AUDITUL SECURITĂȚII INFORMAȚIONALE

Certificarea SMSI

Agenda

1. Ce este cerificarea SMSI conform ISO 27001, beneficii, dinamica certificării
2. Fluxul activităților de certificare SMSI
3. Documentarea auditului

Ce este cerificarea SMSI conform ISO 27001

Ce este certificarea

- Certificarea de conformitate a sistemelor de management, a personalului sau a produselor cu cerințele predefinite
- Reprezintă acțiunea unei terțe părți (organism de certificare)
- ce demonstrează că organizația furnizează servicii și/sau produse
- în conformitate cu un anumit standard referențial
- **Asigurarea** că sistemul a fost creat, implementat și funcționează conform cu cerințele standardului de referință
- sau că persona deține calificarea de profesionist în aria respectivă

Cine poate ceritfca conformitatea SMSI cu ISO 27001

- O organizație trebuie să treacă o procedură de certificare
- Dirijată de către o organizație de certificare autorizată (organism de certificare RCBs înregistrat, sau organizație de audit).
- ISO oferă o listă de cca 50 RCBs din peste 30 de state dezvoltate, așa ca SUA, Anglia, Germania etc.

ISO Registered Certified Bodies,

http://isolegalization.com/iso-registered-certified-bodies-list

Beneficiile certificării SMSI

- **Angajamentul Managementului/**responsabilitatea față de securitatea informațiilor
  - Alocarea resurselor umane, de timp, efort, finanțare etc.)
  - Selectarea controalelor și pentru aplicarea acestor controale în cadrul organizației
- **Eficiența securității informațiilor**
  - Creșterea gradului de conștientizare a securității informațiilor în cadrul organizației
  - Protecția adecvată a bunurilor organizaționale
  - Eficacitatea controalelor este măsurată și raportată
- **Conformitatea cu cerințele legale**
  - Demonstrează respectarea proactivă a autorităților de reglementare
  - Poate fi folosit ca cadru comun pentru alte standarde/cerințe de reglementare
  - Risc redus de răspundere
- **Construirea și menținerea încrederii**
  - Utilizată pentru a valida practicile de securitate și pentru a oferi încredere terților
  - Eficiență operațională obținută prin procese repetate de monitorizare a conformității
  - Conferă încredere/garanții partenerilor de afaceri, colaboratorilor, administrației că SMSI elaborat și implementat în organizația certificată corespunde standardelor în vigoare
- **Îmbunătățire continuă**
  - Permite dezvoltarea unei organizații introspective, agile și reziliente
  - Oferă suport pentru menținerea și îmbunătățirea permanentă a SMSI

Avantajele certificării SMSI

- Conferă încredere că SMSI elaborat și implementat de organizație corespunde standardelor în vigoare
- Oferă suport pentru menținerea și îmbunătățirea permanentă a SMSI
- Conferă partenerilor de

