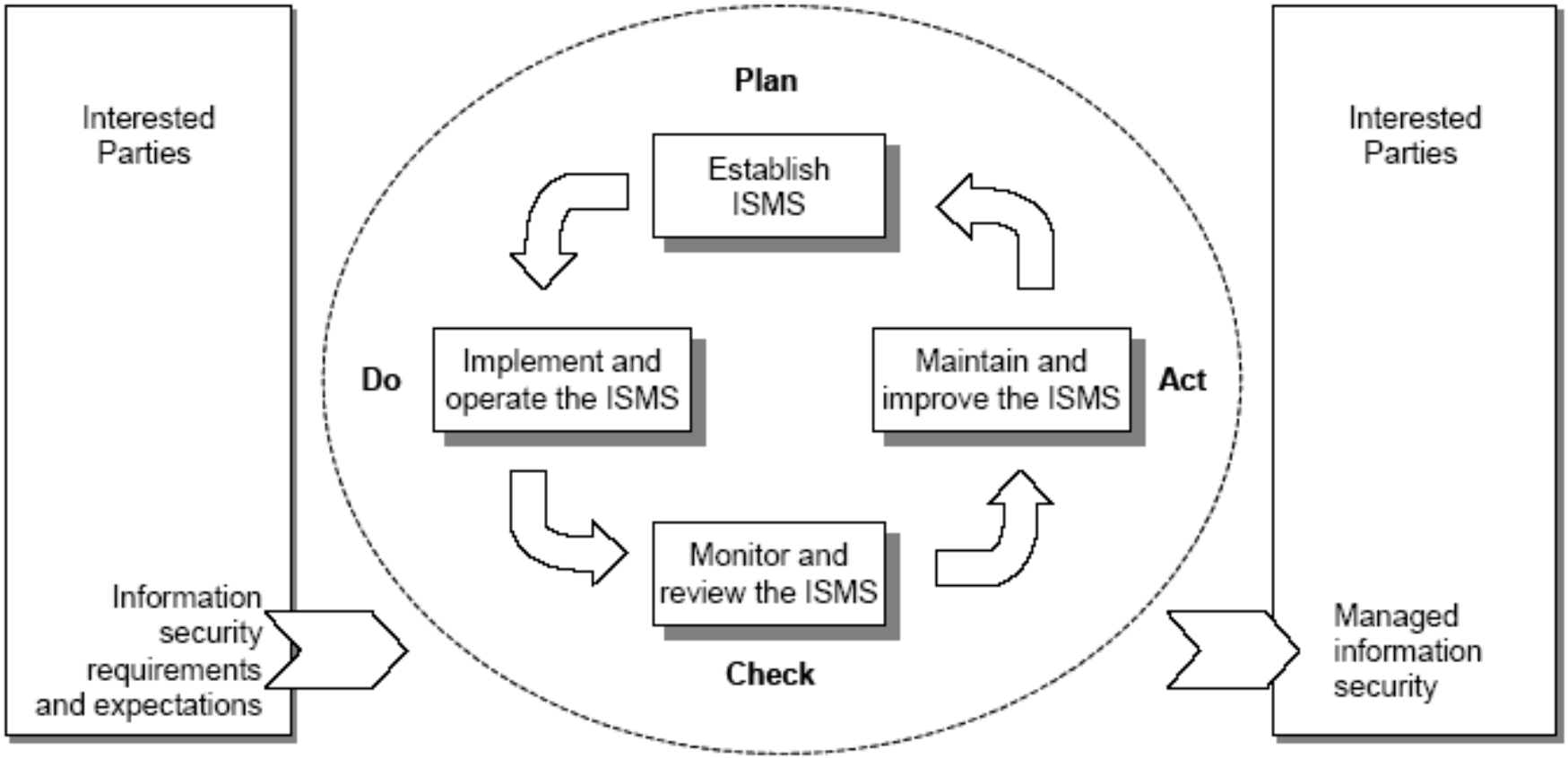
AS-NZ 4360:2004 Risk Management Standard

Pendekatan ISO 27001

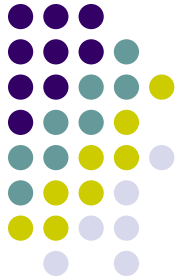


- understanding an organization’s information security requirements and the need to establish policy and objectives for information security;
- implementing and operating controls to manage an organization's information security risks in the context of the organization’s overall business risks;
- monitoring and reviewing the performance and effectiveness of the ISMS; and
- continual improvement based on objective measurement.

