WEBINAR RECORDED

PECB

ISO/IEC 27001 vs SOC 2 vs ISAE 3000: Choosing the Right Assurance Path for Your Organization

APRIL 1 | 03:00 PM CEST

Peter Geelen
Cybersecurity Expert and Managing Director of CyberMinute

Erik Spaans
Director of ES Audit

#GlobalLeadingVoices

Agenda

- Introduction
- ISO > ISO 27001
- ISAE 3000/3402
- SOC2
- Comparison ISO 27001 vs Assurance
- Take aways

Introduction

ISO 27001, ISAE 3000/3402 or SOC2?

ISO 27001, ISAE 3000/3402 or SOC2?

Introduction

- Standards vs regulations
- ISO
  - International Standards
- ISAE
  - International Standard for Assurance Engagements
  - developed by: IAASB
    - International Auditing and Assurance Standards Board
  - supported by: IFAC
    - International Federation of Accountants
- SOC2
  - System and Organization Controls 2
  - AICPA
    - (American Institute of Certified Public Accountants)

IAASB
AN IFEA BOARD

AICPA®

Third Party Assurance?

Què?

- Giving Assurance
  - Giving security to the client or a third party.
  - A reasonable degree of certainty (material imperfections are found)
- By an Auditor
  - Expert (certified, qualified)
  - Conducting audits
  - The research area
- From an independent party
  - No connection with or dependence on the auditee

ISO 27001

Best practices and audit principles

PECB

ISO

International Standards Organisation

- Global organization
  - Officially : International Organisation for Standardisation
- National representation
- Standards and Best practices

- https://www.iso.org/about
- *"ISO is the short name for the International Organization for Standardization. It's not an acronym, but a name inspired by the Greek word isos, meaning "equal" – reflecting our mission to create standards that ensure consistency and equality worldwide. Because the organization's full name – and its initials – would vary across languages (for example Organisation internationale de normalisation in French), our founders chose "ISO" as a universal short form that could be recognized globally, regardless of language."*

ISO 27001 (ISMS)

What's in it?

- ISMS = Information Security Management System
- Based on ISO 9001 (QMS, Quality)
- Clauses & Annexes
- Clauses
  - Introduction +
  - 5 Management processes
  - PDCA
- Annex
  - 93 controls
  - PPPT (Process, People, Physical and Technology)

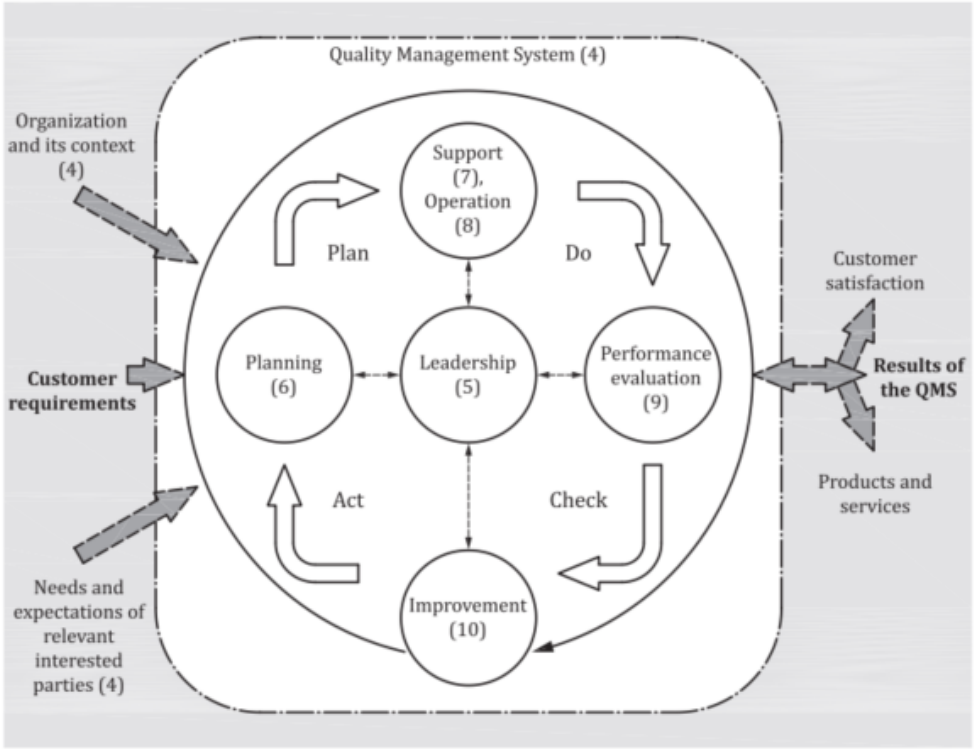
ISO 27001 (ISMS)

Clauses (Based on ISO 9001)

1. Scope of standard (info)
2. Normative references (info)
3. Terms and definitions (info)
4. Context
5. Leadership
6. Planning
7. Support
8. Operation
9. Performance evaluation
10. Improvement

0.3.2 Plan-Do-Check-Act cycle

The PDCA cycle can be applied to all processes and to the quality management system as a whole. Figure 2 illustrates how Clauses 4 to 10 can be grouped in relation to the PDCA cycle.



