Tips Penerapan
Manajemen Keamanan Informasi

Adityo Hidayat, S.Kom, M.B.A, CISA

Biodata

Education

- S1 Ilmu Komputer UGM
- S2 Magister Manajemen UGM
- Mahasiswa S3 Ilmu Komputer UGM

Buku

- Membangun Kota dan Kabupaten Cerdas: Sebuah Panduan Bagi Pemerintah Daerah, Gadjah Mada University Press, 2018

Courses

- Big Data and Analytics Summer School, University of Essex, United Kingdom
- IT Governance with COBIT5
- Blockchain for Business
- DeepLearning.AI TensorFlow Developer

Certifications

- Certified Information Systems Auditor (CISA)

Experience

- Evaluator Eksternal SPBE KemenpanRB
- TransJakarta O/D Analytics
- Tim Analitika Pusdatinrenbang PPN/Bappenas

Websites

- PortalReksadana.com
- SepedaSehat.com
- gebetSaham.com

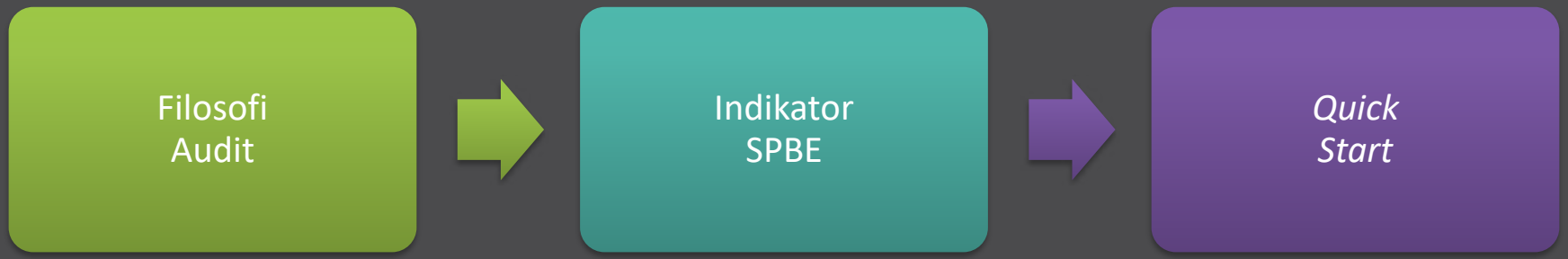
Passion

- Coding
- Cycling
- Coffee

Contact

- E-Mail: adityo.hidayat@gmail.com
- WA: 08112511989

Agenda



Kuntji!

Persyaratan indikator SPBE tentang keamanan informasi

Ruang lingkup, sasaran, *best practices*

Filosofi Audit

Information System

- *Collects and evaluate evidence to determine whether IS resources adequately safeguard assets, maintain data integrity/availability, provide relevant and reliable information, achieve organizational goals effectively*
- *Internal controls that provide reasonable assurance that business, operational and control objectives will be met, and that undesired events will be prevented, detected or corrected in a timely manner*

Internal Controls

- *Policies, procedures, practices and organizational structures, which are implemented to reduce risks*
- *Address undesired events through elements of internal controls: preventive, detection and correction*

Internal Controls

Preventive	• *Detect problems before they arise, prevent errors, omission or malicious act from occuring* • *E.g: segregate duties, access control software, physical access control*
Detective	• *Detect and report the occurence of an error, omission or malicious act* • *E.g: Review of activity logs, hash totals*
Corrective	• *Minimize impact of a threat, correct errors arising from a problem, remedy problems discovered by detective controls* • *E.g: contingency planning, backup procedures, re-run procedures*

Control Objectives

Security	• *Confidentiality* • *Integrity* • *Availability*
Quality	• *Effectiveness* • *Efficiency*
Fiduciary	• *Compliance* • *Reliability*

