Auditul Securității Informaționale

Auditul Securității Sistemelor Economice

- Având în vedere obiectivele controlului, structura sistemului informațional dintr-o întreprindere și recomandările standardelor IFAC – IAPS 1008, controlul intern al sistemului informațional poate fi clasificat în două categorii:
  - Controlul managementului sistemului informațional.
  - Controlul aplicațiilor informatice.

Standarde privind tratarea riscurilor și controlului din cadrul sistemelor informatice economice

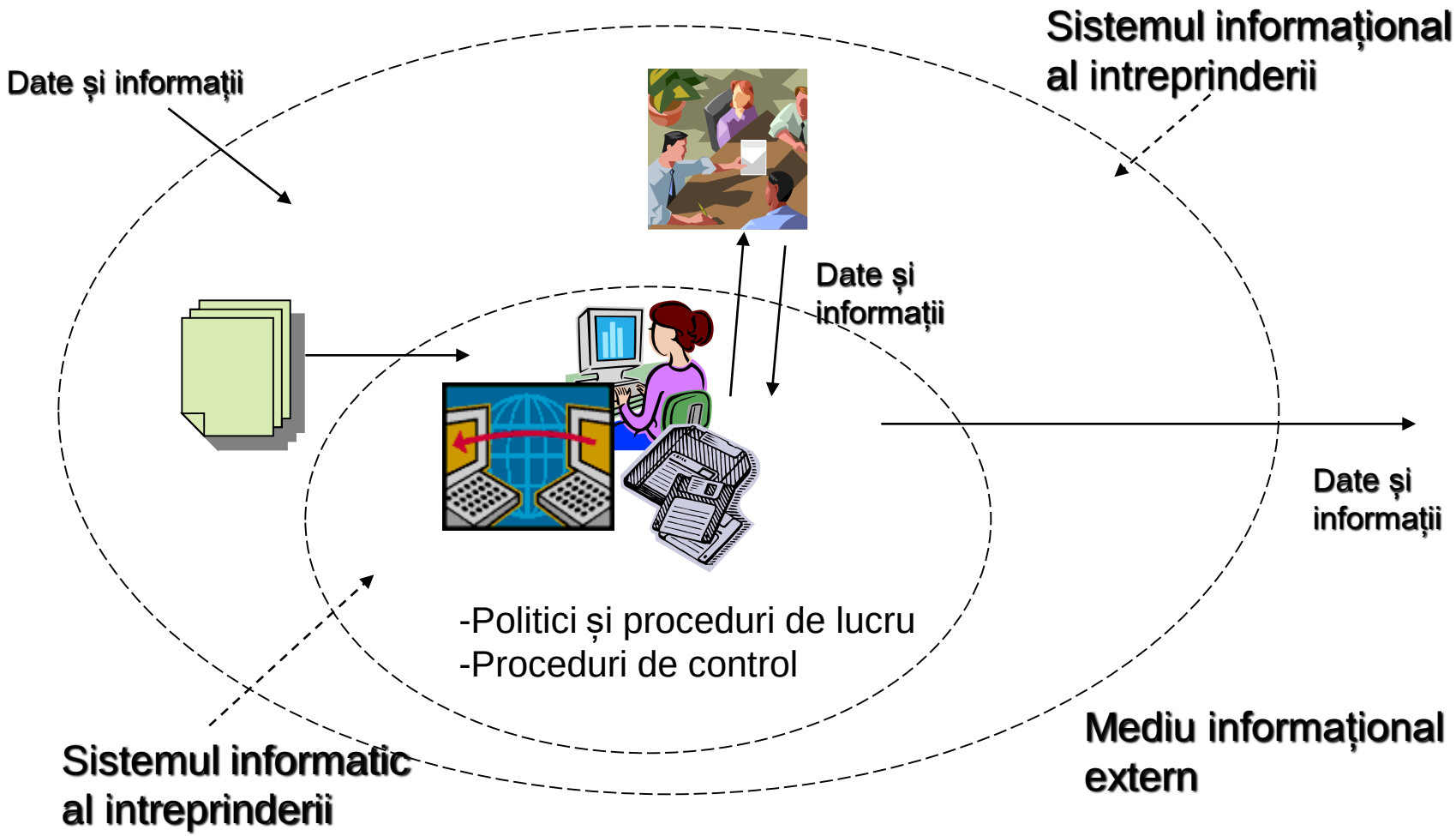
ISACA - CobiT (***C****ontrol* ***Ob****jectives for* ***I****nformation and related* ***T****echnology*)