Penggunaan “PDCA”



Sejarah ISO 27001:2005 (ISMS)

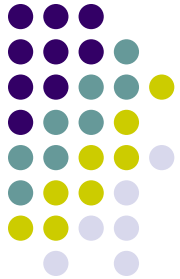


- ISO 27001:2005 atau yang disebut juga ISO 17799:2005-2 adalah suatu standar keamanan yang diperuntukkan bagi institusi yang akan mengelola dan mengontrol *Information Security* nya,
- Standar manajemen informasi diperkenalkan pertama kali pada tahun 1995, *Institut Standard Britania (BSI)* : BS 7799,
- ISO 17799 standard mengenai manajemen informasi pada 1 Desember 2000,
- *ISMS* merupakan suatu **proses** dan bukan suatu **produk**, dalam hal ini dapat diartikan sebagai suatu proses yang bertujuan untuk mengidentifikasikan dan meminimalkan resiko keamanan informasi sampai ketingkat yang dapat diterima, proses dimaksud haruslah dapat dikelola sesuai dengan standar yang telah ditetapkan.
- Badan Standard Internasional (ISO) telah memperkenalkan Standar ini dengan konsep “Sistem Manajemen" ke dalam bidang keamanan, yang secara garis besar dapat dikatakan sebagai suatu perangkat yang diambil dari sistem yang berkualitas untuk menyimpan / memelihara proses keamanan

Establish ISMS

1. Mendefinisikan ruang lingkup
2. Mendefinisikan kebijakan keamanan informasi
3. Mendefinisikan cara melakukan analisa resiko
4. Mengidentifikasi resiko
5. Melakukan analisa & evaluasi resiko.
6. Mengidentifikasi dan evaluasi cara untuk penanggulangan resiko
7. Memilih kontrol yang diambil dari obyektif kontrol.
8. Meminta persetujaun manajemen terhadap sisa resiko
9. Meminta otorisasi/perintah manajemen untuk melaksanakan ISMS
10. Membuat “Statement of Applicability”

2: Define ISMS Policy



1. includes a framework for setting objectives and establishes an overall sense of direction and principles for action with regard to information security;
2. takes into account business and legal or regulatory requirements, and contractual security obligations;
3. aligns with the organization's strategic risk management context in which the establishment and maintenance of the ISMS will take place;
4. establishes criteria against which risk will be evaluated (see 4.2.1c)); and
5. has been approved by management.

No	Kebijakan	Acuan
1	Bank melaksanakan pengelolaan Teknologi Sistem Informasi pada organisasinya	- SKDIR BI No No.27/164/KEP/DIR tahun 1995 pasal 2 dan pasal 3 butir 1
2	Direktorat I&T melaksanakan pengamanan sistem informasi di lingkungan Bank	- SKDIR BI No No.27/164/KEP/DIR tahun 1995 pasal 3 butir 1
3	Direktorat I&T melaksanakan pengawasan, pengendalian TSI pada Bank	- Lampiran SK BI No No.27/164/KEP/DIR tahun 1995
4	I&T Security Department memberikan layanan pengelolaan	- SE No. 001/TEK/ITY.OSS/2004 tahun 2004

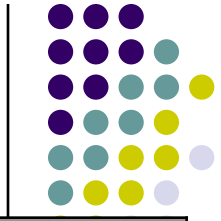
Dan seterusnya …

Basel II: Indicative Risk Categorisation[1]

