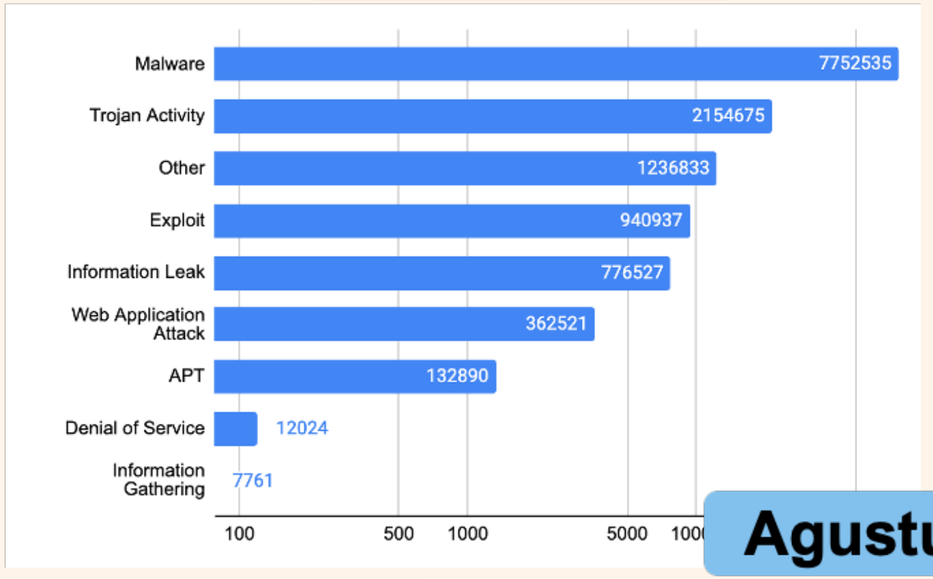
SOSIALISASI IMPELEMENTASI KEAMANAN INFORMASI, KEAMANAN SIBER, DAN DATA PRIVASI

ISO27001:2022

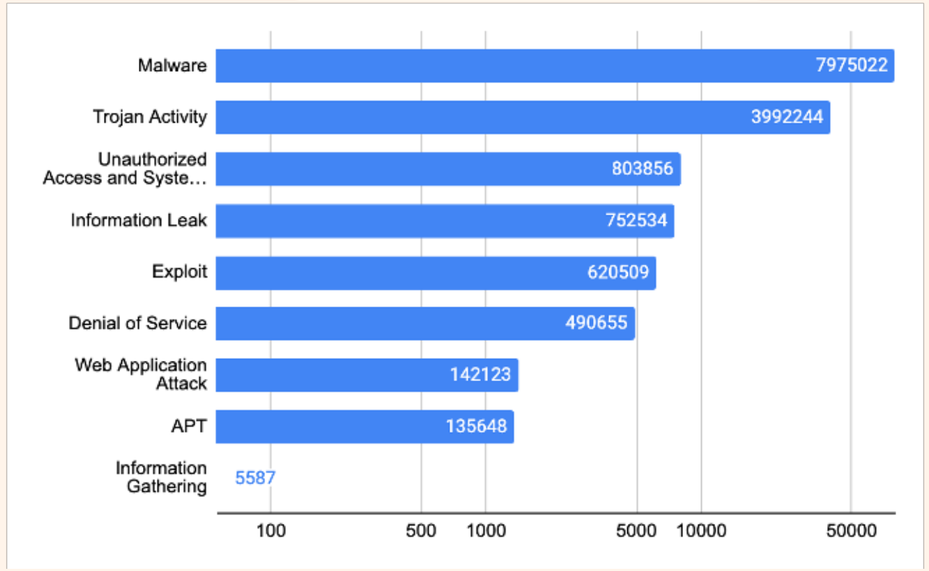
Landskap Ancaman Siber Indonesia

Landskap Ancaman Siber Indonesia

Juli 2024

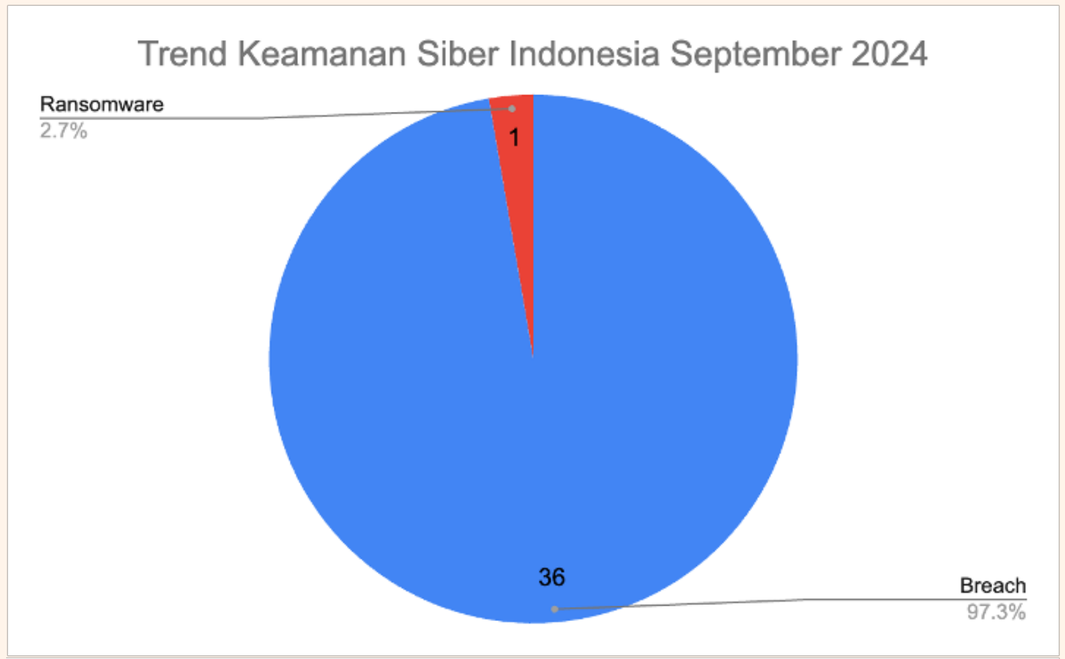


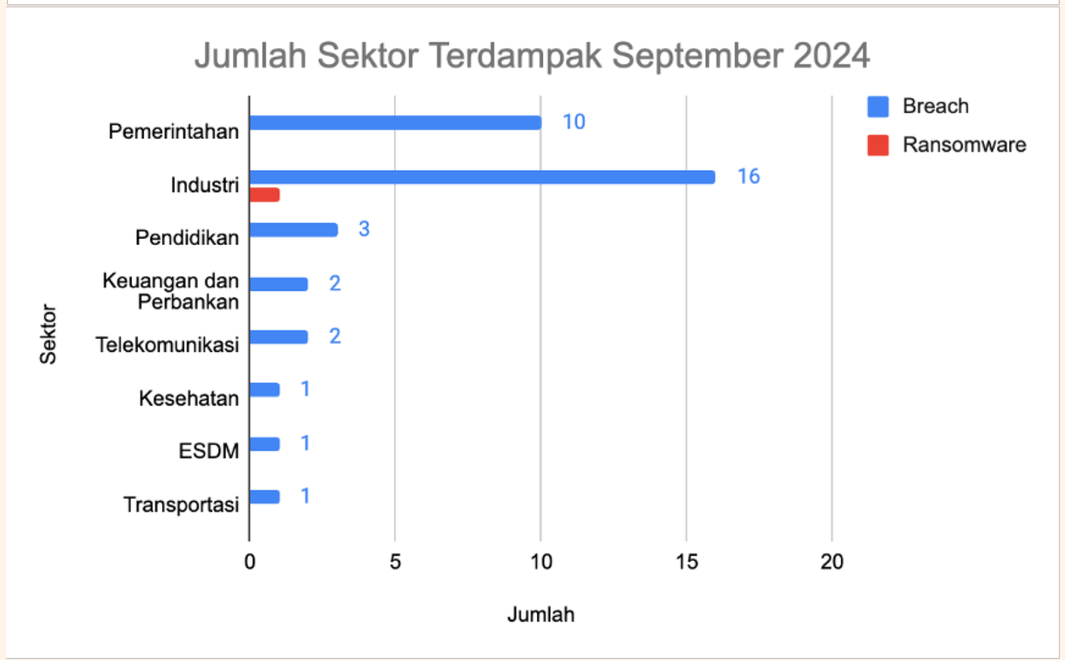
Agustus 2024



Sumber: Laporan Hasil Monitoring Bulanan IDSIRTII Tahun 2024

Landskap Ancaman Siber Indonesia





sumber : CTI & OSINT

Landskap Ancaman Siber Indonesia

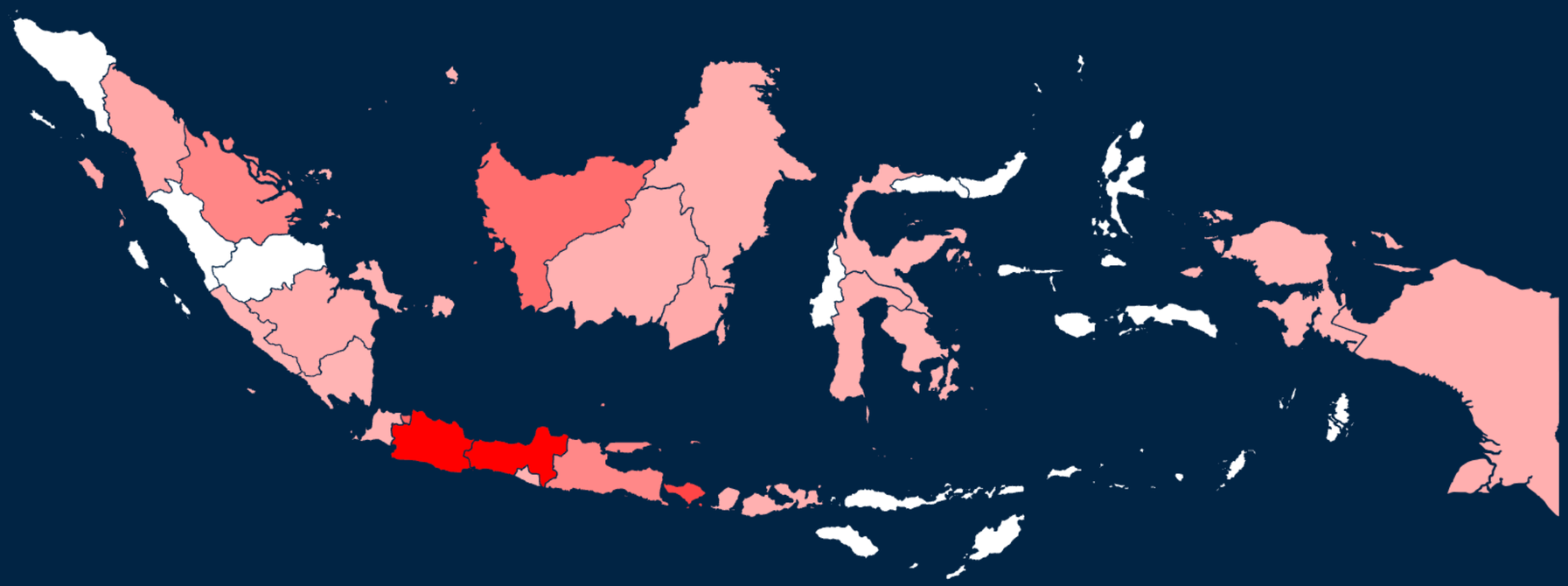
INFORMASI SERANGAN SIBER

TARGET SERANGAN - [2024-10-18 S/D 2024-11-18]

DUNIA | INDONESIA

PERINGKAT SERANGAN

US	12,768,440
CN	1,074,656
GB	751,853
RU	706,607
_V2_REGION_NA	548,515



0 — 5,078,710

FROM: 2024-10-18 TO: 2024-11-18

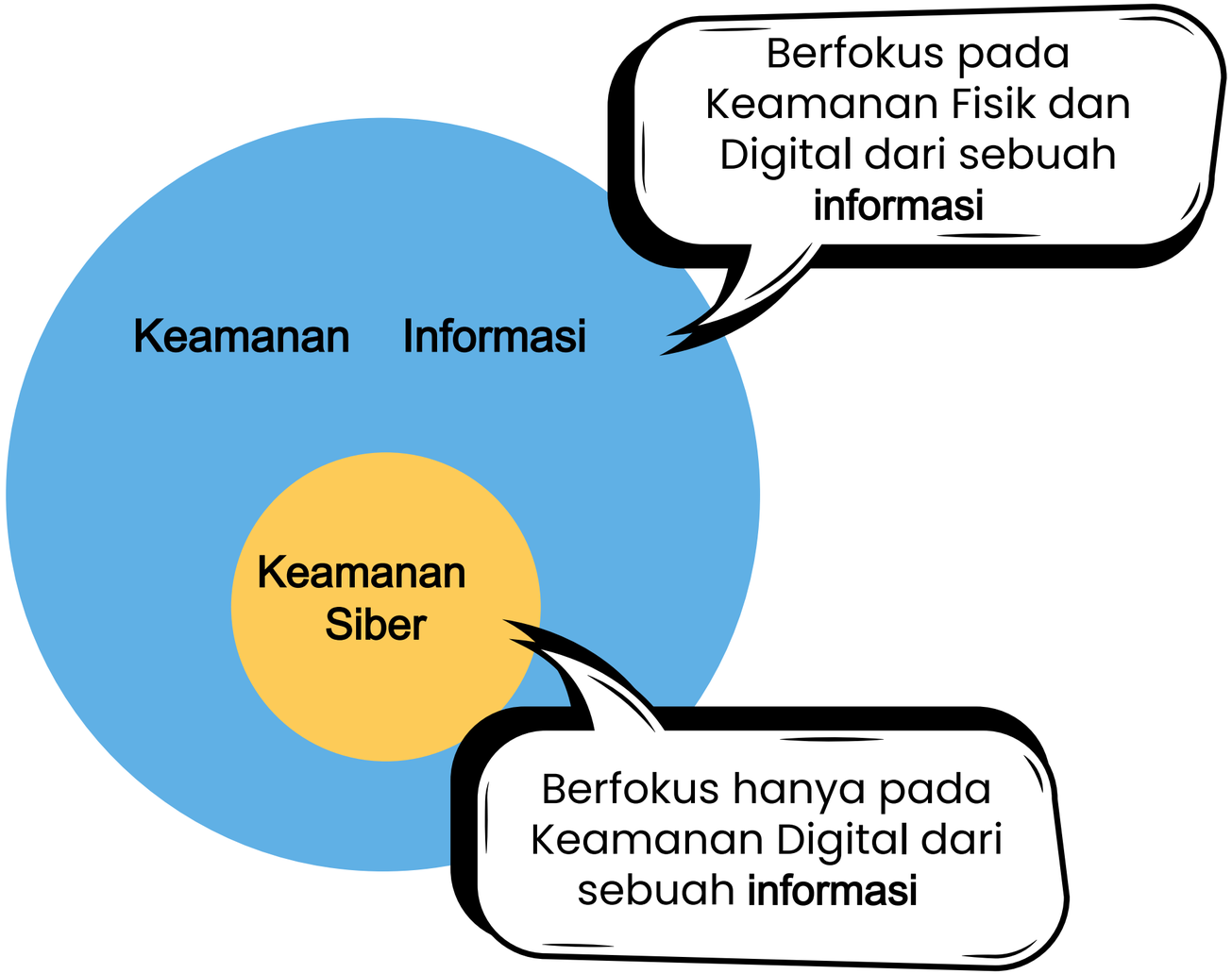
LIVE FEED

TIME	COUNTRY	PORT

sumber : bssn.go.id

Keamanan Informasi & Keamanan Siber

Keamanan Informasi & Keamanan Siber



Apa itu Informasi ?