- *cel mai puternic instrument și cadru de lucru pentru implementarea și auditarea controlului din cadrul sistemelor informatice de gestiune.*
- *este orientat către managementul sistemelor informaționale, departamentelor de control intern, auditorilor și în special proprietarilor (acționari sau asociați) care utilizează tehnologia informației în cadrul afacerilor, pentru a le asigura confidențialitatea, integritatea și disponibilitatea datelor și informațiilor.*

- **CobiT**-ul conține următoarele documente:
  - Prezentarea generală (Executive Summary).
  - Cadrul de lucru (Framework).
  - Obiectivele controlului (Control Objectives).
  - Ghidul pentru management (Management Guidelines).
  - Ghidul pentru audit (Audit Guidelines).
  - Instrumentele de implementare (Implementation Tool Set).

- ***IFAC***
  - *ISA – 400: reglementează evaluarea riscurilor și a controlului intern.*
  - *ISA – 401: reglementează procesul de audit în cadrul sistemelor informatice.*
  - *IAPS – 1008: reglementează evaluarea riscurilor și controlului intern din cadrul sistemelor informatice.*

Sisteme Informatice Economice (S.I.E.)



Controlul în cadrul sistemului informațional

- După identificarea și evaluarea riscurilor din sistemul informatic se trece la evaluarea și testarea controalelor stabilite pentru minimizarea sau eliminarea riscurilor.
- *auditorul trebuie să cunoască, să identifice și să testeze toate tipurile de controale existente.*

Controlul intern *asigură prevenirea, detectarea (identificarea) și corectarea evenimentelor (problemelor) cauzate de către factorii de risc*.

- *preventiv*: De exemplu în cadrul controlului preventiv din sistemul informațional pot fi cuprinse: segregarea sarcinilor și responsabilităților; controlul accesului la resursele din sistem (pe bază de cartele sau carduri de acces); stabilirea unor proceduri clare de introducere a datelor în sistem.
- *detectiv*: De exemplu în cadrul controlului detectiv din sistemul informațional pot fi cuprinse: validarea intrărilor de date prin caractere de control; mesajele de eroare din cadrul aplicațiilor informatice; procedura de identificare a dublurilor înregistrărilor bazei de date.
- *corectiv*: De exemplu: procedurile de recuperare a datelor; procedurile de relansare a aplicațiilor informatice.

- **Obiectivele controlului intern specifice sistemului informatic** pot fi:
  - asigurarea securității fizice și logice a resurselor informaționale;
  - asigurarea integrității aplicațiilor informatice (în special a celor de gestiune) prin:
    - verificarea și autorizarea intrărilor de date;
    - acuratețea, integritatea și securitatea prelucrărilor și tranzacțiilor de date;
    - acuratețea, integritatea și securitatea rapoartelor;
    - integritatea bazelor de date;
  - asigurarea eficienței dezvoltării sau achiziției de aplicații informatice și asigurarea concordanței acestora cu obiectivele întreprinderii;
  - asigurarea eficacității și eficienței operațiilor și procedurilor din sistem;
  - asigurarea concordanței dintre procedurile, respectiv operațiile din sistem și reglementările legale și regulamentele interne în vigoare;
  - asigurarea recuperării datelor și continuarea activității în caz de dezastre sau evenimente neprevăzute.

- *Controlul managementului sistemului informațional*
  - auditorul trebuie să identifice, să evalueze și să testeze următoarele:
    - Controlul organizării sistemului informatic;
    - Controlul proiectării și implementării sistemului informatic;
    - Controlul procedurilor și operațiilor din sistem;
    - Controlul organizării securității sistemului;
    - Controlul asigurării calității sistemului.

- *Controlul aplicațiilor informatice*
  - *Controlul intrării datelor*
  - *Controlul prelucrării (procesării), tranzacțiilor de date și a fișierelor de date*
  - *Controlul ieșirilor de date și informații*

- ***Controlul intrării datelor***
  - asigură autenticitatea, acuratețea și integralitatea datelor introduse în sistem, precum și respingerea, corectarea sau reintroducerea datelor eronate.

- *Controlul prelucrării (procesării), tranzacțiilor de date și a fișierelor de date*
  - asigură acuratețea și integralitatea prelucrărilor și tranzacțiilor, integritatea datelor stocate, atât pe loturi, cât și în timp real (online), precum și corectarea datelor eronate.

- *Controlul ieșirilor de date și informații*
  - asigură faptul că ieșirile sistemului sunt reale, corecte, integrale, securizate și distribuite în timp util utilizatorilor și factorilor decizionali corespunzători (autentificați).