NOTE Numbers in brackets refer to the clauses in this International Standard.

Figure 2 — Representation of the structure of this International Standard in the PDCA cycle

PECB

ISO 27001 (ISMS)

Annex

ISO 27001 Annex = Derived from ISO 27002 (compacted)

1. Scope of standard (info)
2. Normative references (info)
3. Terms and definitions (info)
4. Structure of document (info)
5. Organisational controls (37)
6. People controls (8)
7. Physical Controls (14)
8. Technological controls (34)

ISO 27001 (ISMS)

Operational capabilities

Logical grouping of essential processes

1. #Governance
2. #Asset_management
3. #Information_protection
4. #Human_resource_security
5. #Physical_security
6. #System_and_network_security
7. #Application_security
8. #Secure_configuration
9. #Identity_and_access_management
10. #Threat_and_vulnerability_management
11. #Continuity
12. #Supplier_relationships_security
13. #Legal_and_compliance
14. #Information_security_event_management
15. #Information_security_assurance

ISO Standards vs Certification

ISO vs IAF

- ISO
  - Management of Standards & best practices
- IAF (International Accreditation Forum) = Certification
  - Members
    - Accreditation Groups
      - Afrac (Africa), APAC (Asia Pacific), ARAC (Arab), EA (EU), IAAC (Inter American), SADCA (South Africa)
    - Country level
      - Anab (US), BELAC (BE), COFRAC (FR), Dakks (DE), RVA (NL), …
    - Association members
      - IQNet, IPC, GlobalG.A.P., IIAO …

ISO 27001 (ISMS)

Implementation vs audit

- Implementation
  - Program & projects
  - Getting things done
- Audit (ref ISO 27006 & ISO 17021-1 §9.4.4.2)
  - Focus on evidence
  - People
  - Documentation (policies & procedures)
  - Proof of Operations

