Netwerkcafé “Trends in Cybercrime”

gezien vanuit het audit-perspectief

KIVI, regio Gelderland

Datum: 1 december 2025
Locatie: ICT Academie Apeldoorn

PROFESSIONALS IN CERTIFICATION ISO 27001

Procertify
Professionals in certification

Informationsecurity

Assurance or ISO?

Mischa van der Vliet • 06 25057951 • mischa@procertify.nl

Mischa van der Vliet RE

Register EDP-auditor (RE)

Lead auditor 27001/9001/14001/20000

>250 Assurance audits

>500 ISO audits

ISO audits: former owner of DigiTrust

But: not the expert! Open discussion to enforce knowledge development among us all. Trying to combine ISO27001 and SOC2 environments.

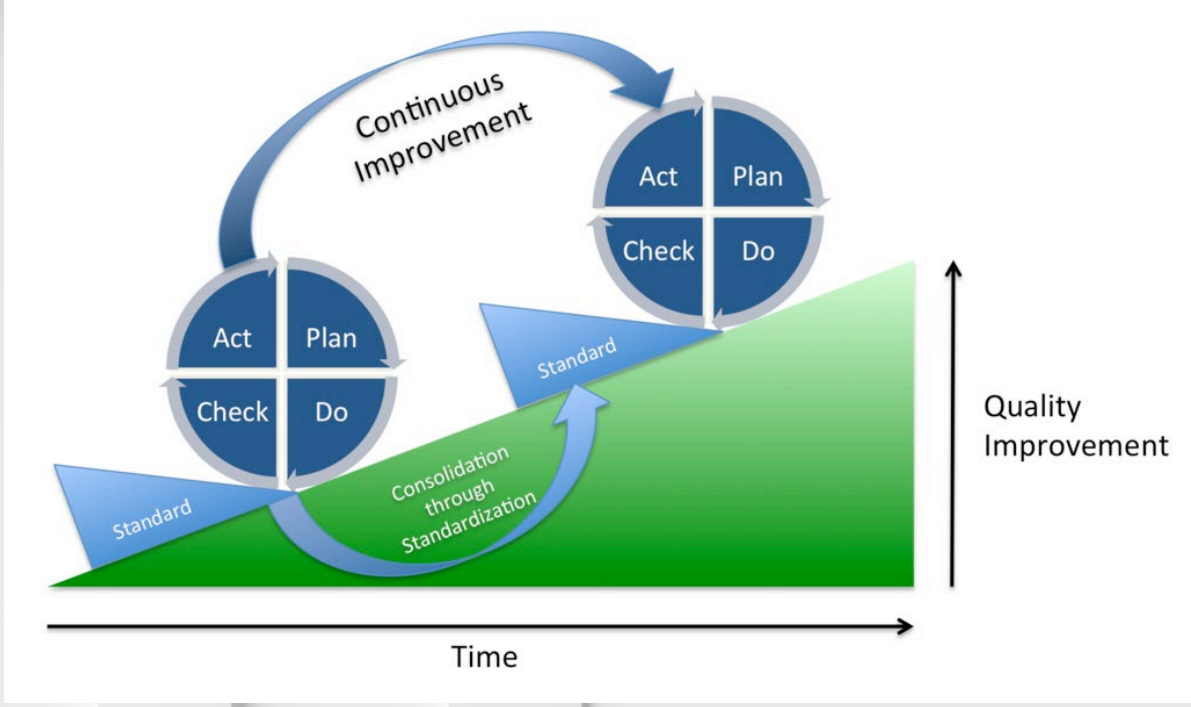
Programma

19.30-20.15 Deepdive ISO27001

20.15-21.00 Deepdive SOC2

https://www.youtube.com/watch?v=AICj_2HvniQ

1. Deepdive 27001:2022



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)

General information 0-3

Introduction, scope, normative references, terms and definitions

Context of the organization 4

Create the ISMS Scope that sets the boundaries of your system and the applicability of the controls

Leadership 5

Top management to document a Policy Statement with employees and clients

Planning 6

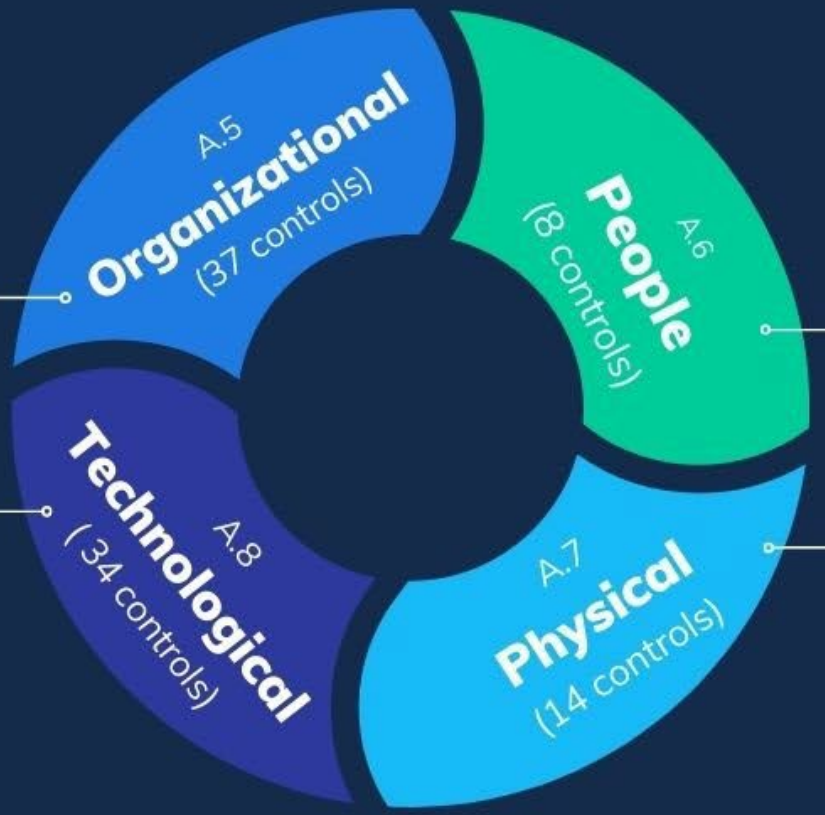
Establish, measure and monitor objectives based on risks and opportunities

usecure

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



There are no new controls in this area

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:

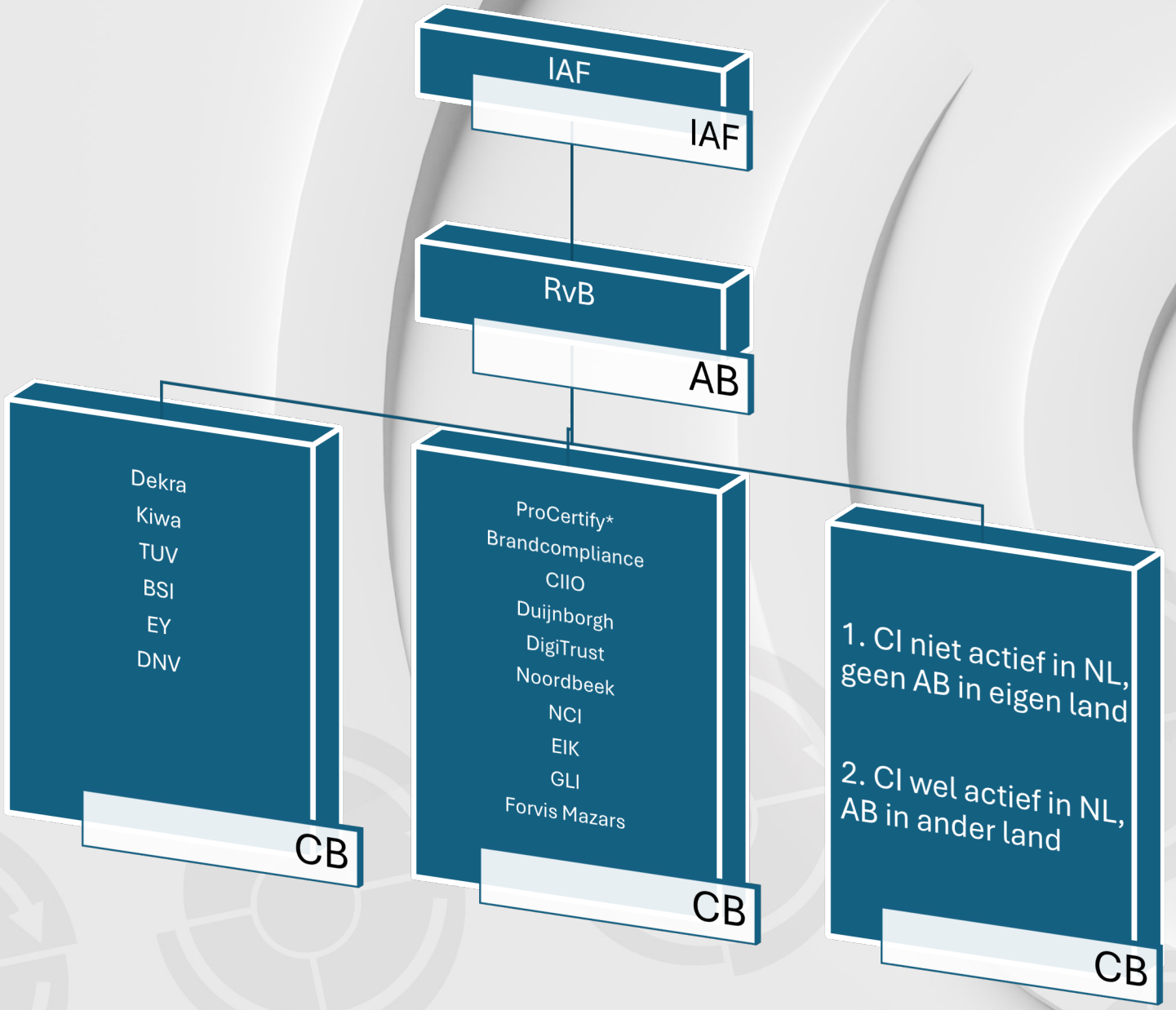
- 7.4: Physical security monitoring

How many organizations have worldwide ISO27001?

How many in the NL?

Which ISO number 1, 2 and 3 worldwide?

Standards	Number of certificates	Number of sites
ISO 9001:2015	837 052	1 249 317
ISO 14001:2015	300 410	526 046
ISO 45001:2018	185 166	309 056
ISO IEC 27001:2013	48 671	81 264
ISO 22000:2018	30 811	36 630
ISO 13485:2016	32 963	52 950
ISO 50001:2018	24 924	61 370
ISO 20000-1:2018	3 670	6 652
ISO 37001:2016	7 894	15 952
ISO 22301:2019	3 524	11 232
ISO 39001:2012	1 670	2 982
ISO 55001:2014	668	2 134
ISO 20121:2012	293	433
ISO 29001:2020	206	244
ISO 44001:2017	132	163


IAF
IAF
RvB
AB
Dekra
Kiwa
TUV
BSI
EY
DNV
CB
ProCertify*
Brandcompliance
CIIO
Duijnborgh
DigiTrust
Noordbeek
NCI
EIK
GLI
Forvis Mazars
CB
1. CI niet actief in NL, geen AB in eigen land
2. CI wel actief in NL, AB in ander land
CB

The International Accreditation Forum (IAF) is a worldwide association of accreditation bodies and other bodies interested in conformity assessment in the fields of management systems, products, processes, services, personnel, validation and verification and other similar programmes of conformity assessment.

77 Accreditation Bodies

Accreditation Body Name

Filter

Serbia
(ATS) Accreditation Body of Serbia

View Profile →

Austria
(AA) Akkreditierung Austria

View Profile →

RAAD VOOR ACCREDITATIE

Over de RvA

Bijna ieder land binnen Europa heeft een nationale accreditatie-instantie. In Nederland is dat de RvA. Onze primaire taak bestaat uit het accrediteren en geaccrediteerd houden van conformiteitbeoordelende organisaties: laboratoria, inspectie-instellingen, certificatie-instellingen en verificatie-instellingen. Zodat het vertrouwen in de kwaliteit van producten en diensten ook echt gerechtvaardigd is.

ISO 27001

Registratienummer oplopend (A-Z)

Vorige

Volgende

Items **1** - **17** van **17**

Disciplines

- [ ] Managementsysteemcertificatie-instellingen (17)

INTERNATIONAL STANDARD

ISO/IEC 27018:2019

Edition 2
2019-01

Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

ISO IEC

ISO/IEC 27001:2022

Edition 3
2022-10

rity, cybersecurity and
n — Information
ment systems —

ISO IEC

INTERNATIONAL STANDARD

ISO/IEC 24760-1:2019

Edition 2
2019-05

identity management — Part 1:

ISO IEC

ISO IEC

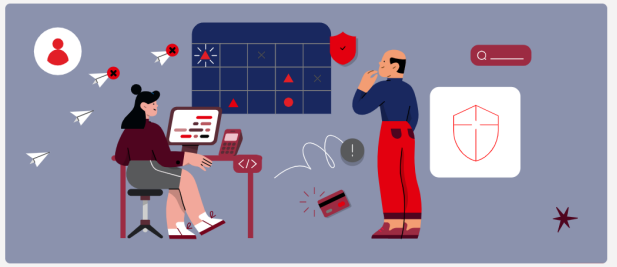
International Standard

ISO/IEC 29146:2024

nformation technology — Security
— A framework for
access mana ement

Edition 2
2024-01

Threat intelligence and why it matters for cybersecurity



In today's digital age, the question isn't whether you'll experience a cybersecurity attack, but when this might occur. Cybercriminals strike when you least expect it, with devastating consequences for your day-to-day operations. If your organization is lucky, it can block the attacker and limit further damage.

For many, that's not the case – getting back to business-as-usual can take days, or even months. So it's important to **detect signs of malicious activity** ahead of a damaging attack, predict what will happen and take preventive action. That's the value of cyber threat intelligence (CTI).

CTI is about collecting information that helps information security teams create a strong defensive strategy. Modern organizations are increasingly recognizing the value of cyber threat intelligence, with many planning to invest more in their threat intelligence in

25701

International Standards covering almost all aspects of technology, management and manufacturing.

172

Members representing ISO in their country. There is only one member per country.

843

Technical committees and subcommittees to take care of standards development.

