Auditul Securității Informației (ASI)

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

Доверяй, но проверяй!

Introducere în Auditul TI

Agenda

- Audit – scurt istoric
- Definiție și tipuri de audit TI
- Obiectiv, scop, sarcini
- Locul auditului TI în sistemul de control intern.
- Organizații profesionale
- Legislație, regulamente
- Factori de dezvoltare a TI și a funcției de audit TI
- Analiza standardelor, abordărilor și a practicilor recunoscute

Definiție și tipuri de audit

- **Auditul** reprezintă activitatea de prezentare a opiniilor și recomandărilor independente și obiective, orientate spre îmbunătățirea activității organizației. Auditul intern ajută organizațiile să-și atingă obiectivele propuse, utilizând o abordare sistematizată privind evaluarea și sporirea eficienței proceselor de gestiune a riscului, control si management corporativ. (Institute of Internal Auditors, IIA)
- ***Auditul poate fi***:
  - Intern
  - Extern
- Tipuri de audit:
  - Financiar
  - Integrat
  - Operațional
  - Audit TI (ИТ процессы, информационные системы, технологии и инфраструктура)
  - Conformare (SOX-404, PCI-DSS, BS-25999, ISO-2700x и др.)
  - Specializate (auditul unor domenii înguste, de obicei coordonate cu top managementul)
  - Identificarea / Investigarea potențialelor fraude (“forensic”).

Audit SI – scurt istoric

- Auditul ca meserie a aparut pentru prima oara in SUA, anii ‘60, concomitent cu apariția primelor mijloace de prelucrare automatizată a datelor
- Autoarea primului standard în domeniu a devenit organizația ”Asociația auditorilor mijloacelor electronice de prelucrare a datelor” creată în cadrul Institutului American al Auditorilor Publici Certificați (AICPA)
- În anul 1994 asociația sus menționată a fost redenumită în ISACA (Asociația internațională a profesioniștilor în domeniul managementului și controlului TI)
- ISACA = 140000 membri, 200 chaptere, în 80 tări ale lumii.
- CISA = 118000 profesioniști
- CISM = 28000 profesioniști
- CRISC = 18000 profesioniști
- CGEIT = 6000 profesioniști

Obiectul Auditului SI

- Auditul SI este o disciplină ce vizează securitatea tehnologiilor informaționale, ce permite a răspunde la următoarele întrebări:
  - Cât de securizate sunt tehnologiile informaționale pentru a atinge obiectivele de busines ale organizației?
  - Există careva ”locuri înguste” sau domenii problematice în arhitectura sistemelor informatice, infrastructură sau organizația TI?
  - Cât de eficient sunt utilizate și cat de securizate sunt resursele informationale ?
  - Sunt oare tehnologiile informaționale și resursele de suport utilizate capabile să asigure un nivel adecvat de control al activității de busines și de protecție a activelor?
  - Sunt oare asigurate confidențialitatea, integritatea și accesibilitatea datelor și a informației prelucrate cu ajutorul sistemelor informatice ?
  - Au fost oare implementate măsuri de control al TI și cât de eficiente sunt ele ?

Obiectivele Auditului

Obiectivele sunt:

- Prezentarea informației actuale și veridice despre starea SI sau despre starea unui anumit domeniu TI, precum și despre riscurile cheie identificate
- Sporirea eficienței operaționale în rezultatul utilizării secuizate a resurselor TI
- Identificarea domeniilor ce necesită atenție și efort adițional pentru sporirea nivelului de securitate
- Identificarea și evaluarea riscurilor de securitate
- Definirea măsurilor de minimizare a riscurilor
- Modernizarea sistemului de control intern al tehnologiilor informaționale
- Evaluarea nivelului de securitate informațională în organizație și corespunderea necesităților de busines
- Asigurarea unui nivel acceptabil de încredere în sistemele informatice de raportare financiară
- Asigurarea conformității legislației în vigoare in domeniul SI și TI