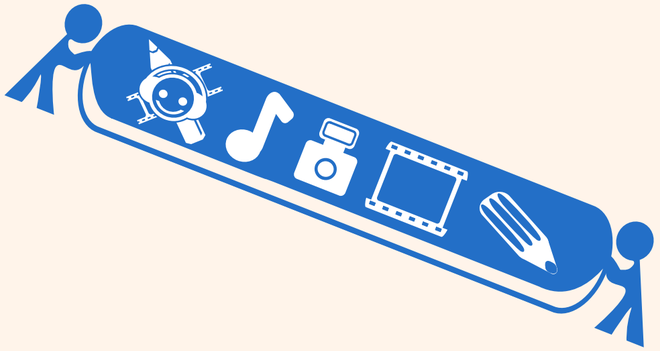
Informasi adalah **DATA** yang telah diolah sehingga memiliki makna bagi penerima atau pengguna.

Dapat dianggap sebagai **ASET** karena memiliki nilai yang penting dalam berbagai konteks.

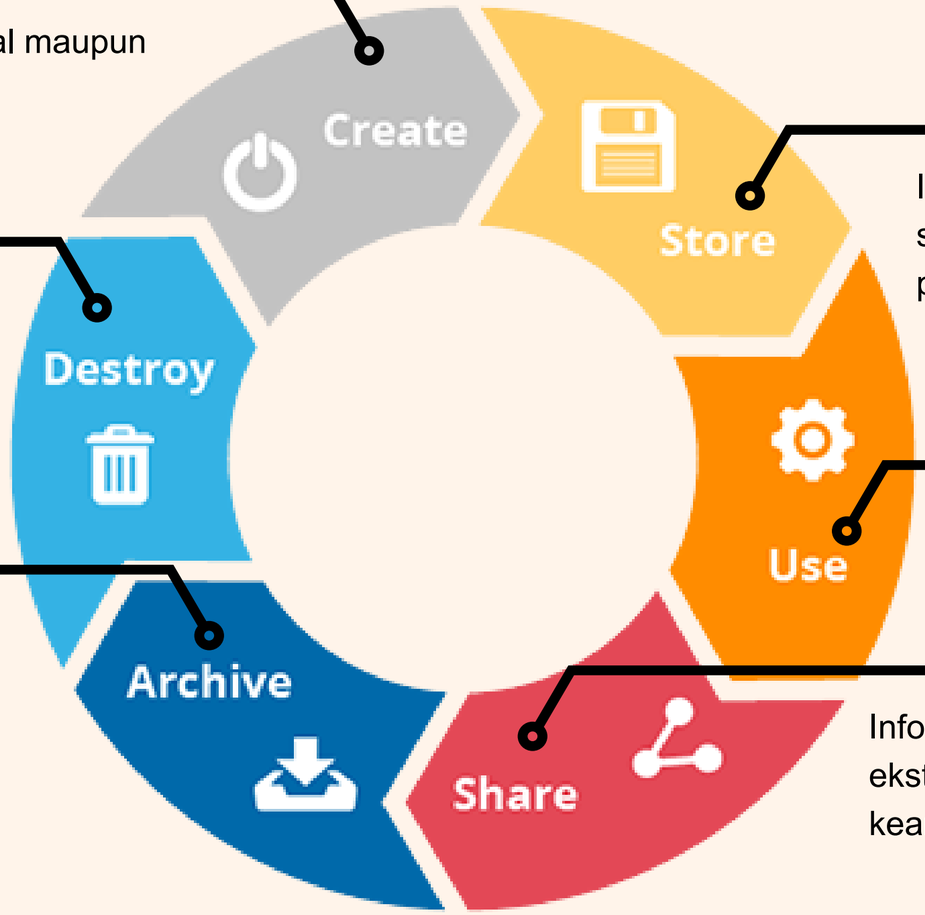
Data = Informasi = Aset

Informasi dapat menjadi aset dalam bisnis karena dapat digunakan untuk mengambil keputusan yang tepat, mengidentifikasi peluang baru, dan meningkatkan efisiensi operasional.

Siklus Hidup Informasi



Informasi dibuat, baik berupa data digital maupun fisik



Informasi disimpan di lokasi yang aman, seperti database, file server, atau penyimpanan lokal .

Informasi digunakan untuk mendukung kegiatan operasional atau pengambilan keputusan .

Informasi dibagikan, baik secara internal maupun eksternal, dengan tetap mempertimbangkan keamanan dan privasi .

Informasi yang sudah tidak diperlukan dihancurkan secara aman untuk mencegah kebocoran .

Informasi yang sudah tidak aktif dipindahkan ke arsip untuk penyimpanan jangka panjang .

Klasifikasi Informasi

Public	Internal Only	Confidential	Restricted
Data that may be freely disclosed to the public	Internal data not meant for public disclosure	Sensitive data that if compromised could negatively affect operations	Highly sensitive corporate data that if compromised could put the organization at financial or legal risk.

Konsep Dasar
Keamanan Informasi

Menjaga **kerahasiaan** informasi dengan cara memastikan informasi hanya dapat diakses oleh pihak yang berwenang.

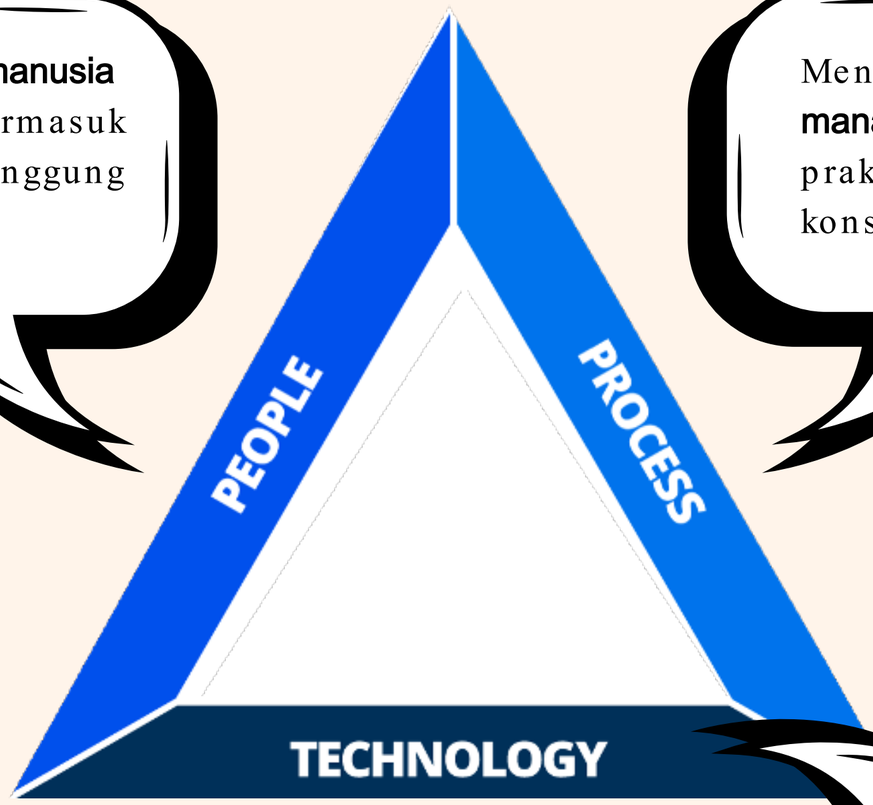
Menjaga **keaslian** informasi dengan cara mastikan akurasi, kelengkapan dan metode pengolahannya.

Menjaga **ketersediaan** informasi dengan cara memastikan informasi selalu dapat di akses pada saat dibutuhkan.

Pilar Keamanan Informasi & Keamanan Siber

Menekankan pentingnya **peran manusia** dalam menjaga keamanan, termasuk kesadaran, pelatihan, dan tanggung jawab individu

Mencakup **kebijakan, prosedur, dan manajemen risiko** untuk memastikan praktik keamanan diterapkan secara konsisten



Mendukung keamanan melalui sistem maupun alat-alat **parimeter keamanan** yang dapat diimplementasikan

Pengenalan ISO27001

Pengenalan ISO27001
mengapa perlu ?

COMPANY BRANDING

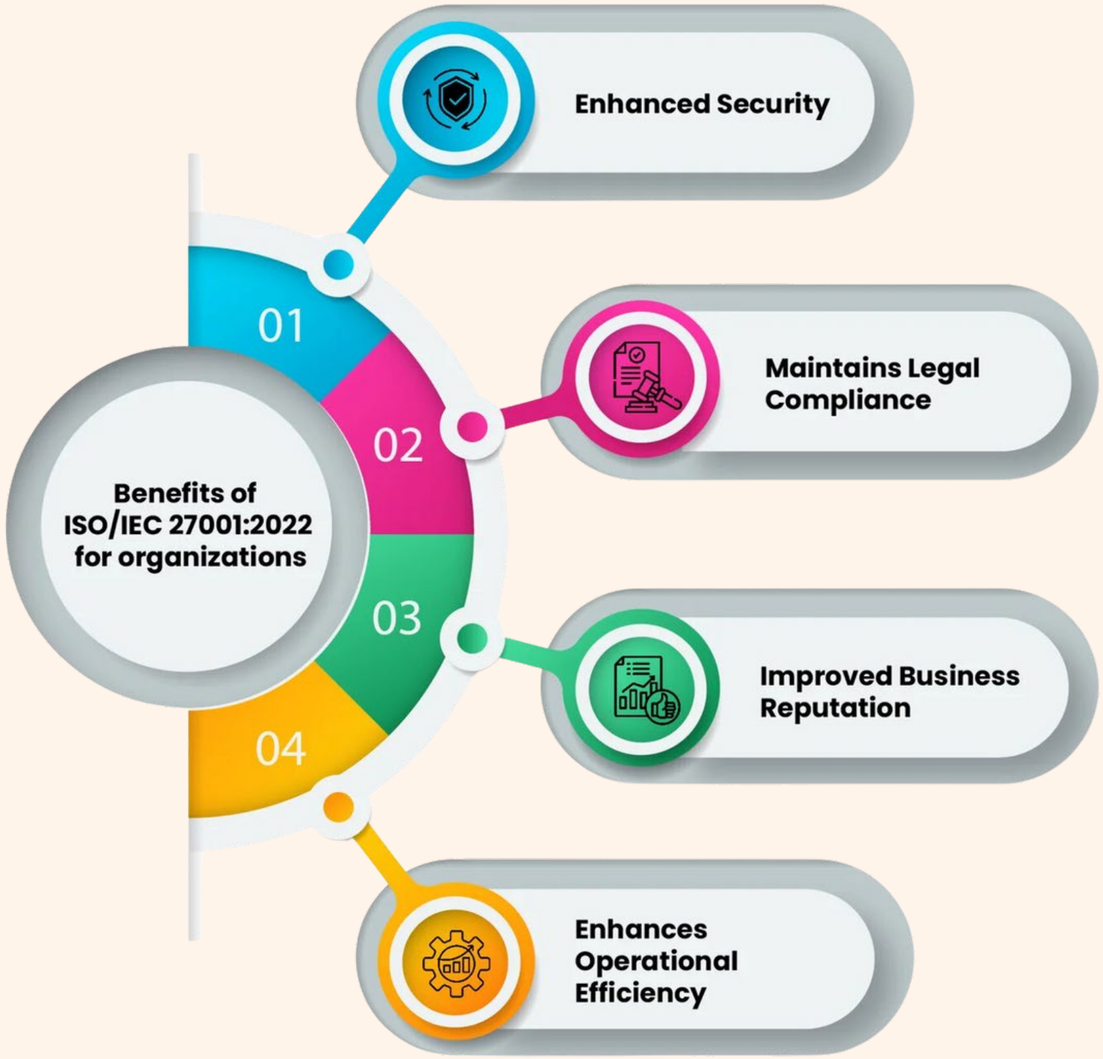
- Menerapkan standar ISO27001 dapat memiliki dampak positif terhadap citra dan reputasi perusahaan .
- Menunjukkan kepada klien, pelanggan, dan pemangku kepentingan bahwa organisasi serius pada keamanan informasi .

ORGANIZATION IMPROVEMENT

- Dapat menjadi alat yang kuat untuk meningkatkan efektivitas, efisiensi, dan ketahanan organisasi secara keseluruhan .
- Bukan hanya tentang memastikan kepatuhan terhadap standar, tetapi juga tentang meningkatkan proses bisnis, pengelolaan risiko, dan budaya keamanan informasi di seluruh organisasi .

Pengenalan ISO27001

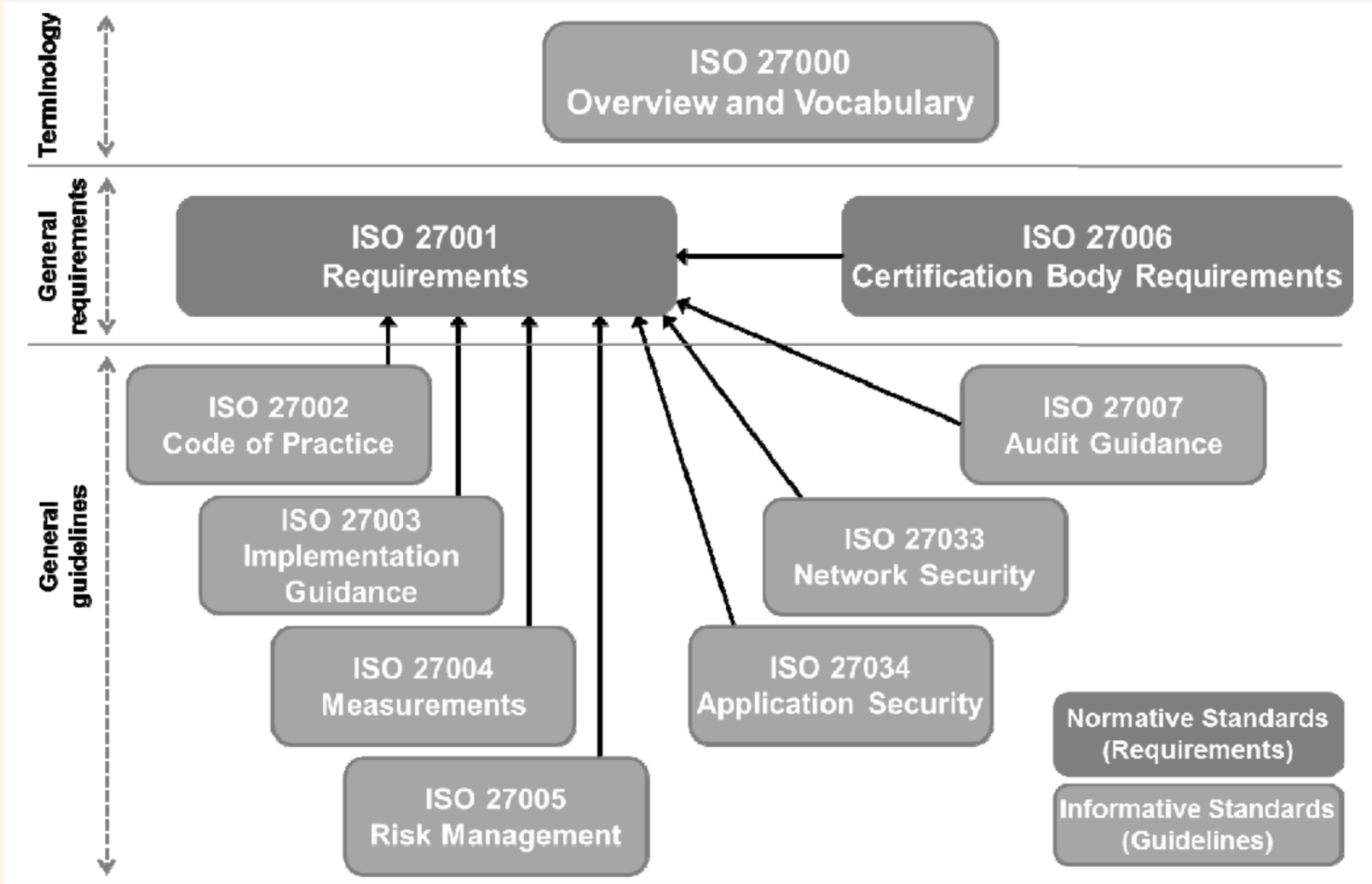
Manfaat Implementasi



Pengenalan ISO27001

- ISO 27001 adalah standar internasional untuk Information Security Management System (ISMS).
- Memberikan kerangka kerja untuk melindungi informasi organisasi secara sistematis dan terukur.
- Berfokus pada aspek keamanan informasi, keamanan siber, dan data pribadi

Standar Keluarga 27000



Standar Keluarga 27000

8.12	Pencegahan kebocoran data	**Kontrol** Langkah-langkah pencegahan kebocoran data harus diterapkan pada sistem, jaringan, dan peranti lain yang memproses, menyimpan, atau mentransmisikan informasi sensitif.

