Auditul Securității Informației (ASI)

Motto
în God we trust. Everyone else we audit!
B. Baczko*

Доверяй, но проверяй!

Cadrul conceptual de audit

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. Introducere
2. Esența Auditului SecInf (ASI)
3. Cadrul definitoriu de audit
4. Mod de abordare, cadrul de referință, flux

1. Introducere

(Succint istoric, importanța, motivația, beneficiile)

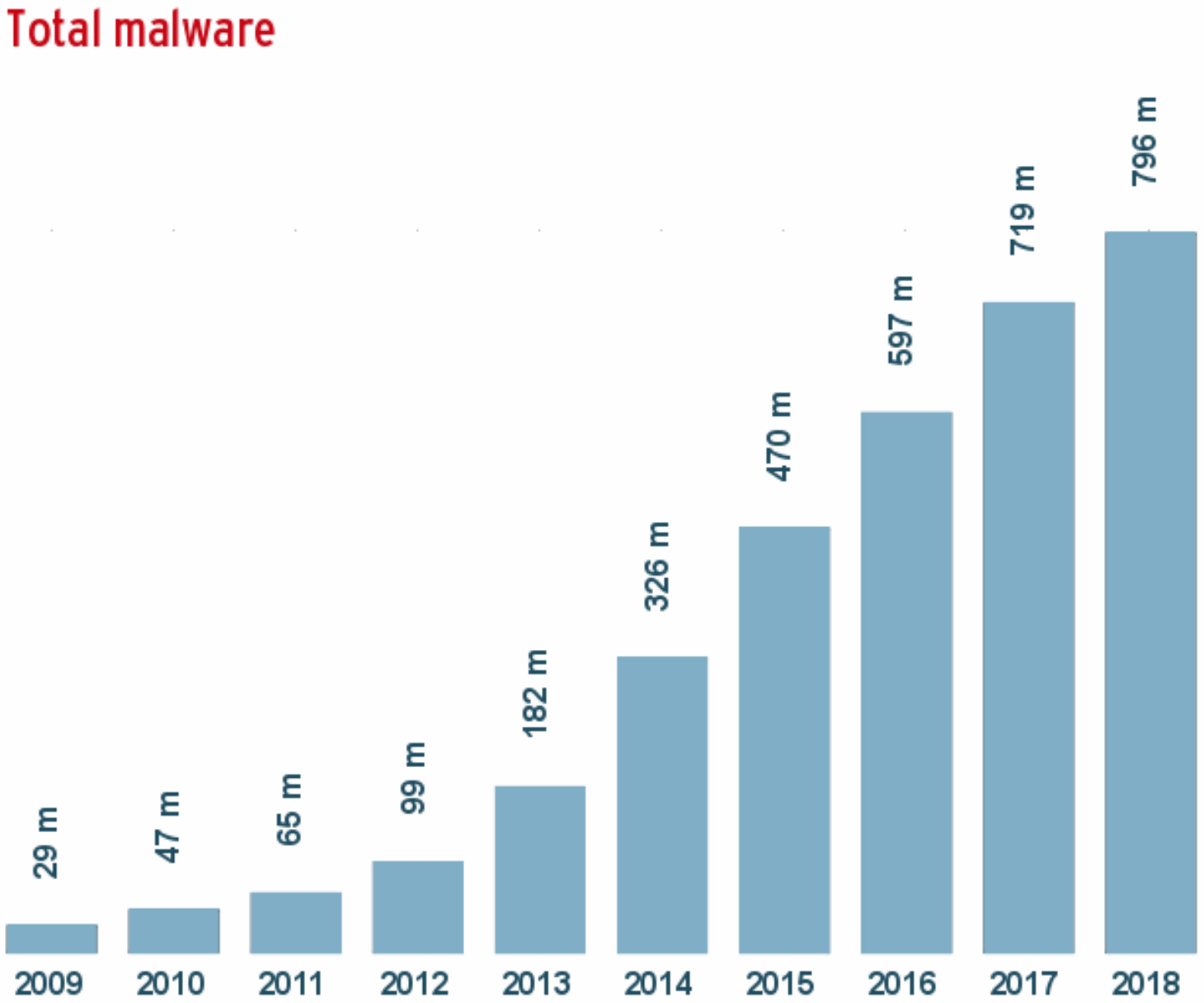
Apariție concept ASI

- Conceptul de ASI a apărut relativ recent (1995)
- În țări high-tech ale lumii (SUA, Marea Britanie, Germania, Canada)
- Ca parte importantă a managementului afacerilor, întreprinderilor, statului, societății
- Ca parte semnificativă a MSI (controale de audit)
- Răspunde intereselor experților în afaceri și SMSI

De ce ASI este actual, important?

