UNIVERSITAS AMIKOM YOGYAKARTA
Creative Economy Park

MATA KULIAH CYBER SECURITY

Program Studi Magister Informatika

Universitas AMIKOM Yogyakarta
Tahun 2025

Creative Economy Park

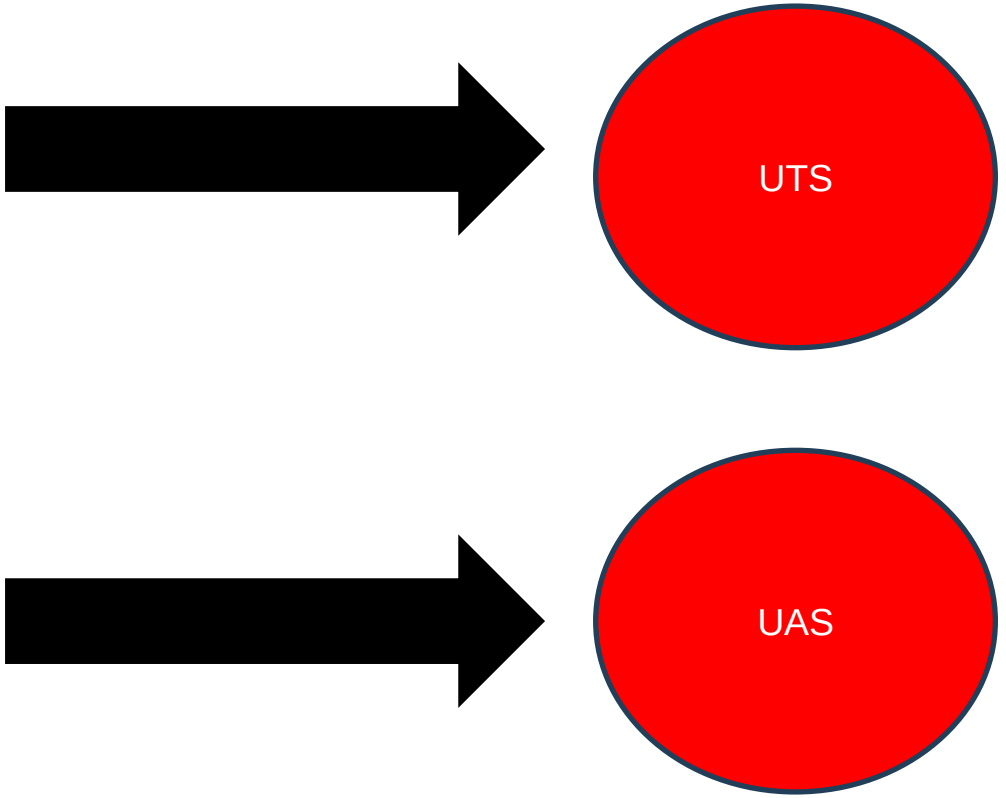
Dr. Ir. Yoga Sahria, S.Kom., M.Kom.

Fakultas Ilmu Komputer

Universitas AMIKOM Yogyakarta
Jln RingRoad Utara, Depok, Condongcatur
Yogyakarta

Outline Mata Kuliah Selama 1 Semester

1. Ruang lingkup keamanan cyber menurut framework Cyber Security Body of Knowledge (CyBoK)
2. Serangan infrastruktur jaringan
3. Malware
4. Serangan aplikasi desktop dan web
5. Social engineering
6. Solusi pengamanan data dan sistem modern
7. Regulasi dan kebijakan cyber law di Indonesia
8. Implementasi kebijakan keamanan TI
9. Penetration testing
10. Digital Forensic



UNIVERSITAS AMIKOM YOGYAKARTA
Creative Economy Park

Cyber Security Framework

PERTEMUAN 7

Universitas AMIKOM Yogyakarta
Tahun 2025

Creative Economy Park

Dr. Ir. Yoga Sahria, S.Kom., M.Kom.
Fakultas Ilmu Komputer
Universitas AMIKOM Yogyakarta
Jln RingRoad Utara, Depok, Condongcatur
Yogyakarta

Cyber Security Framework

Minggu 7

Dr. Ir. Yoga Sahria, S.Kom., M.Kom.

Apa itu Cyber Security Framework (CSF)?

- Framework adalah dasar dari semua kebijakan dan proses program keamanan Anda
- Framework harus menyatukan persyaratan yang harus dipenuhi oleh program keamanan Anda

a) Business goal
b) Regulatory requirements
c) Technical requirements
d) Industry requirements

Apa itu Cyber Security Framework (CSF)?

- Sebuah pondasi untuk menerapkan keamanan siber
- Serangkaian dokumentasi kebijakan dan prosedur yang mengatur implementasi dan manajemen berkelanjutan dari keamanan organisasi

1. Roadmap atau blueprint perusahaan untuk keamanan siber
2. Tidak menjamin perusahaan secara otomatis akan patuh
3. Tidak menjamin perusahaan otomatis lebih aman

Mengapa Perlu CSF?

- Best practice terbaik dari industri
- Membantu memastikan perusahaan memiliki informasi yang diatur untuk persyaratan kepatuhan (compliance req)
  - Faktor lain: kebutuhan regulasi / kontrak kerja
- Membantu perusahaan berkomunikasi dengan Perusahaan mitra menggunakan bahasa yang sama
- Membantu perusahaan menilai keamanan mereka sendiri dan memberikan roadmap untuk perbaikan
  - Memberi gambaran hal2 yang perlu ditingkatkan lagi

Frameworks

General Frameworks

1. COBIT (Control Objectives for Information and Related Technologies)
2. ISO (International Organization for Standardization) 27001 Series
3. AICPA Trust Services Principles and Criteria
4. NIST Cyber Security Framework (CSF)
5. NIST SP 800-53
6. CIS Critical Security Controls