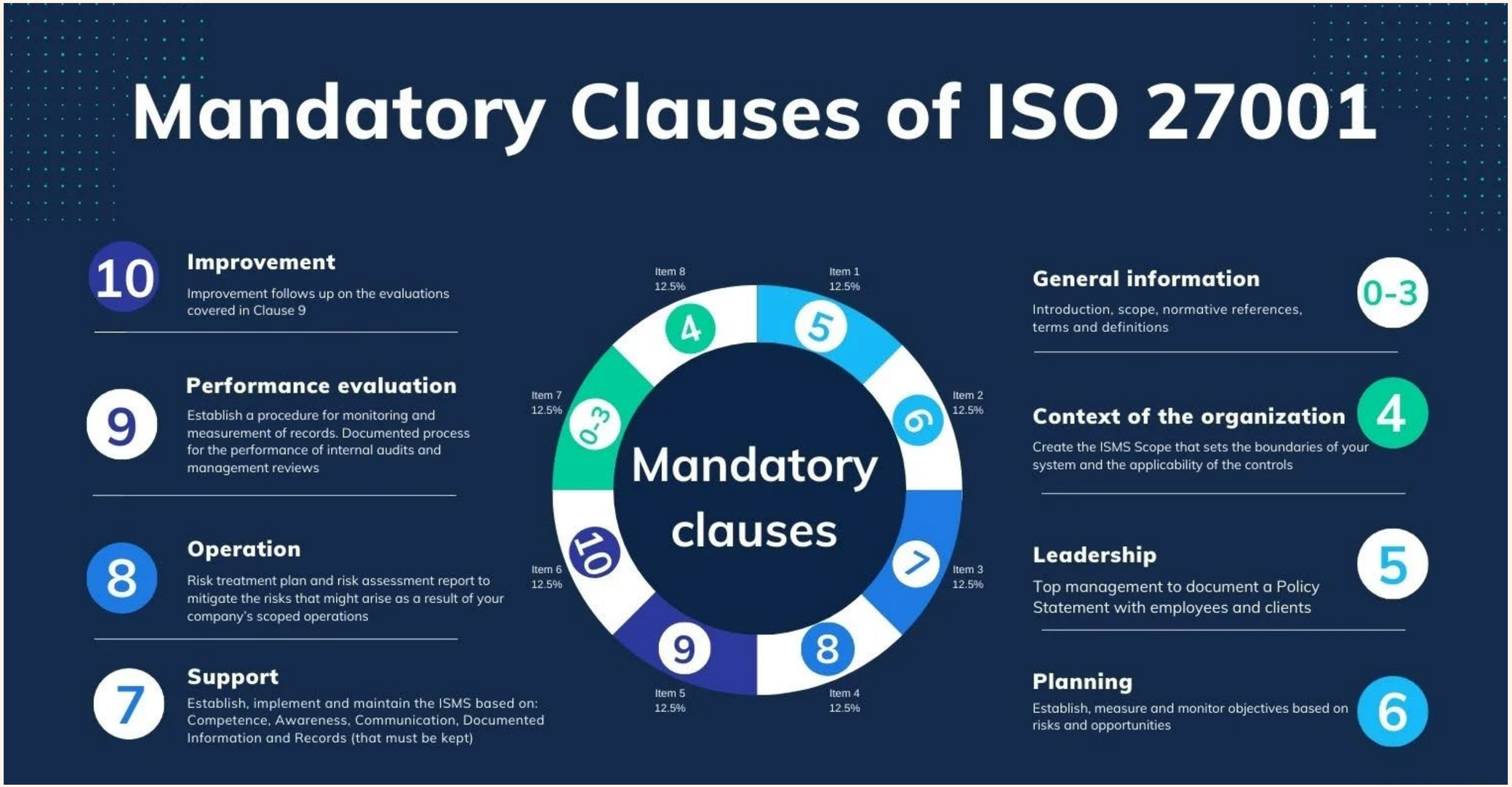
SNI ISO/IEC 27002:2022

Tujuan
Untuk mendeteksi dan mencegah pengungkapan dan ekstraksi informasi yang takterotorisasi oleh individu atau sistem.

Panduan
Organisasi sebaiknya mempertimbangkan hal-hal berikut untuk mengurangi risiko kebocoran data:

a) mengidentifikasi dan mengklasifikasi informasi untuk memproteksi kebocoran (misalnya informasi personal, model penetapan harga, dan desain produk);
b) memonitor saluran kebocoran data (misalnya surel, transfer fail, peranti mobil (*mobile*), dan peranti penyimpanan portabel);
c) bertindak untuk mencegah informasi bocor (misalnya mengarantina surel yang berisi informasi sensitif).

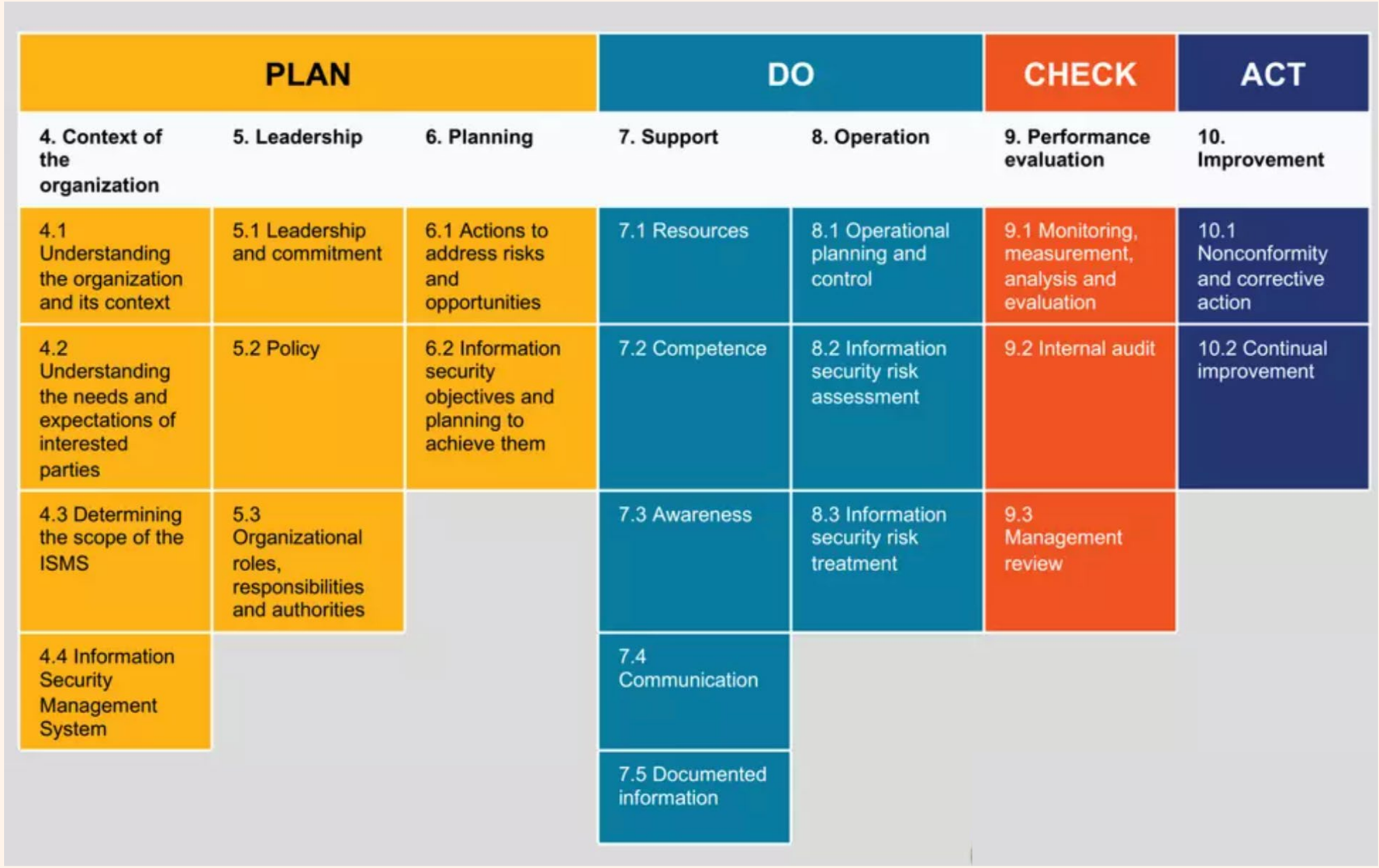
ISO27001


Mandatory Clauses of ISO 27001
10
Improvement
Improvement follows up on the evaluations covered in Clause 9
9
Performance evaluation
Establish a procedure for monitoring and measurement of records. Documented process for the performance of internal audits and management reviews
8
Operation
Risk treatment plan and risk assessment report to mitigate the risks that might arise as a result of your company's scoped operations
7
Support
Establish, implement and maintain the ISMS based on: Competence, Awareness, Communication, Documented Information and Records (that must be kept)
Item 8 12.5%
Item 1 12.5%
Item 7 12.5%
Item 2 12.5%
Item 6 12.5%
Item 3 12.5%
Item 5 12.5%
Item 4 12.5%
Mandatory clauses
General information
Introduction, scope, normative references, terms and definitions
0-3
Context of the organization
Create the ISMS Scope that sets the boundaries of your system and the applicability of the controls
4
Leadership
Top management to document a Policy Statement with employees and clients
5
Planning
Establish, measure and monitor objectives based on risks and opportunities
6

ISO27001


ISO 27001
Annex A Control Themes
New organizational controls include:
5.7: Threat Intelligence
5.23: Information security for use of cloud services
5.30: ICT readiness for business continuity
A.5
Organizational
(37 controls)
A.6
People
(8 controls)
There are no new controls in this area
A.8
Technological
(34 controls)
A.7
Physical
(14 controls)
New technological controls include:
8.9: Configuration management
8.10: Information deletion
8.11: Data masking
8.12: Data leakage prevention
8.16: Monitoring activities
8.23: Web filtering
8.28: Secure coding
New physical controls include:
7.4: Physical security monitoring

ISO27001 PDCA Cycle



PLAN			DO		CHECK	ACT
4. Context of the organization	5. Leadership	6. Planning	7. Support	8. Operation	9. Performance evaluation	10. Improvement
4.1 Understanding the organization and its context	5.1 Leadership and commitment	6.1 Actions to address risks and opportunities	7.1 Resources	8.1 Operational planning and control	9.1 Monitoring, measurement, analysis and evaluation	10.1 Nonconformity and corrective action
4.2 Understanding the needs and expectations of interested parties	5.2 Policy	6.2 Information security objectives and planning to achieve them	7.2 Competence	8.2 Information security risk assessment	9.2 Internal audit	10.2 Continual improvement
4.3 Determining the scope of the ISMS	5.3 Organizational roles, responsibilities and authorities		7.3 Awareness	8.3 Information security risk treatment	9.3 Management review	
4.4 Information Security Management System			7.4 Communication			
			7.5 Documented information			

ISO27001

Klausul 4: Konteks Organisasi

Mengidentifikasi faktor internal, eksternal, serta kebutuhan pihak terkait.

Output:

- Statement of Applicability (SoA): Daftar kontrol keamanan yang relevan.
- Dokumen ruang lingkup ISMS.

Klausul 5: Kepemimpinan

Peran manajemen puncak dalam memberikan dukungan, arahan, dan kebijakan.

Output:

- Kebijakan keamanan informasi yang ditandatangani.
- Struktur peran dan tanggung jawab keamanan informasi.

Klausul 6: Perencanaan

Analisis risiko dan peluang keamanan informasi.

Output:

- Risk Assessment Report: Dokumen penilaian risiko.
- Risk Treatment Plan (RTP): Rencana mitigasi risiko.
- Tujuan keamanan informasi yang terukur.

ISO27001

Klausul 7: Dukungan

Penyediaan sumber daya, pelatihan, kesadaran, dan dokumentasi untuk mendukung ISMS.

Output:

- Rekaman pelatihan dan kompetensi staf.
- Kebijakan komunikasi internal dan eksternal.
- Informasi terdokumentasi, seperti panduan, prosedur, dan laporan.

Klausul 8: Operasi

Implementasi rencana operasional untuk pengendalian risiko keamanan informasi.

Output:

- Risk Treatment Implementation Records: Rekaman pelaksanaan mitigasi risiko.
- Bukti pelaksanaan prosedur operasional keamanan informasi.

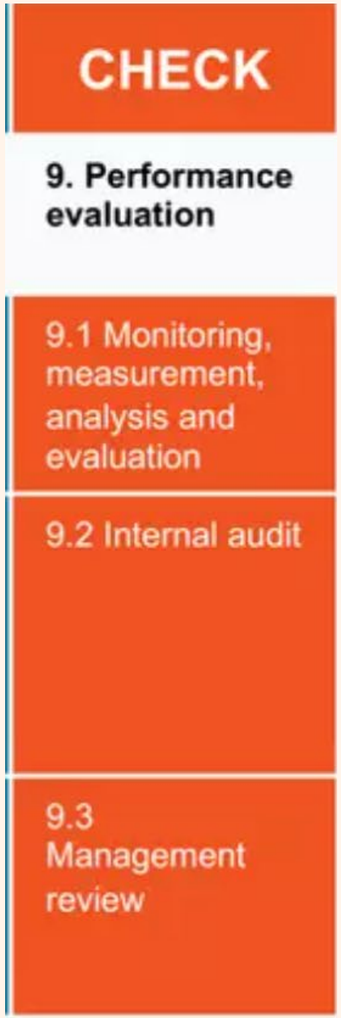
ISO27001

Klausul 9: Evaluasi Kinerja

Proses untuk memantau, mengukur, dan mengevaluasi ISMS, termasuk audit internal.

Output:

- Laporan audit internal yang mendetail.
- Tinjauan manajemen yang berisi analisis efektivitas ISMS dan peluang perbaikan.