afaceri, colaboratorilor,

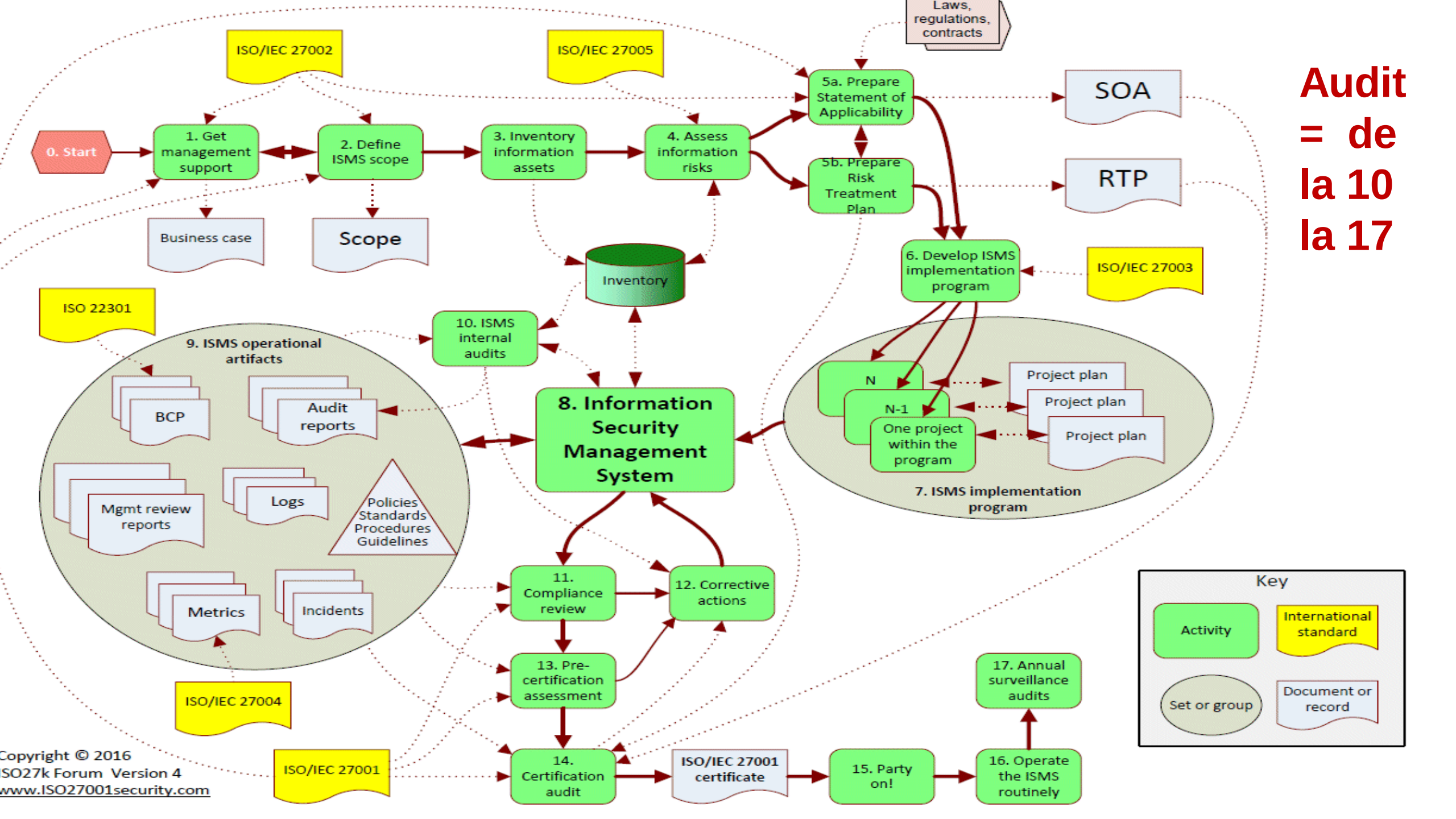
administrației garanții

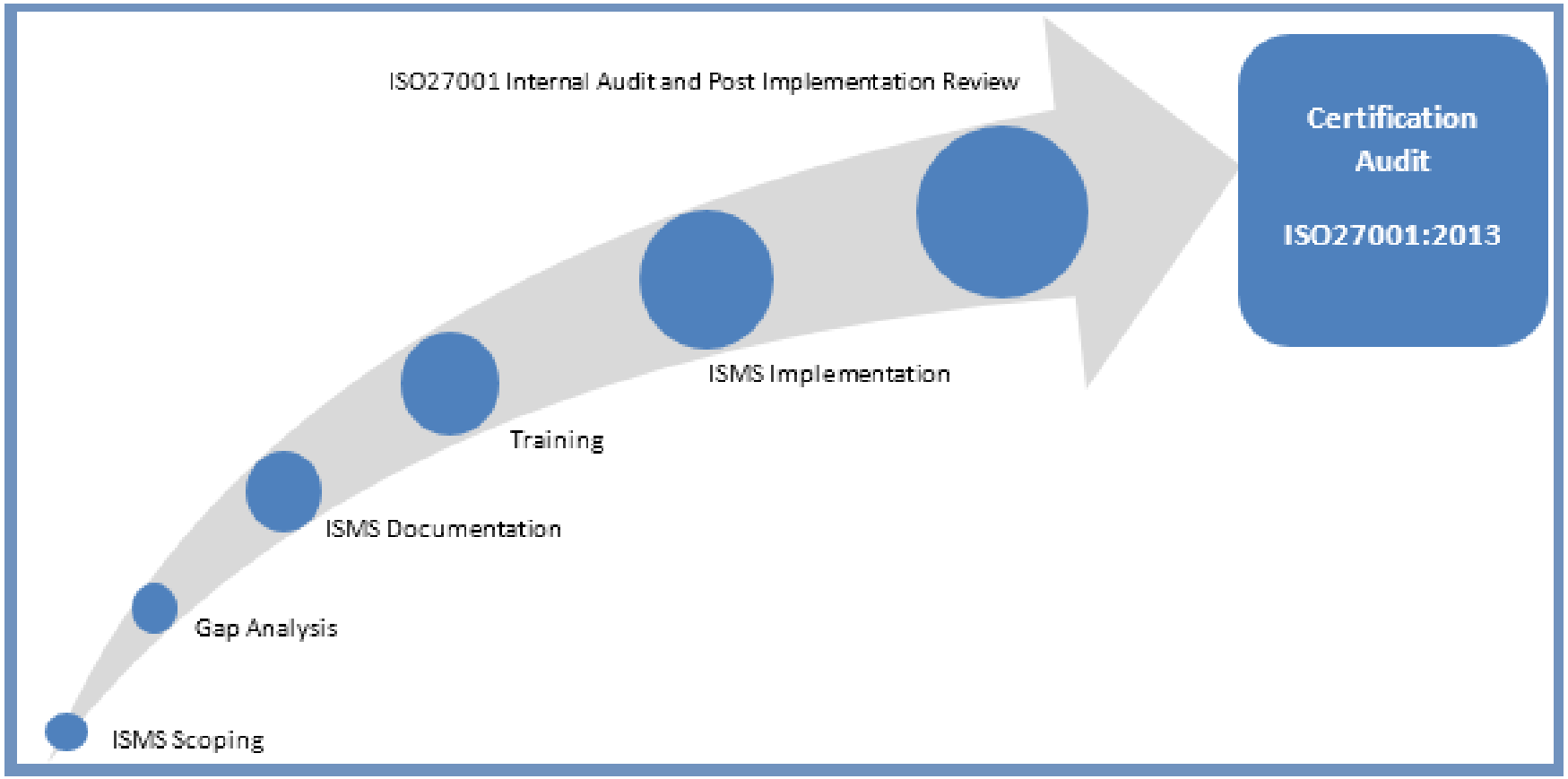
referitoare la managementul

securității informațiilor în

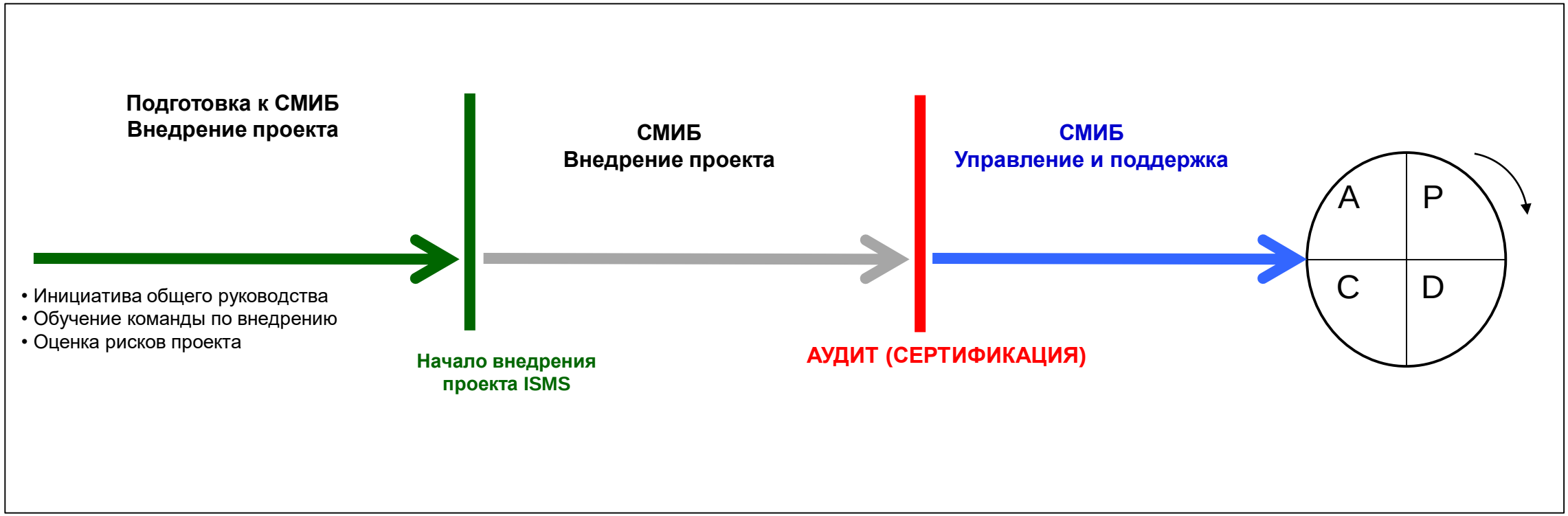
organizația certificată

Fluxul activităților de certificare SMSI

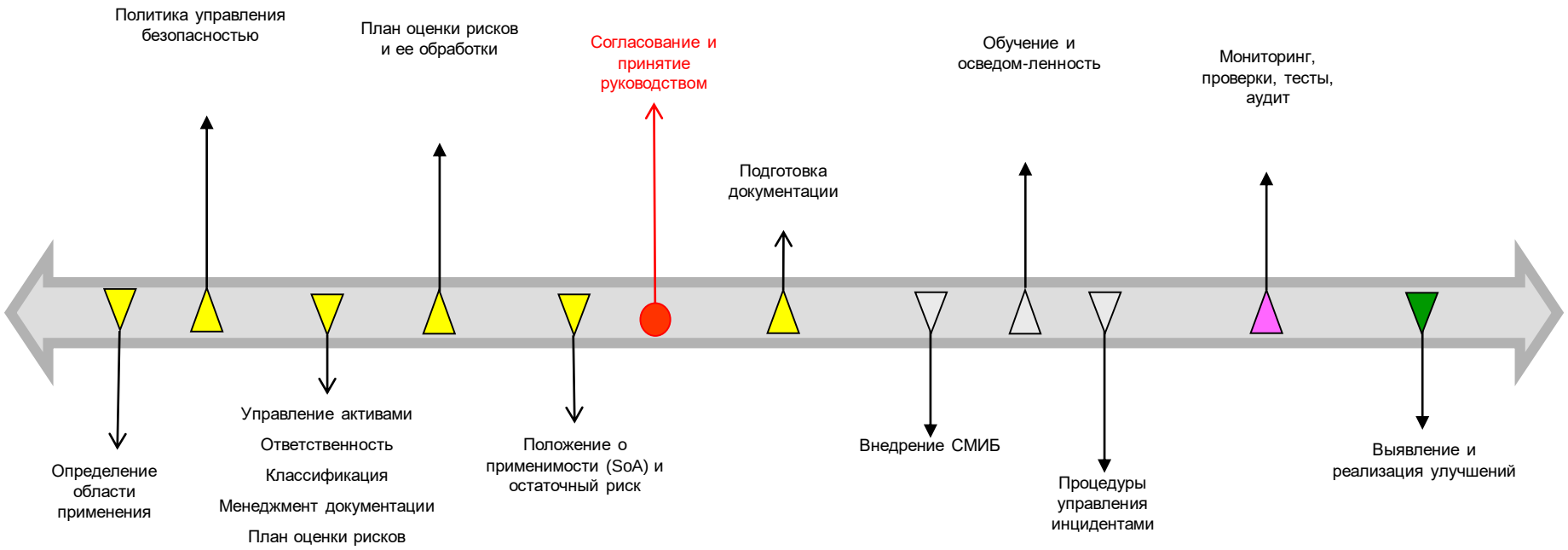

Audit = de la 10 la 17
ISO/IEC 27002
ISO/IEC 27005
Laws, regulations, contracts
