



Certified Information
Systems Auditor.[®]
An ISACA[®] Certification



Certified Information
Security Manager.[®]
An ISACA[®] Certification



Certified in Risk
and Information
Systems Control.[®]
An ISACA[®] Certification



International
Organization for
Standardization



THE CAREER IN GOVERNANCE, RISK & COMPLIANCE

Presented by:

Rungga Reksya Sabilillah



Who am I

Rungga Reksya Sabilillah

(Technical Consulting Manager at MII)
@Telegram: rungga

Experience:

Teacher of TIK SDIT (2007)
Wushu Athlete at the PORDA II Banten (2006)
Leader of Wushu Gunadarma (2007-2008)
Assistant of IT Lab (2008-2009)
IT Support (2009)
IT Auditor at Conventional Bank (2010-2013)
IT Auditor at Sharia Bank (2013-2015)
Security and Infrastructure Auditor at Media (2015)
IT Consultant (2015 – Now)

Formal Education:

S1 – Information Technology (2005-2009)
S2 – Information System Management (2011-2013)

Non-Formal Education:

 ITIL® Intermediate - Service Operation



International Organization for Standardization

Lead Auditor ISO/IEC 27001
Lead Auditor ISO/IEC 20001
Lead Auditor ISO 22301



 EC-Council

Disaster Recovery Professional

Glossary



Information Security (NIST SP 800-53 R5):

The protection of information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Cybersecurity (NIST CSF v 1.1):

The process of protecting information by preventing, detecting, and responding to attacks.

Cybersecurity (NIST SP 800-53 R5):

Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

Glossary



Information Security Policy (NIST SP 800-53 R5):

Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information.

Information Security Risk (NIST SP 800-53 R5):

The risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or systems.

What is security governance?

Security governance is the means by which you control and direct your organisation's approach to security. When done well, security governance will effectively coordinate the security activities of your organisation. It enables the flow of security information and decisions around your organisation.

Just as security is the responsibility of everyone within an organisation, security decision making can happen at all levels. To achieve this, an organisation's senior leadership should use security governance to set out the kinds of security risks they are prepared for staff to take, and those they are not.