Basel II Definition	Morgan Stanley language	Description	Examples
Processes	Products flaws	Failure due to inadequate or inappropriate product development, product quality, product complexity.	Product defects
	Selection, Sponsorship & Exposure	Failure to investigate clients per guidelines and/or to monitor client exposure limits	Failure to investigate clients
	Advisory Activities	Losses arising from inappropriate advice given to internal and external parties, eg legal action.	Disputes over performance of advisory activities
	Process Execution	Losses resulting from an inadequate organisational structure or operational processes.	Miscommunication, data entry, missed deadlines, delivery failure.
	Project Management	Losses arising from inadequate project planning, management and monitoring.	Late delivery
	Financial Management	Losses due to inadequate internal payment/settlement processes, reconciliation failures and budget management.	Missed payment penalties
	Internal Reporting	Losses due to inadequate / inaccurate reporting that is produced to aid internal business decision making.	Inaccurate internal reporting
	External Reporting	Losses due to inadequate / inaccurate reporting to external parties, e.g. shareholder / regulatory / financial / tax / stock exchange / security breaches / security surveillance.	Failed mandatory reporting obligation
	Customer intake and documentation	Losses resulting due to inappropriate / inefficient customer acceptance processes and supporting documentation.	Client information / documentation missing
	Client Service & Interaction	Losses or failure due to inadequate or inappropriate servicing of client needs.	Failure to meet client expectations
	Trade Counterparties	Losses arising from counterparty misperformance (excluding client and third parties)	Misperformance of broker
	Insurance	Loss resulting from inappropriate, or inadequate insurance (including over and under insurance)	Lack of insurance cover
	Suitability, Disclosure & Fiduciary	Unintentional or negligent failure to meet professional obligation to specific clients.	Breach of privacy, aggressive sales, account churning.

[1]The risk categories outlined in Appendix 1 are to be considered and reviewed during the course of the RCA roll-out and if appropriate will be altered.

Basel II: Indicative Risk Categorisation[1]



Basel II Definition	Morgan Stanley language	Description	Examples
External	Business Disruption	Loss resulting from events interrupting the ability to carry out business as usual activities	Failure of electricity supply.
	Ethical & Environmental risk	Buildings / business practices pollute locality / environment, spillage, breach of planning and building regulations in locality.	Breach of ethical policy.
	Physical Asset Risk	Losses arising from loss or damage to physical assets from natural disaster or other events.	Natural disaster.
	Outsourcing	Losses resulting from outsourced operations to external vendors.	Failure of outsourcer.
	External Fraud	Losses due to acts of a type intended to defraud, misappropriate property or circumvent the law, by a third party.	Theft, forgery.
	External IT Security	Losses due to errors, omissions or misrepresentation of data and/or arising from the lack of reliable data to base, rates, pricing, provisions, etc	Hacking, theft of information.
Systems[2]	Systems Architecture / Infrastructure	Loss resulting from inadequate or inappropriate IT architecture. Such losses can be contingent on architecture and infrastructure flaws such as network availability and communications.	Failure to integrate systems
	Systems availability and performance	Loss resulting from the inadequate or unavailable systems	Underperformance, Inadequate configuration management.
	Systems development/ Implementation	Loss resulting from inadequate or failed systems development or implementation. Including failure of system to meet needs, system not delivered on time, system not delivered on budget	Insufficient capacity to meet current or planned business needs.
	Internal IT Security	Loss resulting from inappropriate or unauthorised access to data or systems. Data can be compromised in terms of confidentiality, integrity and/or availability.	Physical and logical security provides inadequate protection.
	Data Integrity / Corruption	Losses due to errors, omissions or misrepresentation of data and/or arising from the lack of reliable data to base, rates, pricing, provisions, etc	Data sources unknown / inconsistent / not documented.

[1] The risk categories outlined in Appendix 1 are to be considered and reviewed during the course of the RCA roll-out and if appropriate will be altered.