- Dependență crescută a tuturor genurilor de activitate de TIC și de sistemul de securitate a informațiilor
  - ➢Un nou mod de a lucra, învăța, comunica, cumpăra, efectua tranzacții, a se distra etc.
- Vulnerabilitatea crescândă a activităților informaționale bazate pe IT, Intranet, Internet, Extranet
- Protecția informațiilor, independent de domeniu *(educație, comerț..),* mărimea firmei *(mică – mare), nivel (individual, local, global)* impune, mai întâi de toate, evaluarea stării inițiale: fără audit – nu e posibil MSI

Doar un exemplu: dinamica malware în ultimii 10 ani



Sursa https://www.av-test.org/en/statistics/malware)

În mai puțin de 10 ani numărul victimelor a crescut de peste 27 ori!

Ritm alarmant pentru societate!!!

Motivația/scopul sau *Când este util ASI*?

- **Cu titlu preventiv pentru:**
  - Auto-evaluare = aprecierea eficacității unei organizații, a unui sistem, produs, proces etc.
  - Respectarea politicii, cerințelor, reglementărilor de SecInf
  - Implementarea unor noi componente IS/IT sau îmbunătățirea IS/IT
  - Monitorizarea propunerilor auditurilor precedente
  - Certificarea conformității unor standarde (e.g. ISO 27k)
- **Cu titlu curativ în situații delicate:**
  - Faliment (insucces) al prestațiilor
  - Suspiciuni privind funcționarea corectă a SMSI

Beneficiile auditului de securitate

- Conștientizarea valorii resurselor informaționale
- Documentarea riguroasă a procedurilor informaționale de pe poziția SecInf
- O mai bună înțelegere de către conducere și angajați a obiectivelor și problemelor organizației în domeniul SecInf
- Asumarea responsabilității pentru riscurile reziduale

Efectuarea auditului de succes presupune

- Participarea activă a conducerii societății
- Obiectivitatea, independența, competența, profesionalismul înalt al auditorilor
- O procedură de verificare bine structurată
- Implementarea activă a măsurilor propuse pentru asigurarea și consolidarea securității (audit de supraveghere)

2. Esența Auditului SecInf (ASI)

(Definiție, sarcini, rezultate, utilizatorii, scop, obiective, ASI)

Esența auditului securității informațiilor =

- O verificare specială a stării de protecție, a organizării și eficienței protecției informațiilor conform
- cerințelor, normelor și/sau standardelor stabilite (diverse controale)
- în scopul asigurării protecției informațiilor

Funcțional ASI poate fi definit ca:

- Examinarea profesională a unor informații
- Cu scopul de a exprima o evaluare responsabilă și independentă a acestora
- De către o persoană independentă și responsabilă pentru activitatea sa
- Conform unor reguli stabilite
- în standarde, norme legale sau profesionale ce constituie criterii de calitate și a elibera un certificat special de formă prestabilită

Operațional ASI constă în:

- Identificarea
- Înregistrarea
- Stocarea
- Analiza datelor care afectează SecInf și
- Elaborarea recomandărilor de creștere a SecInf

Dimensiunile principale ale auditului SecInf

1. *Obiectul (-ele) auditului*
2. *Perspectiva temporală*
3. *Tipul (-rile) de audit*

Sarcinile auditului SecInf

1. Evaluarea nivelului actual de securitate
2. Analiza riscurilor asociate cu posibilitatea implementării amenințărilor
3. Localizarea blocajelor în sistemul de protecție
4. Evaluarea conformității cu standardele existente
5. Elaborarea recomandărilor pentru îmbunătățirea securității

Exemple de sarcini/obiective ASI

1. Evaluarea nivelului actual de securitate
2. Analiza riscurilor asociate cu posibilitatea implementării amenințărilor
3. Localizarea blocajelor în sistemul de protecție
4. Evaluarea conformității cu standardele existente
5. Elaborarea recomandărilor pentru îmbunătățirea securității

Rezultatele așteptate ale auditului

Sunt grupate în câteva documente specifice:

1. Raportul de audit
2. Recomandări pentru a aborda vulnerabilitățile și a minimiza riscurile informaționale
3. Când să se efectueze următorul audit?
4. Care este aria lui? etc.