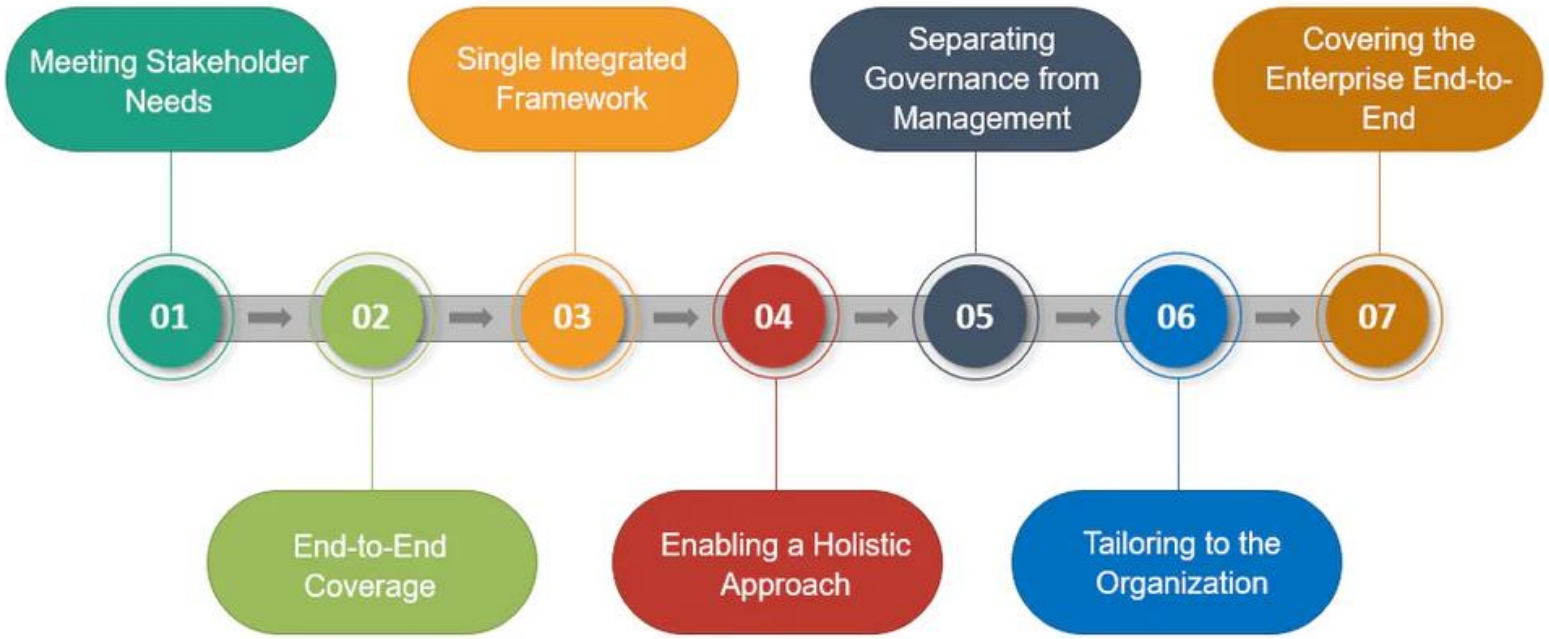
Specific Frameworks

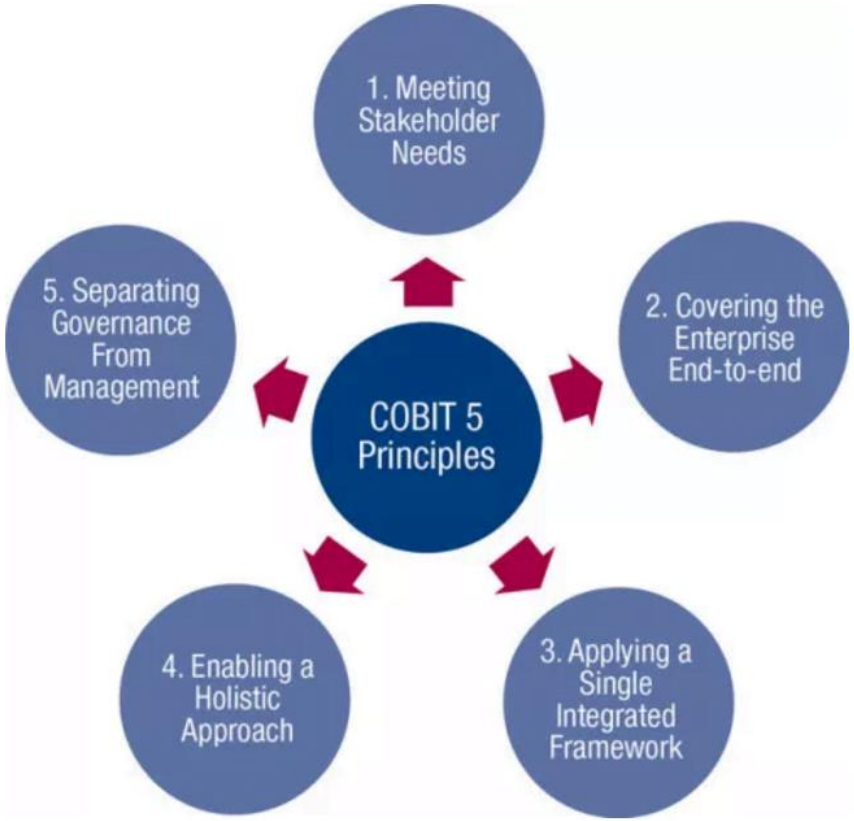
1. HITRUST CSF (Health Information Trust Alliance Common Security Framework)
2. PCI DSS (Payment Card Industry Data Security Standard)

COBIT

- Dikeluarkan oleh ISACA, sekarang versi 5
- Fokus awalnya untuk mengurangi risiko teknis di organisasi
- Berkembang di COBIT 5 untuk menselaraskan IT dengan bisnis/rencana strategis
  - Keseimbangan tingkat risiko dan penggunaaan sumber daya
  - Terdapat pemisahan yang tegas antara governance dengan management