Filosofi SPBE

Kebijakan

Tata Kelola

Manajemen

*"**Nyuruh**"-nya sudah benar?*

***Eksekusi**nya sudah benar?*

Dikembangkan → Ditetapkan → Digunakan → Dievaluasi

Indikator SPBE Terkait Keamanan Informasi

[8] Kebijakan Internal
Manajemen Keamanan Informasi

- Penetapan Ruang Lingkup
- Penetapan Penanggung Jawab
- Perencanaan
- Dukungan Pengoperasian
- Evaluasi Kinerja
- Perbaikan Berkelanjutan

[9] Kebijakan Internal
Audit TIK

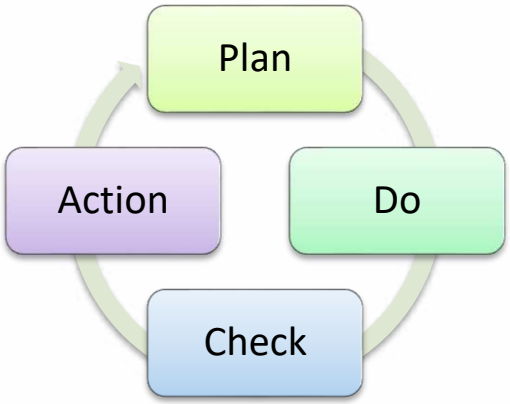
Audit Infrastruktur

Audit Aplikasi

Audit Keamanan

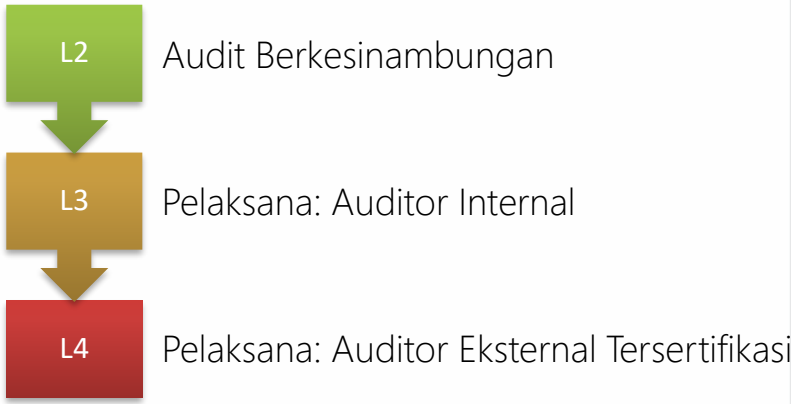
Indikator SPBE Terkait Keamanan Informasi

- [22] Penerapan Manajemen Keamanan Informasi



Output: Kebijakan, Prosedur

- [29] Audit Infrastruktur
- [30] Audit Aplikasi
- [31] Audit Keamanan



Output Audit merupakan ***Audit Report*** yang berisi temuan dan rekomendasi

"Pengendalian Keamanan Informasi"

Tingkat 1 (Kebijakan/Standar)

- Kebijakan Keamanan Informasi
- Peran dan tanggung jawab organisasi keamanan informasi
- Klasifikasi informasi
- Kebijakan Pengamanan Akses Fisik dan *Logic*
- Manajemen Kelangsungan Usaha (*Business Continuity Management*)
- Ketentuan Penggunaan Sumber Daya TIK

Tingkat 2 (Prosedur/Panduan)

- Prosedur pengendalian dokumen
- Prosedur pengendalian rekaman
- Prosedur audit internal SMKI
- Prosedur tindakan perbaikan dan pencegahan
- Prosedur penanganan informasi (penyimpanan, pelabelan, pengiriman/pertukaran, pemusnahan)
- Prosedur penanganan insiden/gangguan keamanan informasi
- Prosedur pemantauan penggunaan fasilitas teknologi informasi

Panduan Penerapan Sistem Manajemen Keamanan Informasi Berbasis Indeks Keamanan Informasi (Indeks KAMI)
Kementerian Komunikasi dan Informatika, 2017

