Auditul Securității Informației (ASI)

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

Доверяй, но проверяй!

Sistemul de control TI

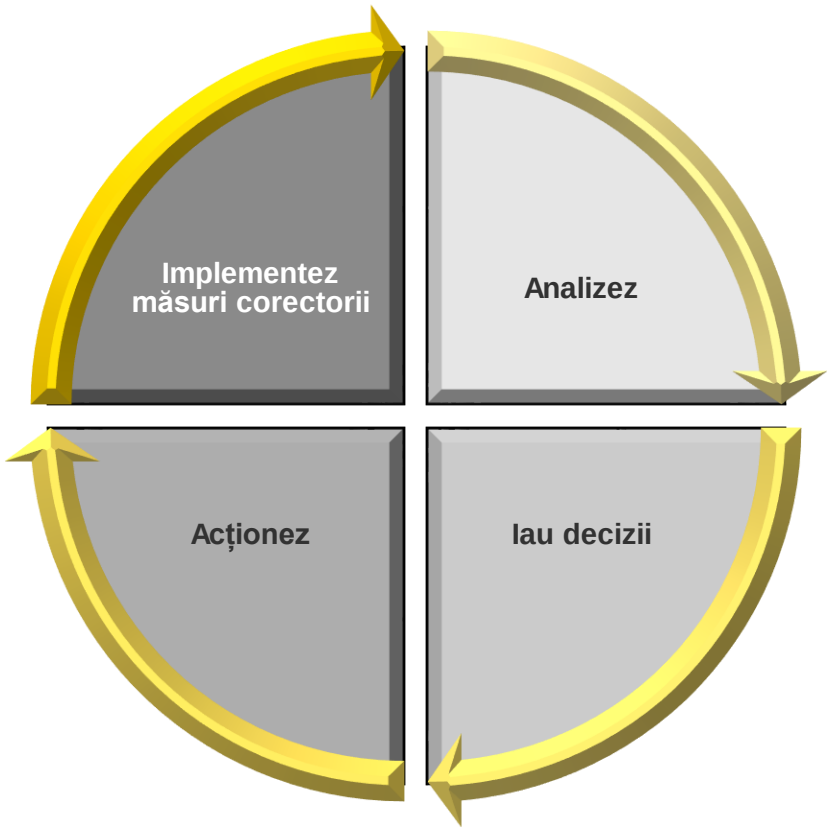
Ce este un control ?

Control - orice acțiune realizată de organul de gestiune pentru a spori probabilitatea atingerii obiectivelor (IIA)

Control – norme, proceduri și structuri organizate, elaborate pentru asigurarea garanțiilor rezonabile, că obiectivele de busines vor fi atinse, iar evenimentele nedorite vor fi anihilate sau identificate și corectate(COSO)