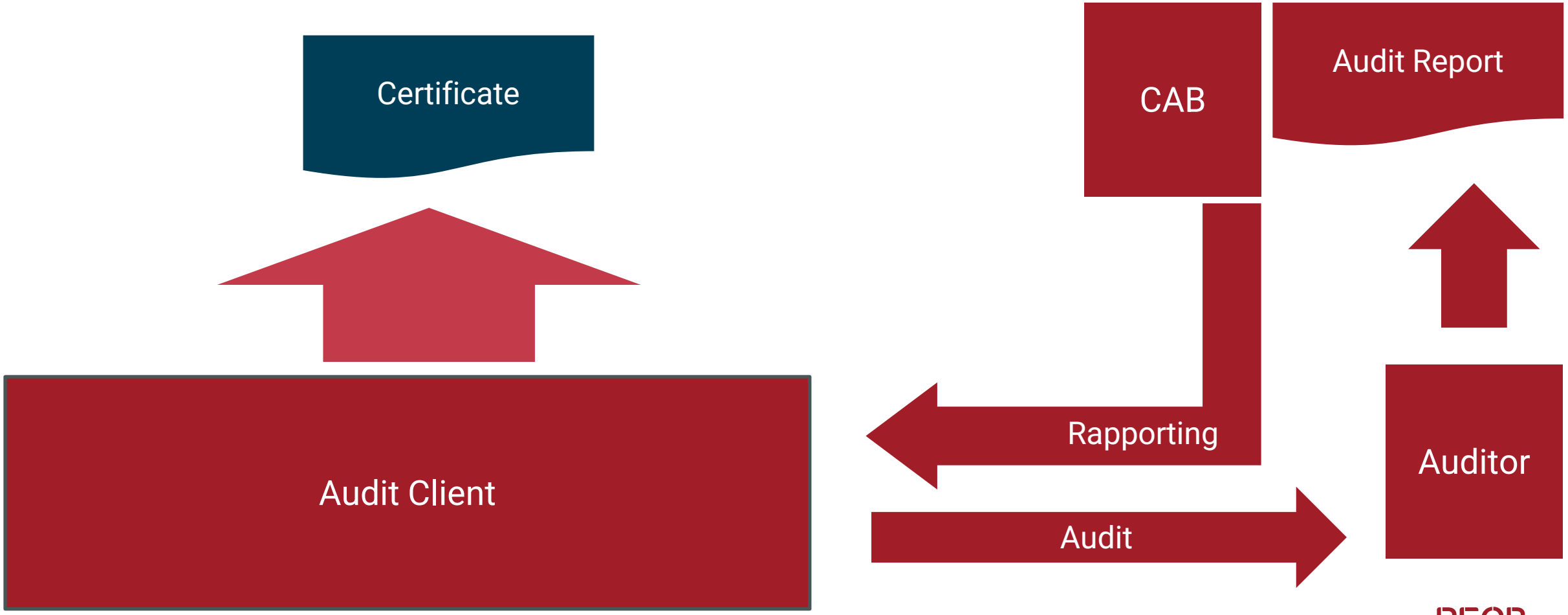
ISO 27001 Audit

Audit

- ISO 27006 (ISMS audit)
  - ISO 17021-1
  - Management system audit
- ISO19011
  - Guidelines for auditing management systems
- IAF MD series (Mandatory Documents)
  - IAF MD13:2023 Knowledge Requirements for Accreditation Body Personnel for Information Security Management Systems (ISO/IEC 27001)
  - IAF MD26:2023 Transition Requirements for ISO/IEC 27001:2022
  - IAF MD 1:2023 IAF Mandatory Document for the Audit and Certification of a Management System Operated by a Multi-Site Organization

ISO 27001 Audit

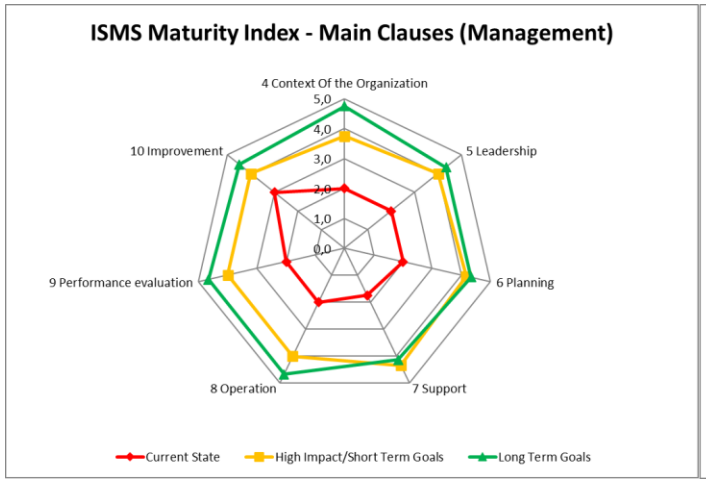
Audit

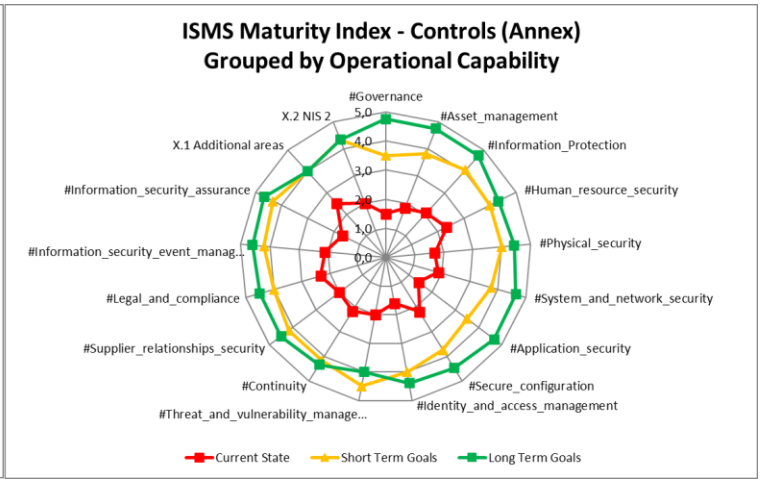


ISO 27001 Audit

Audit principles

- Compliance
  - Do what you say (set rules and follow them)
  - Say what you do (document your processes)
- Efffectiveness, less focus on efficiency
  - Get results
- Continual improvement = Growth based
  - Get in control
  - Start small
  - Ref. CMMI





PECB

ISAE 3000/3402 & SOC2

Assurance

PECB

ISAE

International Standard for Assurance Engagements

- ISAE 3000
- ISAE 3402

ISAE 3000

“Normal” Assurance report

- A "normal" assurance report, in which the assurance is given about historical non-financial information. Formerly also called a Third Party Communication.
- 2 shapes:
  - ISAE 3000A
    - Attestation assignment – The organization makes a claim (our system of internal control has in the period of ... up to and including ... to the best of our knowledge.
    - The auditor tests whether this claim is true.
  - ISAE 3000D
    - Direct assignment – The organization instructs the auditor to investigate something and the auditor makes an independent statement about this.