Audit Aplikasi

Perencanaan

Business Requirement, Software Requirement, Software Design

Pengembangan

Software Implementation, Testing, Installation

Pengoperasian

Software Usage

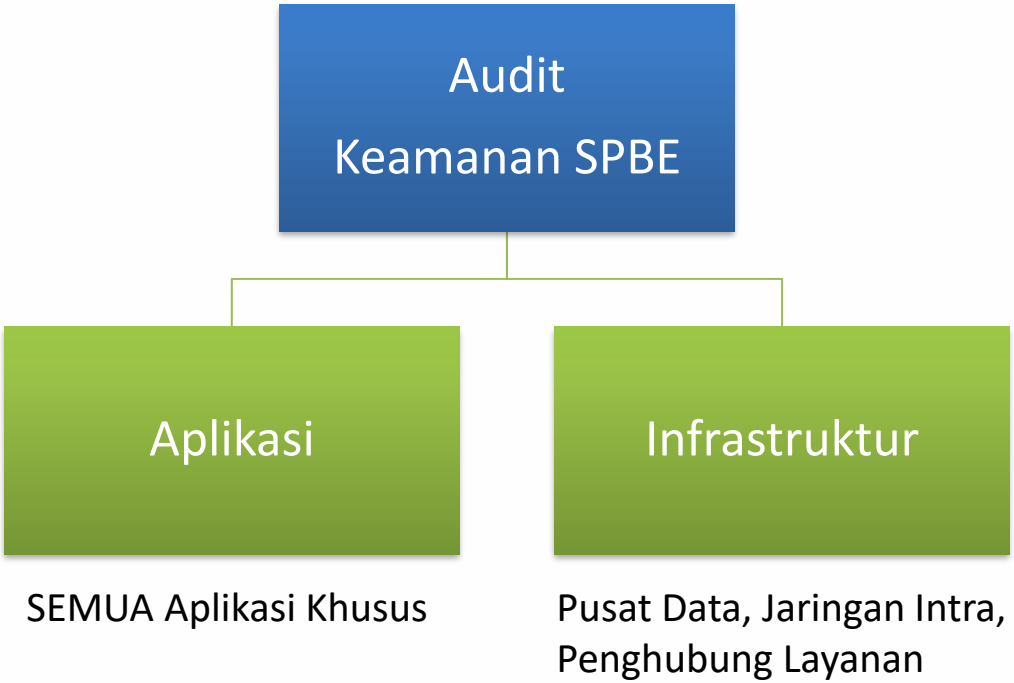
Pemeliharaan

Software Maintenance, Configuration Management

Audit Infrastruktur

Perencanaan	Pengembangan	Pengoperasian
Pemeliharaan	Kepatuhan	Sertifikasi

Audit Keamanan



Pedoman Audit Keamanan
akan ditetapkan oleh BSSN

Quick Start

COBIT 2019

Kitab yang memuat pedoman seluruh semesta urusan tata kelola TIK, tidak bersifat mengikat

ISO 27001

Persyaratan manajemen keamanan informasi yang bersifat mengikat dan diakui secara global

Ruang Lingkup

“ Pengembangan sistem, operasional pengolahan data & jaringan, proses settlement dan rekonsiliasi pada Layanan *Payment Gateway* dari penerbit uang elektronik ”