- *Permit companiei crearea unui sistem de protecție optim al raportului cost/calitate (eficiența)*
- *Adecvat sarcinilor curente și obiectivelor de afaceri.*

Participanții în procesul de audit și monitorizare

- Managementul corporației, acționarii
- Serviciul de control intern
- Serviciul IT
- Serviciul de securitate
- Echipa de audit

Utilizatorii auditului

- Managementul companiei
- Serviciul de Securitate
- Serviciul de informatizare
- Serviciul de control intern/audit

Interni

- Acționarii societății
- Organisme de reglementare
- Clienții companiei

Externi

Obiectivele auditului

- Asigurare/creștere a securității informațiilor (CIA+..)
- Creștere a eficienței exploatării IS/IT
- Creșterea eficienței și calității procedurilor de securitate
- Creșterea calității SMSI
- Control al acțiunilor utilizatorilor în rețeaua corporativă
- Evaluare și reevaluare în timp util al riscurilor informaționale
- Elaborarea planurilor optime de dezvoltare SMSI

3. Cadrul definitoriu de audit

Definiție audit

- **Audit =** *„un proces sistematic, independent și documentat pentru obținerea probelor de audit (înregistrări, declarații de fapte sau alte informații care sunt relevante și verificabile) și evaluarea în mod obiectiv pentru a determina măsura în care criteriile de audit (setul de politici, cerințe, proceduri, măsuri) sunt îndeplinite”.*
  - *Examinarea profesională a unei informații*
  - *Cu scopul de a exprima o evaluare responsabilă și independentă a acesteia*
  - *De către o persoană independentă și responsabilă pentru activitatea sa*
  - *Conform unor reguli dinainte stabilite*
  - *în standarde, norme legale sau profesionale ce constituie criterii de calitate*

Note explicative a definiției de audit *(ISO 27000)*

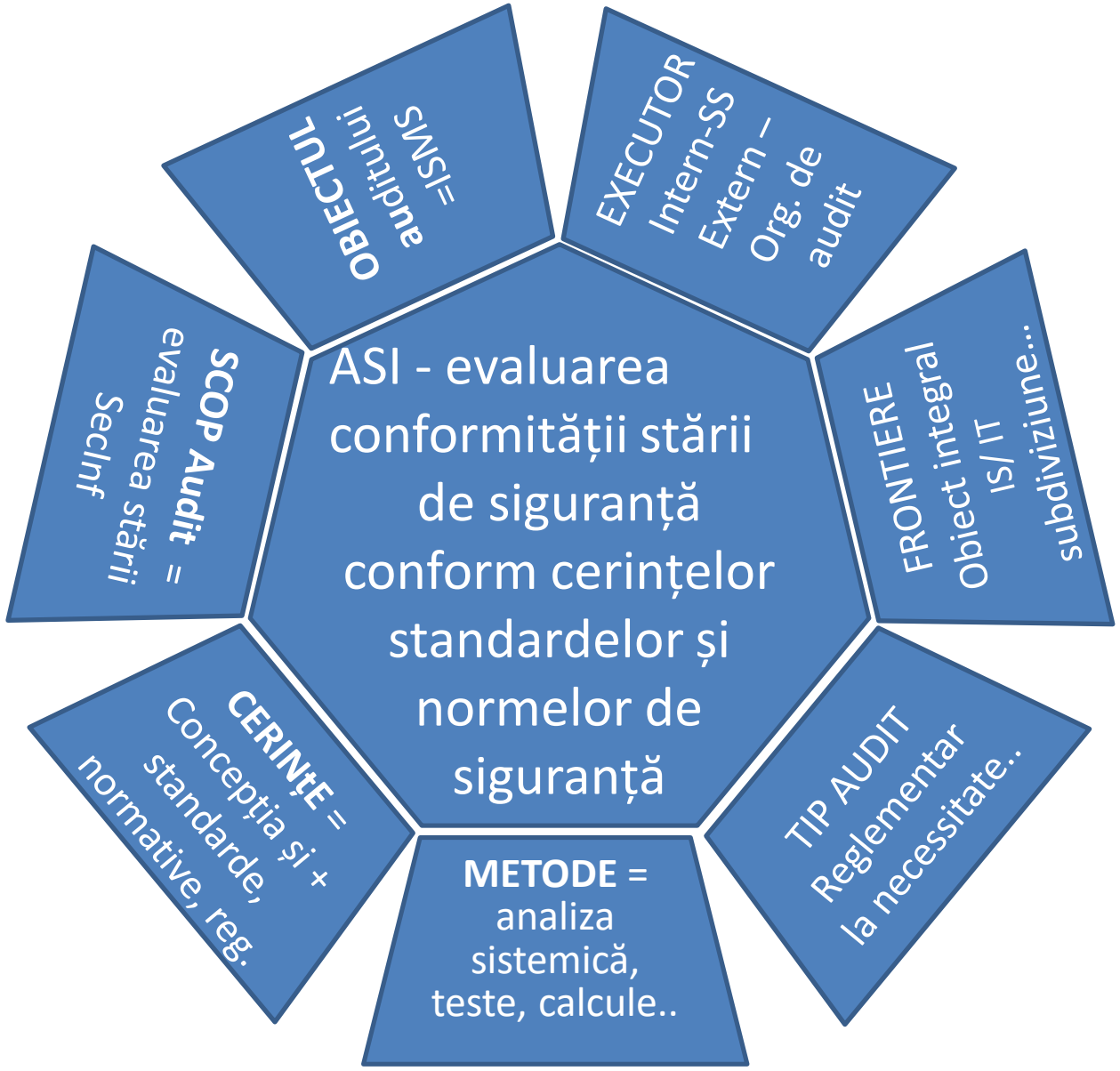
1. Auditul poate fi intern*, extern** sau combinat
2. Auditul intern este efectuat de către organizația auditată sau de către o parte externă în numele său.
3. "Dovezile de audit" și "criteriile de audit" sunt conforme ISO 19011.