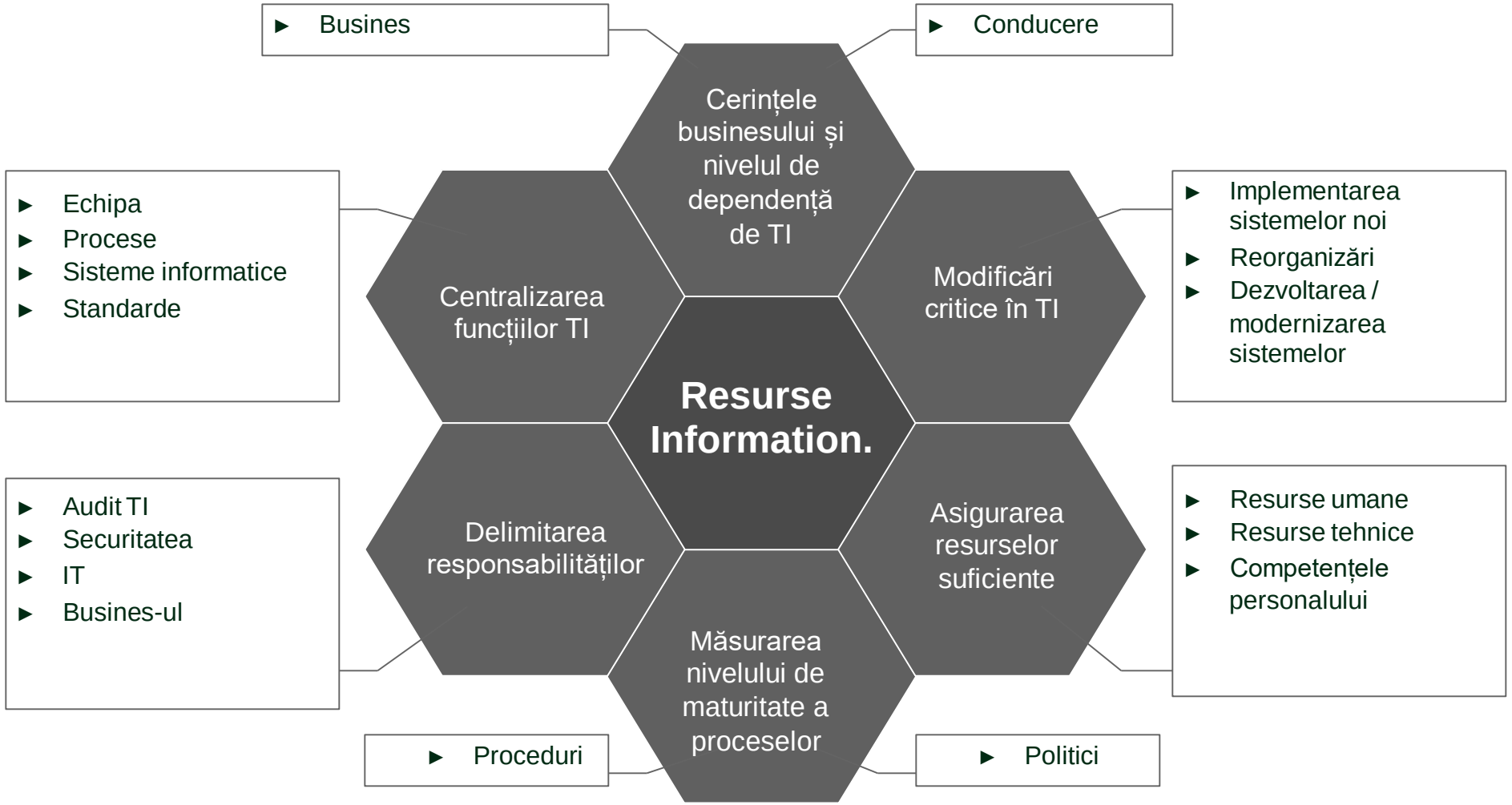
Sarcinile Auditului SI

- Formarea recomandărilor către conducerea organizației privind sporirea securitatii serviciilor TI oferite și îmbunătățirea sistemului de control
- Controlul eficienței operaționale a controalelor de securitate
- Controlul executării și respectării politicilor și regulamentelor interne
- Evaluarea SMSI la general
- Întocmirea rapoartelor în rezultatul efectuării auditului SI
- Identificarea și păstrarea dovezilor de audit și a celor, ce confirmă realizarea procedurilor de control
- Controlul nivelului de conformare legislației în vigoare (Guvern, BNM, etc).