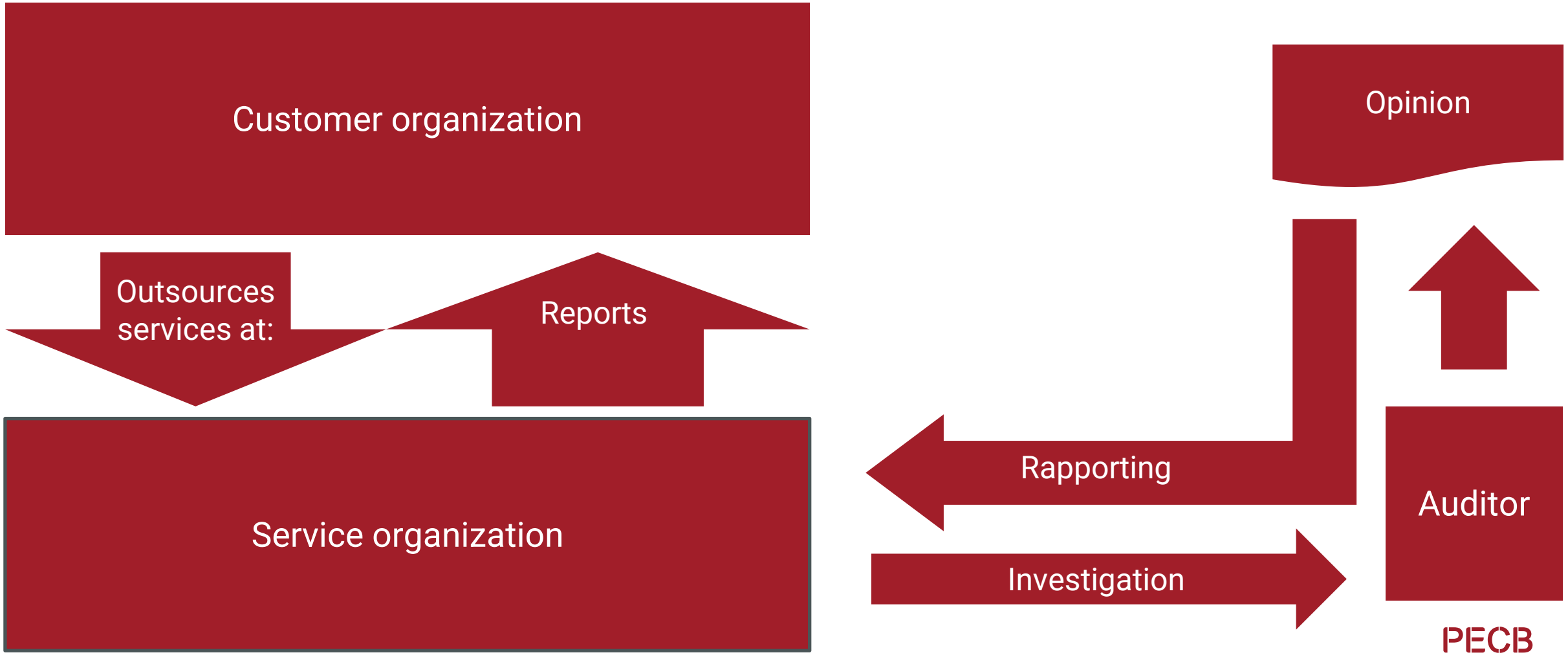
ISAE 3000/3402

Advanced Assurance report

- Is a combination of 2 standards from accountancy:
  - 3000 – assurance
  - 402 – Audits of entities that use a service organization
- An ISAE 3402 therefore also falls under the ISAE 3000 standard!

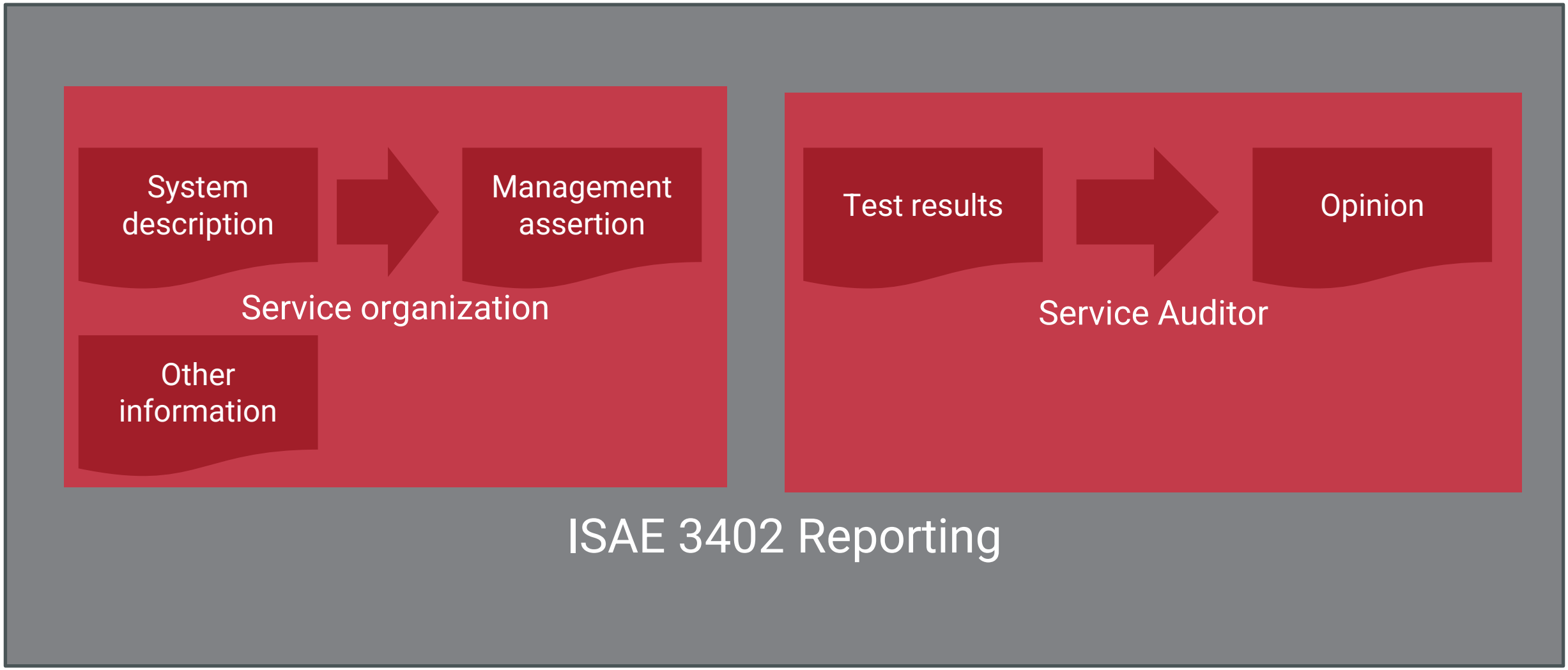
Assurance (ISAE & SOC2)