Cobit 5


Meeting Stakeholder Needs
Single Integrated Framework
Separating Governance from Management
Covering the Enterprise End-to-End
01
02
03
04
05
06
07
End-to-End Coverage
Enabling a Holistic Approach
Tailoring to the Organization


1. Meeting Stakeholder Needs
2. Covering the Enterprise End-to-end
3. Applying a Single Integrated Framework
4. Enabling a Holistic Approach
5. Separating Governance From Management
COBIT 5 Principles

ISO 27001/27002

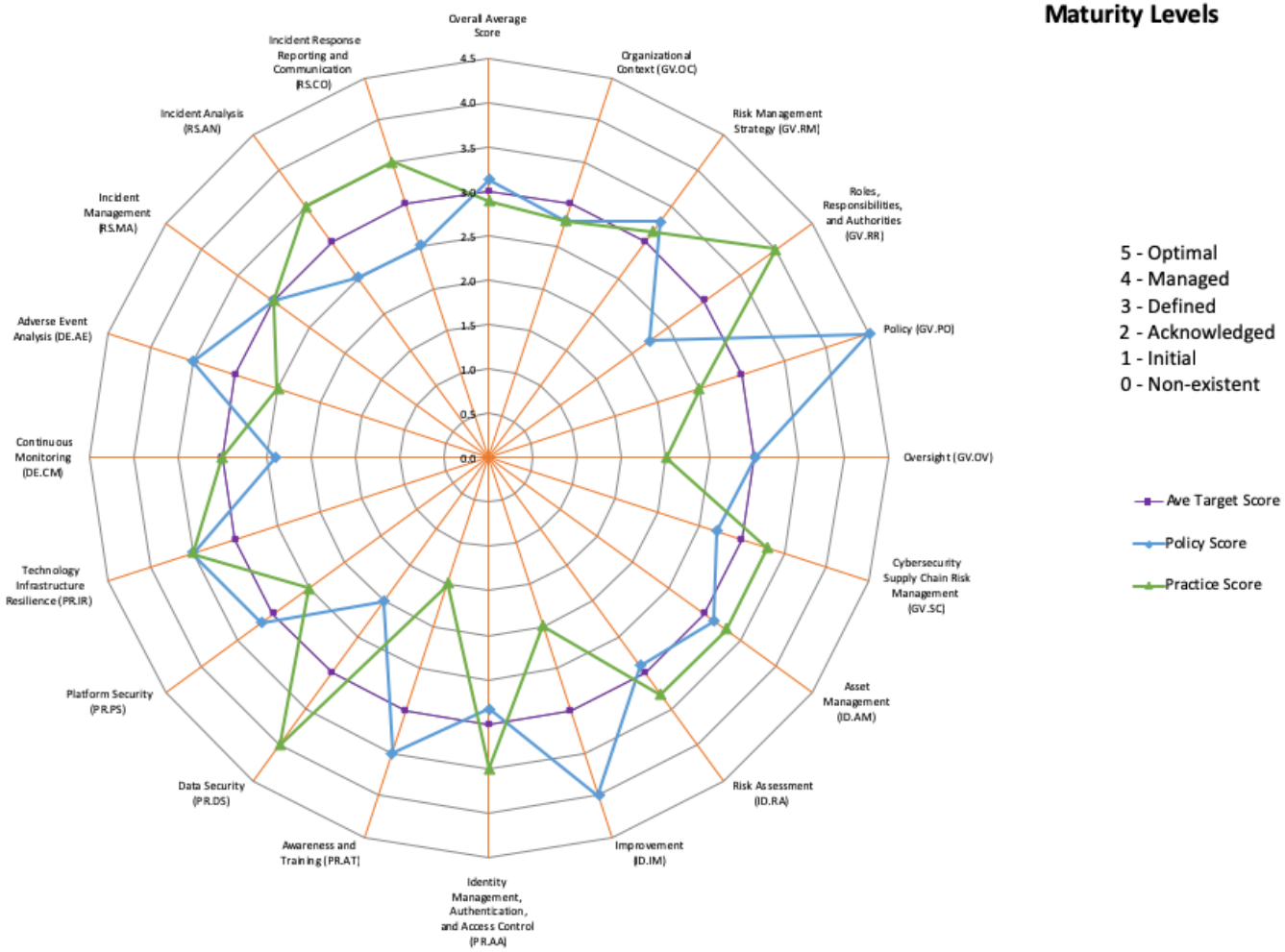
- The grandfather of all other standards
- Dikembangkan untuk memenuhi kebutuhan organisasi internasional atau global
- ISO menggunakan pendekatan berbasis risiko dan teknologi netral
- Mendefinisikan proses perencanaan (**PDCA**) menjadi enam bagian:
  1. Tentukan kebijakan keamanan
  2. Tentukan ruang lingkup Sistem Manajemen Keamanan Informasi
  3. Lakukan penilaian risiko
  4. Kelola risiko yang teridentifikasi
  5. Pilih tujuan dan kontrol yang akan diterapkan
  6. Siapkan pernyataan penerapan

NIST CSF

- Security best practice framework
- Dikembangkan oleh pemerintah US untuk menjadi framework keamanan siber berbasis risiko
- Awalnya dirancang untuk keuangan negara, energi, kesehatan, dan sistem penting lainnya untuk melindungi informasi dan aset fisik mereka dari serangan dunia maya
- Mudah diadaptasi atau disesuaikan untuk kebutuhan masing-masing perusahaan

