SECTIO AUREA

# Workshop
# Implementarea practica a Directivei NIS
# (Legea nr. 362/2018)
# 03 Februarie 2023
# Vom astepta 5 Minute

SECTIO AUREA

# Agenda

- Introducere Invitati speciali
- Introducere Madalin Bratu & Sectio Aurea
- **Implementarea cerintelor legii. Etape, Recomandari** - Madalin Bratu
- **Pregatirea pentru audit** - Open panel: Madalin Bratu & Ilie Voinea
- Studiu de caz - **Aplicatie inovativa pentru asigurarea detectiei atacurilor cibernetice la nivelul ICS Scada**. Si nu numai – Cosmin Macaneata, Omega Trust
- QA

# Invitati speciali

**Ilie Voinea este** un foarte bun specialist in Data Privacy si securitatea informatiilor si un specialist IT cu o fundatie practica foarte solida in intretinerea mediilor IT complexe.

Ilie a participat la mai multe focus groups ale ISACA, si a fost coautor la publicatia ISACA - GHID PRACTIC PENTRU OSE.
**Este Auditor atestat NIS.**

**Cosmin Macaneata** este un specialist cu o indelungata experienta in auditarea IT si securitatii cibernetice inca din 2004. Cosmin este Managing partner la Omega Trust. Compania Omega Trust este specializată în zona auditului şi testării securităţii cibernetice.

**Este Auditor atestat NIS.**


Intro
Madalin Bratu & Sectio Aurea

# Sa ne cunoastem

## Madalin Bratu

- **20** ani de experienta in domeniul serviciilor IT si a securitatii cibernetice
- **10** ani experienta regionala in Servicii integrate de suport, Cloud (IBM)
- **6** ani experienta in proiecte locale de cybersecurity
  - Audit de Securitate / testare de Securitate
  - Implementare de sisteme de management al securitatii si al GDPR
  - Experienta practica in coordonarea implementarii diverselor tehnologii de securitate
  - Experienta aplicata in externalizarea serviciilor de suport si monitorizare de Securitate
  - **Consultant specializat in implementarea Directivei NIS, cu referinte**
- **2** ani experienta proiecte globale de cybersecurity

https://www.phi.ro/fondator

SECTIO AUREA

# Ce este

O companie de servicii avansate in cybersecurity cu o misiune simpla:
Sa facem disponibile capabilitati avansate in cybersecurity catre clienti care isi doresc sa isi protejeze afacerea, in mod flexibil si competitiv.
De la Companii medii pana la corporatii.

phi (sau φ din alfabetul grecesc vechi), numit si numarul lui Fibonacci, numarul de aur, proportia divina, sectiunea de aur (*sectio aurea* in latina) este un numar esential, prezent in toate domeniile de activitate (matematica, biologie, design, arhitectura, biologie).

phi sta la baza a tot ce este natural, frumos, bine proportionat.

$$\varphi = (a+b)/\ a = a\ /\ b$$

$$\varphi = 1{,}618033\ldots$$

Cu noi, va veti dezvolta armonios, natural, relevant.

DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ
AUDITOR ATESTAT GENERAL
Seria CLE nr. 8020 din 23.03.2022

SRAC CERTIFICAT nr.407 ISO/IEC 27001

SRAC CERTIFICAT nr.12650 ISO 9001

SECTIO AUREA

# Ce facem?

## Check

Evaluam nivelul de expunere la afacerii la amenintarile cibernetice, prin
Audit de Securitate, Testare de Securitate, Servicii avansate de Testare "RedTeam“ si Audit Securitate in Cloud.

Evaluam nivelul de conformitate al afacerii la cerintele actuale GDPR, Directiva NIS prin Audit de conformare.

## Plan&Do

Continuam sa va asistam sa aplicati masuri adecvate, ca sa optimizati sistemele din punct de vedere al securitatii, prin

CISO si DPO on Demand

## Act

Va optimizam capacitatea de a raspunde la incidente de Securitate prin servicii foarte avansate de augmentare a SOCului.

Optimizare SOC

Evaluare Incident Response

Exercitii Incident Response

Suport Incident Response

Threat Hunting & Security Forensics

SECTIΦ AUREA

# Servicii proactive

Daca “norocul îi ajută pe cei care sunt pregatiti” atunci capabilitatile noastre proactive va aduc noroc.

**Audit de Securitate**

- Cu noi poţi face fata mai uşor incertitudinii. Iţi construim o abordare structurata a felului in care iţi identifici ameninţările de securitate si cum iţi administrezi riscurile.