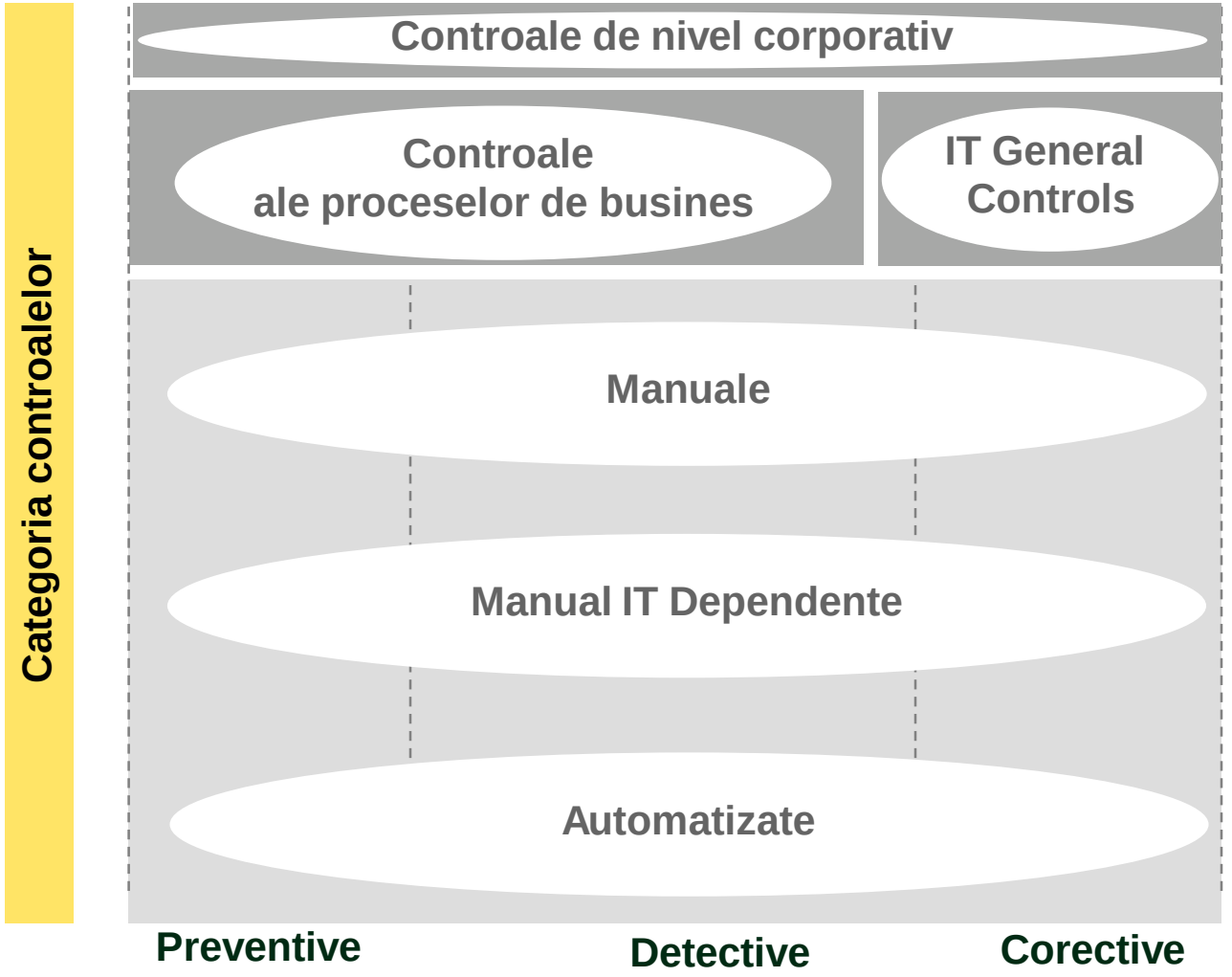
Controlul este un proces

Un control este un proces deoarece presupune o consecutivitate de activități, realizarea cărora de la început și până la sfarșit asigură îndeplinirea condițiilor de minimizare a riscului



Reieșind din definiția de mai sus, existența ușii închise la intrarea în camera cu servere sau activarea jurnalului de înregistrare a actiunilor în sistem nu pot fi numite controale!

Categorii și tipuri de controale



Tipurile de controale după modul de acțiune

- **Preventive**: servesc pentru preîntâmpinarea unor evenimente legate de realizarea riscului
- **Detective**: servesc pentru identificarea evenimentelor de realizare a riscului și asigură bază pentru luarea deciziilor
- **Corective**: permit înlăturarea parțială sau completă a urmărilor realizării riscului

Procedura de control a fost proiectată pentru a preveni acțiunea?

