Auditul Securității Informației (ASI)

Motto
în God we trust. Everyone else we audit!
Baczko, 2007: 787

Доверяй, но проверяй!

Principiile auditului

Titular de curs și autor: Tudor Bragaru, dr., conf. univ.
Tel. oficiu (330/4) 067-56-04-34 e-mail: theosnume@gmail.com

Agenda

1. Principii generale ale auditului
2. Principiile Auditului IT/IS conform CobIT

1. Principiile generale ale auditului

Principii de audit

1. **Independență**: bază pentru imparțialitatea și obiectivitatea concluziilor de audit
   - *Auditorii sunt independenți de activitatea auditată și liberi de ambiguități și conflicte de interese*
   - *Auditorii își mențin o gândire obiectiva de-a lungul procesului de audit pentru a asigura ca atât constatările cat și concluziile auditului vor fi bazate exclusiv pe dovezi obiective*
2. **Abordarea bazată pe dovezi**: *metoda rațională* pentru a obține concluzii/rezultate fiabile și reproductibile *într-un proces de audit sistematic*

Trei principii de bază ale auditului intern

1. **Principiul universalității** – *auditul se aplică tuturor:*
   - *Organizațiilor*
   - *Funcțiilor*
2. **Principiul independenței** – aceasta funcție trebuie situată la cel mai înalt nivel ierarhic
3. **Principiul periodicității -** funcție permanentă în cadrul entității, care se exercită periodic

Principiul universalității

Universalitatea auditului intern este explicată în funcție de:

1. Aria de aplicabilitate
2. Scopul
3. Rolul
4. Profesionalismul persoanelor implicate

Principii referitoare la auditori

1. **Conduita etică =** *baza profesionalismului. Încrederea, integritatea, confidențialitatea* și discreția sunt esențiale pentru auditare.
2. **Prezentarea corectă =** *obligația de a raporta corect și precis.*
3. **Grija profesionala necesara** = *aplicarea diligenței și raționamentului în auditare.* Un factor esențial îl constituie competenta.

Constatările auditului

1. Constatările auditului, concluziile auditului și rapoartele de audit reflecta în mod corect și precis activitățile de audit.
2. Trebuie raportate obstacolele întâmpinate în timpul auditului și divergențele de opinie nerezolvate intre echipa de audit și auditat
3. Auditorii acționează cu grija necesară în conformitate cu importanța sarcinii îndeplinite și încrederea care le este acordată de clienți și alte părți Interesate. Un factor esențial îl constituie competența.

Principiile auditului IS/IT

Auditul IT/IS

1. An IT audit is the process of collecting and evaluating evidence of an organization's information systems, practices, and operations.
2. The evaluation of obtained evidence determines if the information systems are safeguarding assets, maintaining data integrity, and operating effectively to achieve the organization's goals or objectives.
3. A control is developed to mitigate a known risk to a level acceptable by Senior Management.
4. The concept of attaining a secure computing environment (ie, an ideal state free from risk or danger) by mitigating the vulnerabilities associated with computer use.

Risks Types

- Strategic
- Compliance
- Market
- Operational
- Environmental
- Reputational
- Market

Application Risks

1. Unauthorized and/or erroneous transactions
2. Processing inefficiencies due to incomplete data entry
3. Access control violations
4. Data entry errors undetected
5. Breach of system integrity and loss of critical data
6. Non-compliance with federal and state laws regarding computer and data communications use
7. Destruction of critical information by unauthorized users
8. Impairment of the Organization’s reputation

Security Domains

1. Access Control Systems and Methodology
2. Telecommunications and Network Security
3. Business Continuity Planning and Disaster Recovery Planning
4. Security Management Practices
5. Security Architecture and Models
6. Law, Investigation, and Ethics
7. Application and Systems Development Security
8. Cryptography
9. Computer Operations Security
10. Physical Security

CoBIT Domains

- Plan and Organize
  - PO 8 – Manage Quality
- Acquire and Implement
  - AI 2 - Acquire and Maintain Application Software
  - AI 6 - Manage Changes
  - AI 7 - Install and Accredit Solutions and Changes
- Deliver and Support
  - DS 5 - Ensure Systems Security
- Monitor and Evaluate
  - ME 2 - Monitor and Evaluate Internal Control

Internal Controls 101

- Primary Objectives of Internal Controls
  - Accurate Financial Information
  - Compliance with Policies and Procedures
  - Safeguarding Assets
  - Efficient Use of Resources
  - Accomplishment of Business Objectives and Goals

Point of View

- Security Perspective
  - Security requirements early în SDLC process.
  - Ensure legal, regulatory, contractual, and internal compliance requirements.
  - Follows industry best practices.
  - Testing during development, QA, pre and post production.
- Audit Perspective
  - Compliance to legal, regulatory, contractual, and internal compliance requirements.
  - Appropriate evidence is documented.
  - Business objectives and goals are maintained.
  - Each audit point is reached during the SDLC phases.

Referințe bibliografice

1. ISO/IEC 27007:2017. Guidelines for information security management systems auditing
2. ISO/IEC TR 27008:2011. Guidelines for auditors on information security controls
3. ISO/IEC 19011:2018. Ghid pentru auditarea sistemelor de management
4. Аверченков В.И. Аудит информационной безопасности: учеб. пособие для вузов . – 3-е изд., стереотип. – М. : ФЛИНТА, 2016. – 269 с.
5. Курило А.П., Милославская Н.Г., Сенаторов М.Ю. Основы управления информационной безопасностью: учебное пособие, 2-е изд., испр.– М.: Горячая линия –Телеком, 2016. – 244с.
6. IGlossary of Key Information Security Term. NISTIR 7298, Revision 2, 2013. https://csrc.nist.gov/glossary/
7. FAQ About the ISO27k http://www.iso27001security.com/html/faq.html, http://www.iso27001security.com/