

# Implementarea SMSI

# Fazele implementării SMSI

- ▶ Plan 1: Stabilirea importanței securității informației
- ▶ Plan 2: Definirea sferei SMSI
- ▶ Plan 3: Definirea politicii de securitate
- ▶ Plan 4: Stabilirea rolurilor și responsabilităților
- ▶ Plan 5: Identificarea și clasificarea resurselor
- ▶ Plan 6: Identificarea și evaluarea riscurilor
- ▶ Plan 7: Selectarea opțiunilor de tratare a riscului
- ▶ Do 8: Implementare și funcționare SMSI
- ▶ Do 9: Întocmirea declarației de aplicabilitate
- ▶ Do 10: Instruirea și pregătirea personalului
- ▶ Check 11: Monitorizarea și controlul performanțelor SMSI
- ▶ Act 12: Menținerea SMSI și îmbunătățirea continuă

# Plan 1: Stabilirea importanței securității informației

- ▶ Identificarea și documentarea obiectivelor afacerii
- ▶ Identificarea proceselor de business
- ▶ Identificarea sistemelor și proceselor TI
- ▶ Identificarea dependenței afacerii de sistemele TI
- ▶ Identificarea cerințelor de protecție pentru sistemele TI

## Plan 2: Definirea sferei SMSI

- ▶ Descrierea organizației
- ▶ Descrierea afacerii, obiective
- ▶ Descrierea locației geografice
- ▶ Procese de afacere incluse în sferă
- ▶ Sisteme TI incluse în sferă
- ▶ O schemă fizică generală a locației
- ▶ Diagrame ce reflectă arhitectura SI (aplicații, flux de date, fizic, rețea logic și fizic)

# Plan 3: Definirea politicii de securitate

- ▶ Reprezintă demonstrarea atenției și angajamentului managementului pentru securitatea informației
- ▶ Stabilește directivele managementului pentru managementul securității informației
- ▶ Conține:
  - ▶ Definiția securității informației
  - ▶ O declarație a managementului privind securitatea informației
  - ▶ O scurtă descriere a principiilor, principalelor politici, standarde și cerințe de conformare;
  - ▶ O definire a responsabilităților generale și specifice
  - ▶ Referință la documente care pot susține implementarea Politicii

## Plan 4: Roluri și responsabilități în cadrul SMSI

- ▶ Comitetul de conducere responsabil de securitatea informației
- ▶ Ofițerul de securitate a informației (OSI)
- ▶ Diferite echipe cu destinație specială
  - ▶ Echipa de intervenție la incidente
  - ▶ Echipa de instruire în domeniul securității
  - ▶ Echipa de planificare a continuității
  - ▶ Echipa de restabilire în caz de dezastru

## Plan 4: Roluri și responsabilități în cadrul SMSI

- ▶ Posesor resurse
- ▶ Gestionar resurse
- ▶ Conducători de subdiviziune
- ▶ Utilizatori

# Plan 5: Indentificarea resurselor

- ▶ Registrul resurselor organizației
  - ▶ Informațiile
  - ▶ Softuri aplicative
  - ▶ Servicii de suport
  - ▶ Bunuri fizice (hard)
  - ▶ Infrastructură (încăperi, sisteme de menținere)
  - ▶ Personalul
- ▶ Identificarea și înregistrarea începe cu cele mai critice resurse



# Plan 5: Clasificarea resurselor

- ▶ Clasificarea se face pentru toate resursele importante
- ▶ Clasificarea se face conform criteriilor:
  - ▶ Confidențialitate
  - ▶ Integritate
  - ▶ Disponibilitate
  - ▶ Autenticitate
  - ▶ Non-Repudiere
- ▶ Scări de clasificare
  - ▶ Critic
  - ▶ Important
  - ▶ Normal
  - ▶ Nesemnificativ

# Plan 6: Identificarea și evaluare riscurilor

- ▶ Analiza amenințărilor
- ▶ Analiza vulnerabilităților
- ▶ Analiza riscurilor
- ▶ Evaluarea riscurilor

# Plan 7: Selectarea opțiunilor de tratare a riscului

- ▶ Opțiunile de tratare a riscului
- ▶ Definirea politicilor de securitate
- ▶ Definirea procedurilor
- ▶ Identificarea soluțiilor de securitate
- ▶ Evaluarea cost-eficienței opțiunilor
- ▶ Pregătirea Planului de tratare cu indicarea opțiunilor
- ▶ **Obținerea aprobării Managementului**

# Do 8: Implementare și funcționare SMSI

- ▶ Implementarea planului de tratare a riscurilor
- ▶ Planificarea proiectului de implementare
- ▶ Pregătirea măsurilor de securitate
- ▶ Testarea măsurilor de securitate
- ▶ Implementarea măsurilor de securitate
- ▶ Stabilirea indicatorilor de măsurare a eficienței
- ▶ Revizuirea riscului rezidual