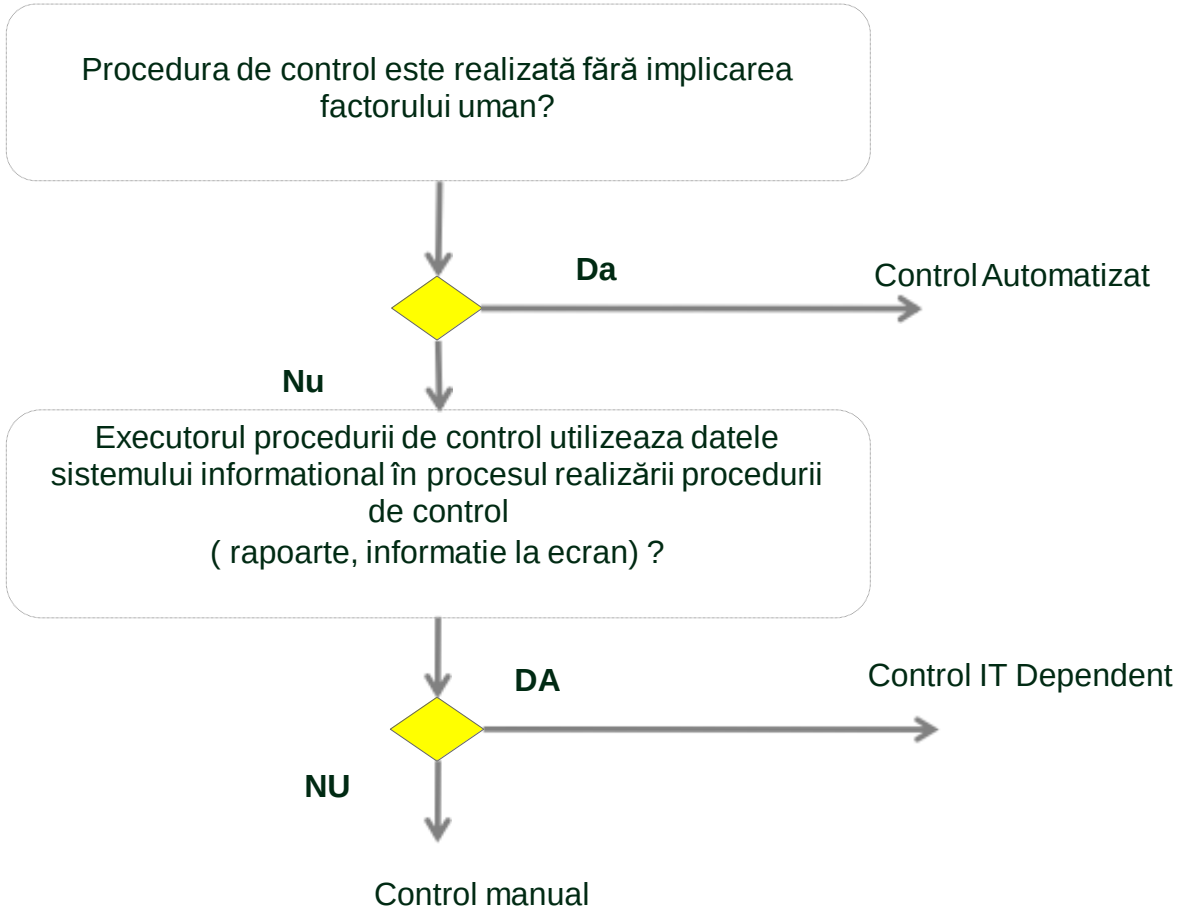
Control preventiv

Procedura de control a fost proiectată pentru a identifica eroarea?

Control de detectare

O practică eficientă de implementare a unui sistem de control intern eficient este implementarea unei combinații de controale de diferite tipuri ce acoperă un risc!