	Function	Category	ID
What processes and assets need protection?	Identify	Asset Management	ID.AM
		Business Environment	ID.BE
		Governance	ID.GV
		Risk Assessment	ID.RA
		Risk Management Strategy	ID.RM
		Supply Chain Risk Management	ID.SC
What safeguards are available?	Protect	Identity Management & Access Control	PR.AC
		Awareness and Training	PR.AT
		Data Security	PR.DS
		Information Protection Processes & Procedures	PR.IP
		Maintenance	PR.MA
		Protective Technology	PR.PT
What techniques can identify incidents?	Detect	Anomalies and Events	DE.AE
		Security Continuous Monitoring	DE.CM
		Detection Processes	DE.DP
What techniques can contain impacts of incidents?	Respond	Response Planning	RS.RP
		Communications	RS.CO
		Analysis	RS.AN
		Mitigation	RS.MI
		Improvements	RS.IM
What techniques can restore capabilities?	Recover	Recovery Planning	RC.RP
		Improvements	RC.IM
		Communications	RC.CO

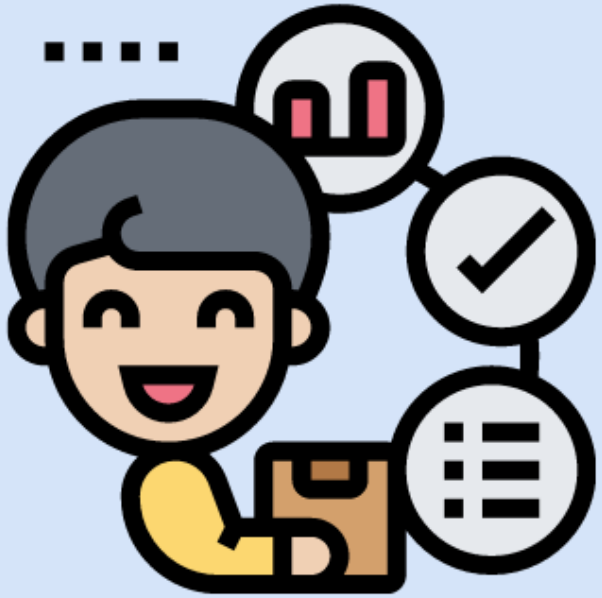
	NIST CSF 2.0 Categories	# of Controls	Target Score	2024 Policy Score	2024 Practice Score
	Overall Average Score		3.00	3.14	2.85
GOVERN (GV)	Organizational Context (GV.OC)	(5)	3.00	2.80	2.80
	Risk Management Strategy (GV.RM)	(7)	3.00	3.29	3.14
	Roles, Responsibilities, and Authorities (GV.RR)	(4)	3.00	2.25	4.00
	Policy (GV.PO)	(2)	3.00	4.50	2.50
	Oversight (GV.OV)	(3)	3.00	3.00	2.00
	Cybersecurity Supply Chain Risk Management (GV.SC)	(10)	3.00	2.70	3.30
IDENTIFY (ID)	Asset Management (ID.AM)	(7)	3.00	3.14	2.71
	Risk Assessment (ID.RA)	(10)	3.00	2.90	3.30
	Improvement (ID.IM)	(4)	3.00	4.00	2.00
PROTECT (PR)	Identity Management, Authentication, and Access Control (PR.AA)	(6)	3.00	2.83	3.50
	Awareness and Training (PR.AT)	(2)	3.00	3.50	1.50
	Data Security (PR.DS)	(4)	3.00	2.00	4.00
	Platform Security (PR.PS)	(6)	3.00	3.17	2.50
	Technology Infrastructure Resilience (PR.IR)	(4)	3.00	3.50	3.50
DETECT (DE)	Continuous Monitoring (DE.CM)	(5)	3.00	2.40	3.00
	Adverse Event Analysis (DE.AE)	(6)	3.00	3.50	2.50
RESPOND (RS)	Incident Management (RS.MA)	(5)	3.00	3.00	3.00
	Incident Analysis (RS.AN)	(4)	3.00	2.50	3.50
	Incident Response Reporting and Communication (RS.CO)	(2)	3.00	2.50	3.50
	Incident Mitigation (RS.MI)	(2)	3.00	4.50	1.50
RECOVER (RC)	Incident Recovery Plan Execution (RC.RP)	(6)	3.00	2.50	3.50
	Incident Recovery Communication (RC.CO)	(2)	3.00	4.50	1.50



Indeks Keamanan Informasi (KAMI)

- Diterbitkan oleh BSSN
- Digunakan sebagai alat bantu untuk melakukan asesmen dan evaluasi tingkat kesiapan penerapan keamanan informasi berdasarkan kriteria SNI ISO/IEC 27001
  - **Utama**: Tata Kelola, Pengelolaan Risiko, Kerangka Kerja, Pengelolaan Aset, Aspek Teknologi
  - **Suplemen**: Pengamanan Keterlibatan Pihak Ketiga Penyedia Layanan, Pengamanan Layanan Infrastruktur Awan dan Perlindungan Data Pribadi.
- Tidak untuk menganalisis kelayakan atau efektivitas pengamanan, tetapi untuk memberikan gambaran kesiapan kerangka kerja keamanan informasi.