**Audit Conformare**

- Cu noi identifici mai rapid si eficace *gap-rile* faţă de cerinţele externe (GDPR, Directiva NIS), vulnerabilităţile afacerii tale la ameninţările interne si externe cât şi planurile detaliate de adopţie a conformării.

**Testare de Securitate.**

- Un test de penetrare identifică şi demonstrează vulnerabilităţi. Vă oferim o nouă înţelegere şi strategii pentru consolidarea posturii de securitate împotriva ameninţărilor cibernetice. Testarea de securitate ajută la identificarea lacunelor de securitate. Testele de simulare phishing ajuta sa reduceti riscurile de Securitate cauzate de factorul uman.

**Audit SecuritateCloud.**

- Asiguraţi-vă că profitaţi la maximum de investiţiile şi resursele dvs. de securitate in cloud-ul Amazon, Microsoft, Google, folosind experienţa noastră.

**Exerciţii Incident Response Tabletop.**

- Vă evaluaţi planul de răspuns la incidente cibernetice prin scenarii definite. Exerciţiile evaluează procesele, instrumentele şi eficienţa răspunsului la atacurile cibernetice atât din punct de vedere strategic, dar si şi tehnic.

**Threat Hunting**

- Experţii noştri în securitate colectează telemetria punctelor finale, ca sa determine ameninţările istorice şi active. Metodologia de lucru depăşeşte o simplă scanare a indicatorilor de compromis în mediul tau si este bazată pe experienţa în răspunsul la intruziunile cibernetice şi adoptă o abordare concentrată, personalizată pentru fiecare client.

SECTIO AUREA

# Servicii reactive

In situatiile speciale, aveti o echipa puternica de nivel superior, pe care sa va bazati.

## Incident Response Retainer.

- Reduceți timpul de răspuns la incident și minimizați impactul unui incident de securitate. Cu acest serviciu, ai un partener de încredere în standby. Această abordare pro activă poate reduce semnificativ timpul de răspuns, Investigare avansată de incidente calificate de securitate
- Primiti Recomandări pentru activitățile de izolare si mitigare a unei breșe de securitate

## Digital Forensics

- Implicam profesionisti acreditati in Digital Forensics si incident response cu experienta aplicata in Big-4, si cele mai mari companii din S&P 500 si FTSE 100.

SECTIO AUREA

# Servicii evolutive

Construiește cu noi, un sistem dinamic si coerent prin care sa iți minimizezi inteligent riscurile afacerii tale.

**CISO & DPO On demand**

- Cu noi poti suplimenta dinamic capabilități. O echipa experimentată te va ajuta sa iți implementezi si sa întreții în organizație un sistem viu de politici, proceduri si mecanisme de optimizare continua a securității sau al confidentialitatii datelor. Într-un regim de munca flexibil si eficace.

**SOC Development.**

- Proiectați și dezvoltați un program de operațiuni de securitate pentru a vă apăra împotriva amenințărilor avansate. Vă ajutăm echipa să planifice și să se pregătească pentru o gamă largă de incidente cibernetice, cu o vastă experiență operațională și cele mai bune practici colectate din prima linie, de o echipă de răspuns la incident cu experiență la nivel global.

**Incident Response Readiness**

- Folosind lecțiile învățate din răspunsul la o gamă largă de amenințări, consultanții Sectio Aurea evaluează capacitatea organizației tale de a gestiona amenințările specifice și oferă îndrumările de care aveți nevoie pentru a realiza îmbunătățiri practice și semnificative. Va evaluăm capacitatea de apărare cibernetică a organizației, care include de obicei centrul lor de operațiuni de securitate (SOC) și răspunsul la incident funcții (IR). După evaluare, primești un raport cu un *road map* detaliat și recomandări de îmbunătățire prioritizate