1 vertegenwoordiger per land

ISO17021

ISO27006

MD1: Multi site

MD2: transfer

MD4: ICT in auditing

MD5: audttime

MD11: Integration

MD12: More countries

BR002-BR012

D, QA,R, VR docs

CB

Procertify

Professionals in certification

Customer

ISO27001

ISO 17021-1:2015

5.	Algemene eisen
5.1	Rechts- en contractuele aangelegenheden
5.2	Management van onpartijdigheid
5.3	Aansprakelijkheid en financiering
6	Structurele eisen
6.1	Organisatiestructuur en directie
6.2	Operationele beheersing
7	Eisen in verband met de middelen
7.1	Competentie van het personeel
7.2	Personeel dat betrokken is bij de certificatieactiviteiten
7.3	Inzetten van individuele externe auditoren en externe technische deskundigen
7.4	Registraties in verband met het personeel
7.5	Uitbesteding
8	Eisen aan informatie
8.1	Openbare informatie
8.2	Certificatiedocumenten
8.3	Verwijzing naar certificatie en gebruik van merken
8.4	Vertrouwelijkheid
8.5	Informatie-uitwisseling tussen een certificatie-instelling en haar klanten
9	Proceseisen
9.1	Activiteiten voorafgaand aan certificatie
9.2	Audits plannen
9.3	Initiële certificatie
9.4	Audits uitvoeren
9.5	Certificatiebeslissing
9.6	Voortzetting van certificatie
9.7	Beroep
9.8	Klachten
9.9	Klantregistraties
10	Managementsysteemeisen voor certificatie-instellingen
10.1	Opties
10.2	Optie A: Algemene managementsysteemeisen
10.3	Optie B: Managementsysteemeisen volgens ISO 9001

HS? No!

Over auditen

ISO 27006-1:2024

Table C.1 — Audit time chart

Number of persons doing work under the organization's control	Quality management system audit time for initial audit (auditor days, d)	Environmental management system audit time for initial audit (auditor days, d)	ISMS audit time for initial audit (auditor days, d)	Additive and subtractive factors	Total audit time
1–10	2	2,5–3	5	See C.3.5	
11–15		3,5	6	See C.3.5	
16–25	3	4,5	7	See C.3.5	
26–45	4	5,5	8,5	See C.3.5	
46–65	5	6	10	See C.3.5	
66–85	6	7	11	See C.3.5	
86–125	7		12	See C.3.5	
126–175	8		13	See C.3.5	
176–275	9	10	14	See C.3.5	
276–425	10	11	15	See C.3.5	
426–625	11	12	16,5	See C.3.5	
626–875	12	13	17,5	See C.3.5	
876–1 175	13	15	18,5	See C.3.5	
1 176–1 550	14	16	19,5	See C.3.5	
1 551–2 025	15	17	21	See C.3.5	
2 026–2 675	16	18	22	See C.3.5	
2 676–3 450	17	19	23	See C.3.5	
3 451–4 350	18	20	24	See C.3.5	
4 351–5 450	19	21	25	See C.3.5	
5 451–6 800	20	23	26	See C.3.5	
6 801–8 500	21	25	27	See C.3.5	
8 501–10 700	22	27	28	See C.3.5	
> 10 700	Follow progression above	Follow progression above	Follow progression above	See C.3.5	

Audittime

ISO 27006-1:2024

Table D.1 — Classification of factors for calculating audit time

	Impact on effort		
	Reduced effort	**Normal effort**	**Increased effort**
Factors (see C.3.5)			
a) complexity of the ISMS: — information security requirements [confidentiality, integrity and availability, (CIA)] — number of critical assets — number of processes and services	— Only little sensitive or confidential information, low availability requirements — Few critical assets (in terms of CIA) — Only one key business process with few interfaces and few business units involved	— Higher availability requirements or some sensitive/confidential information — Some critical assets — 2-3 simple business processes with few interfaces and few business units involved	— Higher amount of sensitive or confidential information (e.g. health, personally identifiable information, insurance, banking) or high availability requirements — Many critical assets — More than 2 complex processes with many interfaces and business units involved
b) the type(s) of business performed within the scope of the ISMS	— Low risk business without regulatory requirements	— High regulatory requirements	— High risk business with (only) limited regulatory requirements
c) previously demonstrated performance of the ISMS	— Recently certified — Not certified but ISMS fully implemented over several audit and improvement cycles, including documented internal audits, management reviews and effective continual improvement system	— Recent surveillance audit — Not certified but partially implemented ISMS: Some management system tools are available and implemented; some continual improvement processes are in place but partially documented	— No certification and no recent audits — ISMS is new and not fully established (e.g. lack of management system specific control mechanisms, immature continual improvement processes, ad hoc process execution)

Audittime

ISO 27006-1:2024

Table D.4 — Impact of [illegible]rs on audit time

		IT complexity		
		Low (from 3 to	Medium (from 5 to 6)	High (from 7 to 9)
Business complexity	High (from 7 to 9)	+5 % to +20 %	+10 % to +50 %	+20 % to +100 %
	Medium (from 5 to 6)	−5 % to −10 %		+10 % to +50 %
	Low (from 3 to 4)	−10 % to −30 %	−5 % to −10 %	+5 % to +20 %

Audittime

ISO 27003:2017

Explanation Cl 4-10 of 27001

4 Context of the organization

4.1 Understanding the organization and its context

Required activity

The organization determines external and internal issues relevant to its purpose and affecting its ability to achieve the intended outcome(s) of the information security management system (ISMS).

Explanation

As an integral function of the ISMS, the organization continually analyses itself and the world surrounding it. This analysis is concerned with external and internal issues that in some way affect information security and how information security can be managed, and that are relevant to the organization's objectives.

Analysis of these issues has three purposes:

— understanding the context in order to decide the scope of the ISMS;

— analysing the context in order to determine risks and opportunities; and

— ensuring that the ISMS is adapted to changing external and internal issues.

ISO 27006-1:2024

Controls in ISO/ IEC 27001:2022, Annex A [a]	System testing	Visual inspection	Possible evidence of design and implementation of controls
5.2 Information security roles and responsibilities			— Allocated roles and responsibilities for implementation, operation and management of information security
5.3 Segregation of duties			— Identified conflicting duties or areas of responsibility, and corresponding rules for segregation
5.4 Management responsibilities			— Management statements and support for information security objectives, policies, procedures, etc. — Mentioning of personal responsibility for information security of personnel
5.5 Contact with authorities			— Defined contact points with relevant authorities — Rules for reporting incidents — Content of information flow from and to relevant authorities
5.6 Contact with special interest groups			— Membership and defined contact points with special interest groups, or other forums and associations [e.g. Computer Emergency Response Teams (CERTs), cybersecurity agencies] — les on what can be discussed within such izations — ent of information flow from and to such ganizations
5.7 Threat intelligence			— Approach to collecting relevant threat intelligence — Analysis of threat intelligence in relation to the organization and its dissemination to appropriate parties
5.8 Information security in project management			— Established information security in project management throughout the project life cycle, e.g. in requirements definition, testing — For a sample of projects, identified information security risks and corresponding risk treatment