Sasaran Keamanan Informasi

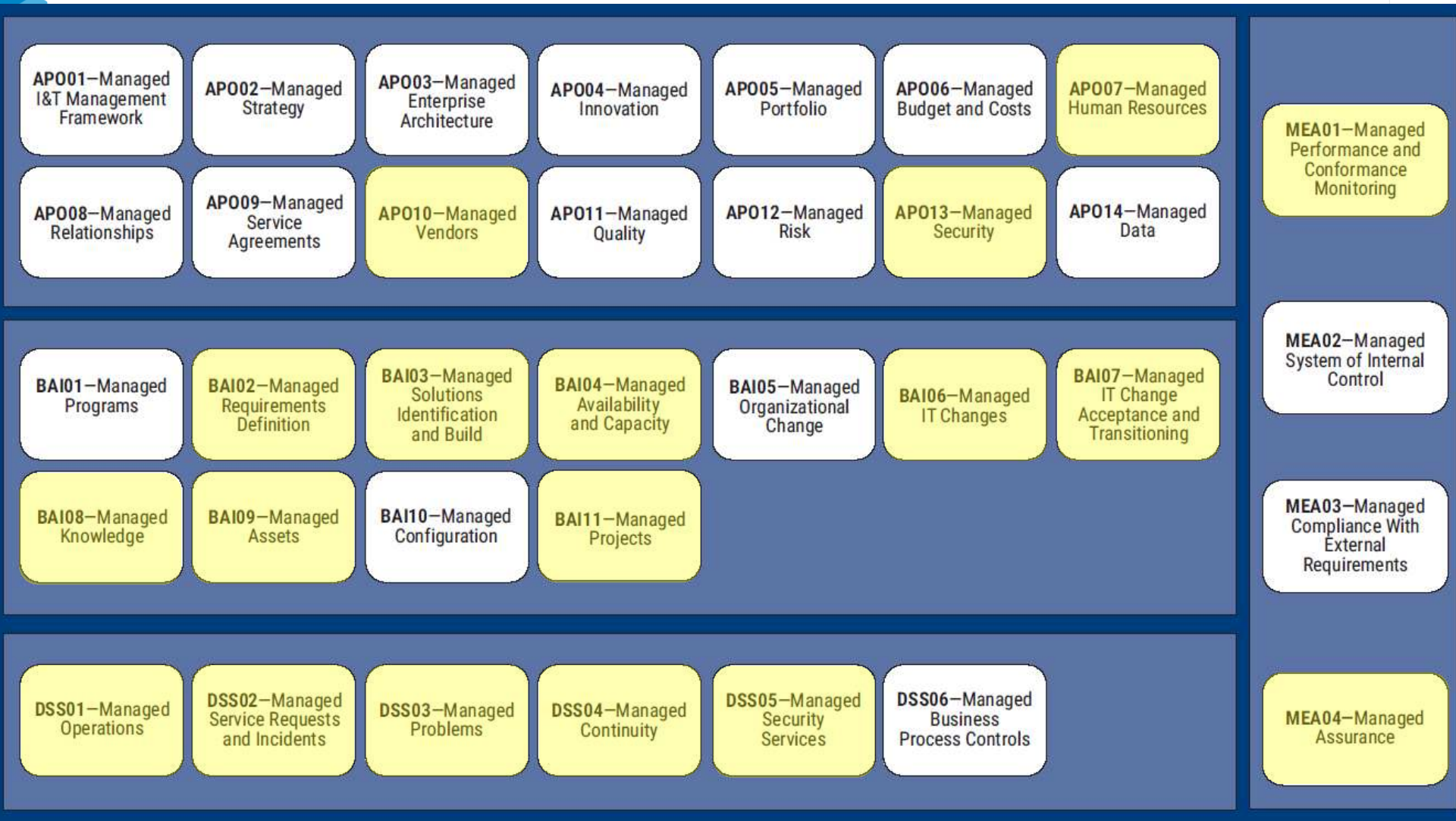
1. Tercapainya 100% pengolahan transaksi *e-money*
   Mulai dari tapping hingga pelimpahan
2. Transaksi *defect* tidak lebih dari 2%.
   Defect = salah potong tarif (ketidaksesuaian *deduct*)
3. Kapasitas sistem *payment processing* 1 juta trx/day
4. Ketersediaan sistem *payment processing* 98%