ISO27001

Klausul 10: Peningkatan

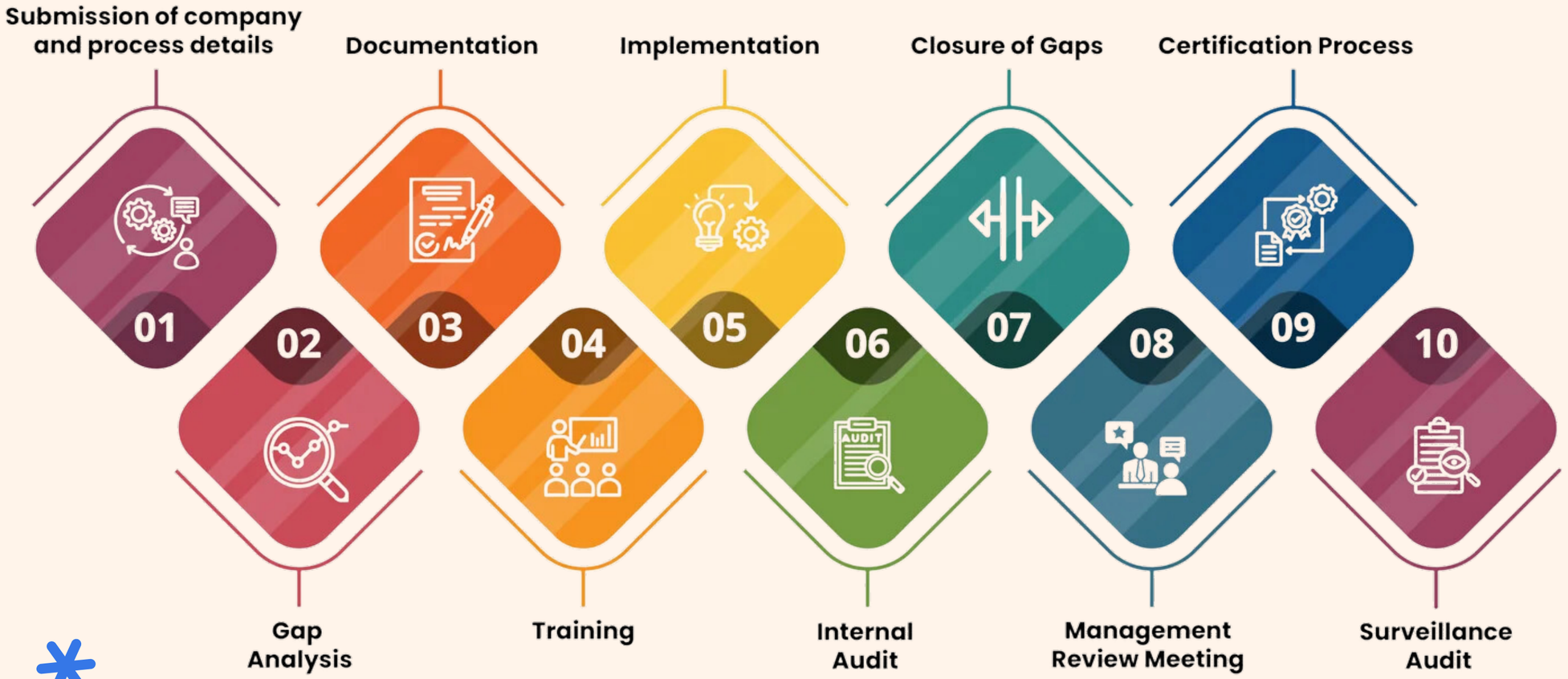
Tindakan korektif dan peningkatan berkelanjutan ISMS berdasarkan temuan dari evaluasi.

Output:

- Laporan ketidaksesuaian dan tindakan korektif.
- Catatan peningkatan berkelanjutan ISMS.

Alur Proses ISO27001

Alur Proses ISO27001



Kontrol Keamanan

Before

ISO27001:2013 - 114 Kontrol Keamanan

After

ISO27001:2022 - 93 Kontrol Keamanan

Kontrol Keamanan ISO27001:2022

Kontrol Keamanan

Kontrol Baru

11 Kontrol keamanan baru

Penggabungan

24 Penggabungan beberapa kontrol

Diperbaharui

58 Kontrol diperbaharui

Kontrol Keamanan

5. Organizational controls	6. People controls	8. Technological controls
5.1. Policies for information security	6.1. Screening	8.1. User endpoint devices
5.2. Information security roles and responsibilities	6.2. Terms and conditions of employment	8.2. Privileged access rights
5.3. Segregation of duties	6.3. Information security awareness, education and training	8.3. Information access restriction
5.4. Management responsibilities	6.4. Disciplinary process	8.4. Access to source code
5.5. Contact with authorities	6.5. Responsibilities after termination or change of employment	8.5. Secure authentication
5.6. Contact with special interest groups	6.6. Confidentiality or non-disclosure agreements	8.6. Capacity management
5.7. Threat intelligence	6.7. Remote working	8.7. Protection against malware
5.8. Information security in project management	6.8. Information security event reporting	8.8. Management of technical vulnerabilities
5.9. Inventory of information and other associated assets		8.9. Configuration management
5.10. Acceptable use of information and other associated assets	**7. Physical controls**	8.10. Information deletion
5.11. Return of assets	7.1. Physical security perimeter	8.11. Data masking
5.12. Classification of information	7.2. Physical entry	8.12. Data leakage prevention
5.13. Labelling of information	7.3. Securing offices, rooms and facilities	8.13. Information backup
5.14. Information transfer	7.4. Physical security monitoring	8.14. Redundancy of information processing facilities
5.15. Access control	7.5. Protecting against physical and environmental threats	8.15. Logging
5.16. Identity management	7.6. Working in secure areas	8.16. Monitoring activities
5.17. Authentication information	7.7. Clear desk and clear screen	8.17. Clock synchronization
5.18. Access rights	7.8. Equipment siting and protection	8.18. Use of privileged utility programs
5.19. Information security in supplier relationships	7.9. Security of assets off-premises	8.19. Installation of software on operational systems
5.20. Addressing information security within supplier agreements	7.10. Storage media	8.20. Network security
5.21. Managing information security in the ICT supply chain	7.11. Supporting utilities	8.21. Security of network services
5.22. Monitoring, review and change management of supplier services	7.12. Cabling security	8.22. Segregation of networks
5.23. Information security for use of cloud services	7.13. Equipment maintenance	8.23. Web filtering
5.24. Information security incident management planning and preparation	7.14. Secure disposal or re-use of equipment	8.24. Use of cryptography
5.25. Assessment and decision on information security events		8.25. Secure development life cycle
5.26. Response to information security incidents		8.26. Application security requirements
5.27. Learning from information security incidents		8.27. Secure system architecture and engineering principles
5.28. Collection of evidence		8.28. Secure coding
5.29. Information security during disruption		8.29. Security testing in development and acceptance
5.30. ICT readiness for business continuity		8.30. Outsourced development
5.31. Legal, statutory, regulatory and contractual requirements		8.31. Separation of development, test and production environments
5.32. Intellectual property rights		8.32. Change management
5.33. Protection of records		8.33. Test information
5.34. Privacy and protection of PII		8.34. Protection of information systems during audit testing
5.35. Independent review of information security		
5.36. Compliance with policies, rules and standards for information security		
5.37. Documented operating procedures		

Kontrol Keamanan

Baru

- 5.7 Threat Intelligence
- 5.23 Information security for cloud services
- 5.30 ICT readiness for business continuity
- 7.4 Physical security monitoring
- 8.9 Configuration Management
- 8.10 Information Deletion
- 8.11 Data Masking
- 8.12 Data Leakage Prevention
- 8.16 Monitoring Activities
- 8.23 Web Filtering
- 8.28 Secure Coding

Implementasi

Kontrol Keamanan Baru

ISO27001:2022

Implementasi Kontrol Keamanan Baru ISO27001:2022

Jumlah Kontrol Baru

Terdapat 11 Kontrol Keamanan Baru pada ISO27001:2022

Kontrol Organisasi

Terdapat 3 Kontrol keamanan baru terkait dengan keamanan organisasi, kontrol tersebut adalah 5.7 , 5.23 , dan 5.30

Kontrol Fisik

Terdapat 1 Kontrol keamanan baru terkait dengan keamanan fisik, kontrol tersebut adalah 7.4

Kontrol Teknologi

Terdapat 7 Kontrol Keamanan Baru terkait keamanan teknologi, kontrol tersebut adalah 8.9 , 8.10 , 8.11 , 8.12 , 8.16 , 8.23 , 8.28

5.7 Threat Intelligence

5.7	Intelijen ancaman	**Kontrol** Informasi yang berkaitan dengan ancaman keamanan informasi harus dikumpulkan dan dianalisis untuk menghasilkan intelijen ancaman.

5.7 Intelijen ancaman

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif #Detektif #Korektif	#Konfidensialitas #Integritas #Availabilitas	#Mengidentifikasi #mendeteksi #Merespons	#Manajemen_ancaman_dan_kerentanan	#Pertahanan #Resiliensi

Tujuan

Untuk Memberikan kesadaran tentang lingkungan ancaman organisasi sehingga dapat dilakukan tindakan mitigasi yang tepat.

5.23 Keamanan informasi untuk penggunaan layanan cloud

5.23	Keamanan informasi untuk penggunaan layanan *cloud*	**Kontrol** Proses untuk akuisisi, penggunaan, manajemen, dan keluar dari layanan *cloud* harus ditetapkan sesuai dengan persyaratan keamanan informasi organisasi.

5.23 Keamanan informasi untuk penggunaan layanan *cloud*

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi	#Keamanan_hubungan_pemasok	#Tata_kelola_dan_Ekosistem #Proteksi

Tujuan
Untuk menentukan dan memanajemeni keamanan informasi untuk penggunaan layanan *cloud*.

5.30 Kesiapan TIK untuk kontinuitas bisnis

5.30	Kesiapan TIK untuk kontinuitas bisnis	**Kontrol** Kesiapan TIK harus direncanakan, diimplementasikan, dipelihara, dan diuji berdasarkan sasaran kontinuitas bisnis dan persyaratan kontinuitas TIK.

5.30 Kesiapan TIK untuk kontinuitas bisnis

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Korektif	#Availabilitas	#Merespons	#Kontinuitas	#Resiliensi

Tujuan
Untuk memastikan availabilitas informasi organisasi dan aset terkait lainnya selama disrupsi.

7.4 Pemonitoran keamanan fisik

7.4	Pemonitoran keamanan fisik	**Kontrol** Premis harus terus dimonitor untuk menemukan akses fisik yang takterotorisasi.

7.4 Pemonitoran keamanan fisik

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif #Detektif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi #Mendeteksi	#Keamanan_fisik	#Proteksi #Pertahanan

Tujuan
Untuk mendeteksi dan mencegah akses fisik yang takterotorisasi.

8.9 Manajemen konfigurasi

8.9	Manajemen konfigurasi	**Kontrol** Konfigurasi, termasuk konfigurasi keamanan, perangkat keras, perangkat lunak, layanan, dan jaringan harus ditetapkan, didokumentasikan, diimplementasikan, dimonitor, dan direviu.

8.9 Manajemen konfigurasi

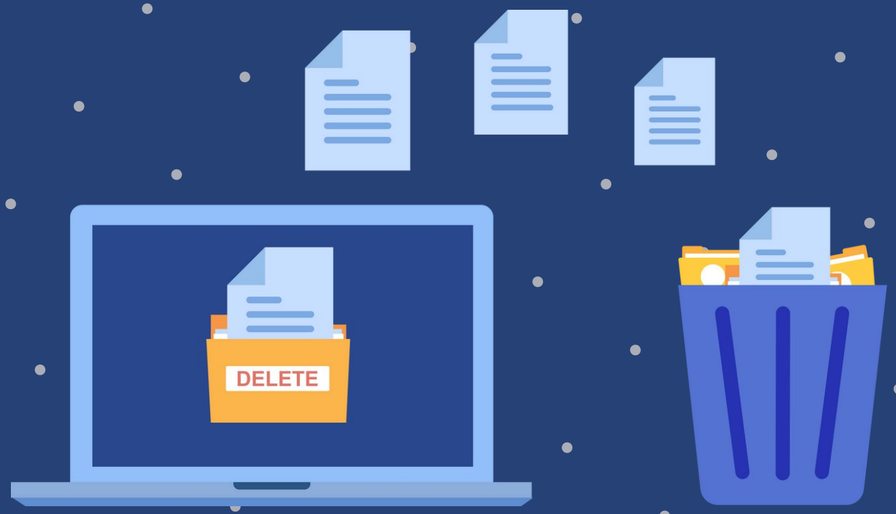
Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi	#Konfigurasi_yang_aman	#Proteksi

Tujuan

Untuk memastikan perangkat keras, perangkat lunak, layanan, dan jaringan berfungsi dengan benar sesuai dengan pengaturan keamanan yang dipersyaratkan, dan konfigurasi tidak diubah secara takterotorisasi atau salah.

8.10 Penghapusan Informasi

8.10	Penghapusan informasi	**Kontrol** Informasi yang disimpan dalam sistem informasi, peranti atau di media penyimpanan lainnya harus dihapus bila tidak lagi diperlukan.



8.10 Penghapusan informasi

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas	#Memproteksi	#Proteksi_informasi #Legal_dan_kepatuhan	#Proteksi

Tujuan

Untuk mencegah eksposur informasi sensitif yang tidak perlu dan untuk mematuhi persyaratan legal, statutori, regalutori, dan kontraktual dalam rangka penghapusan informasi.

8.11 Penyamaran (masking) Data

8.11	Penyamaran (*masking*) data	**Kontrol** Penyamaran data harus digunakan sesuai dengan kebijakan topik spesifik organisasi tentang kontrol akses dan kebijakan topik spesifik terkait lainnya, serta persyaratan bisnis, konsiderasi legislasi yang berlaku.

8.11 Penyamaran (*masking*) data

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas	#Memproteksi	#Proteksi_informasi	#Proteksi

Tujuan
Untuk membatasi pemajanan data sensitif, termasuk PII, dan untuk mematuhi persyaratan legal, statutori, regulatori, dan kontraktual.

8.12 Pencegahan Kebocoran Data

8.12	Pencegahan kebocoran data	**Kontrol** Langkah-langkah pencegahan kebocoran data harus diterapkan pada sistem, jaringan, dan peranti lain yang memproses, menyimpan, atau mentransmisikan informasi sensitif.

8.12 Pencegahan kebocoran data

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif #Detektif	#Konfidensialitas	#Memproteksi #Mendeteksi	#Proteksi_informasi	#Proteksi #Pertahanan

Tujuan
Untuk mendeteksi dan mencegah pengungkapan dan ekstraksi informasi yang takterotorisasi oleh individu atau sistem.

8.16 Pemonitoran Aktivitas

8.16	Pemonitoran aktivitas	**Kontrol** Jaringan, sistem, dan aplikasi harus dimonitor untuk menemukan perilaku anomali dan mengambil tindakan yang tepat untuk mengevaluasi potensi **insiden** keamanan informasi.

8.16 Pemonitoran aktivitas

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Detektif #Korektif	#Konfidensialitas #Integritas #Availabilitas	#Mendeteksi #Merespons	#Manajemen_peristiwa_keamanan_informasi	#Pertahanan

Tujuan
Untuk mendeteksi perilaku anomali dan potensi insiden keamanan informasi.

8.23 Web Filtering

8.23	Pemfilteran web	**Kontrol** Akses ke situs web eksternal harus dimanajemeni untuk mengurangi eksposur konten berbahaya.

8.23 Pemfilteran web

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi	#Keamanan_sistem_dan_jaringan	#Proteksi

Tujuan

Untuk memproteksi sistem agar tidak dibobol oleh perangkat perusak dan untuk mencegah akses ke sumber daya web yang takterotorisasi.

8.28 Pengkodean yang Aman

8.28	Pengkodean yang aman	**Kontrol** Prinsip pengkodean yang aman harus diterapkan pada pengembangan perangkat lunak.

8.28 Pengkodean yang aman

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Keamanan domains
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi	#Keamanan_aplikasi #Keamanan_sistem_dan_jaringan	#Proteksi

Tujuan

Untuk memastikan perangkat lunak ditulis secara aman sehingga mengurangi jumlah kerentanan keamanan informasi potensial dalam perangkat lunak.