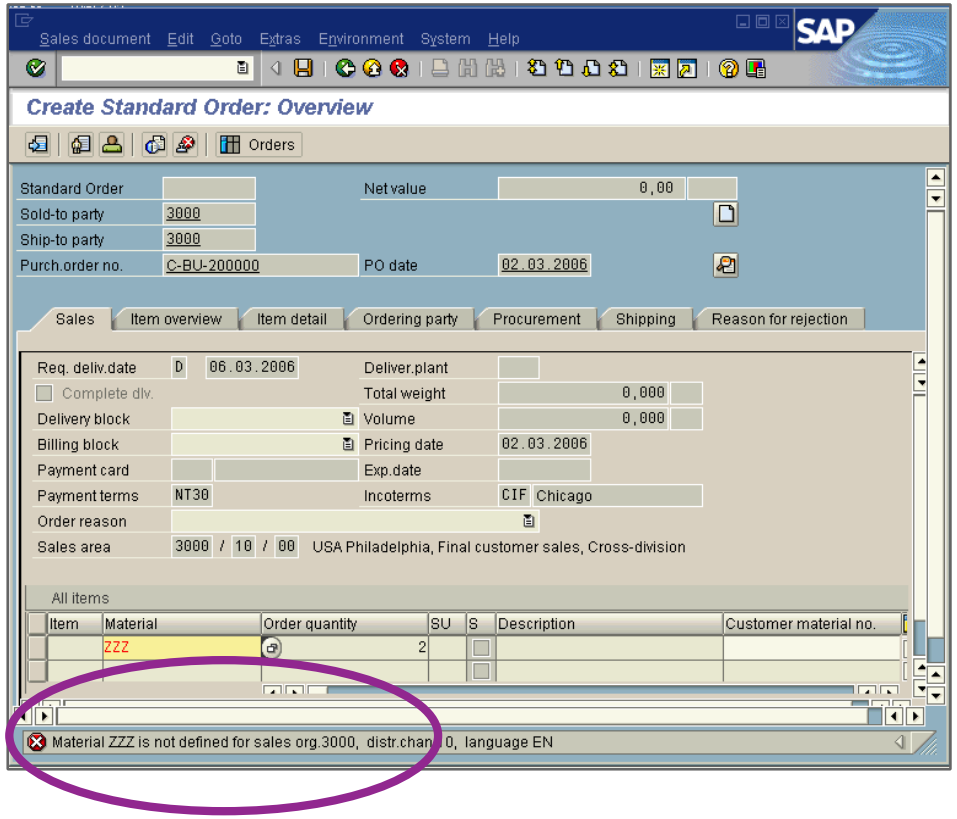
Control automatizat, TI Dependent, Manual



Controale automatizate (Application controls)

Controale realizate în mod automat de sistem, ce au scopul de a asigura completitudinea si corectitudinea prelucrării datelor de la intrarea și până la ieșirea din proces

Spre deosebire de controale IT Generale, aceste controale sunt proiectate și implementate în corespundere cu obiectivele de busines a unui sistem specific.



Tipurile controalelor automatizate

- **Verificarea completitudinii** (eng. Completeness check) – verificarea completitudinii datelor pe parcursul intregului proces
- **Verificarea veridicității** (eng. Validity check) – controale ce asigura, că sunt prelucrate doar date veridice
- **Identificare** (eng. Identification) – identifică univoc utilizatorii sistemului
- **Autentificare** (eng. Authentication) – mecanisme de autentificare în cadrul sistemului
- **Autorizare** (eng. Authorization) – este asigurat faptul, ca doar utilizatorii autorizați pot avea acces la sistem
- **Controale criminalistice** (eng. Forensic controls) – controale, directionate spre asigurarea corectitudinii matematice a informației în condiții sporite de fraudă