Sasaran Keamanan Informasi

No	Nama Sasaran	Target Pengukuran	Tahun Pencapaian			Penanggung Jawab	Program Kerja
			2021	2022	2023		
1	Reliabilitas infrastruktur data center	Uptime data center	95%	95%	100%	• Urusan Infrastruktur Jaringan • Urusan Server dan Keamanan Jaringan	Redundansi perangkat jaringan (Core dan BGP Router, Firewall) Optimasi High Availability Server
2	Ketersediaan layanan LAN dan Wifi	Uptime Wifi	95%	98%	100%	• Urusan Infrastruktur Jaringan • Urusan Layanan	Preventive Maintenance
		Uptime LAN	95%	98%	100%		
3	Insiden Keamanan Informasi	Jumlah Insiden Mayor	0	0	0	Urusan Server dan Keamanan Jaringan	Backup dan Replication secara real time
		Rasio Penanganan Insiden Infrastruktur	90%	95%	100%	Urusan Server dan Keamanan Jaringan	Preventive Maintenance dan Training Kompetensi Berkala
		Rasio Penanganan Insiden Layanan Mahasiswa	60%	80%	100%	• Urusan Aplikasi dan Basis Data • Urusan Website	Training Kompetensi Berkala

Focus Area

COBIT 2019



Process Improvement

COBIT 2019

Domain: Deliver, Service and Support Management Objective: DSS04 - Managed Continuity	Focus Area: COBIT Core Model
Description	
Establish and maintain a plan to enable the business and IT organizations to respond to incidents and quickly adapt to disruptions. This will enable continued operations of critical business processes and required I&T services and maintain availability of resources, assets and information at a level acceptable to the enterprise.	
Purpose	
Adapt rapidly, continue business operations and maintain availability of resources and information at a level acceptable to the enterprise in the event of a significant disruption (e.g., threats, opportunities, demands).	

Key Management Practice
DSS04.01 Define the business continuity policy, objectives and scope.
DSS04.02 Maintain business resilience.
DSS04.03 Develop and implement a business continuity response.
DSS04.04 Exercise, test and review the business continuity plan (BCP) and disaster response plan (DRP).
DSS04.05 Review, maintain and improve the continuity plans.
DSS04.06 Conduct continuity plan training.
DSS04.07 Manage backup arrangements.
DSS04.08 Conduct post-resumption review.

Process Improvement

COBIT 2019

Management Practice	Example Metrics
DSS04.04 Exercise, test and review the business continuity plan (BCP) and disaster response plan (DRP). Test continuity on a regular basis to exercise plans against predetermined outcomes, uphold business resilience and allow innovative solutions to be developed.	a. Frequency of tests b. Number of exercises and tests that achieved recovery objectives

Activities	Capability Level
1. Define objectives for exercising and testing the business, technical, logistical, administrative, procedural and operational systems of the plan to verify completeness of the BCP and DRP in meeting business risk.	2
2. Define and agree on stakeholder exercises that are realistic and validate continuity procedures. Include roles and responsibilities and data retention arrangements that cause minimum disruption to business processes.	
3. Assign roles and responsibilities for performing continuity plan exercises and tests.	
4. Schedule exercises and test activities as defined in the continuity plans.	3
5. Conduct a post-exercise debriefing and analysis to consider the achievement.	4
6. Based on the results of the review, develop recommendations for improving the current continuity plans.	5