0. Start
1. Get management support
2. Define ISMS scope
3. Inventory information assets
4. Assess information risks
5a. Prepare Statement of Applicability
5b. Prepare Risk Treatment Plan
SOA
RTP
Business case
Scope
Inventory
6. Develop ISMS implementation program
ISO/IEC 27003
ISO 22301
10. ISMS internal audits
9. ISMS operational artifacts
BCP
Audit reports
Mgmt review reports
Logs
Policies Standards Procedures Guidelines
Metrics
Incidents
8. Information Security Management System
N
N-1
One project within the program
Project plan
Project plan
Project plan
7. ISMS implementation program
11. Compliance review
12. Corrective actions
13. Pre-certification assessment
14. Certification audit
ISO/IEC 27001 certificate
15. Party on!
16. Operate the ISMS routinely
17. Annual surveillance audits
ISO/IEC 27004
ISO/IEC 27001
Key
Activity
International standard
Set or group
Document or record
Copyright © 2016
ISO27k Forum Version 4
www.ISO27001security.com

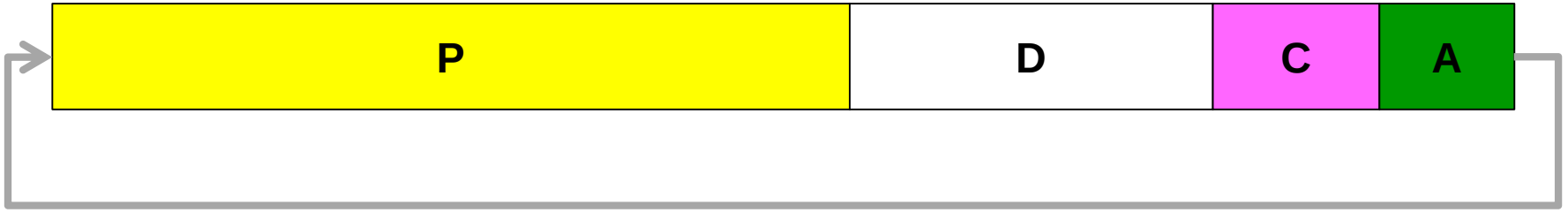

ISO27001 Internal Audit and Post Implementation Review
Certification Audit
ISO27001:2013
ISMS Implementation
Training
ISMS Documentation
Gap Analysis
ISMS Scoping

Стадии внедрения системы менеджмента информационной безопасности (SMSI)