*Prima parte, *a 2-a, **a 3-a parte

Perspectiva auditului

- Respectarea cerințelor legale, de reglementare, contractuale și interne
- Sunt prezentate dovezi adecvate
- Scopul și obiectivele afacerii sunt menținute
- Fiecare obuiectiv de audit este atins

Model conceptual al auditului SecInf



Trei dimensiuni principale ASI

1.Obiectul (-ele) auditului/aria, frontierele

2.Perspectiva temporală (inițial, repetat, de supraveghere)

3.Concepția SecInf: cadrul normativ, standarde, cerințe, reglementări

Trei nivele de audit

- ***Strategic*:** eficiența cu care este organizată, planificată, condusă și controlată SecInf (SMSI)
- ***Tactic*:** utilizarea resurselor IS/IT de aplicații existente sau a celor nou create
- ***Operațional***: derularea proceselor informaționale

- **Criterii de audit** - setul de politici, proceduri și cerințe
- **Dovezi de audit** - înregistrări, fapte, informații referitoare la criteriile de audit, care pot fi verificate
- **Rezultatele auditului -** rezultatul evaluării dovezilor colectate de audit privind respectarea criteriilor de audit
- **Raportul de audit =** Principalul produs de audit, conține (a) descrierea stării actuale a SecInf, (b) vulnerabilitățile detectate și (c) a neconformitățile față de criteriile de audit selectate, (d) recomandări pentru eliminarea vulnerabilităților și minimizarea riscurilor informaționale
- **Auditór** - persoană fizică sau juridică, având responsabilitatea unui audit
- **Auditat –** organizație supusă auditului

- **Program de audit =** set din unul sau mai multe audituri planificate pentru un anumit interval de timp și îndreptate spre un scop comun
- *Proces = misiune.* Se definește pe baza standardelor naționale și internaționale
- *Auditor = calitate dobândită în condițiile legii*
- *Entitate/USE = S.C., Guvern, o operație, o activitate, o tranzacție financiară…*
- *Auditorii analizează informațiile* prin aplicarea tehnicilor și procedurilor unanim recunoscute în domeniu (standarde). Dacă acestea nu sunt unanim recunoscute - nu se aplică.
- *Evaluează și interpretează rezultatele* prin aplicarea unor criterii de evaluare cu referințe (la standarde, norme) și principii "sănătoase" de management (economicitate, eficiență, eficacitate)