SECTIO AUREA

# Expertiza

ISACA
3 CISA
Certified Information Systems Auditor

ISACA
1 CRISC
Certified in Risk and Information Systems Control

ISACA
5 CISM
Certified Information Security Manager

ISACA
1 Cobit Foundation

ISACA
1 CDPSE
Certified Data Privacy Solution Engineer

ISC2
4 CISSP
Certified Information Systems Security Professional

ISC2
1 SSCP
Systems Security Certified Practitioner

ISC2
1 CCSP
Certified Cloud Security Professional

TUV / BSI / PECB
5 ISO/IEC 27001 Lead Auditor

TUV / BSI / PECB
5 ISO/IEC 27001 Lead Implementer

PECB
1 Certified DPO

PECB
1 ISO 22301 Lead Auditor

PECB
1 ISO/IEC 27005 Risk Manager

CompTIA
1 Security+

IAPP
5 CIPP-E
Certified Information Privacy Professional

IAPP
1 CIPT
Certified Information Privacy Technologist

IAPP
4 CIPM
Certified Information Privacy Manager

IAPP
1 FIP
Fellow of Information Privacy

EC-Council
3 CEH
Certified Ethical Hacker

EC-Council
1 LPT
Licensed Penetration Tester

EC-Council
1 ECSA
Certified Security Analyst

GIAC
1 GISP
GIAC Information Security Professional

Offensive Security
3 OSCP
Offensive Security Certified Professional

Offensive Security
1 OSCE
Offensive Security Certified Expert

Togaf
Togaf Certified Architect

ITIL Foundation

# Intro

## Directiva NIS si Legea 362 / 2018

SECTIO AUREA

# Introducere Directiva Europeana NIS si Legea 362/2018

**12 ianuarie 2019**

Directiva NIS (Directiva UE 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016) a fost adoptată în Romania prin legea nr. 362/2018 de către Parlamentul României.

## Scop

Atingerea un standard comun ridicat pentru securitatea rețelelor și informațiilor în toate statele membre ale Uniunii care oferă servicii esențiale pentru societate.

Directiva NIS este o reglementare europeană esențială care asigură sustenabilitatea noii economii digitale.

## Vi se adreseaza Directiva NIS?

# Da

Daca aveti afacerea in urmatoarele sectoare de activitate si indepliniti criteriile legii.

SECTIΦ AUREA

# Care sunt obligatiile legale?

Implementarea cerinţelor minime de securitate in conformitate cu cele mai bune practici din industrie.

Un sistem de reguli, roluri, responsabilitati, proceduri, politici, tehnologii de securitate, pentru protectia infrastucturii IT care sustine serviciul esential

Sistem aliniat cu standarde

Evidente de implementare

## Directiva NIS

- Seteaza cerintele Europene generale

## Legea 362/2018

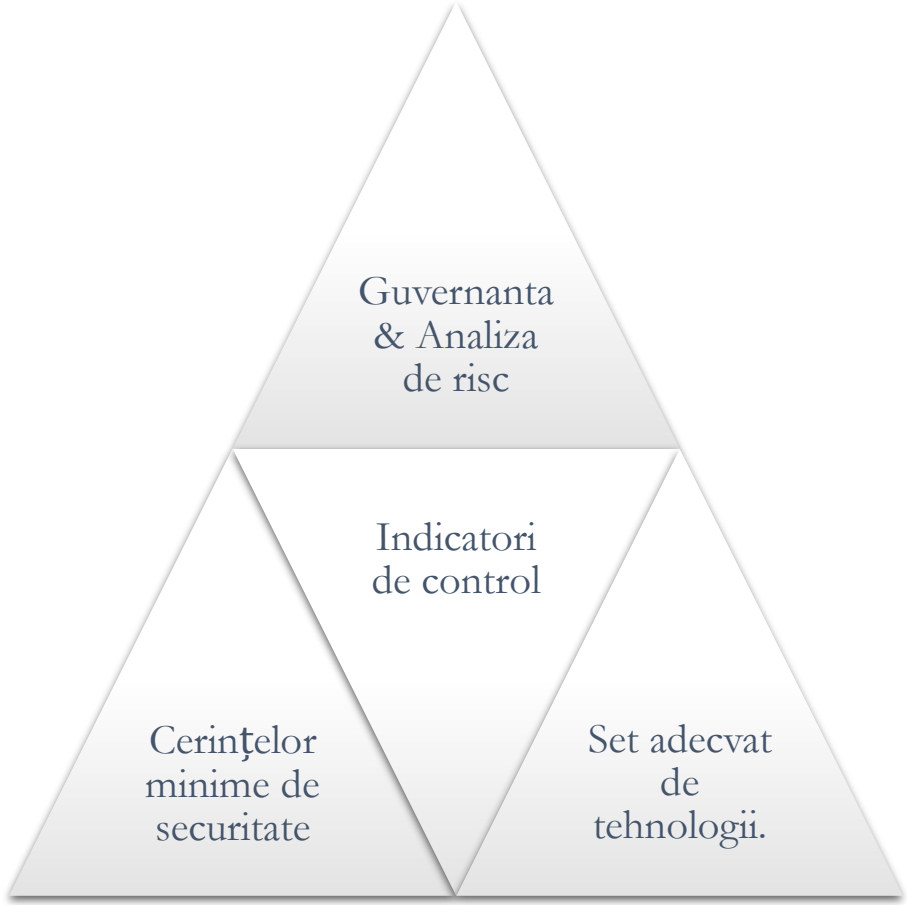
- Implementeaza cerintele directive in Romania