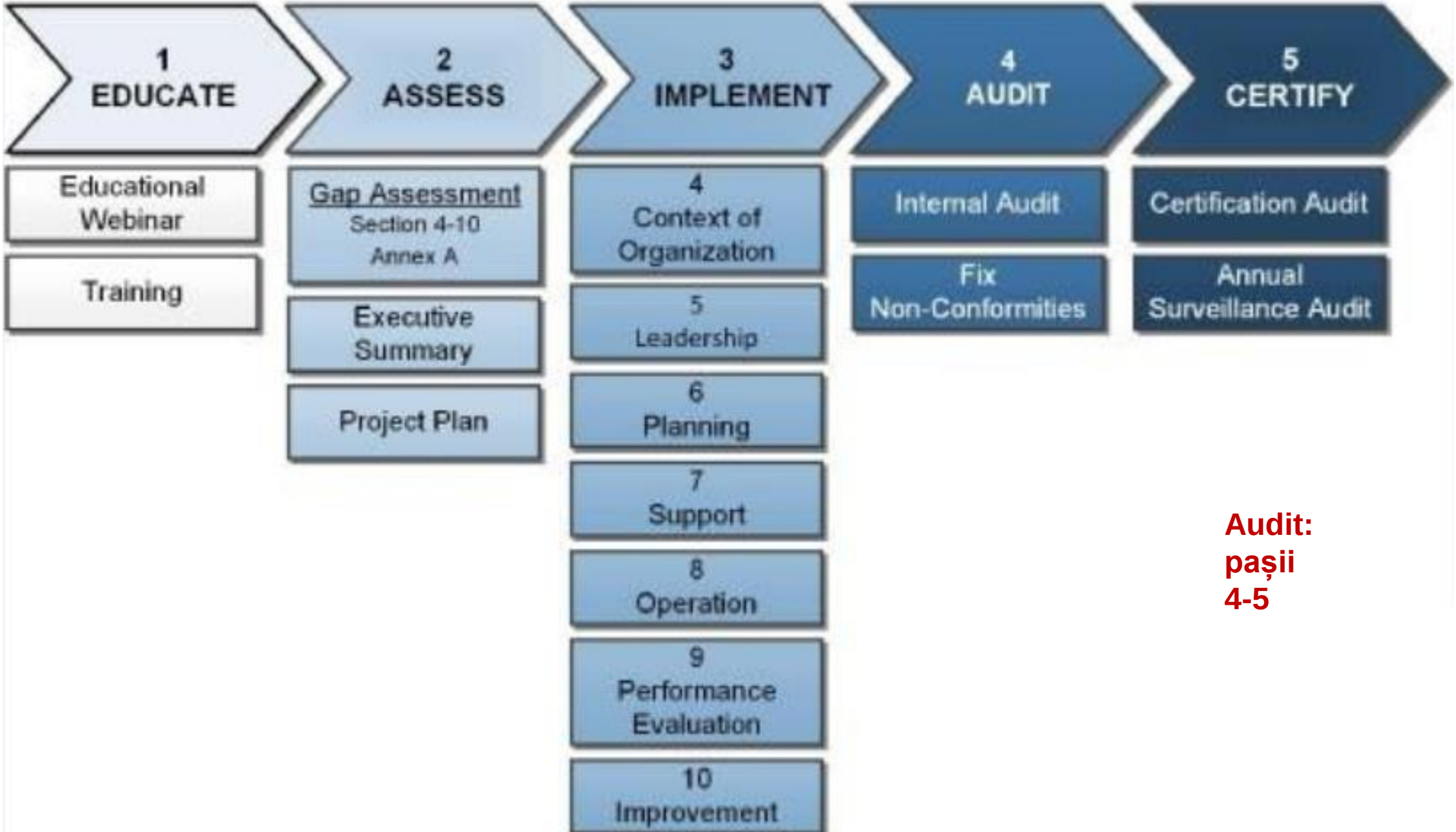


Состав проекта внедрения СМИБ согласно ISO/IEC 27001





5 Step - ISO 27001 Implementation Process

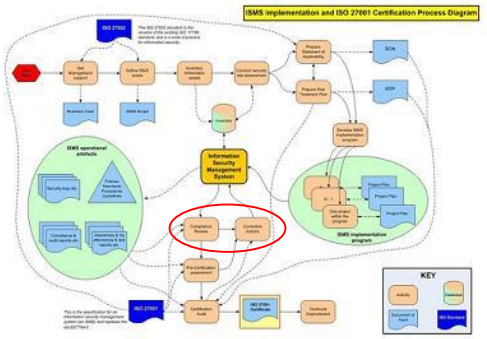


Audit: pașii 4-5

Etapele certificării unui SMSI

1. Contactarea organismului de certificare
2. Inițierea certificării SMSI
3. Semnarea contractului
4. Stabilirea echipei de audit
5. Auditul de evaluare
6. Certificarea
7. Supravegerea organizațiilor certificate

Compliance Review and Corrective Actions

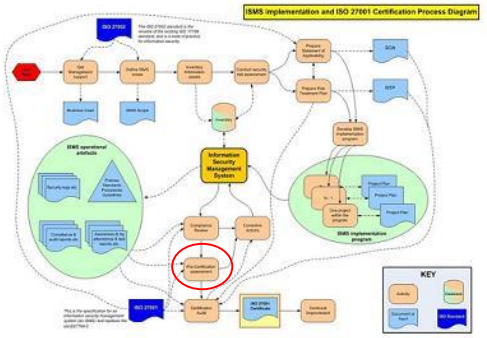


Compliance Review

Corrective actions

- Management must review the organization's ISMS at least once a year to ensure its continuing suitability, adequacy and effectiveness.
- They must assess opportunities for improvement and the need for changes to the ISMS, including the information security policy and information security objectives.
- The results of these reviews must be clearly documented and maintained ("records").
- Reviews are part of the 'Check' phase of the PDCA cycle: any corrective actions arising must be managed accordingly.