Indeks KAMI dan ISO27001



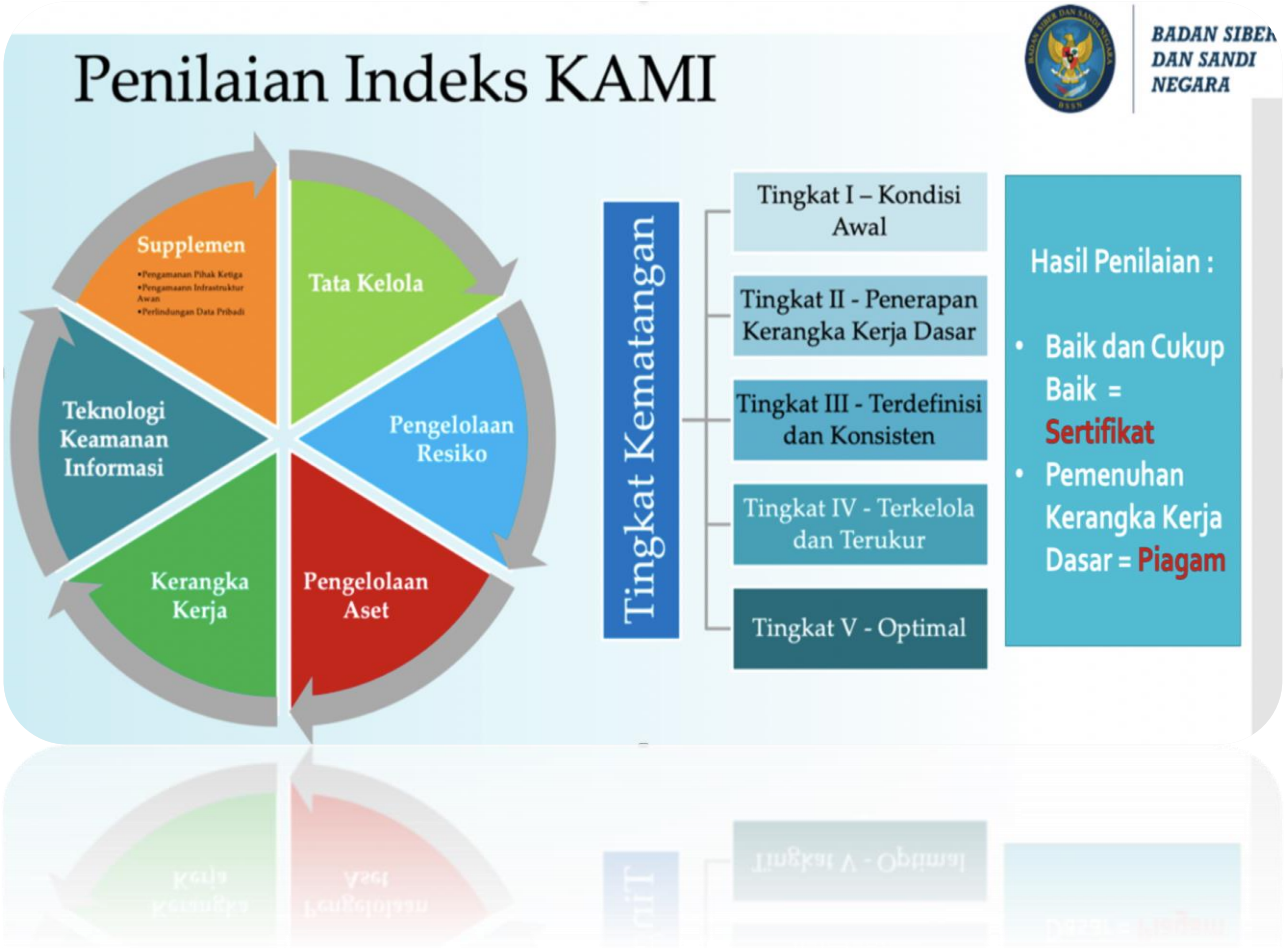
Indeks KAMI adalah alat evaluasi untuk menganalisa tingkat kesiapan pengamanan informasi di suatu organisasi. Ruang lingkup pembahasan memenuhi aspek keamanan yang didefinisikan oleh standar **ISO/IEC 27001:2013**.

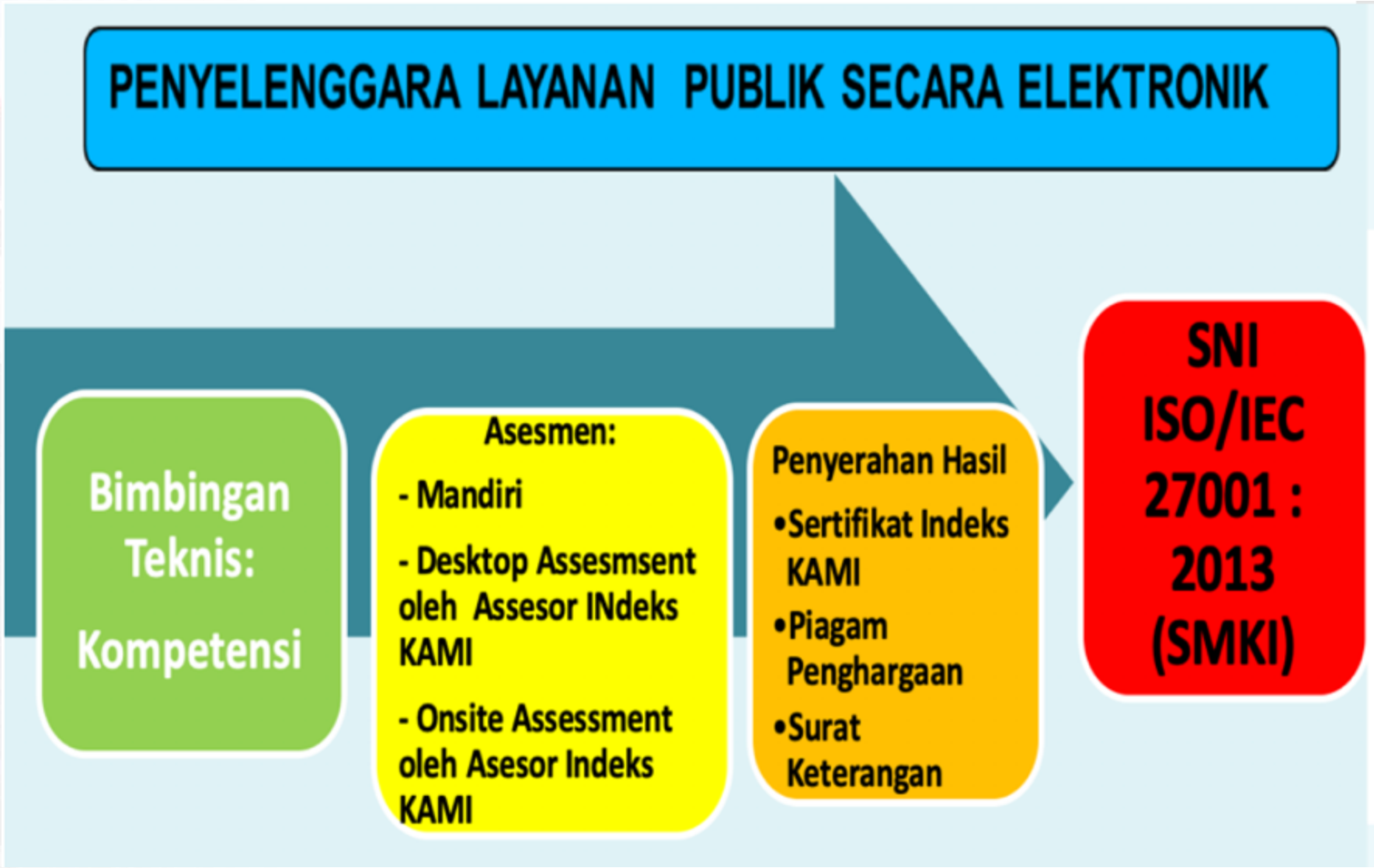
No.	Kontrol Baru pada SNI ISO/IEC 27001:2022	Penambahan pada Indeks KAMI
1	Threat intelligence	Aspek Kerangka Kerja
2	Information security for cloud services	Aspek Pengelolaan Aset
3	ICT readiness for business continuity	Aspek Kerangka Kerja
4	Physical security monitoring	Aspek Teknologi
5	Configuration management	Aspek Teknologi
6	Information deletion	Aspek Pengelolaan Aset
7	Data masking	Aspek Pengelolaan Aset
8	Data leakage prevention	Aspek Teknologi
9	Monitoring activities	Aspek Teknologi
10	Web filtering	Aspek Teknologi
11	Secure coding	Aspek Teknologi