Strategi Implementasi ISO27001:2022

1 Implementasi
5 Kontrol Terpenuhi

5.7 Threat Intelligence

8.23 Web Filtering

WAZUH

+

OPENCTI

8.7 Protection against malware

8.16 Activity Monitoring

8.8 Management of technical vulnerabilities

1 Implementasi
2 Kontrol Terpenuhi

8.8 Management of technical vulnerabilities

atau

sonarqube

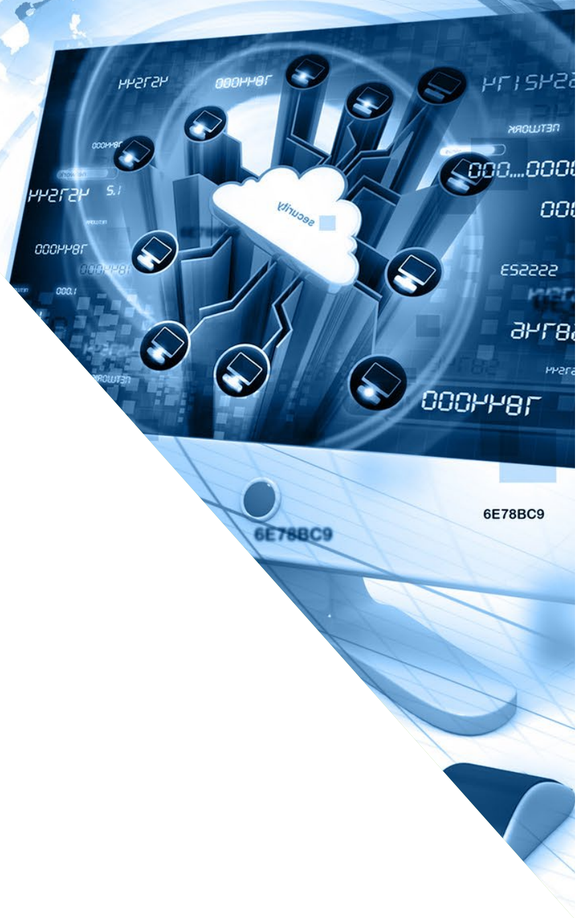
8.28 Secure Coding

Selanjutnya ..
ISO 22701
Privacy Information Management

ISO/IEC 27701:2019

Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management –

Requirement and guidelines



PRABA SINERGI UTAMA

Course aim

To provide a typical framework for extending your ISO/IEC 27001 information security management system (ISMS) including the more specific requirements and guidance for protecting your organization’s personally identifiable information (PII), together constituting a privacy information management system (PIMS)

Benefits of implementing ISO/IEC 27701

Reduces complexity

Generates documentary evidence

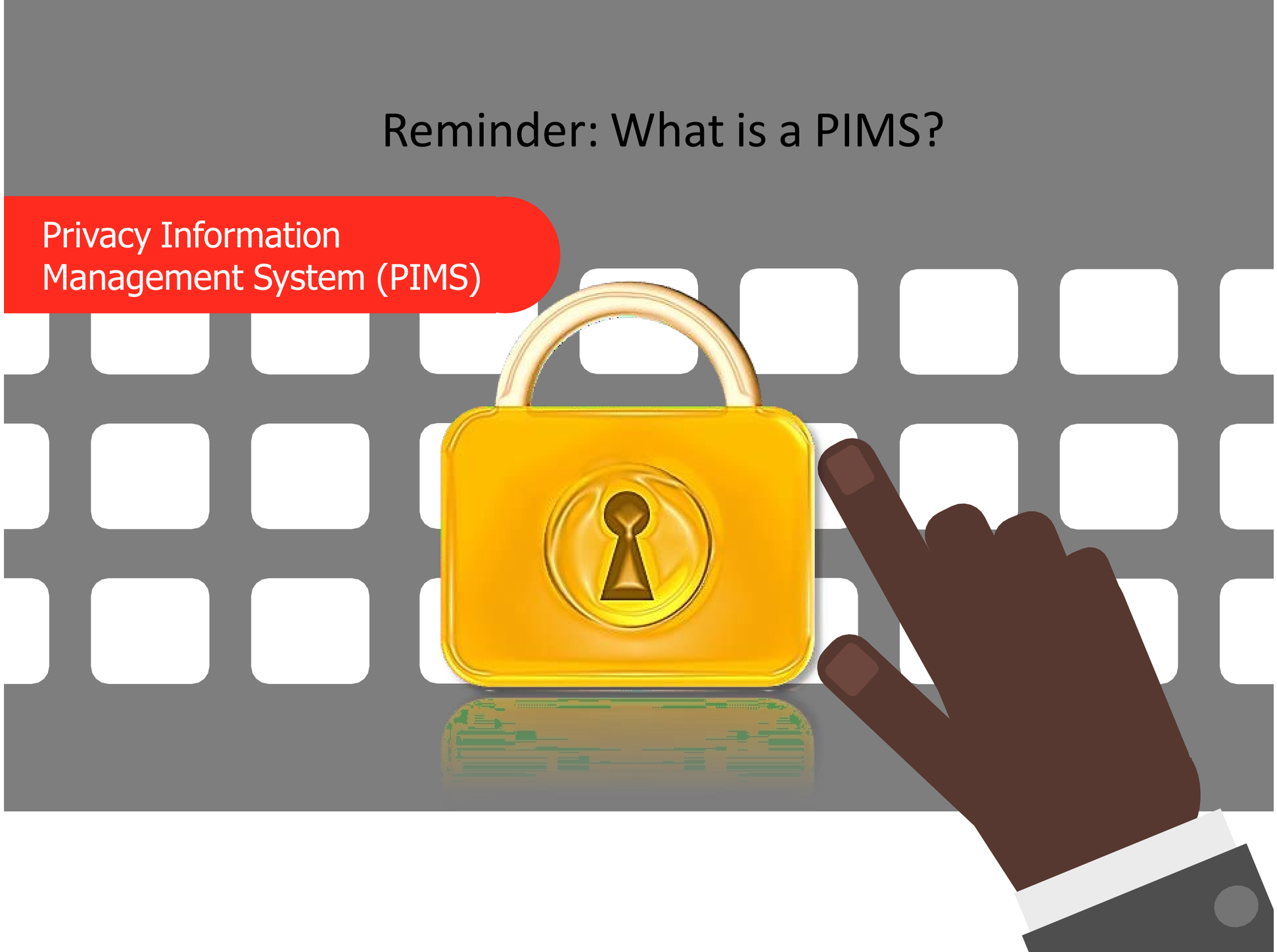
Maps to GDPR and various frameworks

Provides assurance and confidence

Tailored to PII controllers and processors

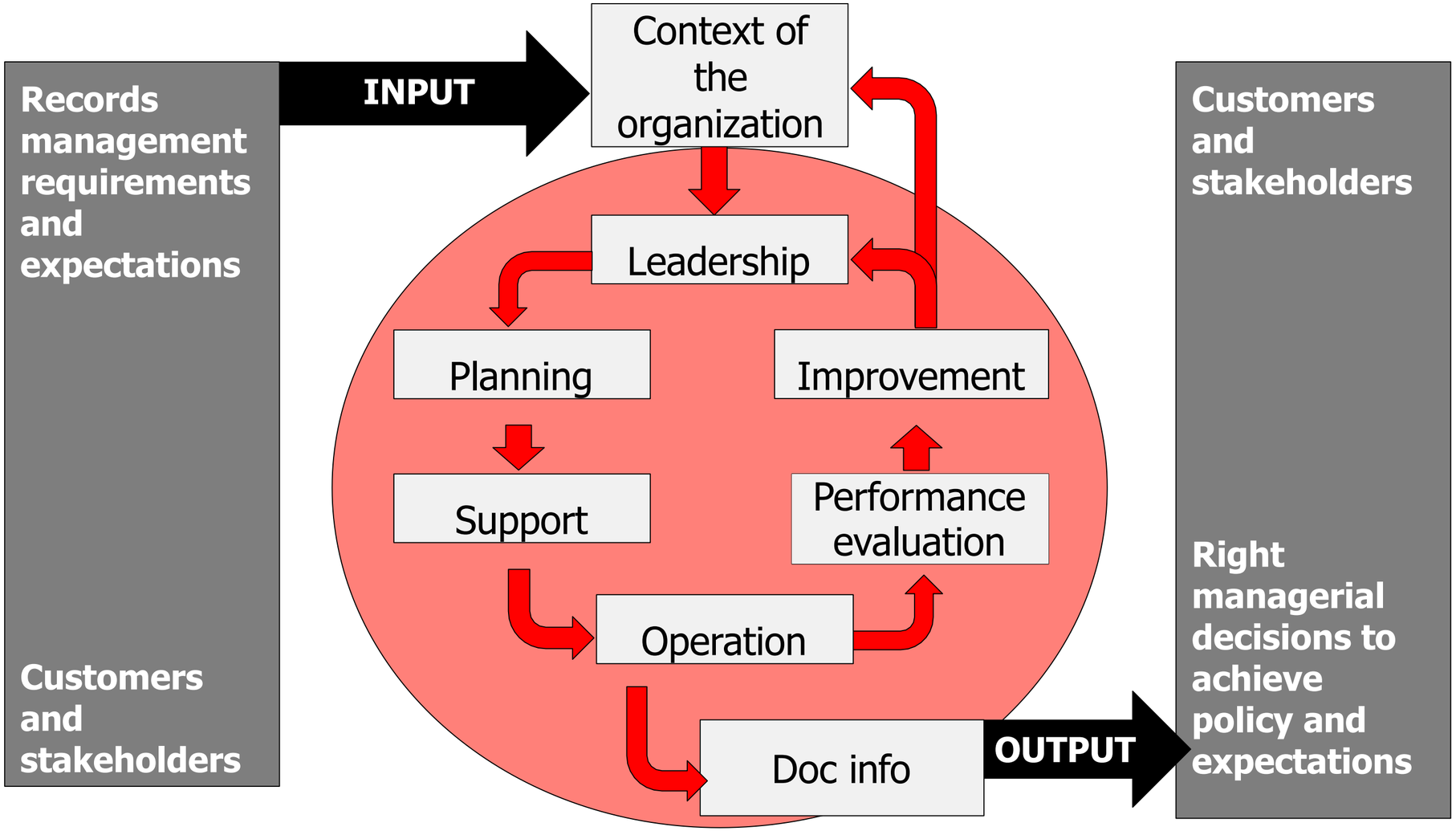
Reminder: What is a PIMS?

Privacy Information Management System (PIMS)



PIMS Plan, Do, Che t cycle

Integration – High level structure



Contents in ISO/IEC 27701

1. Scope
2. Normative Reference
3. Terms, definitions and abbreviations

4 General

Table 1 — Location of PIMS-specific requirements and other information for implementing controls in ISO/IEC 27001:2013

Clause in ISO/IEC 27001:2013	Title	Subclause in this document	Remarks
4	Context of the organization	5.2	Additional requirements
5	Leadership	5.3	No PIMS-specific requirements
6	Planning	5.4	Additional requirements
7	Support	5.5	No PIMS-specific requirements
8	Operation	5.6	No PIMS-specific requirements
9	Performance evaluation	5.7	No PIMS-specific requirements
10	Improvement	5.8	No PIMS-specific requirements

NOTE The extended interpretation of "information security" according to 5.1 always applies even when there are no PIMS-specific requirements.

Table 2 gives the location of PIMS-specific guidance in this document in relation to ISO/IEC 27002.

Table 2 — Location of PIMS-specific guidance and other information for implementing controls in ISO/IEC 27002:2013

Clause in ISO/IEC 27002:2013	Title	Subclause in this document	Remarks
5	Information security policies	6.2	Additional guidance
6	Organization of information security	6.3	Additional guidance
7	Human resource security	6.4	Additional guidance
8	Asset management	6.5	Additional guidance
9	Access control	6.6	Additional guidance
10	Cryptography	6.7	Additional guidance
11	Physical and environmental security	6.8	Additional guidance
12	Operations security	6.9	Additional guidance
13	Communications security	6.10	Additional guidance
14	System acquisition, development and maintenance	6.11	Additional guidance
15	Supplier relationships	6.12	Additional guidance
16	Information security incident management	6.13	Additional guidance
17	Information security aspects of business continuity management.	6.14	No PIMS-specific guidance
18	Compliance	6.15	Additional guidance

NOTE The extended interpretation of "information security" according to 6.1 always applies even when there is no PIMS-specific guidance.

Clause 5: PIMS-specific requirements related to ISO/IEC 27001

Clause 6: PIMS-specific guidance related to ISO/IEC 27002

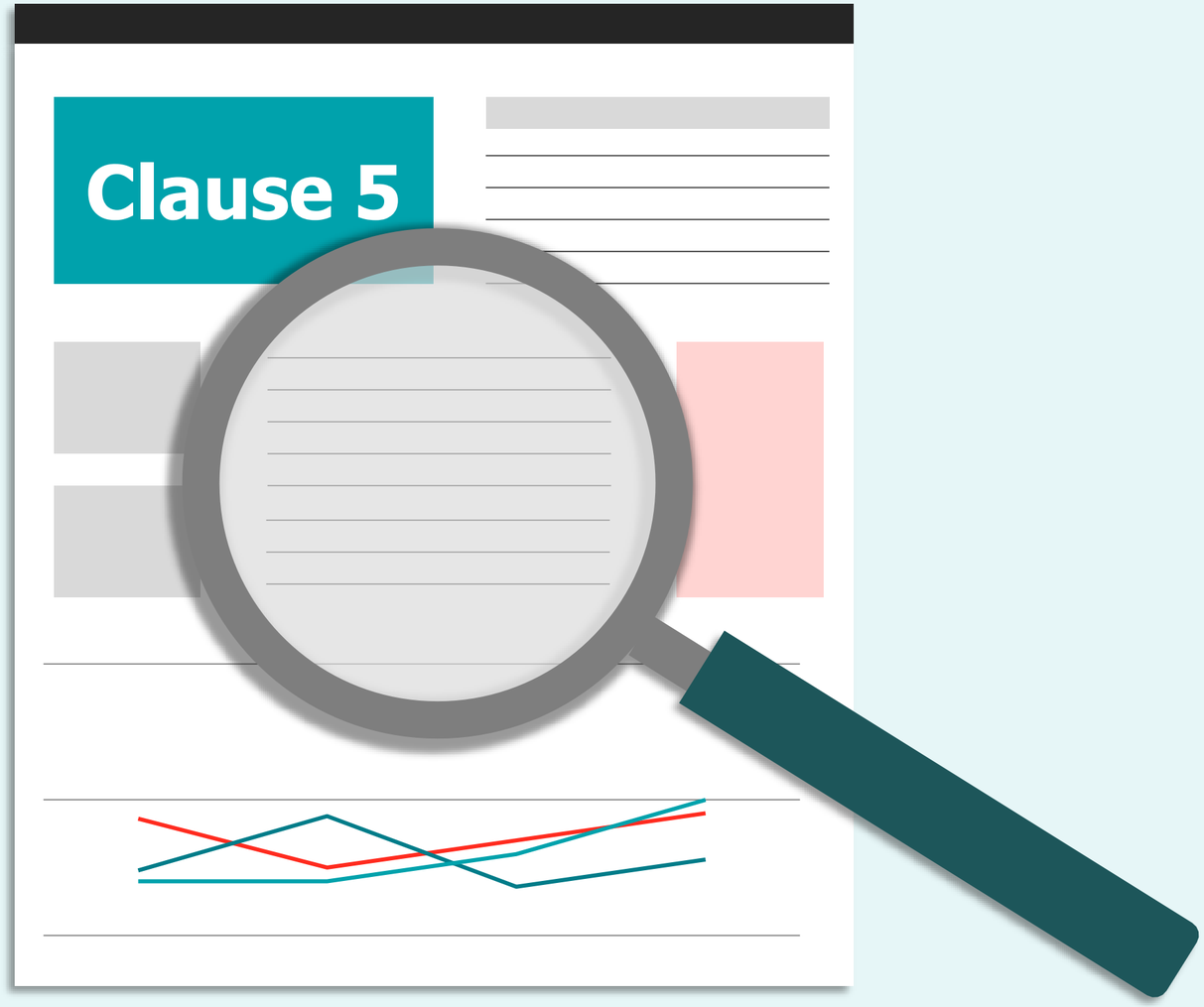
Clause 7: Additional ISO/IEC 27002 guidance for PII controllers