Explanation A5-A8 of 27001 for auditor

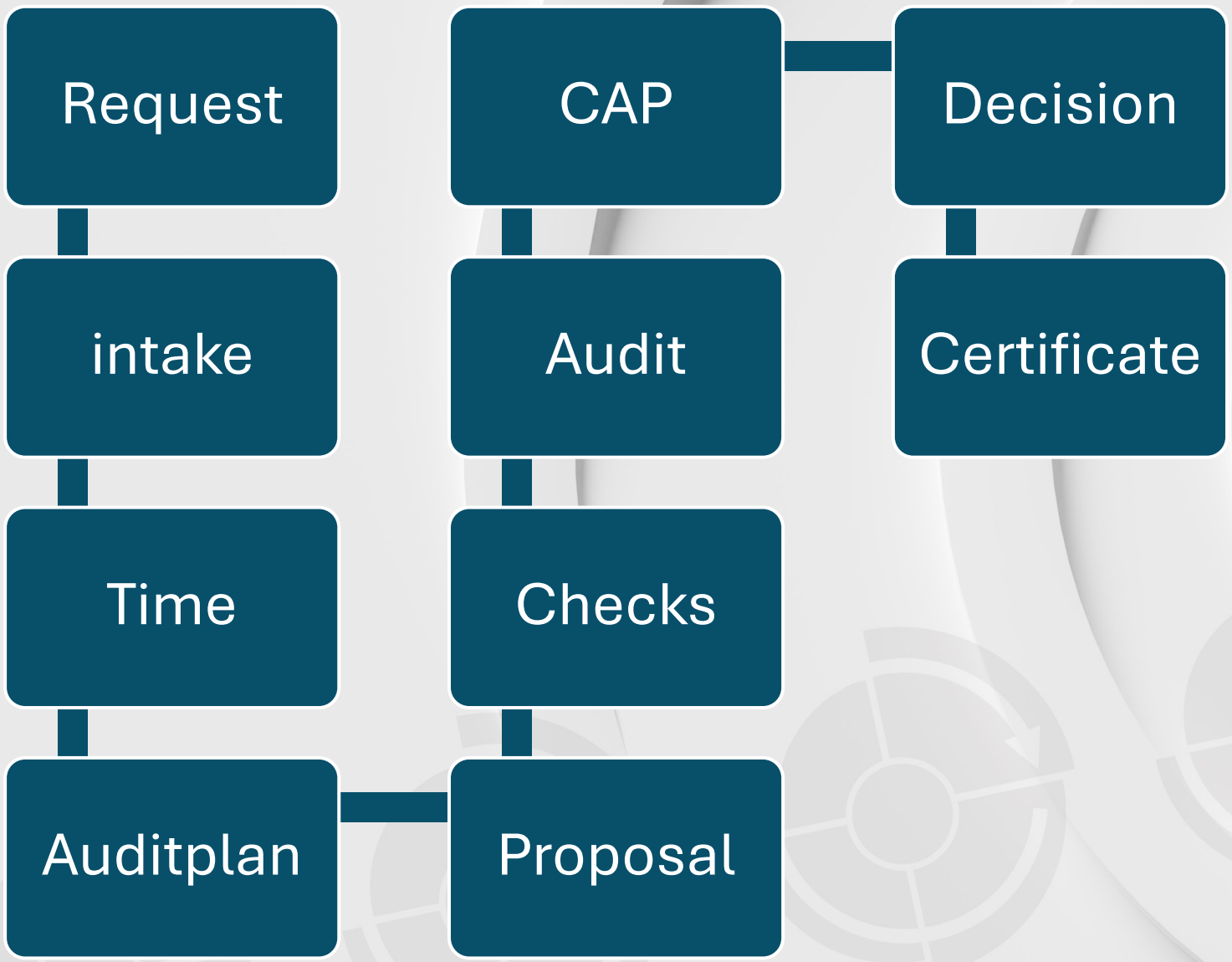
ISO 27007:2020

A.1 Context of the organization (ISO/IEC 27001:2013, Clause 4)	
A.1.1 Understanding the organization and its context (ISO/IEC 27001:2013, 4.1)	
Audit evidence	Audit evidence can be obtained through documented information or other information on: a) the important issues that can affect, either positively or negatively, the ISMS; b) the organization; c) the purpose of the organization; d) the intended out… f the ISMS. Possible sources of t… t issues can include: a) environmental cha… or conditions related to climate, pollution, resource availability, and biod… d the effect these conditions can have on the organization's ability to a… bjectives; b) the external cultural, social, … gal, regulatory, financial, technological, economic, natural and compe… xt, whether international, national, regional or local; c) characteristics or conditions of the orga… h as organizational governance, information flows and decision-making pr… — organizational policies, objectives, and t… rategies that are in place to achieve them; — the organization's culture; — standards, guidelines and models adopted by the organization; — the life cycle of the organization's products and services; — information systems, processes, science and technology underlying information security management;

Explanation C4-10 of 27001 for auditor

ISO 27007:2020

Audit practice guide	Auditors should confirm that the organization: a) has a ~~high-level (e.g. strategic)~~ understanding of the important issues that can affect, either positively or negatively, the ISMS; b) knows the external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its ISMS. NOTE 1 The requirement in ISO/IEC 27001:2013, 4.3 is to "consider the external and internal issues referred to in ISO/IEC 27001:2013, 4.1". An organization can take into consideration something that not necessarily appears in the output. Auditors should also confirm that the intended outcomes include preservation of the confidentiality, integrity and availability of information by applying a risk management process and that risks are adequately managed. Auditors should also verify that the issues include the important topics for the organization, problems for debate and discussion, or changing circumstances and also be verified that the knowledge gained is used to guide the organization's efforts to plan, implement and operate the management system.
Supporting documents	ISO 31000:2018, 5.3 ISO/IEC 27003:2017, 4.1