Indeks Keamanan Informasi (KAMI)

- Indeks Keamanan Informasi (KAMI) merupakan aplikasi yang digunakan sebagai alat bantu untuk melakukan asesmen dan evaluasi tingkat kesiapan (Kelengkapan dan Kematangan) penerapan keamanan informasi berdasarkan kriteria SNI ISO/IEC 27001. Proses evaluasi dilakukan melalui sejumlah pertanyaan di beberapa area berikut:

1. Kategori Sistem Elektronik yang digunakan
2. Tata Kelola Keamanan Informasi
3. Pengelolaan Risiko Keamanan Informasi
4. Kerangka Kerja Keamanan Informasi
5. Pengelolaan Aset Informasi
6. Teknologi dan Keamanan Informasi
7. Suplemen (Tambahan pengukuran dilakukan untuk aspek Pengamanan Keterlibatan Pihak Ketiga Penyedia Layanan, Pengamanan Layanan Infrastruktur Awan (Cloud Service) dan Perlindungan Data Pribadi.




PENYELENGGARA LAYANAN PUBLIK SECARA ELEKTRONIK
Bimbingan Teknis:
Kompetensi
Asesmen:
- Mandiri
- Desktop Assesmsent oleh Assesor INdeks KAMI
- Onsite Assessment oleh Asesor Indeks KAMI
Penyerahan Hasil
•Sertifikat Indeks KAMI
•Piagam Penghargaan
•Surat Keterangan
SNI ISO/IEC 27001 : 2013 (SMKI)

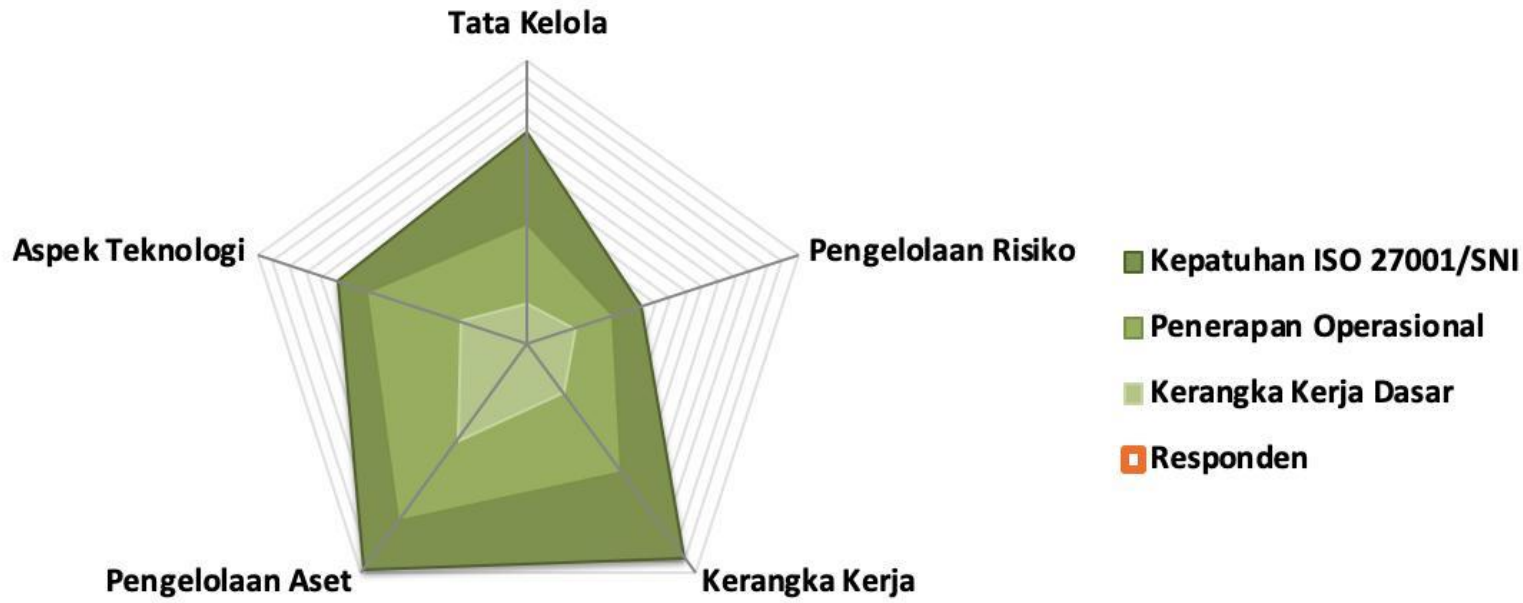
Indeks KAMI (Keamanan Informasi)