[2] Systems include the following areas; Network, software, hardware, and telecommunications.

3: Risk Assessment Approach

- Level of risk
- Metode
  - Qualitative
  - Quantitative
  - Semi-quantitative
- Contoh:
  - BITS
  - OCTAVE
  - Bikin sendiri?
- Tabelnya digambar…!!!!

Level of Risk

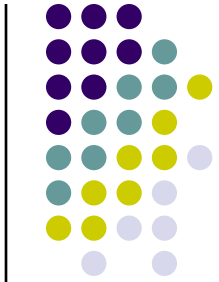
Inherent Risk		*Risk Level*	*Action Plan*
1 - 20	LOW	Diterima	
21 - 40	LOW TO MEDIUM	Diterima	
31 – 60	MEDIUM	Tidak diterima	Dihilangkan, dikurangi, dipindahkan
61 – 80	MEDIUM TO HIGH	Tidak diterima	Dihilangkan, dikurangi, dipindahkan
81-100	HIGH	Tidak diterima	Dihilangkan, dikurangi, dipindahkan

Current Strength of Internal Controls

Risk Control : Kualitas kontrol saat ini/ mitigasi terhadap risiko

Score		
Sangat Kuat	1	Minor
Kuat	2	Limited
Rata-rata	3	Medium
Lemah	4	Significant
Sangat Lemah	5	Major

4: Identify Risk



- Assets within scope
- Threats to assets
- Vulnerabilities
- Impacts

Asset Identification

No	Aset	Pemilik	Lokasi
Aset Informasi			
1	Database Nasabah (CIF, PIN, CardNo.)	Bank	Data Center
2	Database User Access Control (User Id, Access Level, Acces time) – Systems & Applications	Bank	I&T Sec. Dept
3	Asset Information (Vendor, Support, Life Time, Contracts, Licences)	Dir. I&T	I&T PSC Group
4	Database Human Resources Management	HCG	HCG
5	Database IT Budget	Dir. I&T	I&T PSC Group
6	Database Project – Systems & Applications	Dir. I&T	I&T PSC Group
7	Detail Network & Application Configuration	Dir. I&T	I&T PSC Group
8	Security Configuration	Dir. I&T	I&T Sec. Dept
9	Documentation System (Cabling, Network Devices, IP Address)	Dir. I&T	I&T PSC Group
10	Intrusion & Incident Documentation	Dir. I&T	I&T Sec. Dept
Aset Perangkat Lunak			
11	Microsoft Windows 2000 Server	Dir. I&T	Data Center
12	Microsoft Windows 2003 Server	Dir. I&T	Data Center

Impacts

Impact - Potential loss & dampak terhadap shareholder value (nilai bank) dan reputasi bank

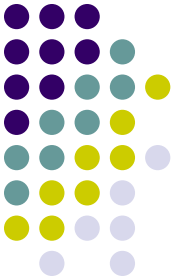
Score			Perhatian media	Pelanggaran terhadap hukum dan regulatory	Pelayanan terhadap nasabah
Sangat Kecil	1	Insignificant	Tidak ada dampak	Tidak ada dampak	Tidak berdampak
Kecil	2	Minor	Potensi menjadi sorotan publik	Percobaan akses ke sistem operasional bank	Dampak dapat diabaikan
Sedang	3	Moderate	Pemberitaan negatif pada media massa	Sistem operasional bank ditembus oleh hacker/cracker	Nasabah lebih banyak yang mengetahui
Besar	4	Major	Eskpos utama (di media massa) lebih dari 1 hari	Investigasi oleh pihak berwajib atau regulatory	Pelayanan terhadap nasabah terganggu lebih dari 24 jam
Sangat Besar	5	Fatal	Menjadi perhatian pemerintah / kehilangan kepercayaan publik	Kegagalan sistem yang menyeluruh / Sistem secara total tidak berfungsi	Ketidaknyamanan yang berarti ke seluruh nasabah / Keresahan timbul dari seluruh nasabah