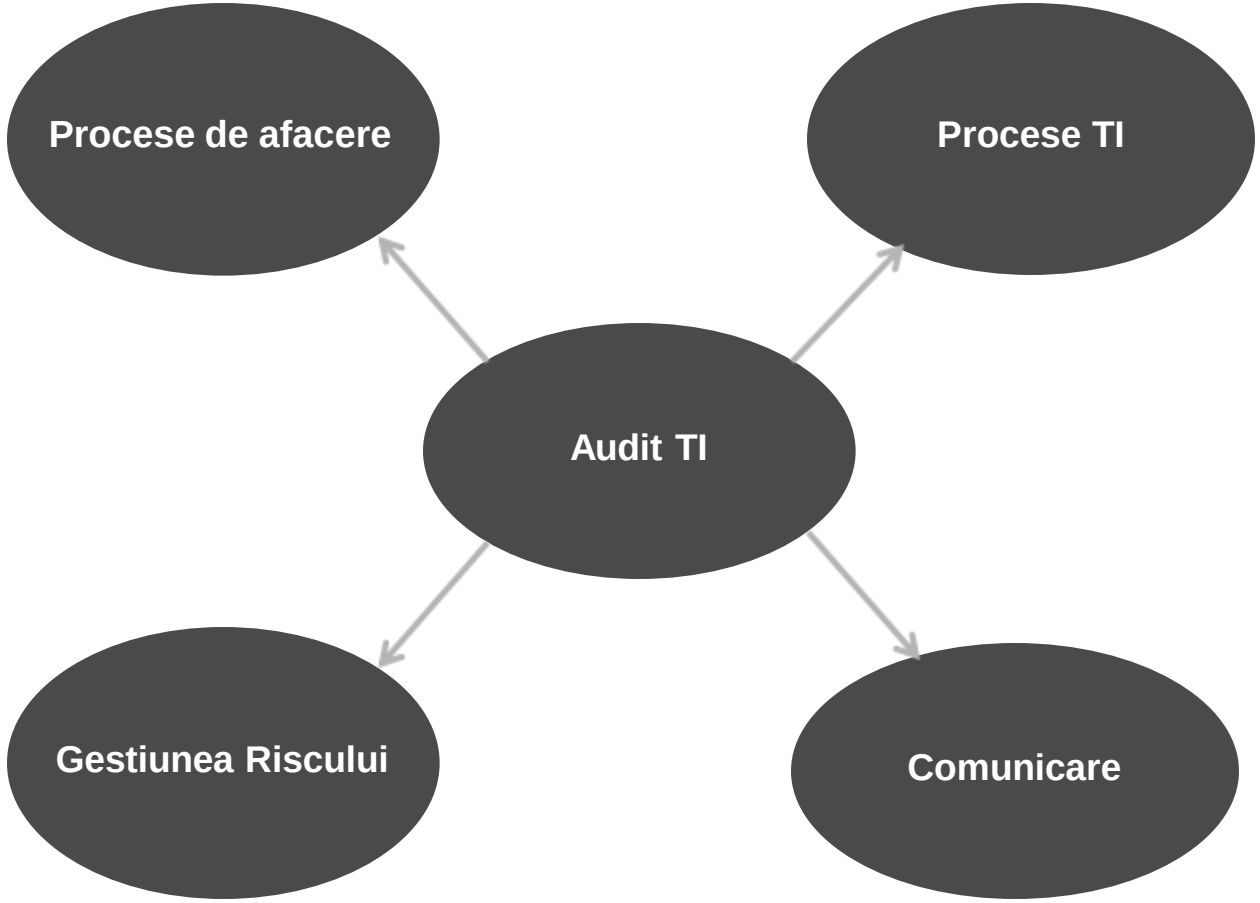
Locul auditului TI în sistemul de control intern