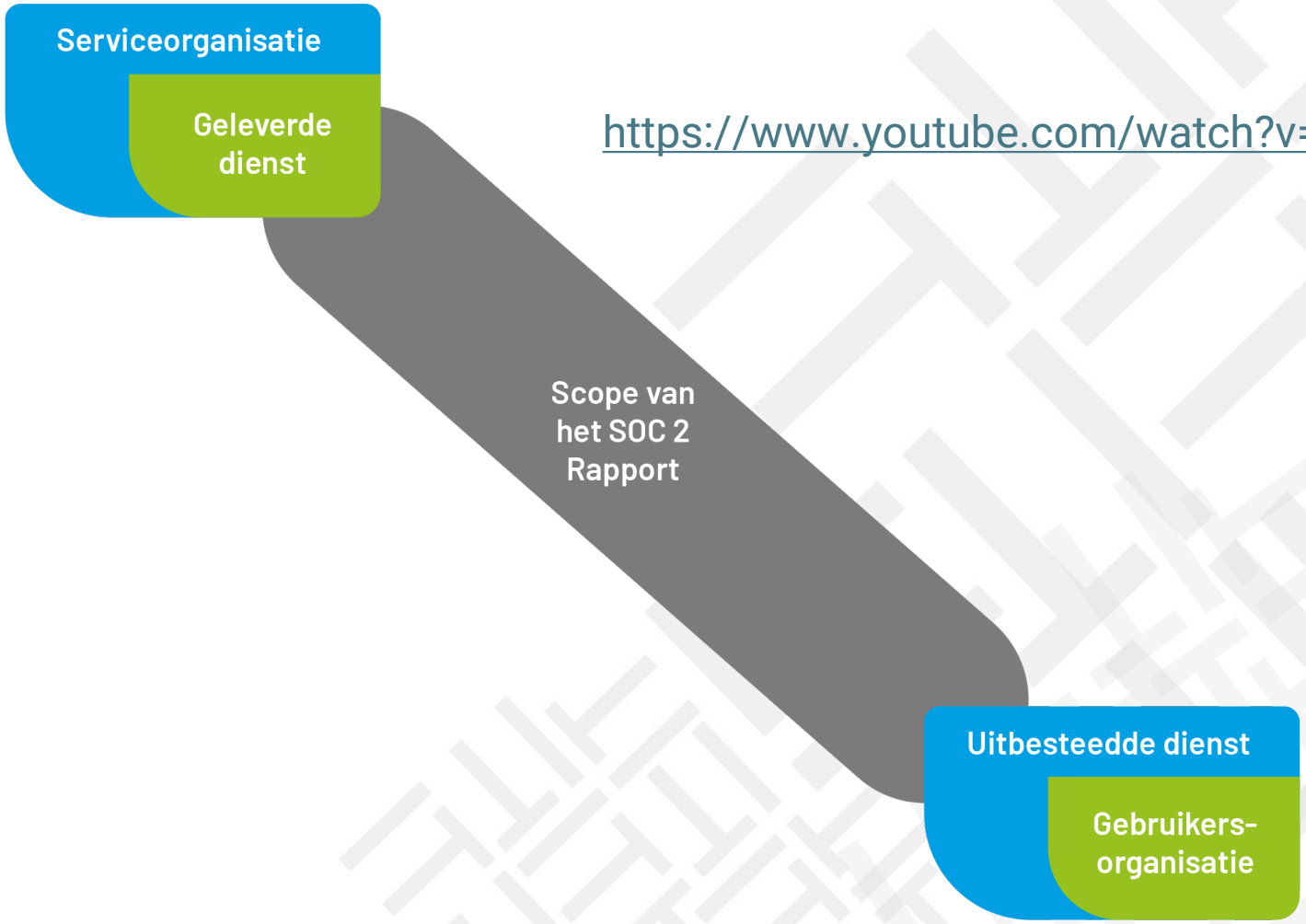

Request
intake
Time
Auditplan
CAP
Audit
Checks
Proposal
Decision
Certificate

AudITvision
IT-auditors

SOC 2

Mischa van der Vliet • 06 25057951 • mischa@auditvision.nl

System and Organization controls (SOC)



https://www.youtube.com/watch?v=41v83rfTkps

Official AICPA SOC badge.

Reasons for an assurance report

These reports can play an important role in:

- Oversight of the organization.
- Vendor management programs.
- Internal corporate governance and risk management processes.
- Regulatory oversight.
- Riskmanagement.
- Demand from customers!

Kind of SOC reports

SOC 1 — SOC for Service Organizations. Service organizations may provide services that are relevant to their user entities' internal control over **financial** reporting and, therefore, to the audit of financial statements. (SSAE18/AT-C 320)

SOC 2 — SOC for Service Organizations: Trust Services. Service organizations may provide services that are relevant to **Security, Availability, Processing Integrity, Confidentiality or Privacy.** (AT-C 205)

SOC 3 — SOC for Service Organizations: Trust Services Criteria for General Use Report. Although the requirements and guidance for performing a SOC 3 examination are similar to those for a SOC 2 examination, the reporting requirements are different. (AT-C 205)

3402←→SOC2

ISAE 3402: Financial driven processes (is IT financial?)
Well known in het market
No standard controls, based on risks

SOC2: Security driven
Less know, but in progress
Standard controls based on TSC 100:2020
5 areas (TSC)
Only a CPA allowed to make a ‘real’ SOC2
In the EU: ISAE3000 SOC2 by a RE or RA

SOC 3←→SOC 2

SOC 3: unqualified opinion

Type 2

No section 4 + 5

wide range of users

Can be put on the website

ISAE3000

Type 1 or Type 2?

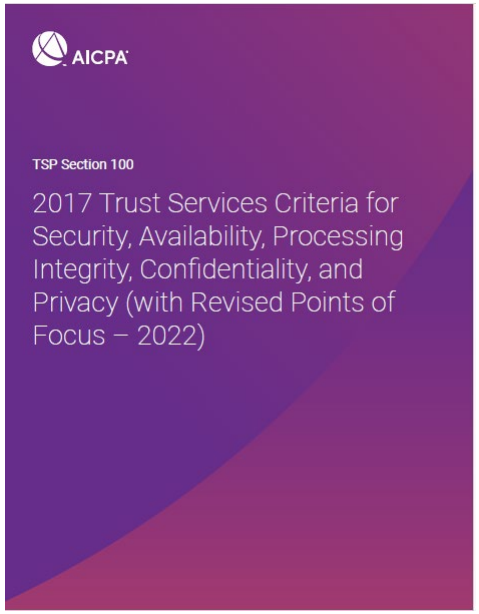
Similar to a SOC 1 report, there are two types of reports:

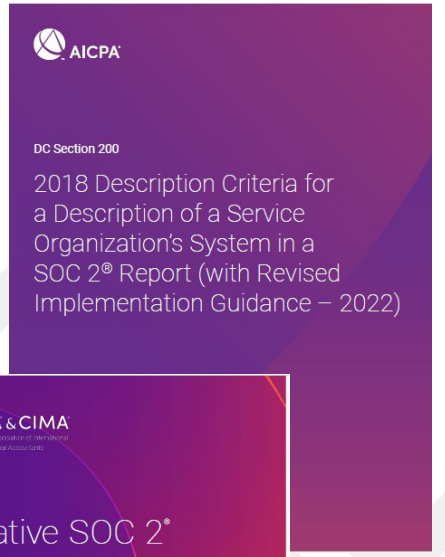
1. A type 1 report on management's description of a service organization's system and the suitability of the design of controls.

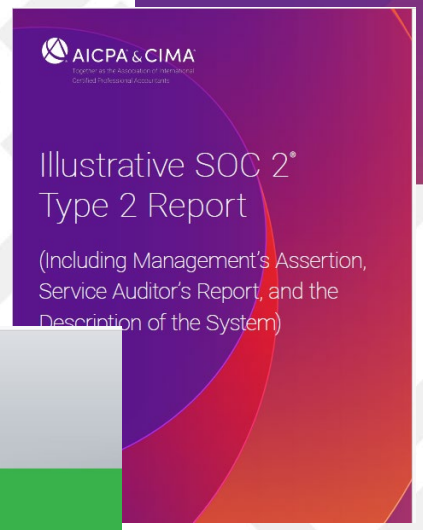
2. A type 2 report on management's description of a service organization's system and the suitability of the design and operating effectiveness of controls.

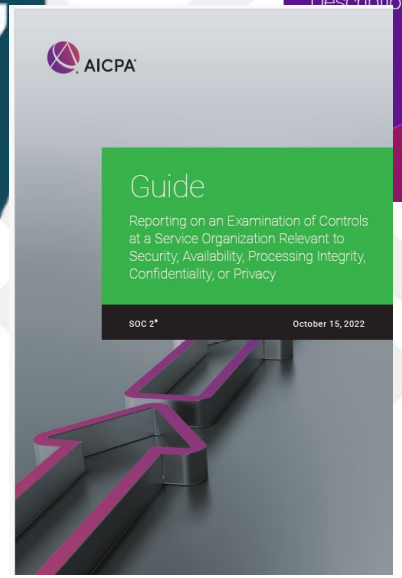
Use of these reports are restricted (not for a SOC 3).