Obiectul(-ele) auditului SecInf

1. Proprietățile fundamentale (CIA)* și suplimentare** ale informației
2. Datele și suporturile de date (inclusiv hârtie, documente primare, centralizatoare, rapoarte etc.)
3. Resursele informatice hard/soft (IT, IS, Web...)
4. Personal (de operare, management, ...)
5. Continuitatea afacerii (după căderi, dezastre...)
6. Planurile de cotigență, managementul incidentelor, riscurilor

**CIA = Confidențialitate, Integritate, Accesibilitate/Disponibilitate*

***Autenticitatea (3.6), accounting, non-repudierea (3.48) și fiabilitatea (3.55) – conform ISO 27000:2018:…*

Riscuri în audit

1. Riscul ca auditorul să exprime o opinie de audit necorespunzătoare, pe baza unor documente, probe greșite; este o funcție a **riscului de detecție**, are 2 componente:
   - **Riscul inerent -** susceptibilitatea modificării unui document sau a dezvăluirii unor părți din document individual sau în legătură cu fapte similare înainte de considerarea unor controale relaționate
   - **Riscul de control-** dacă o astfel de declarație eronată nu va fi prevenită, detectată și corectată pe baza controlului intern al entității, efectuat în timp
2. **Risc de detecție** - riscul că procedurile executate de auditor nu vor detecta o eroare existentă, individuală sau corelată cu alte erori.

Evidența auditului =

- Informația folosită de auditor la atingerea concluziilor pe care se bazează opiniile auditorului= trebuie să respecte următoarele principii:

a) Suficiența eficienței auditului este măsura cantității evidenței auditului. Cantitatea necesară de evidență a auditului este afectată de evaluarea auditorului referitoare la riscul erorilor materiale și la calitatea unei astfel de evidențe.

b) Adecvarea evidenței auditului este o măsură a calității auditului , respectiv a relevanței și fiabilității acesteia în oferirea de suport pentru concluziile pe care se bazează opinia auditorului

Opțiuni/tipuri de audit

Audit general, complet

Punctual, expert

Intern

Extern

Tehnic, activ, instrumental

IS, IT, Web…

Pen test

De conformitate

Audit general, complet, al tuturor aspectelor SecInf = de regulă pentru Certificare/Acreditare

Auditul punctual, specific, al unui oarecare aspect al SecInf = de regulă **Corectiv, IS, IT, Web…**

Audit organizațional vs. Audit tehnic, Instrumental, activ

Audit repetat vs Audit continuu *(de regulă activ, automatizat)* **-** Tip de auditare în care auditorul are acces permanent la sistemul informatic al entității auditate, diferența de timp între momentul producerii evenimentelor urmărite de auditor și obținerea probelor de audit fiind foarte mică. Mai corect ar fi **Audit de Monitorizare**

Audit online - Auditare prin consultarea online a bazelor de date ale entităților auditate, aflate la distanță.

Audit documentar, de verificare a conformității unor norme, standarde etc.

IV. Mod de abordare, cadrul de referință, flux

Trei abordări de audit a SecInf

1. Bazat pe analiza riscurilor (RM, ISO 27005 sau/și ISO 31000) – *metodă universală, dar și cea mai complicată*
2. Bazat pe utilizarea standardelor (e.g. ISO 27001, ISO 27002), pe metode, instrumente și tehnici speciale, ca COBRA, CRAMM, CONDOR etc.– *este f. convenabil, nu este necesar să inventezi nimic*
3. Combinația primelor două – *cel mai frecvent*

Diverse cadre de reglementare ASI

1. CoBIT
2. ISO 27k (1-ISMS, 2- Bune practici,
3. NIST/SP
4. ITIL/familia ISO 20000-k
5. Pe domenii:
   - ✓PCI DSS
   - ✓GDPR ...