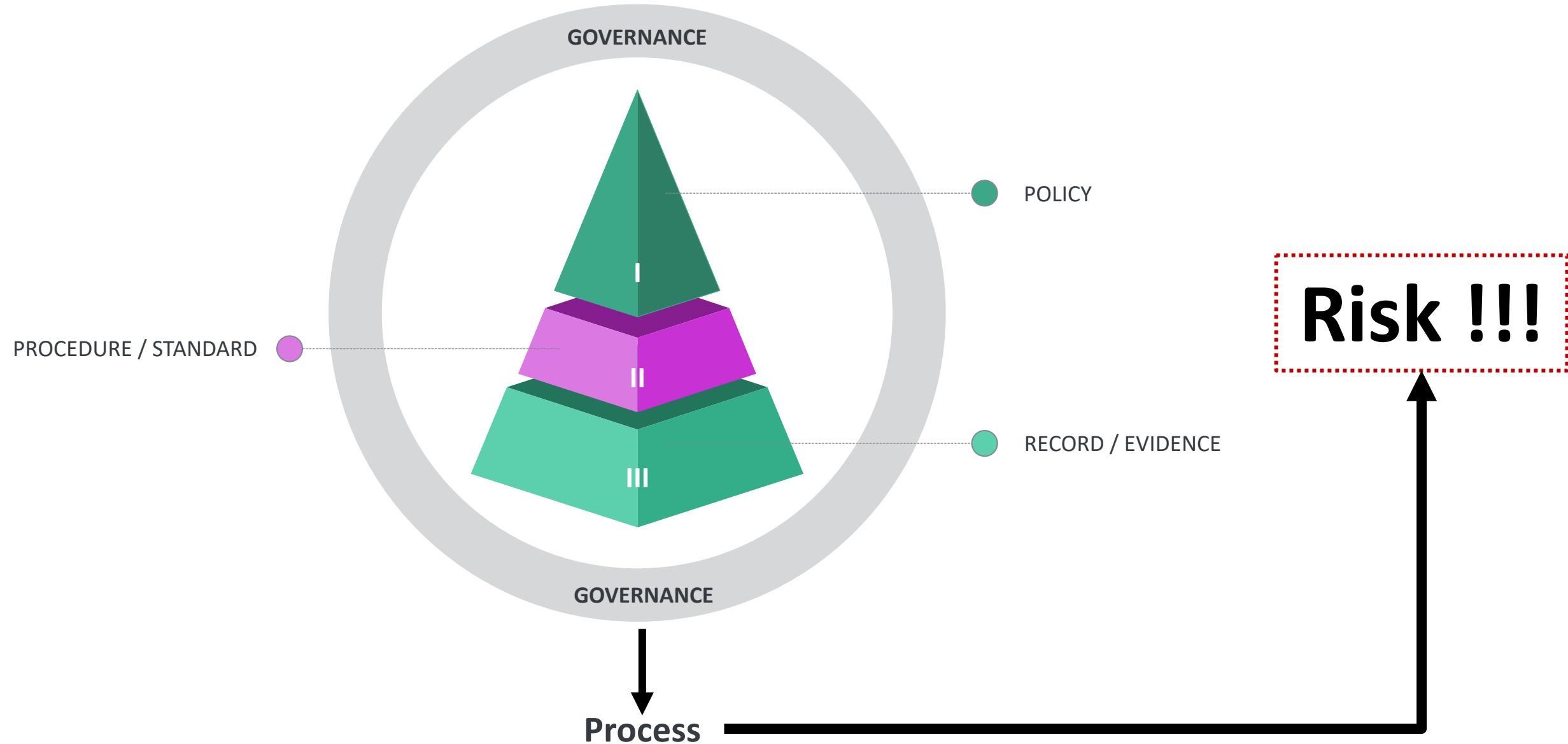


<https://www.ncsc.gov.uk/collection/risk-management-collection/governance-cyber-risk/security-governance-introduction>

There is no 'one size fits all' approach to security governance. The approach you eventually adopt will vary. At one extreme you may choose a formalized security framework, with clearly defined roles and business processes. At the other you may choose a more informal approach to directing, controlling and making security decisions.

NIST describes IT governance as the process of **establishing** and **maintaining** a framework to provide **assurance** that **information security strategies** are **aligned** with and **support business objectives**, are **consistent with applicable laws and regulations** through adherence to **policies** and **internal controls**, and provide assignment of **responsibility**, all in an effort to **manage risk**.

Just for illustration



Framework or Standard ???

Framework for Improving Critical Infrastructure Cybersecurity

Version 1.1

National Institute of Standards and Technology

April 16, 2018

NIST Special Publication 800-53
Revision 5

Security and Privacy Controls for Information Systems and Organizations



ICS > 35 > 35.030

ISO/IEC 27005:2018

Information technology — Security techniques — Information security risk management

NIST Special Publication 800-37
Revision 2

Risk Management Framework for Information Systems and Organizations

A System Life Cycle Approach for Security and Privacy

INTERNATIONAL STANDARD

ISO/IEC
27001

Second edition
2013-10-01

Information technology — Security techniques — Information security management systems — Requirements

INTERNATIONAL STANDARD

ISO
19011

Third edition
2018-07

Guidelines for auditing management systems



Payment Card Industry (PCI)
Data Security Standard

Requirements and Security Assessment Procedures

Version 3.2.1
May 2018

and many more...





The global skills and competency framework for the digital world

Governance:

Defining and operating a framework for **making decisions, managing stakeholder relationships, and identifying legitimate authority**.

Level 6:

- Implements the governance framework to enable governance activity to be conducted.
- Within a defined area of accountability, determines the requirements for appropriate governance reflecting the organisation's values, ethics and wider governance frameworks. Communicates delegated authority, benefits, opportunities, costs, and risks.
- Leads reviews of governance practices with appropriate and sufficient independence from management activity.
- Acts as the organisation's contact for relevant regulatory authorities and ensures proper relationships between the organisation and external stakeholders.



The global skills and competency framework for the digital world

Risk management:

Planning and implementing organisation-wide **processes** and **procedures** for the **management of risk** to the success or integrity of the enterprise.

Level 6:

- Plans and manages the implementation of organisation-wide processes and procedures, tools and techniques for risk management.
- Considers organisation-wide risk and **mitigation activities** within the **context of business risk** as a whole and the organisation's **appetite for risk**.
- Provides leadership on risk management at the organisational and business levels.



The global skills and competency framework for the digital world

Information security:

Defining and operating a framework of security controls and security management strategies.

Level 6:

- **Develops and communicates corporate information security policy, standards and guidelines.**
- Ensures architectural principles are applied during design to reduce risk. Drives adoption and adherence to policy, standards and guidelines.
- Contributes to the development of organisational strategies that address information control requirements. Identifies and monitors environmental and market trends and proactively assesses impact on business strategies, benefits and risks.
- Leads the provision of authoritative advice and guidance on the requirements for security controls in collaboration with subject matter experts.