Responden:
Satuan Kerja
Direktorat
Departemen

Alamat 1
Alamat 2
Kota Kode Pos

(Kode Area) Nomor Telpon
user@departemen_responden.go.id
HH/BB/TTTT

Skor Kategori SE	**: 10**	**Kategori SE**	**Rendah**	
Hasil Evaluasi Akhir:	**Tidak Layak**			
Tingkat Kelengkapan Penerapan Standar ISO27001				**0**
Tata Kelola	: 0	Tk Kematangai	I	
Pengelolaan Risiko	: 0	Tk Kematangan	I	I
Kerangka Kerja Keamanan Informas	: 0	Tk Kematangan	I	s/d
Pengelolaan Aset	: 0	Tk Kematangan	I	I
Teknologi dan Keamanan Informasi	: 0	Tk Kematangan	I	
Pengamanan Keterlibatan Pihak Ke	: 0%			
Pengamanan Layanan Infrastruktur	: 0%			
Perlindungan Data Pribadi	: 0%			



Sumber:
https://www.bssn.go.id/indeks-kami/
indeks KAMI

The Problems

- Dalam prakteknya, CSF sangat banyak, lalu bagaimana memilihnya?
- Top → Bottom
  - Perlu input yang tepat dari stakeholders
  - Tanyakan ke stakeholder 3 tujuan utama program keamanan: Business need, Reputation, Stacking
  - Identifikasikan informasi demografis seperti: *jenis industri, lokasi, jenis data yang ditangani*
- Apapun rekomendasinya sesuaikan dengan kebutuhan!

Bagaimana Memilih Framework

- **Kebutuhan Bisnis: Apakah...**
  - Apakah yang diinginkan pelanggan / calon pelanggan kita?
  - Apakah kami secara kontrak diharuskan untuk menyediakan?
  - Apakah akan meningkatkan pendapatan?
  - Apakah standar regulasi yang mengikat kita di seluruh dunia?
  - Apakah ada biaya pelaksanaan, pemeliharaan, dan sertifikasi?

Bagaimana Memilih Framework

- **Reputation: Apa yang akan...**
  - Puaskah pelanggan yang mungkin menggunakan standar berbeda?
  - Menjawab RFP 400 pertanyaan hanya dengan memberikan sertifikasi atau laporan?
  - Menarik perhatian pengunjung ke website perusahaan?
- **Stacking: Akankah standar ...**
  - Memenuhi semua atau sebagian besar persyaratan yang sama dengan standar lain yang perlu dipenuhi?
  - Mengizinkan untuk menambah standar lain yang ingin dikejar?

Bagaimana Mengimplementasikan *Security Framework* ?

Cybersecurity Best Practices

- Menurut Center for Internet Security, ada lima kontrol yang dianggap paling mendasar dan berharga yang harus dilakukan setiap perusahaan:

1. Inventaris perangkat resmi dan tidak resmi
2. Inventaris perangkat lunak resmi dan tidak resmi
3. Konfigurasi secara aman hardware dan software di perangkat seluler, laptop, workstation, dan server
4. Penilaian dan perbaikan kerentanan yang berkelanjutan
5. Penggunaan hak administratif yang terkontrol

1. Inventaris Perangkat Resmi dan Tidak Resmi

Kelola secara aktif (inventaris, lacak, dan perbaiki) semua perangkat keras di jaringan sehingga hanya perangkat resmi yang diberi akses, dan perangkat yang tidak sah dan tidak terkelola ditemukan dan dicegah untuk mendapatkan akses.

1. Bangun inventaris sistem di jaringan
2. Gunakan DHCP untuk meningkatkan inventaris aset dan membantu mendeteksi sistem yang tidak dikenal
3. Pastikan semua akuisisi peralatan baru secara otomatis memperbarui sistem inventaris
4. Menjaga inventaris aset dari semua sistem yang terhubung ke jaringan
5. Menerapkan otentikasi tingkat jaringan (Kontrol Akses Jaringan)
6. Gunakan sertifikat klien untuk memvalidasi dan mengautentikasi sistem

2. Inventaris perangkat lunak resmi dan tidak resmi

Kelola secara aktif (inventaris, lacak, dan perbaiki) semua perangkat lunak di jaringan sehingga hanya perangkat lunak resmi yang diinstal dan dapat dijalankan, dan perangkat lunak yang tidak sah dan tidak dikelola ditemukan serta dicegah dari penginstalan atau pelaksanaan.

1. Buat daftar perangkat lunak resmi dan versi yang diperlukan di perusahaan
2. Terapkan whitelist aplikasi
3. Menyebarkan alat inventaris perangkat lunak ke seluruh organisasi
4. Mesin virtual dan / atau sistem cloud harus digunakan untuk mengisolasi dan menjalankan aplikasi

3. Konfigurasi hardware dan software secara aman

Menetapkan, menerapkan, dan secara aktif mengelola (melacak, melaporkan, memperbaiki) konfigurasi keamanan laptop, server, dan workstation menggunakan manajemen konfigurasi yang ketat dan mengubah proses kontrol untuk mencegah penyerang mengeksploitasi layanan dan pengaturan yang rentan.