Trust Service Category









SOC 2

Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy.

These reports are intended to meet the needs of a broad range of users that need detailed information and assurance about the controls at a service organization relevant to security, availability, and processing integrity of the systems the service organization uses to process users' data and the confidentiality and privacy of the information processed by these systems.

SOC 2 in NL

SOC2 ® brand is forbidden.

ISAE3000A Assurance report.

Title: System and Organization Controls report.

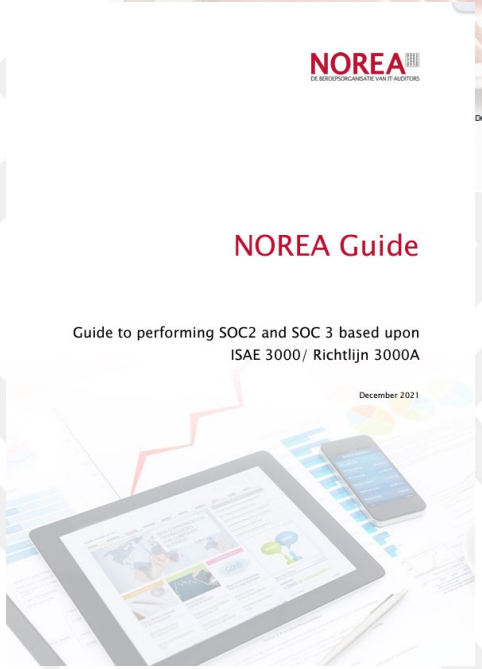
Under Dutch law.

Not a guideline (richtlijn), but a guide (handreiking)!

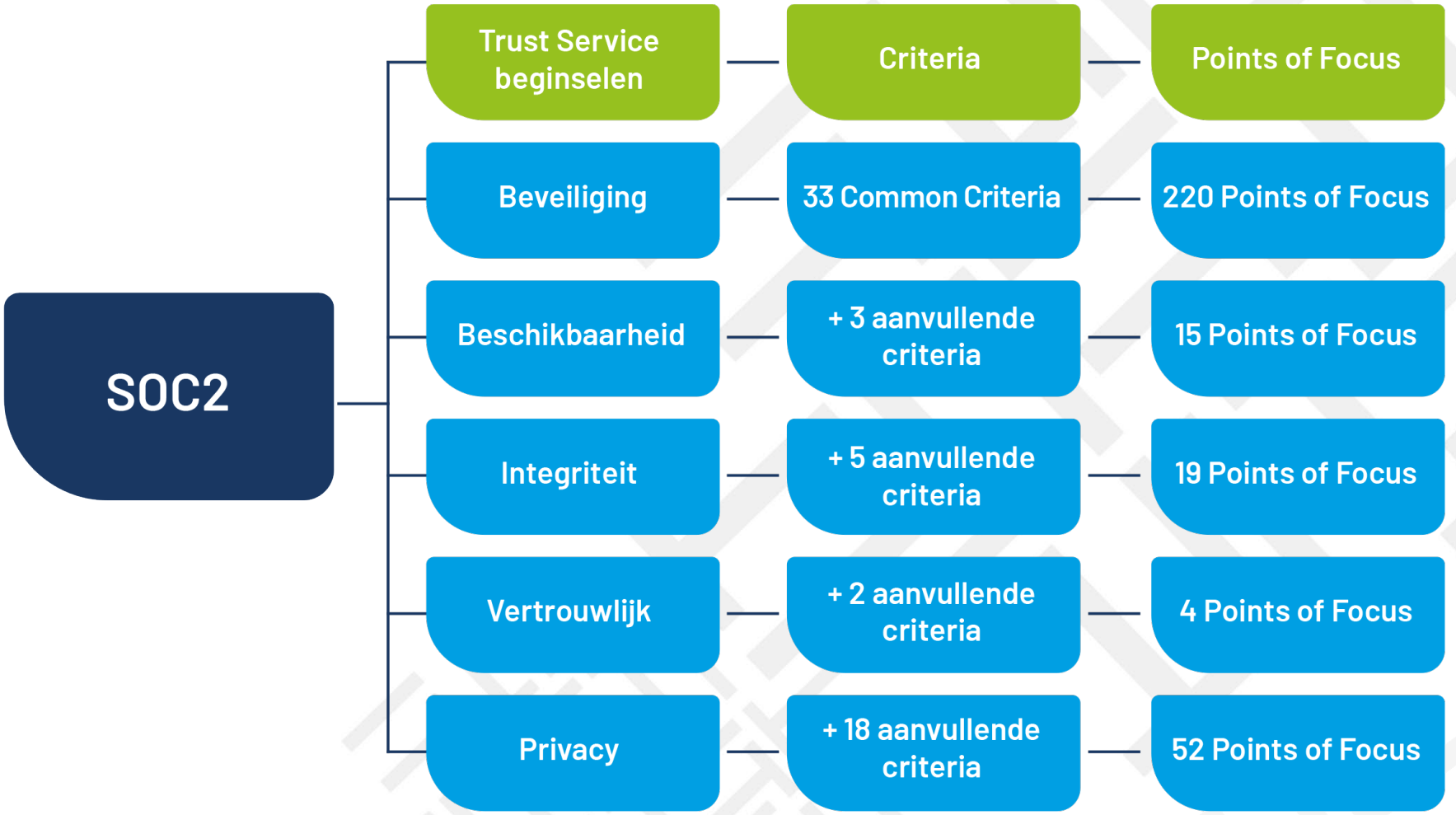
Knowledge necessary of: DC200, TSP100, SOC2 © guide

A ‘real’ SOC2 ® only by a CPA under AICPA.