The global skills and competency framework for the digital world

Audit:

Delivering independent, **risk-based assessments of the effectiveness of processes**, the controls, and the **compliance environment of an organisation**.

Level 6:

- Leads and manages complex audits and programs of audit activity.
- Obtains and manages appropriate specialist expertise to contribute highly specialised technical knowledge and experience.
- Develops organisational policies, standards and guidelines for the conduct of audits. Ensures the objectivity and impartiality of the audit process.
- Identifies areas of risk and specifies audit programs. Ensures audit coverage is sufficient to provide the business with assurance of adequacy and integrity. Authorises the issue of formal reports to management on the effectiveness and efficiency of control mechanisms.

Does Indonesia have regulations regarding information security?



PRESIDEN
REPUBLIK INDONESIA

PERATURAN PEMERINTAH REPUBLIK INDONESIA

NOMOR 71 TAHUN 2019

TENTANG

PENYELENGGARAAN SISTEM DAN TRANSAKSI ELEKTRONIK

DENGAN RAHMAT TUHAN YANG MAHA ESA

PRESIDEN REPUBLIK INDONESIA,

SALINAN

Bagian Keenam Tata Kelola Sistem Elektronik

Pasal 11

- (1) Penyelenggara Sistem Elektronik harus menjamin:
 - a. tersedianya perjanjian tingkat layanan;
 - b. tersedianya perjanjian keamanan informasi terhadap jasa layanan Teknologi Informasi yang digunakan; dan
 - c. keamanan informasi dan sarana komunikasi internal yang diselenggarakan.
- (2) Penyelenggara Sistem Elektronik sebagaimana dimaksud pada ayat (1) harus menjamin setiap komponen dan keterpaduan seluruh Sistem Elektronik beroperasi sebagaimana mestinya.

Pasal 14

- (1) Penyelenggara Sistem Elektronik wajib melaksanakan prinsip pelindungan Data Pribadi dalam melakukan pemrosesan Data Pribadi meliputi:
 - a. pengumpulan Data Pribadi dilakukan secara terbatas dan spesifik, sah secara hukum, adil, dengan sepenuhnya dan persetujuan dari pemilik Data Pribadi;
 - b. pemrosesan Data Pribadi dilakukan sesuai dengan tujuannya;
 - c. pemrosesan Data Pribadi dilakukan dengan menjamin hak pemilik Data Pribadi;
 - d. pemrosesan Data Pribadi dilakukan secara akurat, lengkap, tidak menyesatkan, mutakhir, dapat dipertanggungjawabkan, dan memperhatikan tujuan pemrosesan Data Pribadi;
 - e. pemrosesan Data Pribadi dilakukan dengan melindungi keamanan Data Pribadi dari kehilangan, penyalahgunaan, akses dan pengungkapan yang tidak sah, serta pengubahan atau perusakan Data Pribadi;
 - f. pemrosesan Data Pribadi dilakukan dengan memberitahukan tujuan pengumpulan, aktivitas pemrosesan, dan kegagalan pelindungan Data Pribadi; dan

Does Indonesia have regulations regarding information security?



PERATURAN BADAN SIBER DAN SANDI NEGARA
NOMOR 8 TAHUN 2020
TENTANG
SISTEM PENGAMANAN DALAM PENYELENGGARAAN
SISTEM ELEKTRONIK
DENGAN RAHMAT TUHAN YANG MAHA ESA

KEPALA BADAN SIBER DAN SANDI NEGARA,

Pasal 6

- (1) Kategori Sistem Elektronik berdasarkan asas Risiko terdiri atas:
 - a. **Sistem Elektronik strategis;**
 - b. **Sistem Elektronik tinggi; dan**
 - c. **Sistem Elektronik rendah.**
- (2) Sistem Elektronik strategis sebagaimana dimaksud pada ayat (1) huruf a merupakan Sistem Elektronik yang berdampak serius terhadap kepentingan umum, pelayanan publik, kelancaran penyelenggaraan negara, atau pertahanan dan keamanan negara.
- (3) Sistem Elektronik tinggi sebagaimana dimaksud pada ayat (1) huruf b merupakan Sistem Elektronik yang berdampak terbatas pada kepentingan sektor dan/atau daerah tertentu.
- (4) Sistem Elektronik rendah sebagaimana dimaksud pada ayat (1) huruf c merupakan Sistem Elektronik lainnya yang tidak termasuk pada ayat (2) dan ayat (3).