Clause 8: Additional ISO/IEC 27002 guidance for PII processors

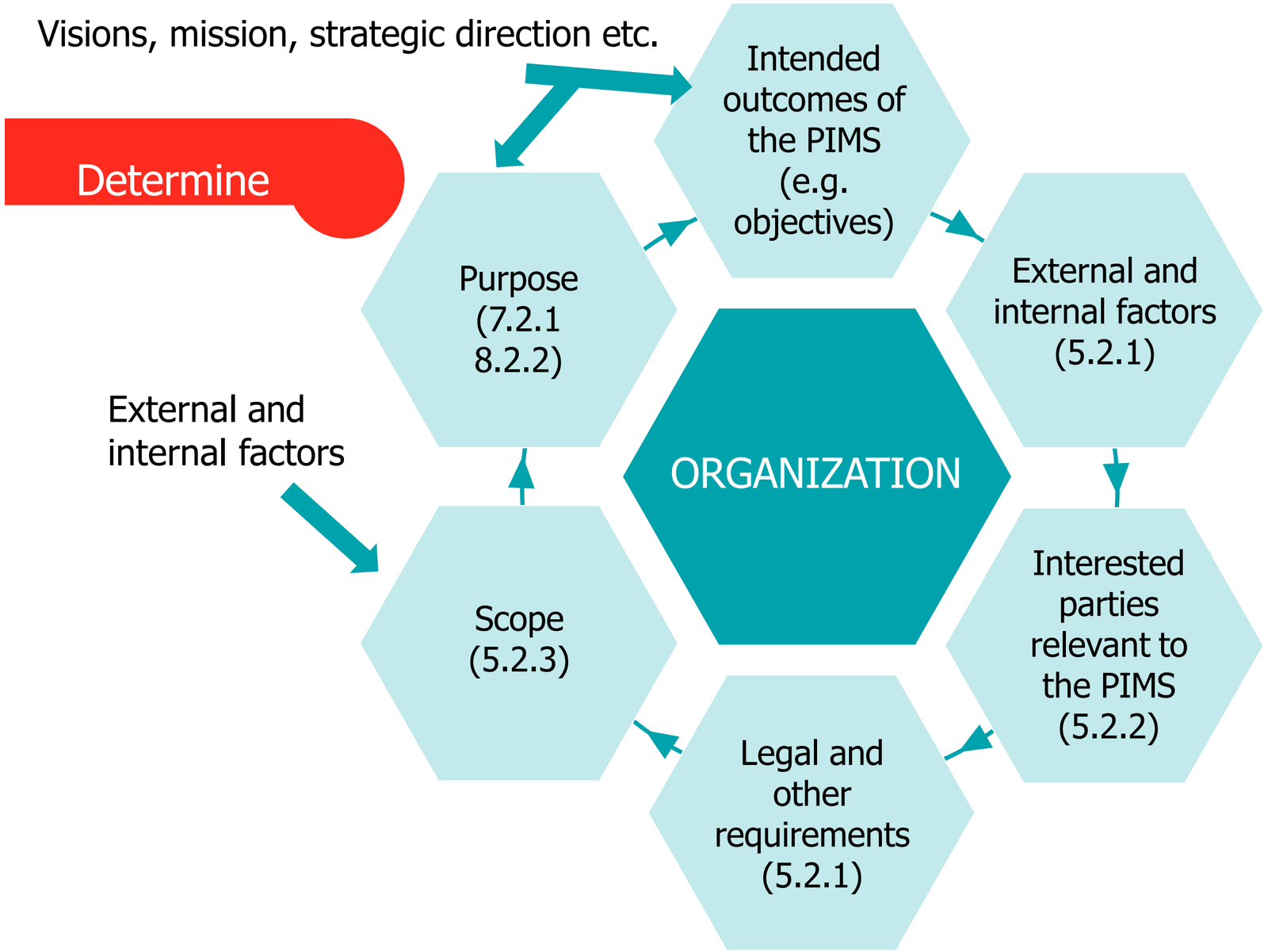
Annex A- F

Annex	Detail
Annex A (informative)	PIMS-specific reference control objectives and controls (PII Controllers)
Annex B (normative)	PIMS-specific reference control objectives and controls (PII Processors)
Annex C (informative)	Mapping to ISO/IEC 29100 Table C.1 — Mapping of controls for PII controllers and ISO/IEC 29100 Table C.2 — Mapping of controls for PII processors and ISO/IEC 29100
Annex D (informative)	Mapping to the General Data Protection Regulation
Annex E (informative)	Mapping to ISO/IEC 27018 and ISO/IEC 29151
Annex F (informative)	How to apply ISO/IEC 27701 to ISO/IEC 27001 and ISO/IEC 27002

Clause 5: PIMS-specific requirements related to ISO/IEC 27001

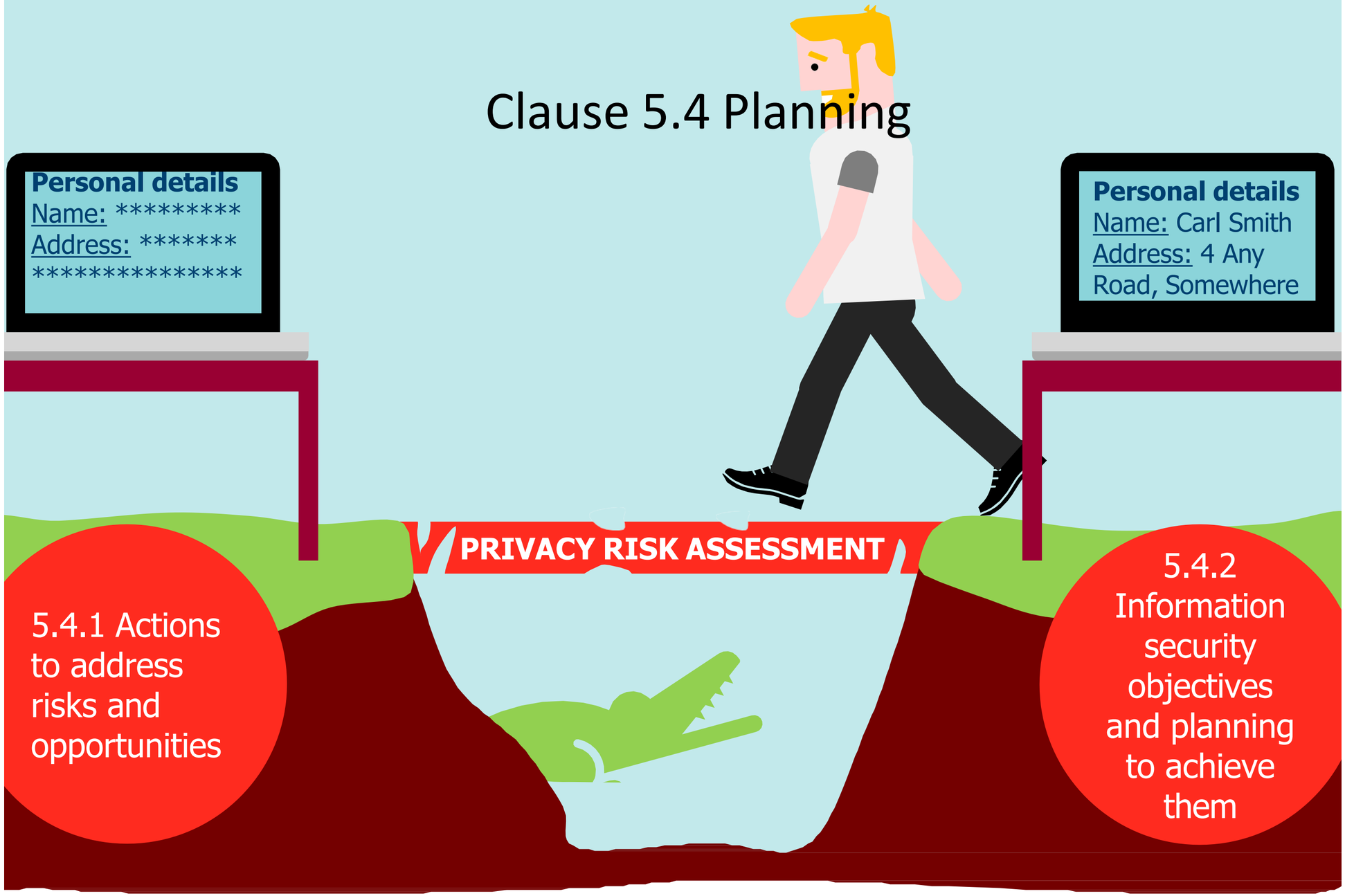


Clause 5.2 Context of the organization

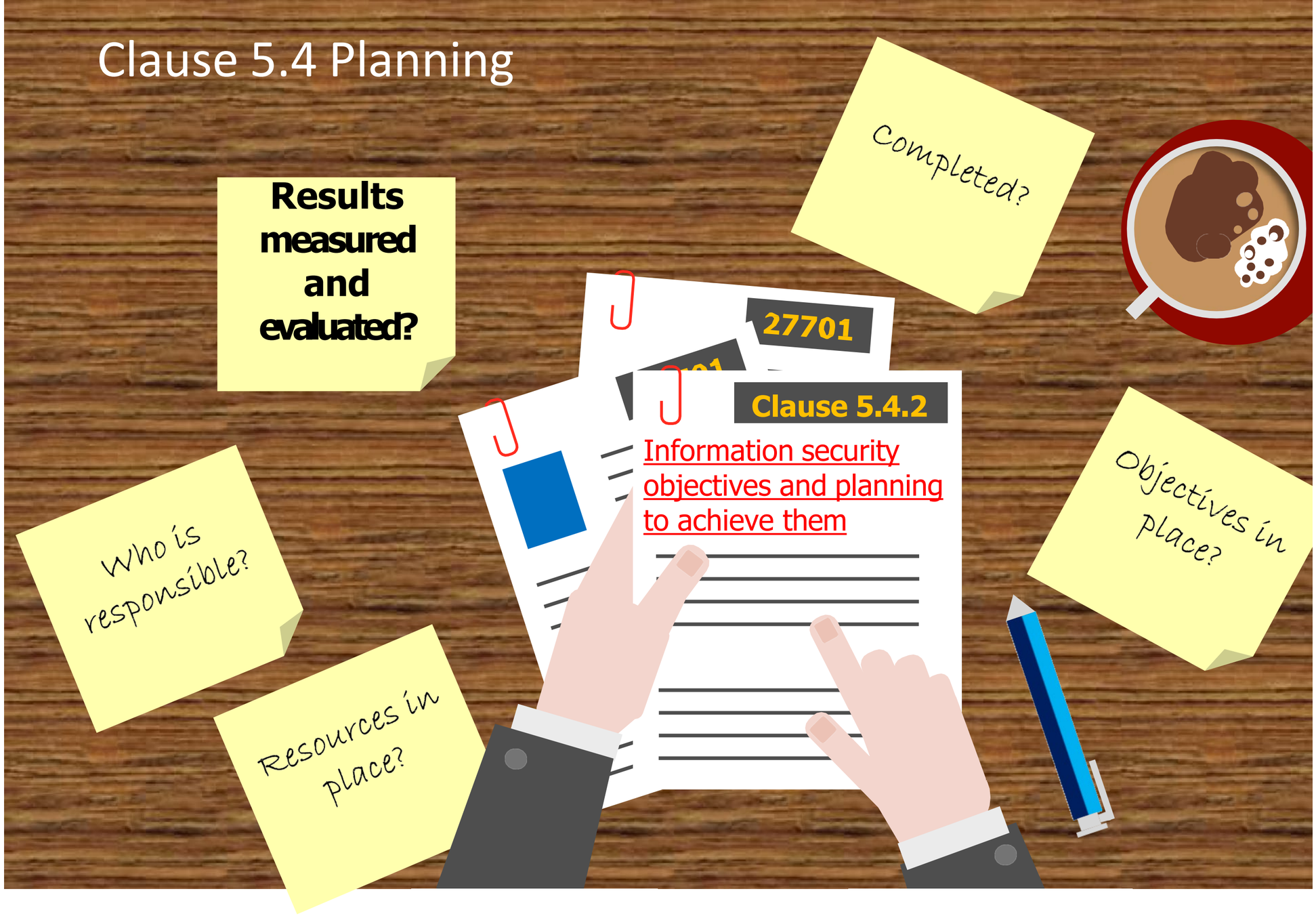



Clause 5 Leadership
Leadership and commitment
Policy
Organizational roles, responsibilities and authorities
Embedding the PIMS in the organization's culture