Exemple de controale automatizate în procesele de busines

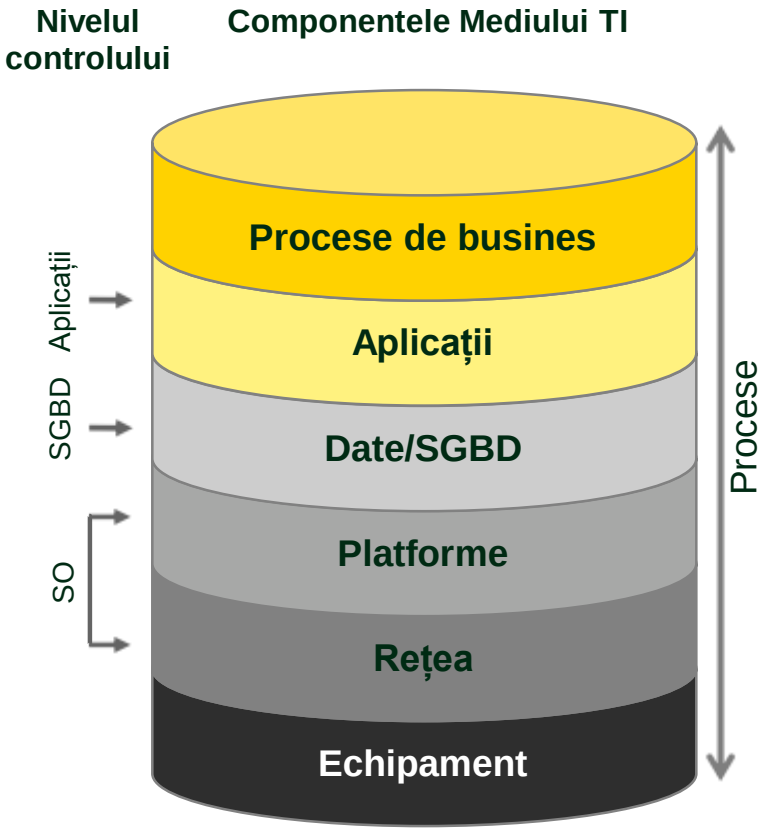
Tipul controlului	Obiectivul controlului	Exemplu de control
Verificarea completitudinii	Completitudinea datelor prelucrate	Dupa achitarea mărfii in sistem, formulele contabile sunt generate și inregistrate in cartea mare
Verificarea autenticității	Prelucrarea doar a datelor veridice	Pentru formarea formulelor contabile sistemul utilizeaza doar conturile din planul de conturi (imposibilă introducerea manuală).
Identificare	Identificarea univoca a utilizatorului sistemului	Colaboratorilor sectiei creditare este interzis accesul la informația despre salariați
Autentificare	Oferirea de mecanisme de autentificare	Pentru efectuarea unei plăți in sistem este necesar de a fi introdusa parola de acces
Autorizare	Acordare acces doar utilizatorilor autorizati	Accesul utilizatorilor la informația despre rapoartele fiscale ale societăților comerciale este permis doar inspectorilor fiscali
Control criminalistic	Corectitudinea matematică și științifica a datelor la intrare și la iesire din proces	Salariul lunar al angajatilor este calculat corect în baza datelor despre salariu introduse in fisa salariatului și a tabelului de evidenta a timpului de lucru

Controale de nivel corporativ / Controale IT Generale

- **Controale de nivel corporativ** – mecanismele de conducere ce sunt stabilite la nivel de companie și au rolul de a atinge obiectivele de activitate. Direct sau indirect au scopul de a minimiza riscurile ce caracterizeaza activitatea (ex. Planificarea strategică, Definirea responsabilităților funcției TI, asigurarea continuității afacerii, evaluarea ruscurilor TI, managementul proiectelor TI, etc.

- **Controale IT Generale** – direcționate spre minizarea nivelului riscului în sistemele informaționale, infrastructura TI și în procesele de gestiune a TI. Indirect asigură realizarea obiectivelor și a sarcinilor de busines în baza funcționării continue a sistemelor și a proceselor TI ce suportă procesele de busines

Controale IT Generale



Controalele IT Generale pot fi realizate la nivelul proceselor TI, precum și la nivelul diferitor componente tehnologice a mediului IT: Hard, Rețea, SO, SGBD sau plicativ

Identificarea controlului

- Care este evaluarea riscului analizat?
- Care sunt instrumentele ce pot previne realizarea riscului?
- Ce tip de control este necesar/aplicabil?
- Va minimiza controlul selectat riscul până la un nivel acceptabil?
- Este necesară o combinație de controale de diferite tipuri?
- Dacă da, atunci care este combinația optimă?