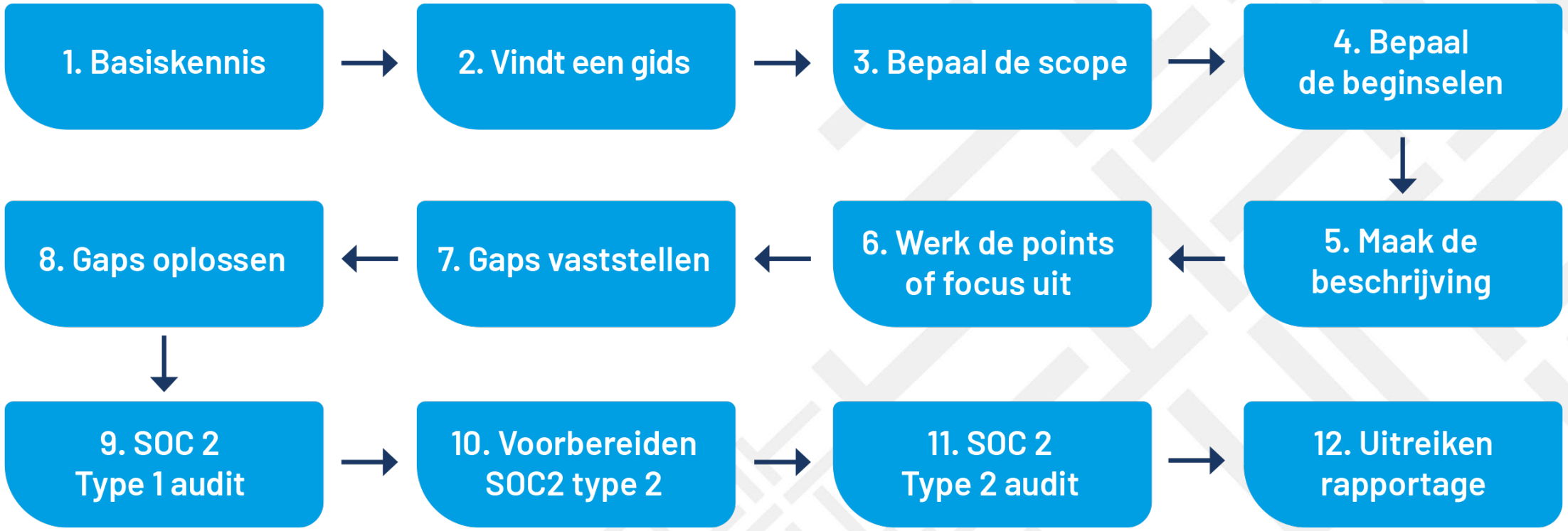
AT-C section 205 = ISAE3000



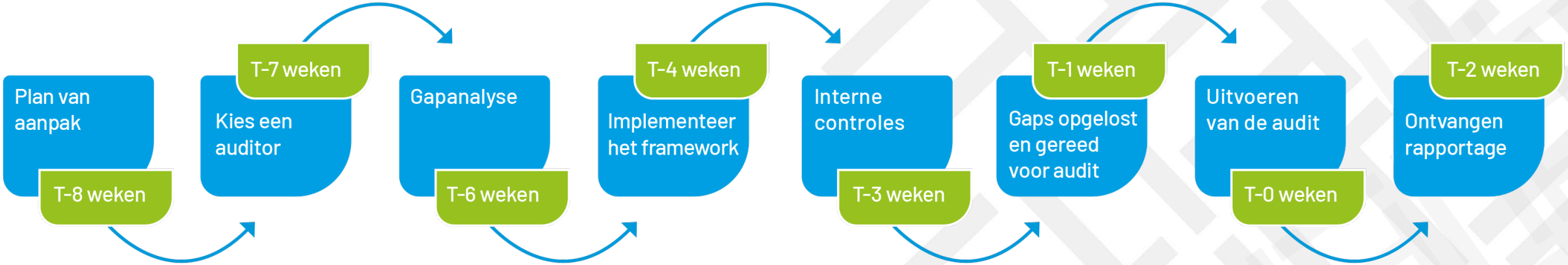
Compilation of TSC100



Process


1. Basiskennis
2. Vindt een gids
3. Bepaal de scope
4. Bepaal de beginselen
5. Maak de beschrijving
6. Werk de points of focus uit
7. Gaps vaststellen
8. Gaps oplossen
9. SOC 2 Type 1 audit
10. Voorbereiden SOC2 type 2
11. SOC 2 Type 2 audit
12. Uitreiken rapportage

Timeline


Plan van aanpak
T-8 weken
T-7 weken
Kies een auditor
Gapanalyse
T-6 weken
T-4 weken
Implementeer het framework
Interne controles
T-3 weken
T-1 weken
Gaps opgelost en gereed voor audit
Uitvoeren van de audit
T-0 weken
T-2 weken
Ontvangen rapportage

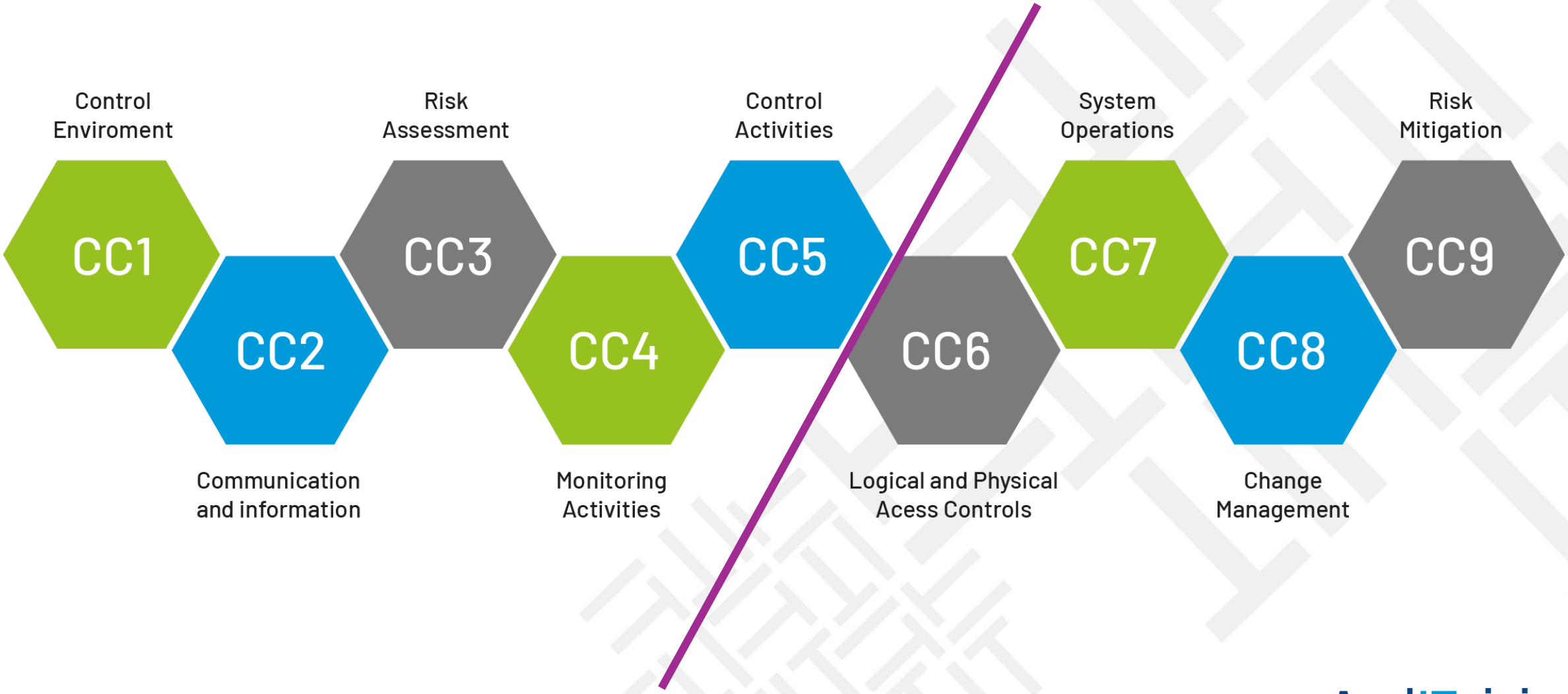
Scope: boundaries

- (a) across an entire entity;
- (b) at a subsidiary, division, or operating unit level;
- (c) within a function relevant to the entity’s operational, reporting, or compliance objectives; or
- (d) for a particular type of information used by the entity.

Scope: which category

- **Security**. Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to achieve its objectives.
- **Availability**. Information and systems are available for operation and use to meet the entity's objectives.
- Processing **integrity**. System processing is complete, valid, accurate, timely, and authorized to meet the entity's objectives.
- **Confidentiality**. Information designated as confidential is protected to meet the entity's objectives.
- **Privacy**. Personal information is collected, used, retained, disclosed, and disposed of to meet the entity's objectives.