## Ordinul 1323/2020

- Precizeaza componentele Sistemului de management

## Decizia nr. 88/2020 a CERT

- Precizeaza standardele si bunele practice la care trebuie sa va raportati



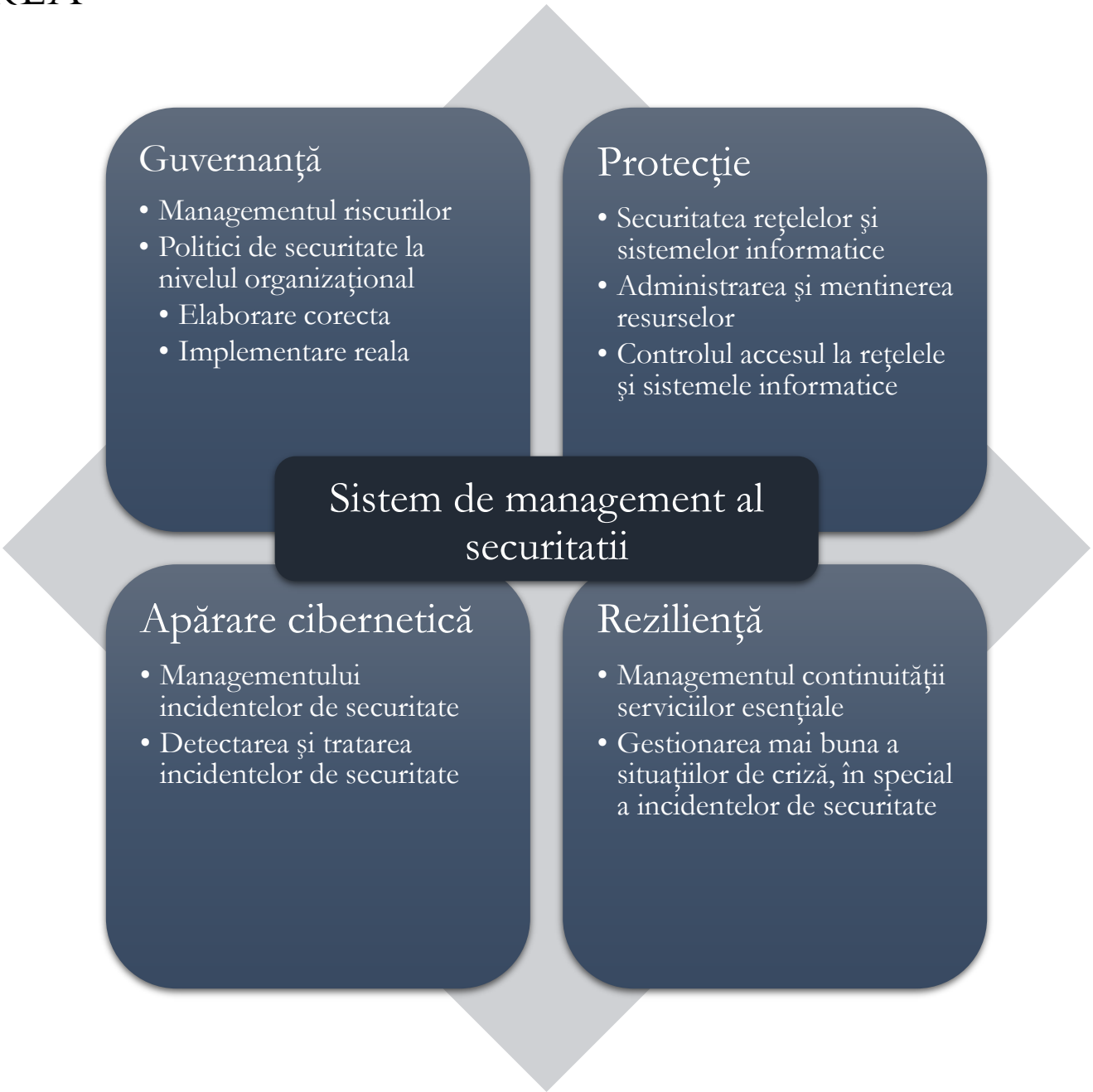

**Penalitati Pana la**

**5%**

**din cifra de afaceri pentru incalcarea legii**

SECTIO AUREA

# Ce insemna conformarea cu legea?




# Si mai concret, ce cere legea?

| | |
|---|---|
| Documentatie | Politica de Securitate, proceduri specifice de lucru |
| Analiza de risc | Se realizeaza conform cu bune practice si standard internationale |
| Masuri de securitate | Administrative, tehnice,fizice |
| Activitati specifice | Monitorizare<br>Raspuns la incidente<br>Management vulnerabilitati<br>Testarea recuperarii in caz de dezastru |