Pasal 9

- (1) Penyelenggara Sistem Elektronik yang menyelenggarakan Sistem Elektronik strategis wajib menerapkan:
 - a. SNI ISO/IEC 27001;
 - b. standar keamanan lain yang terkait dengan keamanan siber yang ditetapkan oleh BSSN; dan
 - c. standar keamanan lain yang terkait dengan keamanan siber yang ditetapkan oleh Kementerian atau Lembaga.
- (2) Penyelenggara Sistem Elektronik yang menyelenggarakan Sistem Elektronik tinggi wajib menerapkan:
 - a. **SNI ISO/IEC 27001 dan/atau standar keamanan lain** yang terkait dengan keamanan siber yang ditetapkan oleh BSSN; dan
 - b. standar keamanan lain yang terkait dengan keamanan siber yang ditetapkan oleh Kementerian atau Lembaga.
- (3) Penyelenggara Sistem Elektronik yang menyelenggarakan Sistem Elektronik rendah wajib menerapkan:
 - a. **SNI ISO/IEC 27001; atau**
 - b. standar keamanan lain yang terkait dengan keamanan siber yang ditetapkan oleh BSSN.

Does Indonesia have regulations regarding information security?



OTORITAS JASA KEUANGAN
REPUBLIK INDONESIA

SALINAN

PERATURAN OTORITAS JASA KEUANGAN
NOMOR 38 /POJK.03/2016
TENTANG

PENERAPAN MANAJEMEN RISIKO DALAM
PENGUNAAN TEKNOLOGI INFORMASI OLEH BANK UMUM

DENGAN RAHMAT TUHAN YANG MAHA ESA

DEWAN KOMISIONER OTORITAS JASA KEUANGAN,

Pasal 5

Wewenang dan tanggung jawab Direksi sebagaimana dimaksud dalam Pasal 4 paling sedikit mencakup:

- a. menetapkan Rencana Strategis Teknologi Informasi dan kebijakan Bank terkait penggunaan Teknologi Informasi;
- b. menetapkan kebijakan, standar, dan prosedur terkait penyelenggaraan Teknologi Informasi yang memadai dan mengomunikasikannya secara efektif, baik pada satuan kerja penyelenggara maupun pengguna Teknologi Informasi;
- c. memastikan:
 1. Teknologi Informasi yang digunakan Bank dapat mendukung perkembangan usaha Bank,

2.

pencapaian tujuan bisnis Bank dan kelangsungan pelayanan terhadap nasabah Bank;

terdapat kegiatan peningkatan kompetensi sumber daya manusia yang terkait dengan penyelenggaraan dan penggunaan Teknologi Informasi;

3.

ketersediaan sistem pengelolaan pengamanan informasi (*information security management system*) yang efektif dan dikomunikasikan kepada satuan kerja pengguna dan penyelenggara Teknologi Informasi;



Yth.

1. Direksi Bank Umum Konvensional; dan
2. Direksi Bank Umum Syariah,
di tempat.

SALINAN

SURAT EDARAN OTORITAS JASA KEUANGAN
NOMOR 21 /SEOJK.03/2017

TENTANG

PENERAPAN MANAJEMEN RISIKO DALAM
PENGUNAAN TEKNOLOGI INFORMASI OLEH BANK UMUM

Sehubungan dengan berlakunya Peraturan Otoritas Jasa Keuangan Nomor 38/POJK.03/2016 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 267, Tambahan Lembaran Negara Republik Indonesia Nomor 5963) selanjutnya disingkat POJK MRTI, perlu untuk mengatur ketentuan pelaksanaan mengenai penerapan manajemen risiko dalam penggunaan Teknologi Informasi oleh bank umum dalam Surat Edaran Otoritas Jasa Keuangan sebagai berikut:

5.2.1.

Disamping itu, Bank perlu mempertimbangkan implementasi standar internasional di bidang pengamanan informasi seperti *International Organization for Standardization (ISO)*, *International Electrotechnical Commission (IEC)*, *Control Objective for Information and Related Technology (COBIT)*, *Information Technology Infrastructure Library (ITIL)* dan standar nasional seperti Standar Nasional Indonesia (SNI), dengan memperhatikan tujuan, kebijakan usaha, ukuran, dan kompleksitas usaha Bank yang meliputi antara lain keragaman dalam jenis transaksi, produk, atau jasa dan jaringan kantor, serta teknologi pendukung yang digunakan.

Kebijakan Pengamanan Informasi

Manajemen Bank harus menetapkan kebijakan dan memiliki komitmen yang tinggi terhadap pengamanan informasi. Kebijakan tersebut harus sesuai dengan penerimaan risiko (*risk appetite*) dan dikomunikasikan secara berkala kepada seluruh pegawai Bank dan pihak ekstern yang terkait. Disamping itu, perlu dilakukan evaluasi kebijakan secara berkala dan apabila terdapat perubahan penting. Kebijakan tentang pengamanan informasi harus mencakup paling

Does Indonesia have regulations regarding information security?