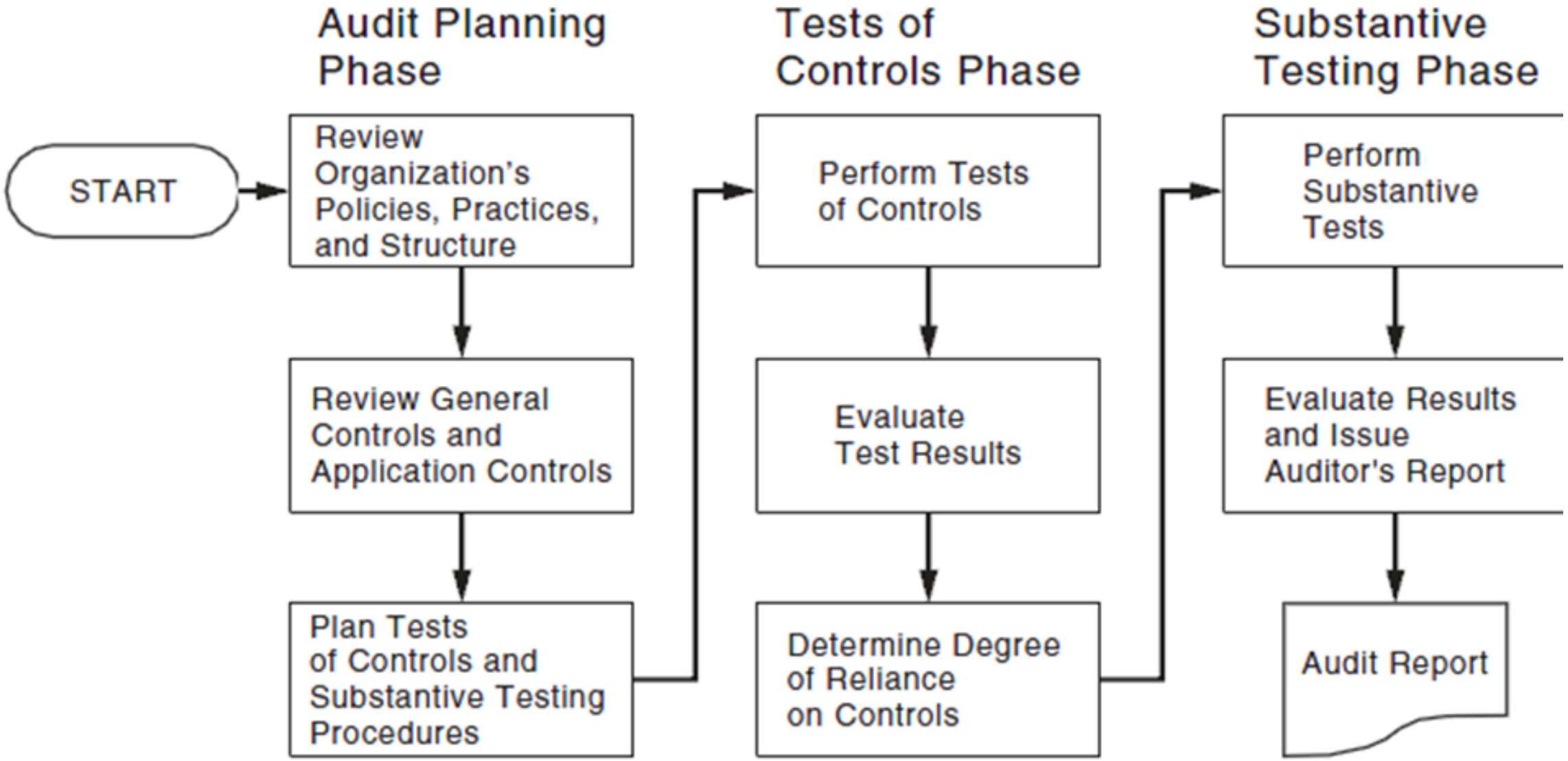
Standarde pentru auditul SecInf

1. ISO/IEC 27001:2017... Information security management systems. Requirements
2. ISO/IEC 27002:2016... Code of practice for information security controls
3. ISO 19011:2018 ... Linii directoare pentru auditarea sistemelor de management
4. ISO/IEC 27007:201... Guidelines for information security management systems auditing
5. ISO/IEC TR 27008:2019… Guidelines for auditors on information security controls

Trei faze de desfășurare ASI

1. **Pregătitoare/preimplementare:** selectare obiect, echipă, scop ASI, politica, metodologia, bugetul ...
2. Implementare/**efectuare audit**: colectarea datelor, execuția controalelor, analiză, evaluare...
3. **Post-implementare audit**: finalizare raport, elaborate plan de corectare/îmbunătățire aprobarea rapoartelor/rezultatelor, măsurilor și monitorizarea planului

Fluxul auditului SecInf



Monitorizarea - oferă dovezi ale evaluării stării SecInf

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/