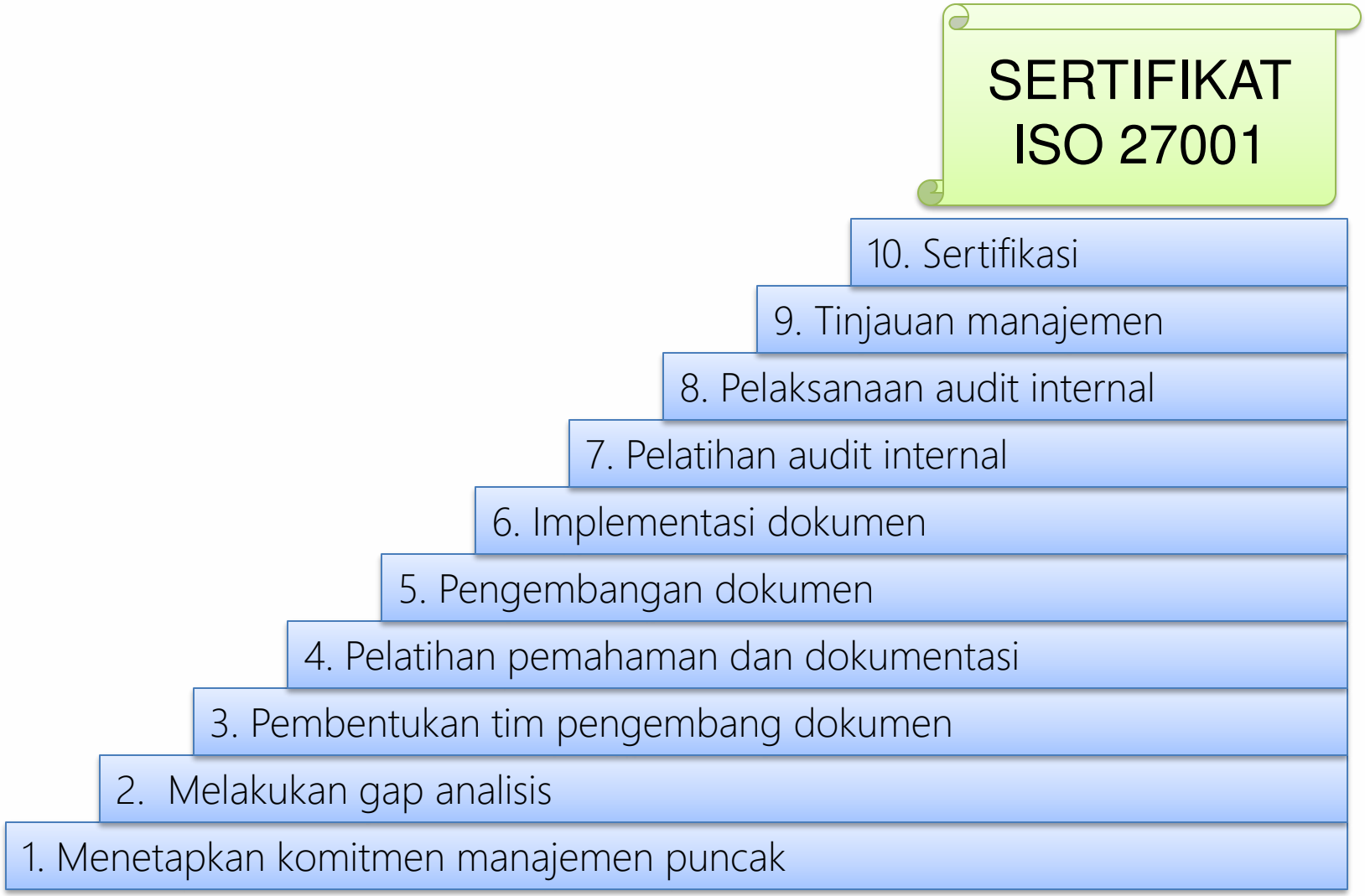
Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Cybermaturity Platform, 2018	PP.RS Develop and Maintain Response Plans; PP.RP Develop and Maintain Recovery Plans
ISF, The Standard of Good Practice for Information Security 2016	BC2.3 Business Continuity Testing
The CIS Critical Security Controls for Effective Cyber Defense Version 6.1, August 2016	CSC 20: Penetration Tests and Red Team Exercises

ISO 27001 Annex

Incident Management

A.16 Information security incident management		
A.16.1 Management of information security incidents and improvements		
Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.		
A.16.1.1	Responsibilities and procedures	*Control* Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.
A.16.1.2	Reporting information security events	*Control* Information security events shall be reported through appropriate management channels as quickly as possible.
A.16.1.3	Reporting information security weaknesses	*Control* Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.
A.16.1.4	Assessment of and decision on information security events	*Control* Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.
A.16.1.5	Response to information security incidents	*Control* Information security incidents shall be responded to in accordance with the documented procedures.
A.16.1.6	Learning from information security incidents	*Control* Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.
A.16.1.7	Collection of evidence	*Control* The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.

Menuju Sertifikasi ISO 27001



Terima Kasih

Mari kita diskusikan