Evaluarea procedurii de control

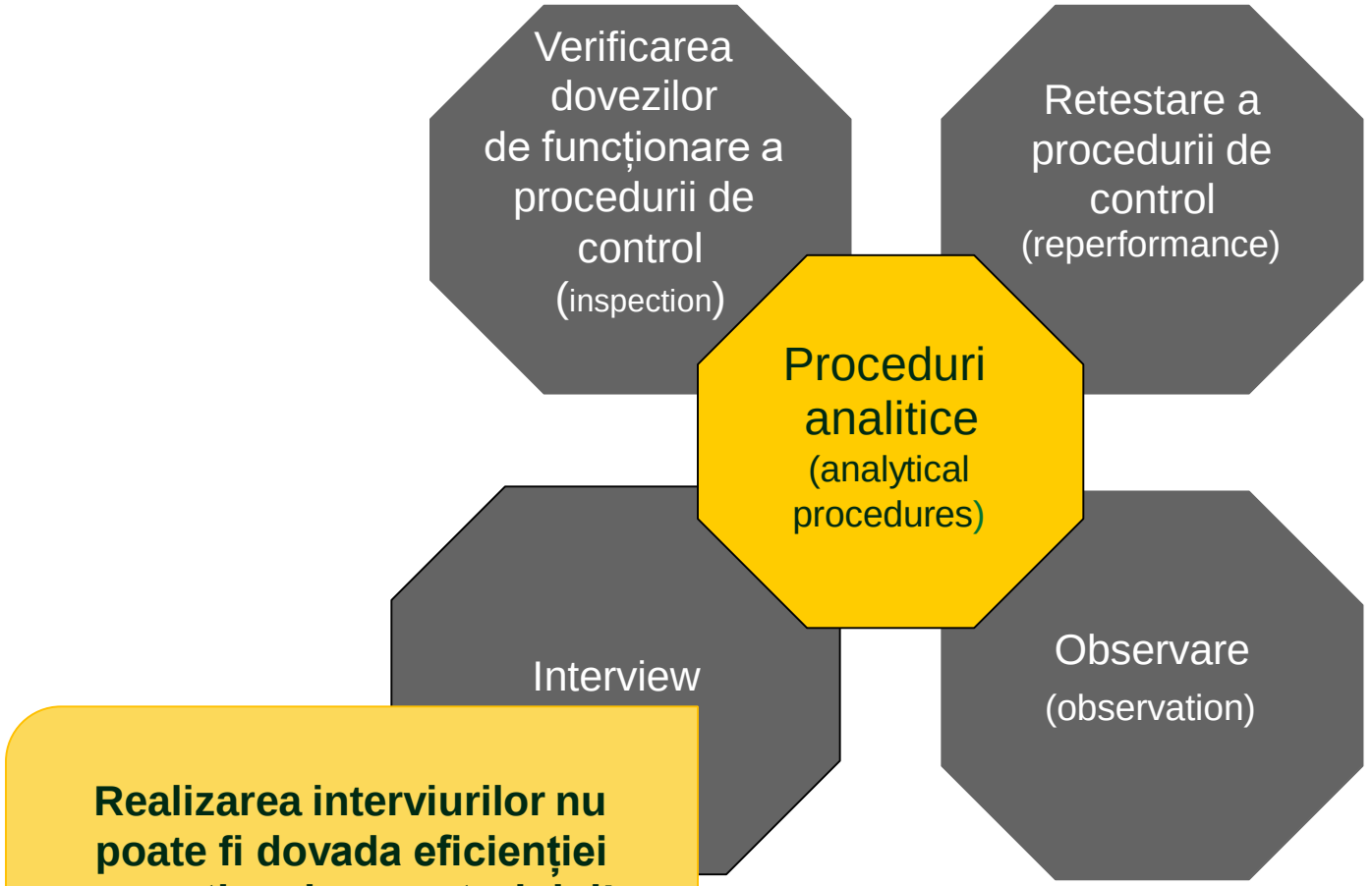
- Controlul este evaluat din doua puncte de vedere:
  - Eficiență design;
  - Eficiență operațională.

- Eficiența design: Acoperă oare controlul propus riscul identificat?
- Eficiența operațională: a fost oare controlul funcțional pe toată perioada analizată, conform design-ului, preîntâmpinând sau identificând la timp evenimentele legate de risc ?

Identificarea și evaluarea controalelor

- Este necesară o analiza inițială a procesului de business pentru a:
  - confirma înțelegerea proceselor implementate, sistemelor utilizate și a procedurilor existente
  - identifica controalele existente în cadrul proceselor
- Testarea controalelor din cadrul procesului în baza unui element
- În rezultatul testării ne asigurăm că:
  - Funcționează conform design-ului
  - A funcționat corect pe toată perioada analizată
  - A funcționat în baza informației veridice
- În baza rezultatelor analizei inițiale definim strategia de audit.