Audit



PECB

Assurance (ISAE & SOC2)



ISAE & SOC 2

Types of reporting

- Type I:
  - Point in time
  - Structure and existence
- Type II:
  - Over time
  - Design, existence and operation
  - over a period of
    - at least 6 months for ISAE 3000 and ISAE 3402 and
    - 3 months for SOC 2

ISAE

System description (ISAE 3000A + ISAE 3402)

- You can make intent in any way you want.
  - For example, according to the PDCA cycle
- The classification is free, the starting point is that the user of the report gets a correct and complete picture of the system of internal control

ISAE

System description - Plan

- Internal organisation (organisation chart);
- Social function;
- Mission and vision;
- Scope of the service to which the report relates;
- Objectives;
- Services and/or products;
- Purpose of this report;
- User Considerations.

ISAE

System description - Do

- Risk management
- Integrity
- Support
- Tasks, responsibilities and powers;
- Policy;
- Management system;
- Management objectives
- Processes and sub-processes;

ISAE

System description - Check

- Monitoring, measuring, analysing and evaluating;
- Internal audits;
- Management review.

ISAE

System description - act

- Reporting and communication;
- Treatment of abnormalities;
- Corrective actions;
- Continuous improvement.

SOC2

System description

SOC 2

System description

- About …
- Type of services provided
- **Principal service commitments and system requirements**
- **Components of the system**
- **Infrastructure**
- **Software**
- **People**
- **Procedures**
- **Data**

SOC 2

System description

- **System of internal control**
- Culture
- Integrity and Ethics
- Competence control
- Risk management
- Management measures
- Information and communication
- Change management
- Monitoring

SOC 2

System description

- Business continuity management
- Compliance with laws and regulations
- Boundaries of the system
- System incidents
- Applicable Trust Service Criteria and related controls
- Complimentary user entity controls
- Subservice organizations
- Third-party access
- Criteria not relevant to the system
- Changes throughout the period

SOC 2

TSC – Trust Service Criteria (full list at end of presentation)

- CONTROL ENVIRONMENT (CC1.1->5)
- COMMUNICATION AND INFORMATION (CC2.1->3)
- RISK ASSESSMENT (CC3.1->4)
- MONITORING ACTIVITIES (CC4.1->2)
- CONTROL ACTIVITIES (CC5.1->3)
- LOGICAL AND PHYSICAL ACCESS CONTROLS (CC6.1->8)
- SYSTEM OPERATIONS (CC7.1->5)
- CHANGE MANAGEMENT (CC8.1)
- RISK MITIGATION (CC9.1->2)