- Auditul TI – parte componentă a diviziunii de audit intern
- Scopul, sarcinile, responsabilitățile, regulamentele și documentele normative sunt definite conform normelor diviziunii de Audit Intern
- Procesul de planificare a activității trebuie integrat cu activitatea diviziunii de Audit Intern al organizatiei
- Procedurile și programele de lucru ale Auditului TI le vor completa pe ale Auditului Intern
- Fiind parte a Auditului Intern, auditul TI trebuie să fie independent în special de TI și Securitate, dar și de orice alte diviziuni în organizație
- Locul Auditului TI în sistemul de control intern depinde de abordarea fiecarei organizații

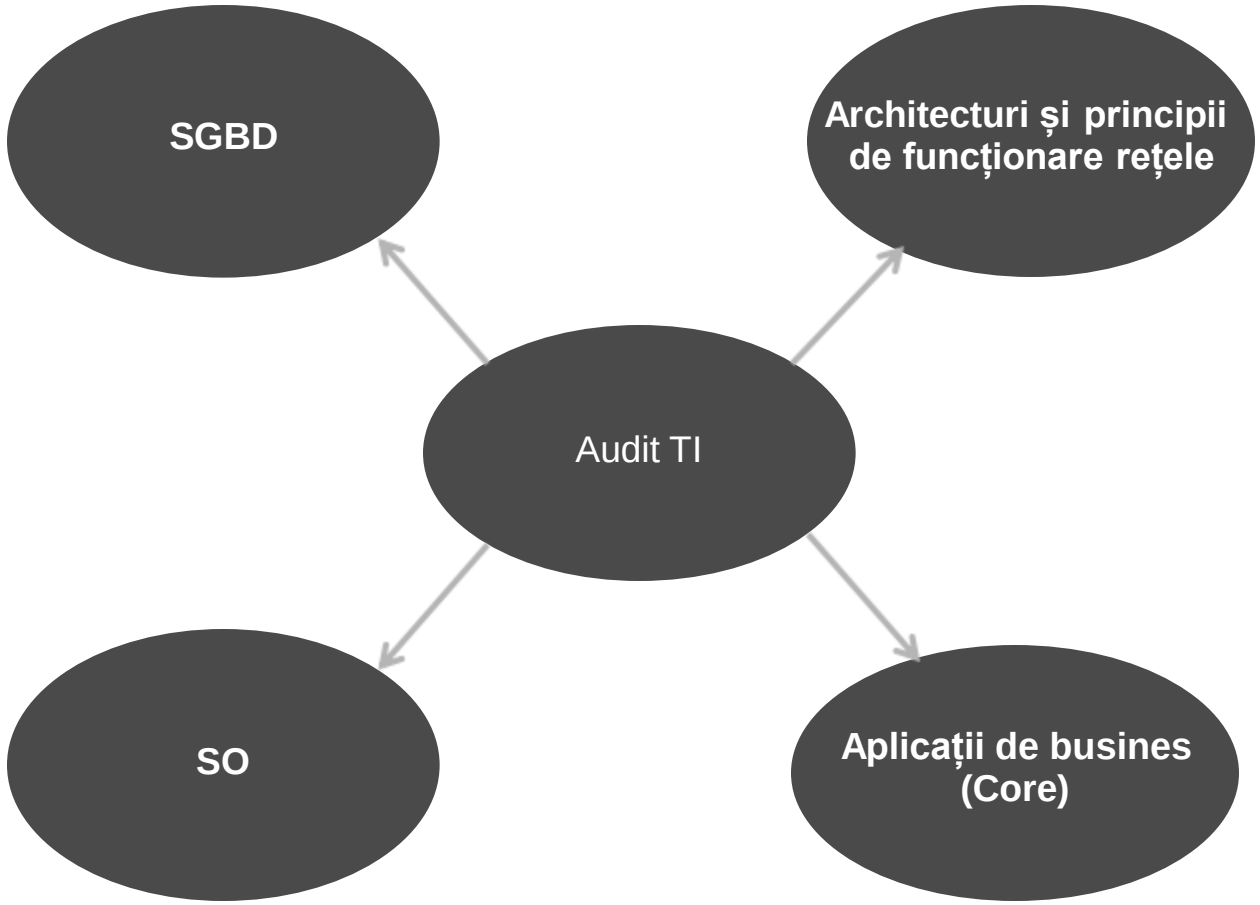
Factori de dezvoltare a TI și a funcției de Audit TI