Compilation of the Common Criteria



AudITvision IT-auditors

Organization of the Trust Services Criteria

Trust Services Category	*Common Criteria*	*Additional Category-Specific Criteria*
Security	X	N/A
Availability	X	X (A series)
Processing Integrity (Over the Provision of Services or the Production, Manufacturing, or Distribution of Goods)	X	X (PI series)
Confidentiality	X	X (C series)
Privacy	X	X (P series)

Beginsel	Aantal criteria
Beveiliging	33 algemene criteria
Beschikbaarheid	33 algemene + 3 aanvullende criteria
Integriteit van processen	33 algemene + 5 aanvullende criteria
Vertrouwelijkheid	33 algemene + 2 aanvullende criteria
Privacy	33 algemene + 18 aanvullende criteria

Points of focus

- The TSC100 presents points of focus for each criteria.
- The points of focus represent important characteristics of the criteria.
- The points of focus may assist management when designing, implementing, and operating controls.
- The points of focus may assist both management and the practitioner.
- Some points of focus may not be suitable or relevant to the entity or to the engagement to be performed.
- In such situations, management may customize a particular point of focus or identify and consider other characteristics based on the specific circumstances of the entity.
- Use of the trust services criteria does not require an assessment of whether each point of focus is addressed.

Reporting Title (nl)

[Name of the service organization]
[Short description of the service]
[Date of the report in case of a type I report]
[The reporting period in case of a type II report]

SOC2® Rapport!!

Relevant to Security [followed by one or more principles: Availability, Processing Integrity, Confidentiality and/or Privacy].

Reporting Content (nl)

- Type 1 or 2
- No minimum periode for the type 2 (3 months suggested).
- Same structure as a 3402:
  - I: management
  - II: IT-auditor
  - III: System
  - IV: Results
  - V: Other information
- Readers who understand the content.

I: management Statement

Management's description of the service organization's system fairly presents the service organization's system that was designed and implemented as of a specific date or throughout the specified period (type I and type II respectively), based on the criteria in [refer to the chapter, paragraphs or page numbers];

The controls stated in management's description of the service organization's system were suitably designed to meet to the applicable criteria (TSP section 100) as at a specific date or throughout the specified reporting period (type I and type II respectively);

The controls stated in management's description of the service organization's system operated effectively throughout the specified period to meet the applicable criteria (TSP section 100) (type II report)

II Independent service auditor's assurance report

Use of the word 'independent' in the title of the section containing the assurance report

- Scope of the engagement (including subservice organizations, user entity control considerations and / or other information)
- The comment that management is responsible for the description of the service organization's system;
- The comment that the engagement is performed in agreement with ISAE 3000, and for Dutch use in agreement with Richtlijn 3000A.
- The opinion:
    - o Fairness of the description
    - o The suitability of the design of controls; and
    - o In a type II report, the operating effectiveness of the controls.

II Deviations

The basis for evaluating materiality is whether a typical user entity or their auditor would change their actions had they been made aware of the exception.

Four kinds of exceptions:

1. Exceptions that are clearly inconsequential
2. Exceptions that do not result in the evaluation of the control as ineffective but that may be considered relevant to a user
3. Exceptions that require additional testing
4. Exceptions that result in the conclusion that the control did not operate effectively throughout the specified period, resulting in the evaluation of the control as ineffective.

II Conclusions

1. Unqualified opinion (only in this case a SOC3 is possible)
2. Qualified opinion (beperking)
3. Adverse opinion (afkeurend)
4. Disclaimer of opinion (onthouding)

III Service organization's description of its system

- The components of the system description as required are as follows:
  - The types of services provided;
  - The main service commitments and system requirements;
- The components of the system necessary for the provision of the service, consisting of:
  - o Infrastructure.
  - o Software.
  - o People.
  - o Procedures.
  - o Data.

- In the case of identified incidents which are the consequence.
- The applicable criteria and any related internal controls.
- If applicable, the necessary Complementary User Entity Controls (CUECs).
- If the use of a sub-service organization and the internal objectives of the sub-service organization.
- Any of the trust service criteria that is not relevant for the system and the reason why the criteria are indicated are not relevant.
- Relevant details of the significant changes relevant details of the significant changes to the system and the internal controls to the system and the internal controls (T2)

III (sub)Sub-service organisations

The inclusive method is applied:

- A description of the services provided by the sub-service organization;
- The necessary internal controls of the sub-service organization to achieve the objectives of the service organization;
- Relevant aspects of the infrastructure, software, people, procedures and data of the sub-service organization;
- Relevant parts of the systems that are the responsibility of the subservice organization.

The carve-out method is applied:

- A description of the services provided by the sub-service organization.
- Each of the trust service criteria which need to be achieved through the internal controls of the sub-service organizations.
- The internal controls that need to be implemented by the sub-service organization achieve the objectives of the service-organizations.

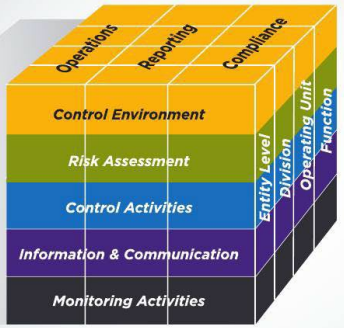
IV The principles, criteria, related controls, tests of controls including conclusion

- Principles and the associated criteria.
- Service organization control activity.
- The test approach.
- The test results per criteria.

V Other information provided by the service organization which is not assessed by the service auditor.

- Future plans for new systems.
- A plan to remediate any exceptions noted in the report.

COSO Internal Control — Integrated Framework Principles



Control Environment

1. The organization demonstrates a commitment to integrity and ethical values.
2. The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
3. Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
4. The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
5. The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

Risk Assessment

6. The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
7. The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.
8. The organization considers the potential for fraud in assessing risks to the achievement of objectives.
9. The organization identifies and assesses changes that could significantly affect the system of internal control.

Control Activities

10. The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
11. The organization selects and develops general control activities over technology to support the achievement of objectives.
12. The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.

Information & Communication

13. The organization obtains or generates and uses relevant, quality information to support the functioning of internal control.
14. The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
15. The organization communicates with external parties regarding matters affecting the functioning of internal control.

Monitoring Activities

16. The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
17. The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

For more information about COSO, visit coso.org.

Recap: In common

ISO 27001 en SOC 2
1. Security focus
2. External demonstration of trust
3. Overlapping controls: ❑ Risk management ❑ Data access management ❑ Physical security ❑ Awareness
4. Both have a set of controls
….

AudITvision IT-auditors

Recap: Difference

ISO 27001	SOC2
Focus on PDCA and improvement	Focus on assurance
Certificate	Report (no SOC2 logo)
Wide range of controls	Fewer controls
Timeline 6-12 months (PDCA)	Timelines more fluid
Short audittime	Long audittime
High over audit	In depth audit (espescially type 2)
More afforable	More expensive
LA-27001 and a CI	RA and RE
For CI procedures to the millimeter	High level procedures: big difference in Q
....	....

SOC2 or ISO27001?

- Demand for assurance is growing

- Impact of Ai-act and Cybersecurity act

- Is SOC2 and ISO27001 not outdated? And is AI the successor?

Procertify
Professionals in certification

ProCertify b.v.
Van der Houven van Oordtlaan 2
7316 AH Apeldoorn

t. 088-2028787

info@procertify.nl
www.procertify.nl