SOC 2

TSC – Additional criteria

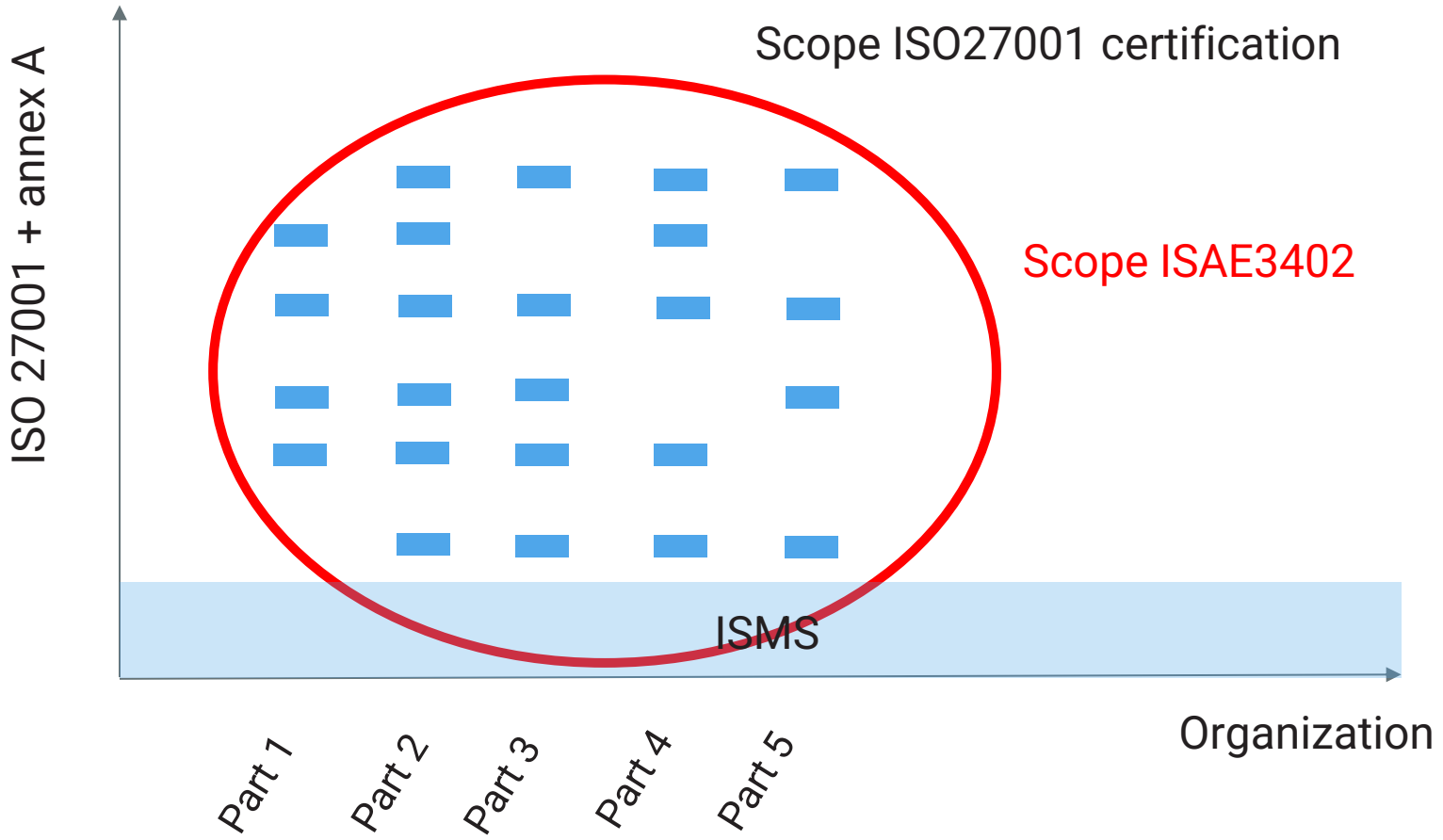
- ADDITIONAL CRITERIA FOR AVAILABILITY (A1.1>3)
- ADDITIONAL CRITERIA FOR CONFIDENTIALITY (C1.1>2)
- ADDITIONAL CRITERIA FOR PROCESSING INTEGRITY (PI1.1>5)
- ADDITIONAL CRITERIA FOR PRIVACY (P1.1>P8.1)

ISO vs ISAE/SOC

The comparison

Third Party Assurance - ISO27001

Scope



PECB

Third Party Assurance - ISO27001

Object of investigation

- ISO 27001
  - The information security management system plus
  - the organization's control measures.
- Assurance
  - The control measures relating to the service(s) outsourced by the customer.

Third Party Assurance - ISO27001

Quality aspects

- ISO 27001
  - CIA
    - Confidentiality
    - Availability
    - Integrity
- Assurance
  - To choose yourself, for example:
    - Accuracy;
    - Completeness;
    - Timeliness;
    - Exclusivity;
    - Correct operation;
    - cover specific (processing) risks.

Third Party Assurance - ISO27001

Standards

- ISO 27001
  - Clauses
  - Annex
- Assurance
  - A limited set of specific standards per service.
  - To be determined by the organization yourself.

Third Party Assurance - ISO27001

Focus

- ISO 27001
  - Prospective (1 > 3 years forward)
  - The certificate is issued for three years
  - based on the quality of the management system.
- Assurance
  - The certificate is issued for a period in the past (maximum 12 months).
  - There is no question of an expectation for the future.
  - There is no validity period!

Third Party Assurance - ISO27001

Focus Assurance

- ISAE 3402
  - Focus on financial information
  - related to the client's financial statements.
- SOC2
  - Focus on non-financial information,
  - especially information security

Third Party Assurance - ISO27001

Depth

- ISO 27001
  - The audit focuses on the functioning of the management system.
  - Continual improvement
  - Feedback loop (with escalation STR/OFI/-nc/+NC)
- Assurance
  - The audit focuses on the design and the existence or operation of the measures.
  - Yearly attestation (no escalation)

Third Party Assurance - ISO27001

Dynamic or static?