Metode de testare a controalelor



Realizarea interviurilor nu poate fi dovada eficienței operaționale a controlului!

Testarea controalelor: Eșantionare

Tip	Periodicitatea realizarii	Numărul minim de elemente pentru testare	Exemplu de control
Manual	Cateva ori pe zi	Nu mai putin de 25	Incidentele TI sunt fixate la timp de către responsabilul sectiei de suport tehnic
Manual	Zilnic	Nu mai putin de 25	Identificarea evenimentelor critice din jurnalul de înregistrare a incidentelor are loc la sfarsitul zilei
Manual	Saptamanal	Nu mai putin de 5	Crearea copiilor de rezerva a datelor are loc saptamanal
Manual	Lunar	Nu mai putin de 2	Testarea posibilității de restabilire adatelor din backup are loc la sfarsitul fiecărei luni calendarisitice
Manual	Semestrial	Nu mai putin de 2	Auditul setărilor parolelor este efectuat simestrial
Manual	Anual	Nu mai putin de 1	Inventarierea drepturilor de acces la sistemul informațional are loc anual
Automatizat	–	Testarea controalelor se realizeaza cate un element, cu condiția că ITGC testate su fost effective, altfel test of 25	Integritatea datelor BD este asigurată cu utilizarea mecanismelor incorporate in sistemul de operare
ITGC	–	Se aplica regulile de mai sus	Accesul la sistemul informational este acordat in baza cererii de acces aprobată de proprietarul sistemului

Deficiențele controalelor

- Deficiență sau neajuns al controlului este evenimentul, care indică următoarele:
  - Controlul nu funcționează conform design-ului
  - Controlul nu a funcționat conform design-ului pe parcursul întregii perioade analizate

- Toate exceptiile trebuie analizate detaliat pentru a:
  - Confirma corectitudinea înțelegerii situației
  - Identifica cauzele exceptiilor
  - Înțelege impactul posibil asupra altor proceduri de audit
  - Întocmi raportul pentru management

Controale compensatorii

Măsuri de compensare – proceduri speciale de control, ce au obiectivul sa compenseze neajunsurile controalelor implementate

Este important să fie evaluată necesitatea și eficiența controalelor compensatorii

Dovezi de audit

- Obținute în procesul de observare:
  - In procesul observatiilor evenimentelor, acțiunilor angajaților, de exemplu inspectarea fizică a camerei cu servere
- Obținute în rezultatul solicitării confirmărilor speciale:
  - Scrisori și afirmații scrise, obținute în rezultatul unei solicitări de informație sau interview (ex. Confirmarea funcțiilor angajaților, diferite screenshot-uri ale ecranelor, etc)
- Dovezile documentale:
  - Interne – Cerere de acces, comandă de prestare a serviciilor, corespondența internă
  - Externe – factura de la furnizor
- Dovezi analitice:
  - Rezultatul efectuării procedurilor analitice sau a verificărilor

Exemplu de matrice de documentare a controalelor

№ ITGC	Procesul	Sub –proces/ obiectivul controlului	Descrierea detaliata a obiectivului controlului	Sistemul informatic	Nivelul	Descrierea Procedurii de control
ITGC.1-05	Managementul modificărilor	Limitarea accesului la funcțiile privilegiate	Accesul la funcțiile privilegiate în sistemele informaționale este limitat conform normelor de securitate aprobate.	1C 8.0, SAP ERP	SO, SGBD, Aplicație	Executorul procedurii de control asigura monitorizarea permanentă a acțiunilor angajaților în cadrul procesului de management al modificărilor

Responsabil	Termenii de executare	Frecventa de executare a procedurii de control	Tipul procedurii de ctrol	Categoria	Rezultatul realizarii procedurii de control	Evaluarea design
Inginer Sectie Securitatea informationala a filialei	Simestrial	Simestrial	Manual	Detective	Raport in rezultatul monitorizării	Eficient

Exercitiu 2. Descriere controale și categorii