OTORITAS JASA KEUANGAN
REPUBLIK INDONESIA

SALINAN

PERATURAN OTORITAS JASA KEUANGAN
REPUBLIK INDONESIA
NOMOR 4 /POJK.05/2021
TENTANG

PENERAPAN MANAJEMEN RISIKO DALAM PENGGUNAAN
TEKNOLOGI INFORMASI OLEH LEMBAGA JASA KEUANGAN NONBANK

DENGAN RAHMAT TUHAN YANG MAHA ESA

DEWAN KOMISIONER OTORITAS JASA KEUANGAN,

Pasal 2

LJKNB sebagaimana dimaksud dalam Pasal 1 angka 1 meliputi:

- a. perusahaan perasuransian, yang terdiri atas:
 1. perusahaan asuransi;
 2. perusahaan reasuransi;
 3. perusahaan asuransi syariah;
 4. perusahaan reasuransi syariah;
 5. perusahaan pialang asuransi;
 6. perusahaan pialang reasuransi; dan
 7. perusahaan penilai kerugian asuransi, sebagaimana dimaksud dalam peraturan perundang-undangan mengenai perasuransian;
- b. dana pensiun sebagaimana dimaksud dalam peraturan perundang-undangan mengenai dana pensiun;
- c. lembaga pembiayaan, terdiri atas:
 1. perusahaan pembiayaan;
 2. perusahaan pembiayaan syariah;
 3. perusahaan modal ventura;
 4. perusahaan modal ventura syariah; dan
 5. perusahaan pembiayaan infrastruktur, sebagaimana dimaksud dalam peraturan perundang-undangan mengenai lembaga pembiayaan;
- d. lembaga jasa keuangan lainnya, terdiri atas:
 1. perusahaan pergadaian sebagaimana dimaksud dalam peraturan perundang-undangan mengenai pergadaian;
 2. lembaga penjamin, terdiri atas:
 - a) perusahaan penjaminan;
 - b) perusahaan penjaminan syariah;
 - c) perusahaan penjaminan ulang; dan

- d) perusahaan penjaminan ulang syariah, sebagaimana dimaksud dalam peraturan perundang-undangan mengenai penjaminan;
3. penyelenggara layanan pinjam meminjam uang berbasis teknologi informasi sebagaimana dimaksud dalam peraturan perundang-undangan mengenai layanan pinjam meminjam uang berbasis teknologi informasi;
4. lembaga pembiayaan ekspor Indonesia sebagaimana dimaksud dalam peraturan perundang-undangan mengenai lembaga pembiayaan ekspor Indonesia;
5. perusahaan pembiayaan sekunder perumahan sebagaimana dimaksud dalam peraturan perundang-undangan mengenai perusahaan pembiayaan sekunder perumahan;
6. badan penyelenggara jaminan sosial sebagaimana dimaksud dalam peraturan perundang-undangan mengenai badan penyelenggara jaminan sosial; dan
7. PT Permodalan Nasional Madani (Persero) sebagaimana dimaksud dalam peraturan perundang-undangan mengenai PT Permodalan Nasional Madani (Persero), yang menggunakan Teknologi Informasi dalam penyelenggaraan usaha.

BAB IX

PENGAMANAN KERAHASIAAN DATA PRIBADI KONSUMEN

Pasal 30

Dalam menyelenggarakan Teknologi Informasi, LJKNB wajib menjamin:

- a. perolehan, pengolahan, penggunaan, penyimpanan, pembaruan, dan/atau pengungkapan data pribadi konsumen dilakukan berdasarkan persetujuan

- 29 -

- konsumen yang bersangkutan, kecuali ditentukan lain oleh ketentuan peraturan perundang-undangan; dan
- b. penggunaan atau pengungkapan data pribadi konsumen sesuai dengan tujuan yang disampaikan kepada konsumen pada saat perolehan data.

A black and white photograph of a man in a dark tuxedo and white shirt, sitting on a chair. He is looking off to the side with a serious expression. In his left hand, he holds an open book or manuscript. His right hand rests on his lap. The background is dark and out of focus.

**GREAT THINGS
NEVER
CAME FROM
COMFORT
ZONES.**

#BAGAIMANA

#CARAKERJA

#ANSWER

#OH

#MUDAH

#SILAHKAN

#HOW

#APA

#TANYA

#JAWAB

#PERTANYAAN

#DIJAWAB