- ISO 27001
  - Dynamic
  - Risk coverage carried out by:
    - Risk-based periodic audit planning (3 years);
    - Evaluation of the results of the previous audit(s);
- Assurance
  - Static
  - Risk coverage carried out by:
    - Selection of measures based on risk analysis for specific customer(s);
    - Sample size
    - **New assignment every year!**

Third Party Assurance - ISO27001

Observations

- ISO 27001
  - Investigate imperfections for systematics and
  - handle them organization-wide
  - with the help of the management system.
- Assurance
  - No need to fix imperfections
  - Reporting
    - External
    - goes to (the auditors) of customers as accountability information

Third Party Assurance - ISO27001

Audit methods

- ISO 27001
  - Mainly interview-based
  - Limited insight into operation
  - Time spent is determined by the standard based on FTE and risk
  - The auditor may not take any evidence with him except (handwritten) notes.
  - Full audit every 3 years, between time-shorter audits in sub-areas
- Assurance
  - (Written) evidence required
  - Reporting goes to (the auditors) of customers as accountability information
  - Time commitment is determined by the auditor
  - For every claim made by the auditor, there must be sufficient supporting evidence in the file
  - A **full audit every year**.

Third Party Assurance - ISO27001

Reporting

- ISO 27001
  - Internal
  - The audit report goes to the Certifying Body,
  - which decides whether or not to issue the **certificate**.
- Assurance
  - External
  - The audit report goes to the auditee.
  - Auditee ensures distribution to (auditors of) **customers**

Third Party Assurance - ISO27001

Assurance Reporting

- ISAE 3402
  - A type 2 statement has a reporting period of at least 6 months.
- SOC2
  - A type 2 statement has a reporting period of at least 3 months.

Third Party Assurance - ISO27001

Transparency

- ISO 27001
  - Public
    - The certificate and
    - Reference to the accompanying statement of applicability
  - provide limited insight into the measures taken.
  - SoA (should not be) not published
- Assurance
  - The audit report shows specific measures taken and their effectiveness during the reporting period.

Third Party Assurance - ISO27001

System Description

- ISAE 3402
  - The system description can be freely arranged,
  - but it must be clear what the system of internal control entails and how it behaves
- SOC2
  - The system description contains mandatory components
    - Service commitments,
    - System requirements,
    - classification of the system into components:
      - Infrastructure, Software, People, Procedures, Data,
      - plus items from the TSC

Third Party Assurance - ISO27001

Control framework

- ISAE 3402
  - The framework is free to choose, both objectives and measures, but this framework must be in line with the system description.
- SOC2
  - The objectives that must be used are the TSC.
  - The CC (common criteria) are mandatory,
  - the others are not.

Third Party Assurance - ISO27001

Cost

- ISO 27001
  - Ref ISO 27006
  - 3 year cycle with yearly audit
  - Initial audit (100%)
  - Surveillance 1 (1/3) > Surveillance 2 (1/3)
  - Recert (2/3)
  - IA>SA1>SA2>RC … SA1>SA2>RC…
- Assurance
  - Yearly full scope
  - 10..50K…+ budget / year.

ISO/IEC 27006-1:2024(en)

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	1,5–2	2,5–3	5	See C.3.5	
11–15	2,5	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	8	12	See C.3.5	
126–175	8	9	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	

PECB

Take aways

PECB Courses

SOC 2 analyst

THANK YOU

✉ peter@cyberminute.com
in https://www.linkedin.com/in/pgeelen/
✉ erikspaans@ziggo.nl
in https://www.linkedin.com/in/erik-spaans-re-cisa-6464431/

WEBINAR RECORDED

PECB

ISO/IEC 27001 vs SOC 2 vs ISAE 3000: Choosing the Right Assurance Path for Your Organization

APRIL 1 | 03:00 PM CEST

Peter Geelen
Cybersecurity Expert and Managing Director of CyberMinute

Erik Spaans
Director of ES Audit

#GlobalLeadingVoices

Annex

Trust Service Criteria SOC 2

CONTROL ENVIRONMENT

CC1.1 COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.
CC1.2 COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
CC1.3 COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
CC1.4 COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
CC1.5 COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

Trust Service Criteria SOC 2

COMMUNICATION AND INFORMATION

CC2.1 COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.
CC2.2 COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
CC2.3 COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.

Trust Service Criteria SOC 2

RISK ASSESSMENT

CC3.1 COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
CC3.2 COSO Principle 7: The entity 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.
CC3.3 COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.
CC3.4 COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.

Trust Service Criteria SOC 2

MONITORING ACTIVITIES

CC4.1 COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
CC4.2 COSO Principle 17: The entity 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.