1. Menetapkan standar konfigurasi aman untuk SO dan software
2. Terapkan manajemen konfigurasi yang ketat, menggunakan image yang aman saat membangun semua sistem baru yang diterapkan di perusahaan
3. Simpan master image di server yang dikonfigurasi dengan aman, divalidasi dengan alat pemeriksa integritas
4. Lakukan semua administrasi remote server, workstation, perangkat jaringan, dan peralatan serupa melalui saluran aman

4. Penilaian dan perbaikan kerentanan yang berkelanjutan

Lakukan asesmen terhadap informasi baru secara terus-menerus untuk mengidentifikasi kerentanan, memulihkan, dan meminimalkan peluang bagi penyerang.

1. Jalankan alat vulnerability scanning otomatis terhadap semua sistem di jaringan
2. Mengorelasikan event log dengan informasi dari vulnerability scans
3. Lakukan vulnerability scanning dalam mode terautentikasi
4. Berlangganan ke layanan intelligent vulnerability
5. Terapkan alat manajemen patch dan update software otomatis
6. Pantau log yang terkait dengan aktivitas scanning dan akun administrator terkait

5. Penggunaan Hak Istimewa Administratif yang Terkendali

Gunakan alat untuk melacak/mengontrol/mencegah/memperbaiki penggunaan, task, dan konfigurasi hak akses administratif pada komputer, jaringan, dan aplikasi.

1. Minimalkan hak istimewa administrator dan hanya gunakan akun administrator bila diperlukan
2. Gunakan tool otomatis untuk menginventarisir semua akun administratif dan memvalidasinya
3. Sebelum menggunakan perangkat baru di lingkungan jaringan, ubah semua kata sandi default
4. Konfigurasikan sistem untuk mencatat log dan peringatan ketika akun ditambahkan atau dihapus dari grup administrator domain
5. Konfigurasikan sistem untuk mencatat log dan peringatan untuk setiap login yang gagal ke akun administrator

PRAKTEK INDEKS KAMI

Indeks KAMI (Keamanan Informasi) Versi 5.0

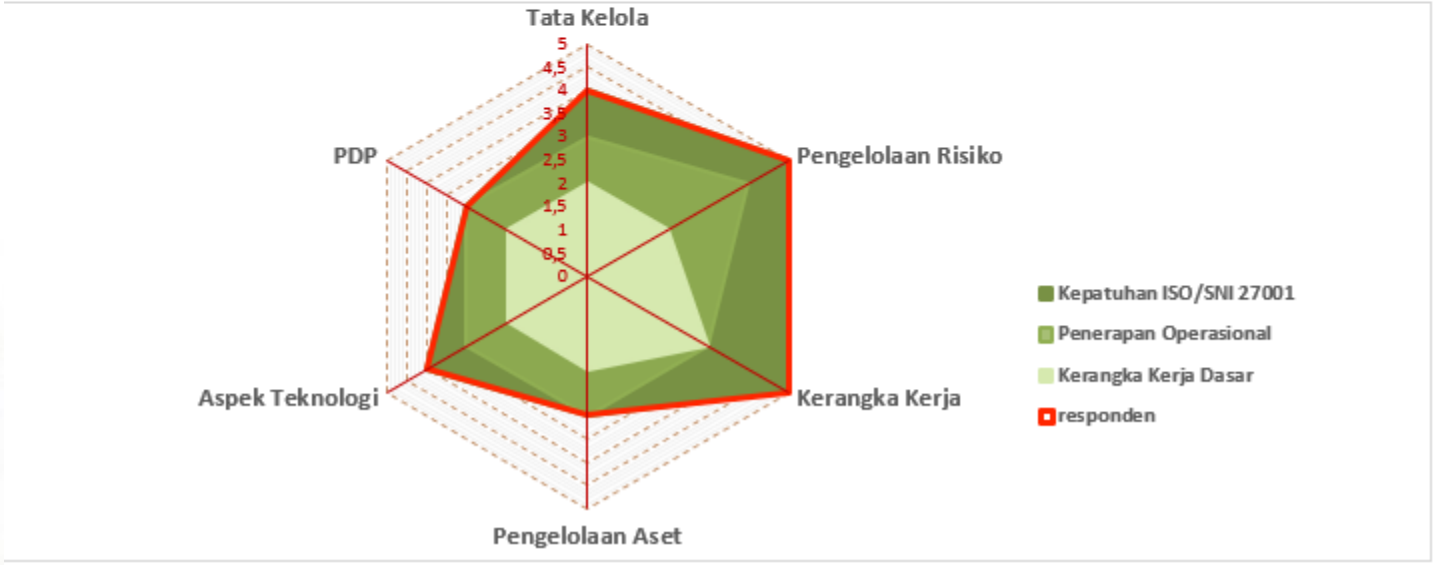
Responden:
Satuan Kerja
Direktorat
Departemen

Alamat 1
Alamat 2
Kota Kode Pos

(Kode Area) Nomor Telpon
user@departemen_responden.go.id
HH/BB/TTTT

Skor Kategori SE	: 44	Kategori SE	Strategis
Hasil Evaluasi Akhir:		**Baik**	
Tingkat Kelengkapan Penerapan Standar			**918**

Tata Kelola	: 126	T. Kematangan	IV	
Pengelolaan Risiko	: 72	T. Kematangan	V	III
Kerangka Kerja Keamanan Informasi	: 192	T. Kematangan	V	s/d
Pengelolaan Aset	: 258	T. Kematangan	III	V
Teknologi dan Keamanan Informasi	: 186	T. Kematangan	IV	
Pelindungan Data Pribadi	: 84	T. Kematangan	III	
Pengamanan Keterlibatan P.Ketiga	: 100	%		



Tugas Evaluasi Indeks Kami

- Evaluasi Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks Keamanan Informasi (Indeks KAMI) Versi 5 di instansi masing-masing Bapak/Ibu/Sdr Bekerja !
- Buatlah laporan dan Analisislah hasil dari indek KAMI di Instansi Bapak/Ibu/Sdr Bekerja !

Any Questions..?

UNIVERSITAS
AMIKOM
YOGYAKARTA