# Do 9: Declarația de aplicabilitate

- ▶ Maparea măsurilor de securitate implementate pe cele din Anexa A, ISO/IEC 27001
- ▶ Menționarea excepțiilor, argumentarea neselectiei, măsurile compensatorii
- ▶ Poate fi utilă pentru eficientizarea controalelor BNM

# Do 10: Instruire personal

- ▶ Identificarea grupurilor de interes
- ▶ Pregătirea planului de instruire
- ▶ Pregătirea programului de instruire
- ▶ Organizarea cursurilor de instruire
- ▶ Menținerea culturii de securitate corporativă

# Check 11: Monitorizarea și controlul performanței SMSI

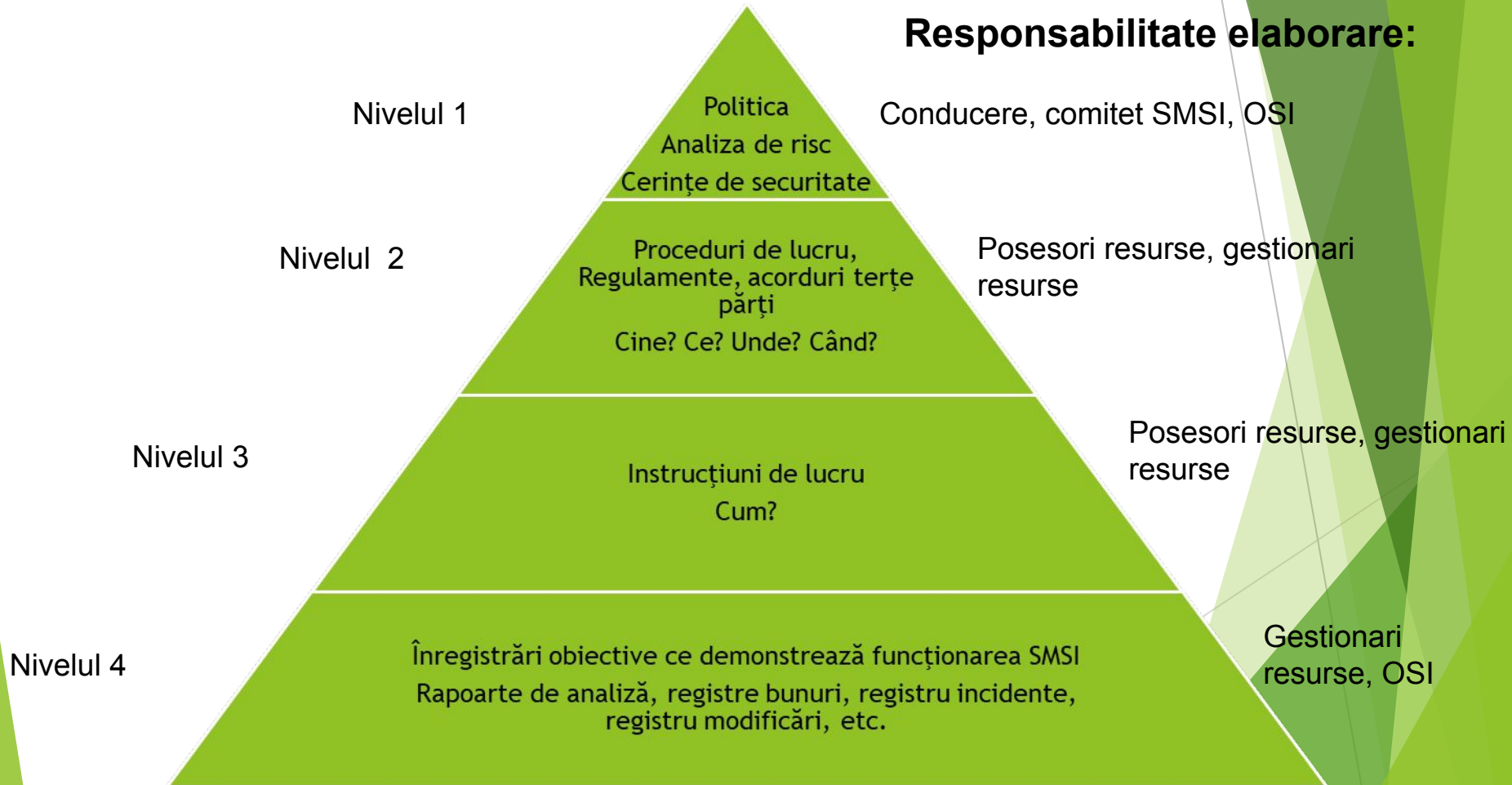
- ▶ Raportarea incidentelor
- ▶ Monitorizare efectuată de OSI
- ▶ Auditul intern
- ▶ Analiza de management

# Act 12: Menținerea SMSI și îmbunătățirea continuă

- ▶ În rezultatul incidentelor
- ▶ Rapoartelor de analiză a SMSI
- ▶ Noi vulnerabilități
- ▶ Schimbări în sistemul informațional
- ▶ Schimbări în legislația în vigoare



# Documentația SMSI



# Concluzii

- ▶ Întrebări & Răspunsuri