Recomandări privind dezvoltarea profesională



Recomandări privind dezvoltarea profesională
Cunoștințe tehnice



Cerințe către și certificări profesionale pentru Auditorul TI

- Cerințe:
  - Cunoașterea tehnologiilor TI
  - Expert în Auditul TI
  - Conformarea coduui de etică al auditorilor
  - Cunoașterea cerințelor de bază legislative și a organismelor regulatorii
  - Instruire și dezvoltare profesională continuă
- Certificări profesionale de bază:
  - Certified Information Systems Auditor (CISA)
  - Certified Internal Auditor (CIA)
  - ISO 27001 Lead Auditor
- Certificări complementare:
  - Certified Information Systems Security Professional (CISSP)
  - Certified in Risk and Information Systems Control (CRISC)
  - Certified Information Security Manager (CISM)
  - Business Continuity Institute Certifications
  - Certified Computer Professional (CCP)
  - Certified Information Privacy Professional (CIPP)
  - Certified Public Accountant (CPA)
  - Forensics Certified Public Accountant (FCPA)
  - Certified Fraud Examiner (CFE)
  - Certified Information Technology Professional (CITP)
- Resurse: isaca.org, theiia.org, isc2.org

Ce facem în lipsa auditorului TI intern

Pot fi utilizate una dintre următoarele abordări:

- Utilizarea resurselor interne:
  - Realizarea unor proceduri de audit TI de către specialiștii IT
  - Re-calificarea specialiștilor în domeniul TI sau a auditorilor interni
  - Implicarea specialiștilor TI sau ofițerului de securitate informațională pentru a acorda suport în analiza aspectelor tehnice, de exemplu acumularea și analiza informației.
- Implicarea resurselor externe:
  - Contractarea organizațiilor externe, specializate în domeniu.
  - Contractarea auditorilor TI în bază de cotnract.
- Abordarea combinată.

Legislație

- Legea privind privind activitatea de audit
- Regulamentul cu privire la sistemele de control intern în bănci/ Revazut
- Regulamentul privind activitatea băncilor în domeniul prevenirii şi combaterii spălării banilor şi finanţării terorismului
- Regulamentul BNM cu privire la modul de întocmire si prezentare a rezultatelor auditului
- Legea cu privire la protecţia datelor cu caracter personal (L/133, HG 1123)
- Legea cu privire la documentul electronic şi semnătura digitală
- Legea privind prevenirea şi combaterea criminalităţii informatice
- Etc.

ORGANIZATIILE, IN FUNCTIE DE INDUSTRIE, POT CADEA SUB INCIDENTA REGLEMENTARILOR DE DOMENIU!