Trust Service Criteria SOC 2

CONTROL ACTIVITIES

CC5.1 COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
CC5.2 COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.
CC5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.

Trust Service Criteria SOC 2

Logical and Physical Access Controls

CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.
CC6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.
CC6.3 The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.
CC6.4 The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.
CC6.5 The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.
CC6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.
CC6.7 The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.
CC6.8 The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.

Trust Service Criteria SOC 2

System Operations

CC7.1 To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.

CC7.2 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.

CC7.3 The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.

CC7.4 The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.

CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.

Trust Service Criteria SOC 2

Change Management

CC8.1 The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.

Trust Service Criteria SOC 2

Risk Mitigation

CC9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.
CC9.2 The entity assesses and manages risks associated with vendors and business partners.

Trust Service Criteria SOC 2

ADDITIONAL CRITERIA FOR AVAILABILITY

A1.1 The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.

A1.2 The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back- up processes, and recovery infrastructure to meet its objectives.

A1.3 The entity tests recovery plan procedures supporting system recovery to meet its objectives.

Trust Service Criteria SOC 2

ADDITIONAL CRITERIA FOR CONFIDENTIALITY

C1.1 The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.
C1.2 The entity disposes of confidential information to meet the entity's objectives related to confidentiality.

Trust Service Criteria SOC 2

ADDITIONAL CRITERIA FOR PROCESSING INTEGRITY

PI1.1 The entity obtains or generates, uses, and communicates relevant, quality information regarding the objectives related to processing, including definitions of data processed and product and service specifications, to support the use of products and services.

PI1.2 The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity's objectives.

PI1.3 The entity implements policies and procedures over system processing to result in products, services, and reporting to meet the entity's objectives.

PI1.4 The entity implements policies and procedures to make available or deliver output completely, accurately, and timely in accordance with specifications to meet the entity's objectives.

PI1.5 The entity implements policies and procedures to store inputs, items in processing, and outputs completely, accurately, and timely in accordance with system specifications to meet the entity's objectives.

Trust Service Criteria SOC 2

ADDITIONAL CRITERIA FOR PRIVACY

P1.1 The entity provides notice to data subjects about its privacy practices to meet the entity's objectives related to privacy. The notice is updated and communicated to data subjects in a timely manner for changes to the entity's privacy practices, including changes in the use of personal information, to meet the entity's objectives related to privacy.

P2.1 The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice. Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons, if required. Such consent is obtained only for the intended purpose of the information to meet the entity's objectives related to privacy. The entity's basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented.

P3.1 Personal information is collected consistent with the entity's objectives related to privacy.

P3.2 For information requiring explicit consent, the entity communicates the need for such consent, as well as the consequences of a failure to provide consent for the request for personal information, and obtains the consent prior to the collection of the information to meet the entity's objectives related to privacy.

Trust Service Criteria SOC 2

ADDITIONAL CRITERIA FOR PRIVACY

P4.1 The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy.
P4.2 The entity retains personal information consistent with the entity's objectives related to privacy.
P4.3 The entity securely disposes of personal information to meet the entity's objectives related to privacy.
P5.1 The entity grants identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provides physical or electronic copies of that information to data subjects to meet the entity's objectives related to privacy. If access is denied, data subjects are informed of the denial and reason for such denial, as required, to meet the entity's objectives related to privacy.
P5.2 The entity corrects, amends, or appends personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity's objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to meet the entity's objectives related to privacy.

Trust Service Criteria SOC 2

ADDITIONAL CRITERIA FOR PRIVACY

P6.1 The entity discloses personal information to third parties with the explicit consent of data subjects, and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy.
P6.2 The entity creates and retains a complete, accurate, and timely record of authorized disclosures of personal information to meet the entity's objectives related to privacy.
P6.3 The entity creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures (including breaches) of personal information to meet the entity's objectives related to privacy.
P6.4 The entity obtains privacy commitments from vendors and other third parties who have access to personal information to meet the entity's objectives related to privacy. The entity assesses those parties' compliance on a periodic and as-needed basis and takes corrective action, if necessary.
P6.5 The entity obtains commitments from vendors and other third parties with access to personal information to notify the entity in the event of actual or suspected unauthorized disclosures of personal information. Such notifications are reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's objectives related to privacy.
P6.6 The entity provides notification of breaches and incidents to affected data subjects, regulators, and others to meet the entity's objectives related to privacy.
P6.7 The entity provides data subjects with an accounting of the personal information held and disclosure of the data subjects' personal information, upon the data subjects' request, to meet the entity's objectives related to privacy.

Trust Service Criteria SOC 2

ADDITIONAL CRITERIA FOR PRIVACY

P7.1 The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet the entity's objectives related to privacy.

P8.1 The entity implements a process for receiving, addressing, resolving, and communicating the resolution of inquiries, complaints, and disputes from data subjects and others and periodically monitors compliance to meet the entity's objectives related to privacy. Corrections and other necessary actions related to identified deficiencies are made or taken in a timely manner.