Likehood

Kemungkinan terjadi - Frekuensi suatu kejadian dapat terjadi tanpa adanya kontrol

Score			Likelihood
Sangat Tidak Mungkin	1	Rare	Dapat diabaikan
Mungkin	2	Unlikely	Kecil kemungkinan terjadi
Kadang-kadang	3	Often	Kemungkinan terjadi sedang / Bisa terjadi
Hampir Pasti	4	Likely	Kemungkinan besar terjadi
Pasti Terjadi	5	Expected	Akan terjadi (dalam segala situasi)

5: Analisa Resiko
6: Evaluasi opsi
7: Select Control
8: Residual Risk



No	Assets	Vulnerabilities	Threats	Outcome	Impact Value	Likelihood	Curent Control	Current Risk Control	Inherent Risk	Control Objective	Additional Control	Action Pla
1	Customer Database Documentation	☐ Data saved in storage disk ☐ Connected to the network ☐ Put on the improper place	☐ people using access to network ☐ people using physically access ☐ storage damage	☐ disclosure ☐ modification ☐ loss/destruction	5	2	OKK08B1,OKK08B2, OKK08B3,OKK10B1, OKK10B2,OKK12B1, OKK14B1,OKK14B3	3	30	OKK08A, OKK10A, OKK12A, OKK14A		Acceptable
2	User Access Control Database Documentation	☐ Data saved in storage disk ☐ Connected to the network ☐ Put on the improper place	☐ people using access to network ☐ people using physically access ☐ storage damage	☐ disclosure ☐ modification ☐ loss/destruction	4	2	OKK08B1,OKK08B2, OKK08B3,OKK10B1, OKK10B2,OKK12B1, OKK14B1	3	24	OKK08A, OKK10A, OKK12A, OKK14A		Acceptable
3	Asset Information (Vendor, Support,Life time, contracts, licences)	☐ Data saved in storage disk ☐ Connected to the network ☐ Put on the improper place	☐ people using access to network ☐ people using physically access ☐ storage damage	☐ disclosure ☐ modification ☐ loss/destruction	3	2	OKK08B1,OKK08B2, OKK08B3,OKK10B1, OKK10B2,OKK12B1, OKK14B1,OKK14B2, OKK14B3	3	18	OKK08A, OKK10A, OKK12A, OKK14A		Acceptable

Lampiran A:
Control Objectives & Controls

Table A.1 – Control objectives and controls

A.5 Security policy		
A.5.1 Information security policy *Objective:* To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.		
A.5.1.1	Information security policy document	*Control* An information security policy document shall be approved by management, and published and communicated to all employees and relevant external parties.
A.5.1.2	Review of the information security policy	*Control* The information security policy shall be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.
A.6 Organization of information security		
A.6.1 Internal organization *Objective:* To manage information security within the organization.		
A.6.1.1	Management commitment to information security	*Control* Management shall actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities.

Contoh dlm kasus ini

Klasifikasi dan Kontrol Aset Informasi	KEBIJAKAN KEAMANAN INFORMASI
Kode : OKK03	

A. Obyektif Kontrol :

1. Terdapatnya aturan dalam memelihara perlindungan yang tepat bagi pengorganisasian aset .
2. Memastikan bahwa aset informasi memperoleh tingkat perlindungan yang tepat.

B. Kontrol :

1. Manajemen harus menetapkan Skema Kepemilikan Sistem *(System Ownership Scheme)* untuk setiap sistem yang dioperasikan atau yang digunakan oleh Bank.
2. Semua aset informasi harus ditentukan kepemilikannya, keberadaannya, serta klasifikasi keamanannya. Informasi / data yang diklasifikasikan sebagai *"public"* atau *"lower protection"* harus disetujui secara formal oleh pemilik sistem atau informasi / data sesuai dengan skema kepemilikan sistem dan informasi / data.
3. Setiap penanggung jawab aset harus menyusun dan memelihara catatan

AS-NZ 4360:2004
Risk Management Standard