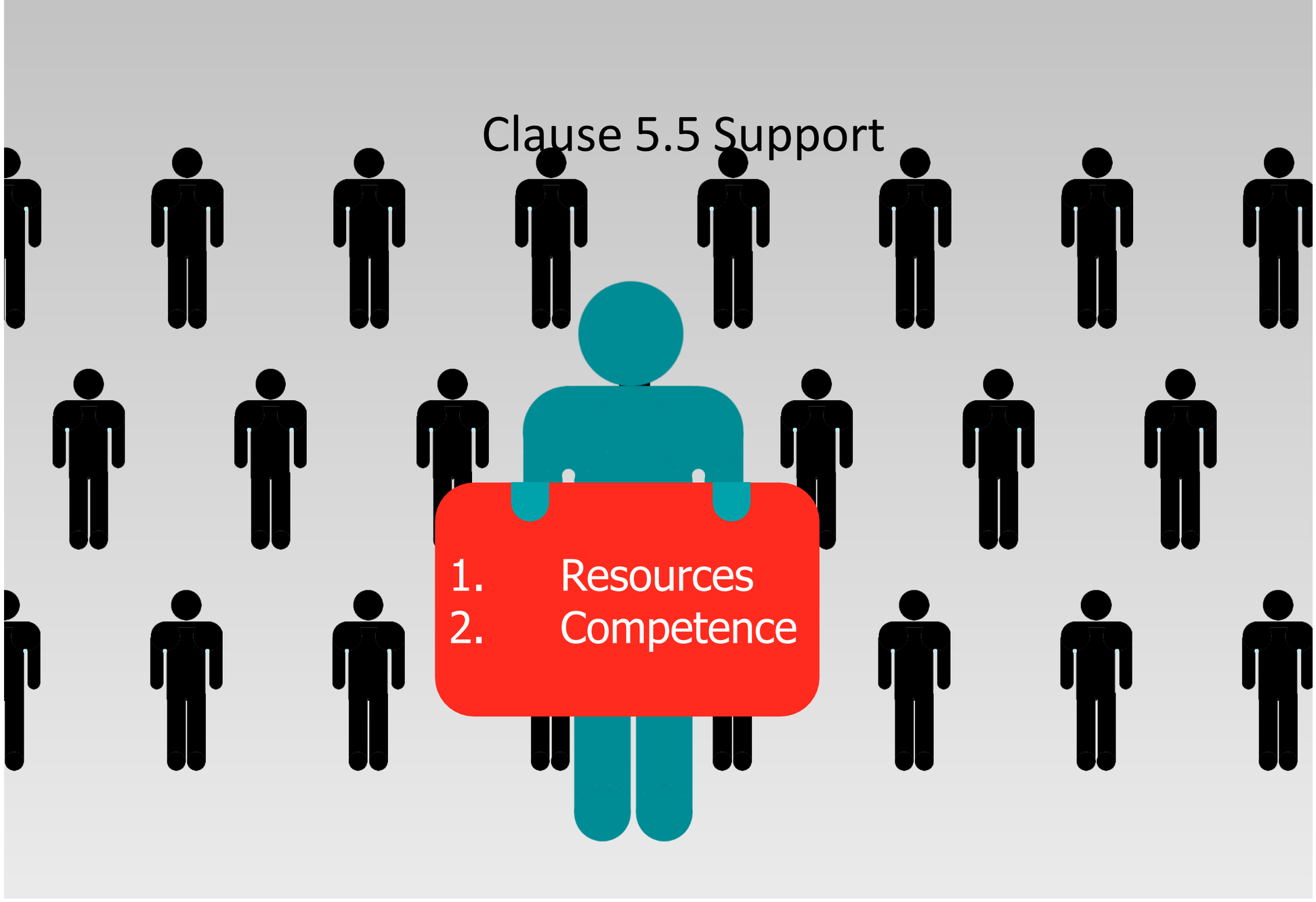
Clause 5.4 Planning



Clause 5.4 Planning

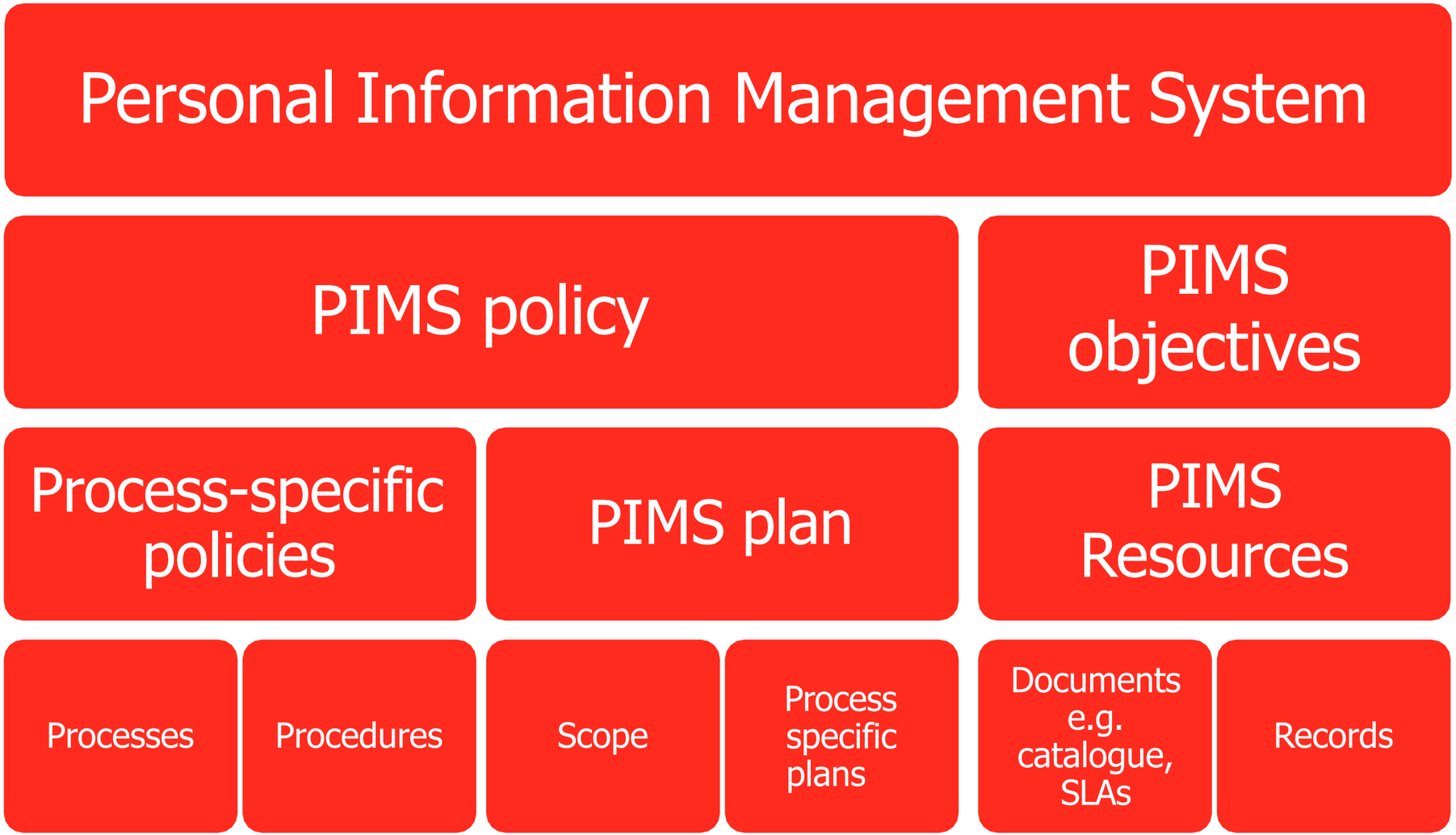


Clause 5.5 Support



Clause 5.5 Support

Clause 5.5.5 Documented information



Clause 5.6 subclauses

Clause 5.7 Performance evaluation

Clause 5.7.1: Monitoring, measuring, analysis and evaluation (9.1)

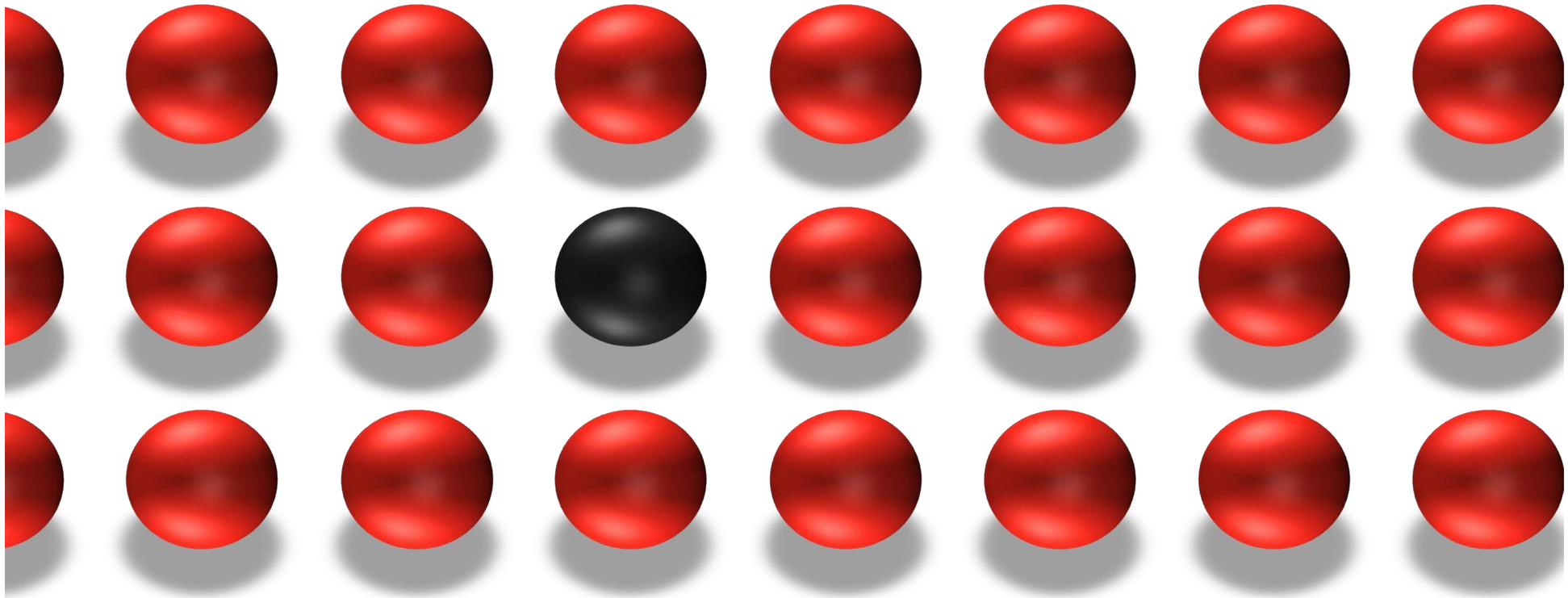
5.7.2 Internal audit (9.2)

5.7.2 Management review (9.3)

Clause 5.8.1 and Clause 5.8.2

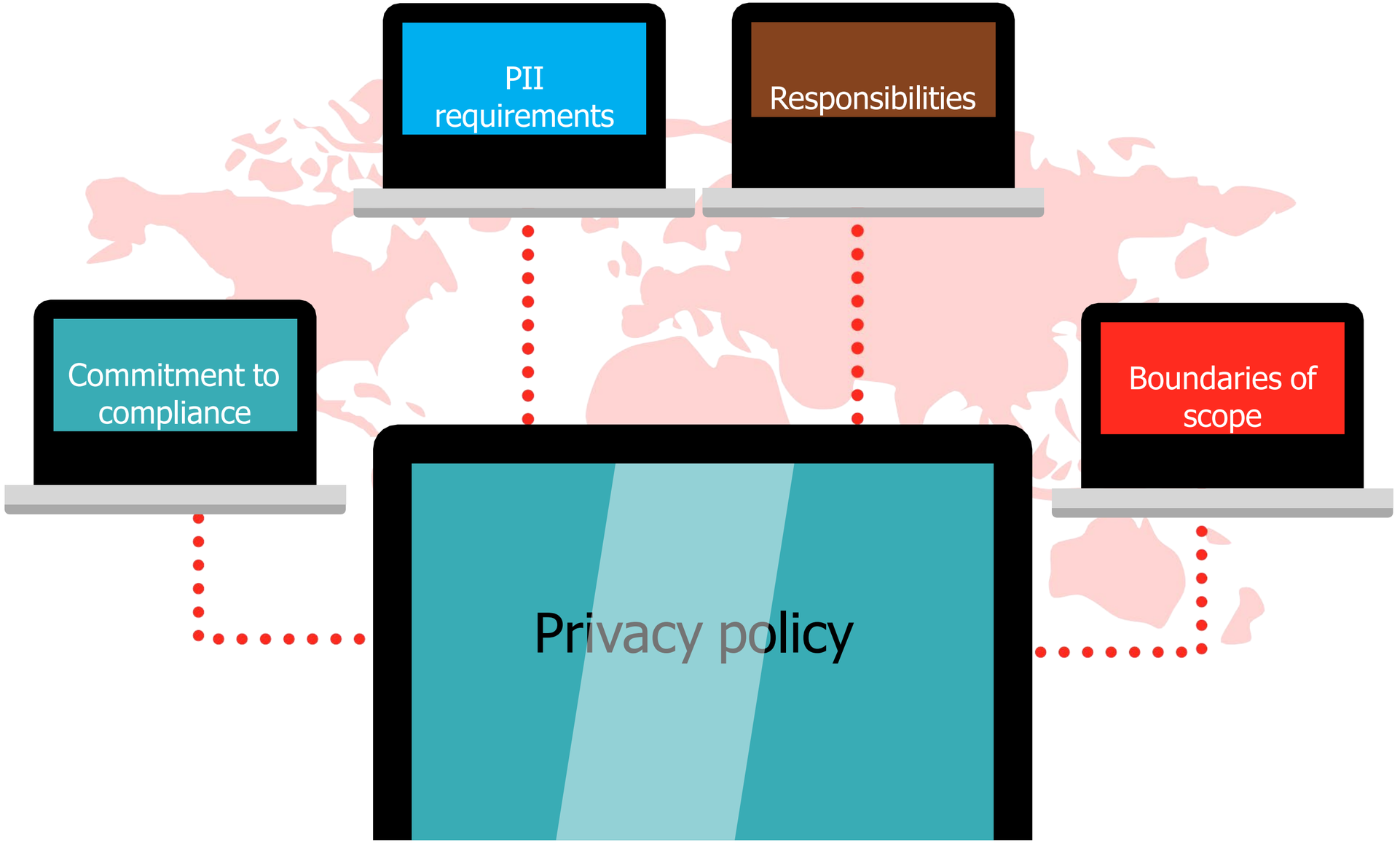
5.8.1 Nonconformity and corrective action (10.1)

5.8.2 Continual improvement (10.2)



Clause 6: PIMS-specific guidance related to ISO/IEC 27002

Clause 6.2 Information security policies

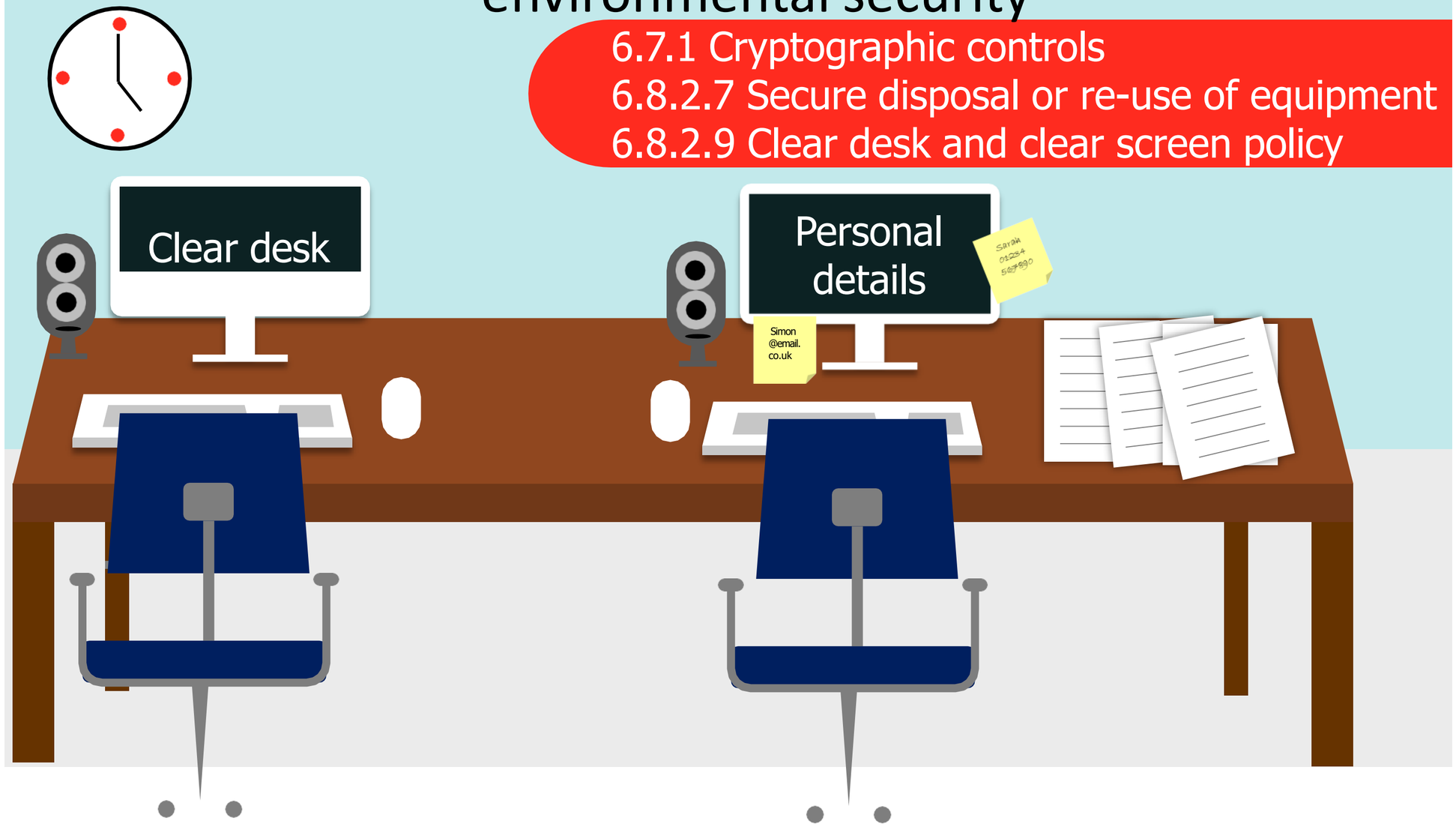


Clause 6.4 Human resource security

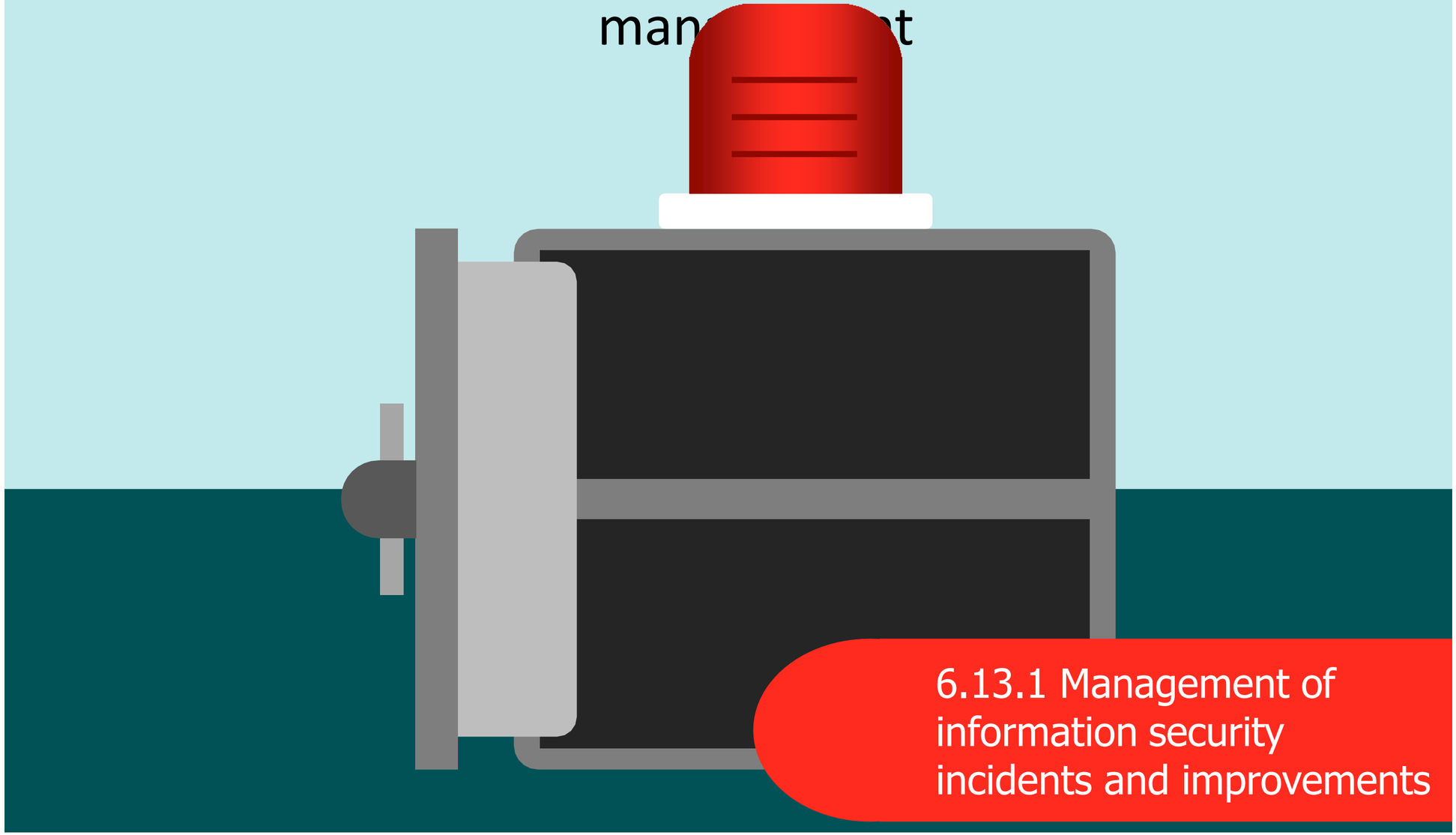
6.4.2.2 Information security, awareness, education and training