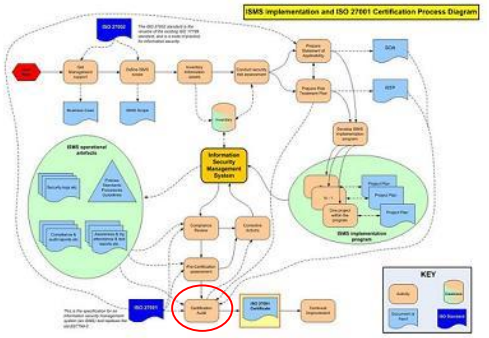
Pre-Certification Assessment



Pre-Certification Assessment

- Prior to certification, the organization should carry out a comprehensive review of the ISMS and SOA.
- The organization will need to demonstrate compliance with both the full PDCA cycle and clause 8 of ISO27001, the requirement for continual improvement.
- Certification auditors will seek evidence (in the form of records of processes such as risk assessments, management reviews, incident reports, corrective actions *etc.*) that the ISMS is operating and continually improving.
- The ISMS therefore needs a while to settle down, operate normally and generate the records after it has been implemented.

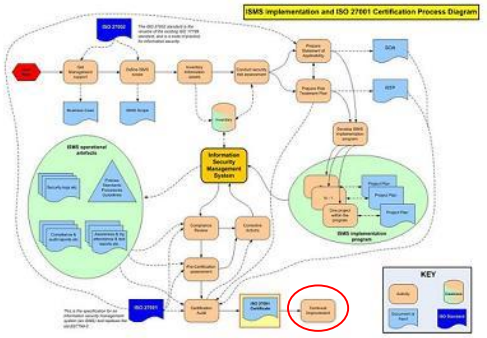
Certification Audit



Certification Audit

- Certification involves the organization's ISMS being assessed for compliance with ISO27001.
- The certification body needs to gain assurance that the organization's information security risk assessment properly reflects its business activities for the full scope of the ISMS.
- The assessors will check that the organization has properly analysed and treated its information security risks and continues managing its information security risks systematically.
- A certificate of compliance from an accredited certification body has credibility with other organizations

Certification Audit



Continual Improvement

- The organization shall continually improve the effectiveness of the ISMS through the use of:
  - The information security policy;
  - Information security objectives;
  - Audit results;
  - Analysis of monitored events;
  - Corrective and preventive actions;
  - Management review.

Documentarea auditului

Mandatory documented information required for certification

1. ISMS scope (as per clause 4.3)
2. Information security policy (clause 5.2)
3. Information security risk assessment *process* (clause 6.1.2)
4. Information security risk treatment *process* (clause 6.1.3)
5. Information security objectives (clause 6.2)
6. Evidence of the competence of the people working in information security (clause 7.2)
7. Other ISMS-related documents deemed necessary by the organization (clause 7.5.1b)
8. Operational planning and control documents (clause 8.1)
9. The *results* of the risk assessments (clause 8.2)
10. The *decisions* regarding risk treatment (clause 8.3)
11. Evidence of the monitoring and measurement of information security (clause 9.1)
12. The ISMS internal audit program and the results of audits conducted (clause 9.2)
13. Evidence of top management reviews of the ISMS (clause 9.3)
14. Evidence of nonconformities identified and corrective actions arising (clause 10.1)
15. Various others subject to specific control in Annex A.

Întrebări de autocontrol

1. Care sunt procesele și activitățile desfășurare în cadrul certificării SMSI?
2. Fluxul de implementare SMSI este același pentru orice organizație din oricare domeniu? Întemeiați
3. Fluxul de certificare SMSI este același pentru orice organizație și orice certificator? Întemeiați