Cerințe internaționale

- Standardele Internaționale de Audit (International Standards on Auditing)
  - Un set de standarde priofesionale ce vizează formarea rapoartelor financiare. Standardele sunt elaborate și revăzute de către asocoația internațională a contabililor (IFAC)
- Prevederi privind standardele de audit (Statements on auditing standards)
  - Reprezintă un ghid pentru auditorii externi și este elaborat de organizația AICPA (Institutul American al Contabililor Publici Certificați). Include un șir de standarde ce vizează auditul financiar, inclusiv tehnologiile informaționale
- Acordul Basel - Cadrul Internaţional pentru măsurarea, standardizarea şi monitorizarea riscului de lichiditate (Basel II, III)
  - Cerințe către suficiența lichidităților de capital. În domeniul TI stabilește cerințe privind necesitatea de a efectua analiza periodică a riscurilor operaționale (riscurile TI sunt parte a riscurilor operaționale)
- Cerințe către sistemele de plăți (PCI DSS)
  - Stabilește cerințe către companiile ce realizeaza prelucrarea și stocarea datelor privind cardurile bancare și comerț electronic. Înafară de cerințe includ și ghid privind auditul de conformmitate
- Cerințe privinde protecția datelor personale și a drepturilor de autor
  - Directiva și recomandări (2016/679), elaborate de parlamentul European si intrate in vigoare in Mai, 2018. Stabilește cerințe privind prelucrarea și stocarea datelor cu caracter personal și a drepturilor de autor
- Sarbanes Oxley Act, section 404
  - Stabilește cecrințe către sistemul de control intern și periodicitatea analizei eficienței acestuia. Se aplică pentru companiile publice, ce se listează la bursa de valori din New York (NYSE)

Analiza generală a standardelor / metodicilor în domeniul TI

Standard/Metodologie	Descriere succintă
CobiT	Metodologie privind gestiunea și controlul Tehnologiilor Informaționale. Implementarea sistemului de control al TI conform respectivei metodologii permite garantarea utilizării eficiente și sigure a TI în organizație
COSO	Cerințe către sistemul de gestiune a riscului în organizație. Include cerințe către sistemul de control intern
IT Infrastructure Library (ITIL), ISO 2000X	Reprezintă o bibliotecă, ce descrie cele mai bune practici privind organizarea lucrului subdiviziunilor TI și a organizațiilor ce prestează servicii TI. ISO 2000 – standard ce prevede același lucru, elaborat în baza ITIL. Diferența este de numarul și denumirea proceselor analizate
ISO 2700X	Un set de standarde în domeniul gestiunii securității informaționale și a riscurilor IT / securitate informațională. ISO include mai bine de 20 de comitete de lucru și acoperă cu diferite standarde întreaga activitate TI
Capability Maturity Model Integration (CMMI)	Un set de modele (metodologii) ce au scop modernizarea / optimizarea proceselor TI în organizații de diferită mărime și diferite domenii de activitate. Metodologii de măsurare a nivelului de maturitate pe diferite domenii
ISO 22301	Standarde, ce descriu criteriile și oferă recomandpri de implementare a sistemului de management al continuității activității organizației și a măsurilor de restabilire după situațiile de forță majoră
TOGAF (the Open Group Architecture Framework)	Reprezintă un set de recomandări privind construirea și menținerea organizată a arhitecturii TI (procese, tehnologii, sisteme, aplicații). Un mare accent se pune pe alinierea necesităților de busines și corespunderea așteptărilor stakeholderilor

Organizații profesionale

- **ISACA** (http://www.isaca.org/) – Asociatia internationala de audit si control al sistemelor informatice
- **The Institute of Internal Auditors** (http://www.theiia.org/)- reprezintă asociația profesionala ce reunește auditorii interni și externi, precum și specialiști în domeniul gestiunii riscurilor
- **ISC2** – Organizatia profesionistilor in domeniul securitatii informationale (e.g RISSPA.ru in Russia)
- **BCI, Institutul de continuitate a afacerii**(http://www.thebci.org/) – asociatia internationala ce reuneste profesionistii in domeniul sistemelor de management al continuității afacerii

- **Moldova IT Audit and Security Professionals –** un grup pe linkedin ce include un număr de 147 membri

Utilizarea rezultatelor auditului TI

- Rezultatele auditului intern prezintă interes doar dacă în cadrul organizației există competențe și experiență suficientă
- Auditorul extern, printre altele, face o evaluare a nivelului de competențe în domeniu, analizează rapoartele de audit, dovezile de audit, calitatea concluziilor și a recomandărilor
- În rezultat, în baza rezultatelor evaluării, compania externă de audit poate lua decizia de a utiliza rezultatele lucrului auditului intern (ex. rezultatele testării anumitor controale).