Clause 6.7 Cryptography and Clause 6.8 Physical and environmental security

6.7.1 Cryptographic controls
6.8.2.7 Secure disposal or re-use of equipment
6.8.2.9 Clear desk and clear screen policy



Clause 6.13 Information security incident management



6.13.1 Management of information security incidents and improvements

Clause 6.13 Information security incident management

How to recognize a PII breach/ security incident

NEWS TODAY

Friday 25th October 20XX £0.65

BREACH!
PII leak in top firm

Vivamus venenatis ornare tortor in tempor.

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Quisque id posuere arcu, et convallis justo. Integer sed ex feugiat, accumsan est a, elementum leo.

Sed id lacus a tortor gravida maximus quis sed lacus. Nam sit amet elit vehicula, vestibulum eros ut, hendrerit metus. Phasellus rutrum

Clause 7: Additional ISO/IEC 27002 guidance for PII controllers

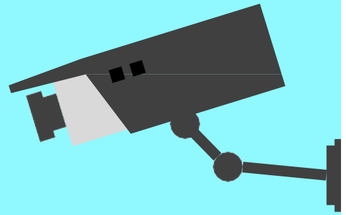
Clause 7.2 Conditions for collection and processing

GDPR

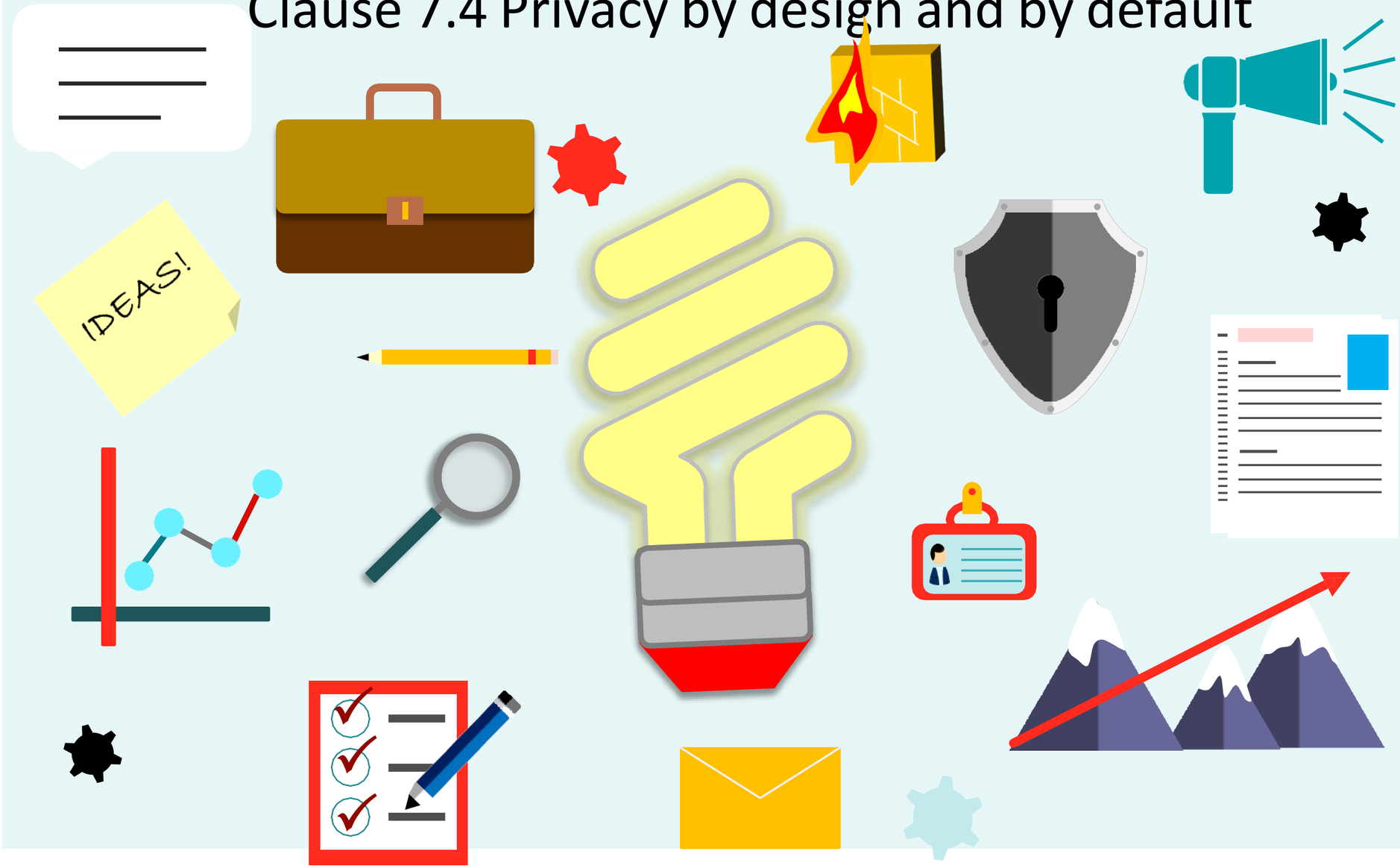
Article 6

Clause 7 Obligations to PII principals

7.3 Obligations to PII principals



Clause 7.4 Privacy by design and by default



Clause 8: Additional ISO/IEC 27002 guidance for PII processors

Clause 8 Conditions for collection and processing

8.2.1 Cooperation agreement

Clause 8.4 Privacy by design and privacy by default

8.4.2 Return, transfer or disposal of PII (1)

Summary Contents in ISO/IEC 27701

1. Scope
2. Normative Reference
3. Terms, definitions and abbreviations
4. General

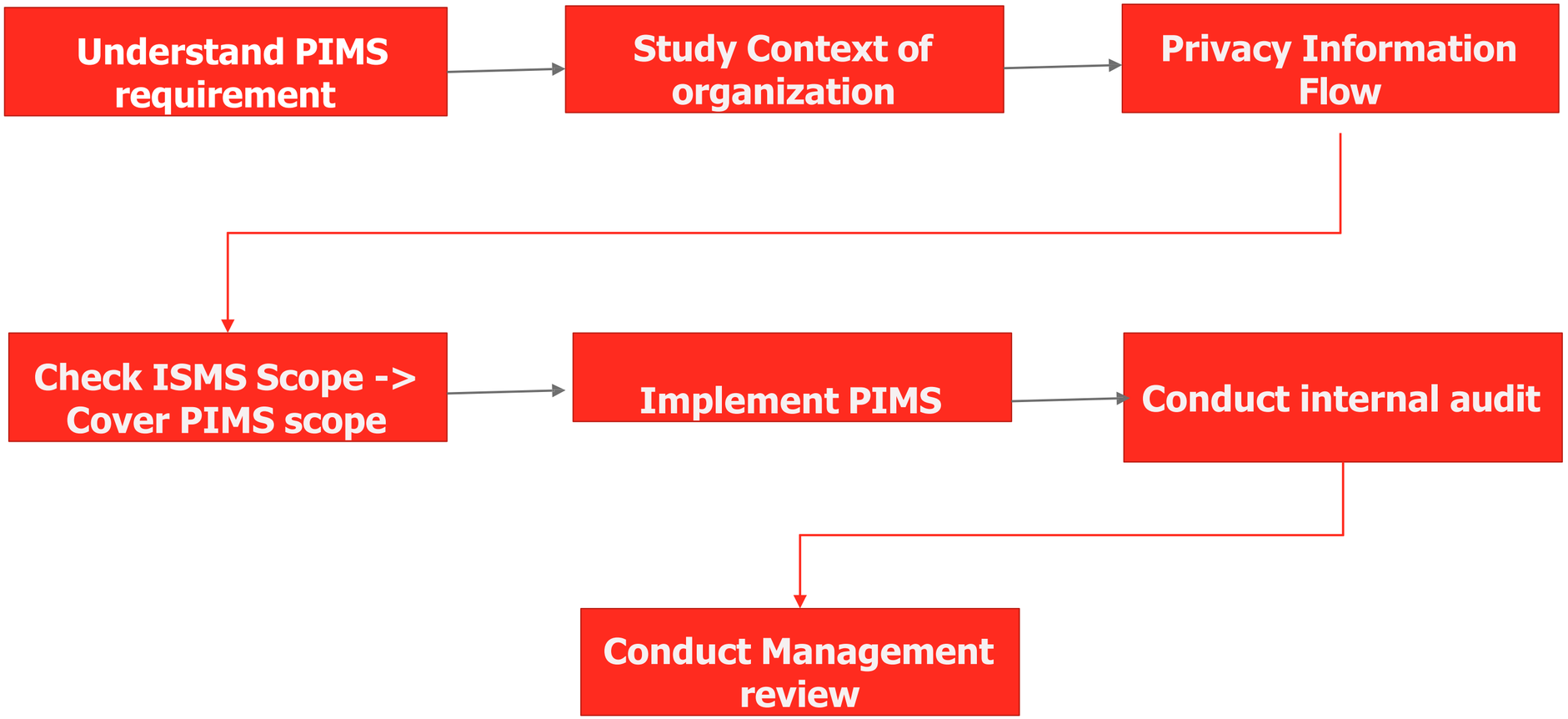
Clause 5: PIMS-specific requirements related to ISO/IEC 27001

Clause 6: PIMS-specific guidance related to ISO/IEC 27002

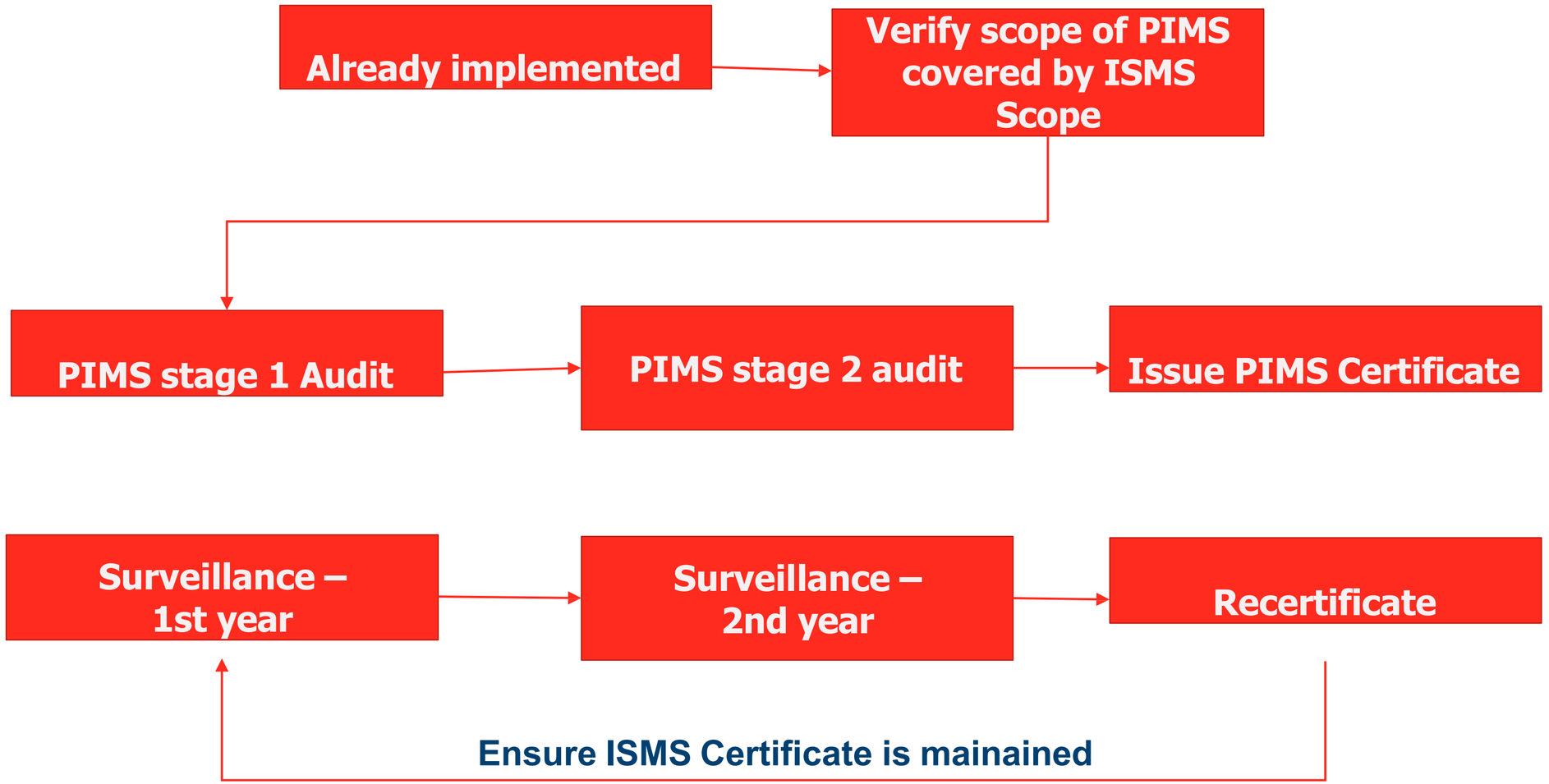
Clause 7: Additional ISO/IEC 27002 guidance for PII controllers

Clause 8: Additional ISO/IEC 27002 guidance for PII processors

Implement for PIMS



Certify for PIMS



Course review and final questions

MANAGEMENT CONSULTING & TRAINING IT AUDIT & COMPLIANCE IT SECURITY ASSESSMENT

PT Praba Sinergi Utama
The Vida Lantai 7 Jl. Raya Perjuangan No. 8 Kebon Jeruk Jakarta Barat 11530

PRABA
SINERGI
UTAMA

PRABA SINERGI UTAMA

BSSN
Verified

Thank You

Contact Us

+(021) 2977-8199

info@prabasinergiutama.com

www.prabasinergiutama.com