**Elemente auditabile**

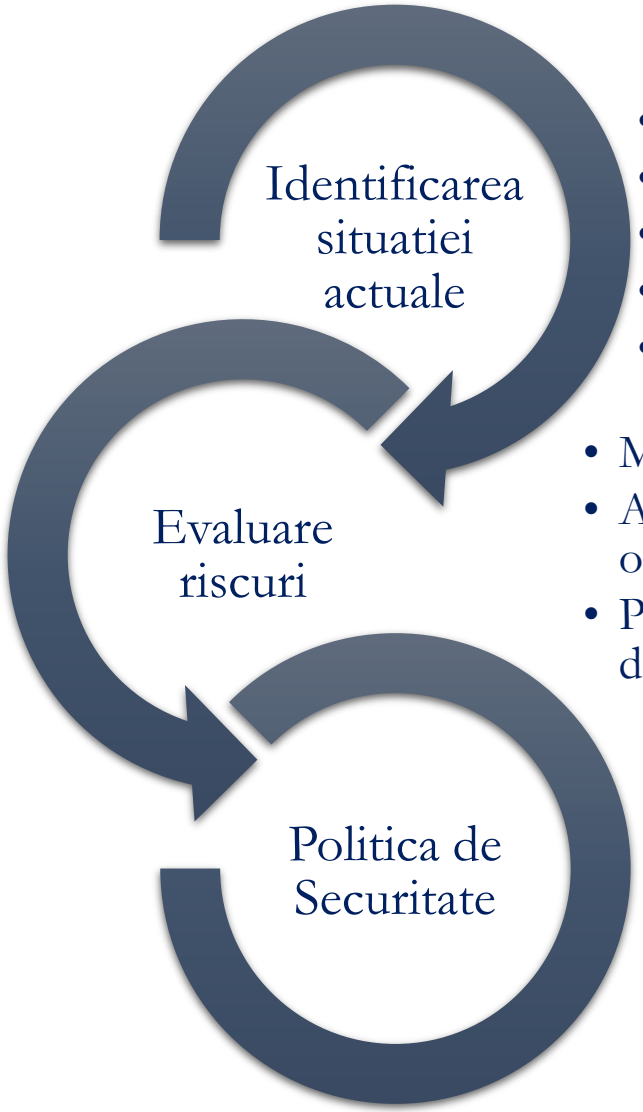
# Etapele de implementare

SECTIΦ AUREA

# Care sunt etapele de conformare?

## #1. **Guvernanta** este cel mai important pas.

Arata o abordare controlata a riscului, sprijinita de management




- Lista activelor, sistemelor şi proceselor organizației
- Arhitectura rețelelor şi sistemelor informatice
- Clasificare informatii
- Owneri
- Corelare Servicii esențiale cu servicii IT si sisteme

- Metodologie de risc agreata si implementata
- Analiza risc reala (audit arhitectura, configuratie, oameni, procese) & Analiza Cost & Beneficiu
- Plan de actiuni agreat de management cu owneri, date, actiuni concrete de remediere

- Aplicabila si adevata intregii organizatii
- Emisa de conducerea executiva

| Indicatori de control conform Ordin 1323 din 26 noiembrie 2020 (selectie) | |
|---|---|
| LASPO | Lista activelor, sistemelor şi proceselor organizației |
| SICAE | Situația cartografică a ecosistemului |
| PRECDI | Procedură privind etichetarea şi clasificarea datelor şi informațiilor |
| SANIS | Schema arhitecturii rețelelor şi sistemelor informatice |
| LASMA | Listă cu acorduri la nivel de serviciu, mecanisme de audit |
| MEGRE | Metodologie de gestionare a riscurilor |
| RERO | Registrul de risc organizațional |
| LIRIE | Lista riscurilor potențiale identificate |
| ARNIS | Analiza riscurilor de securitate |
| PONIS | Politica de securitate |

SECTIO AUREA

# #1. Guvernanta (sumar)

**Centralizati si analizati ce se poate reutiliza**

- Proceduri existente de lucru, ISO, fise de post, Contracte de munca, Contracte cu terte parti, Liste de inventar, procese

**Asigurati un suport corect al analizei de risc**

- Liste de inventar ale activelor si ownerii
- Modele fizice si logice ale arhitecturii IT
- Identificati serviciile esentiale si infrastuctura IT pe care se sprijina

**Analiza de risc**

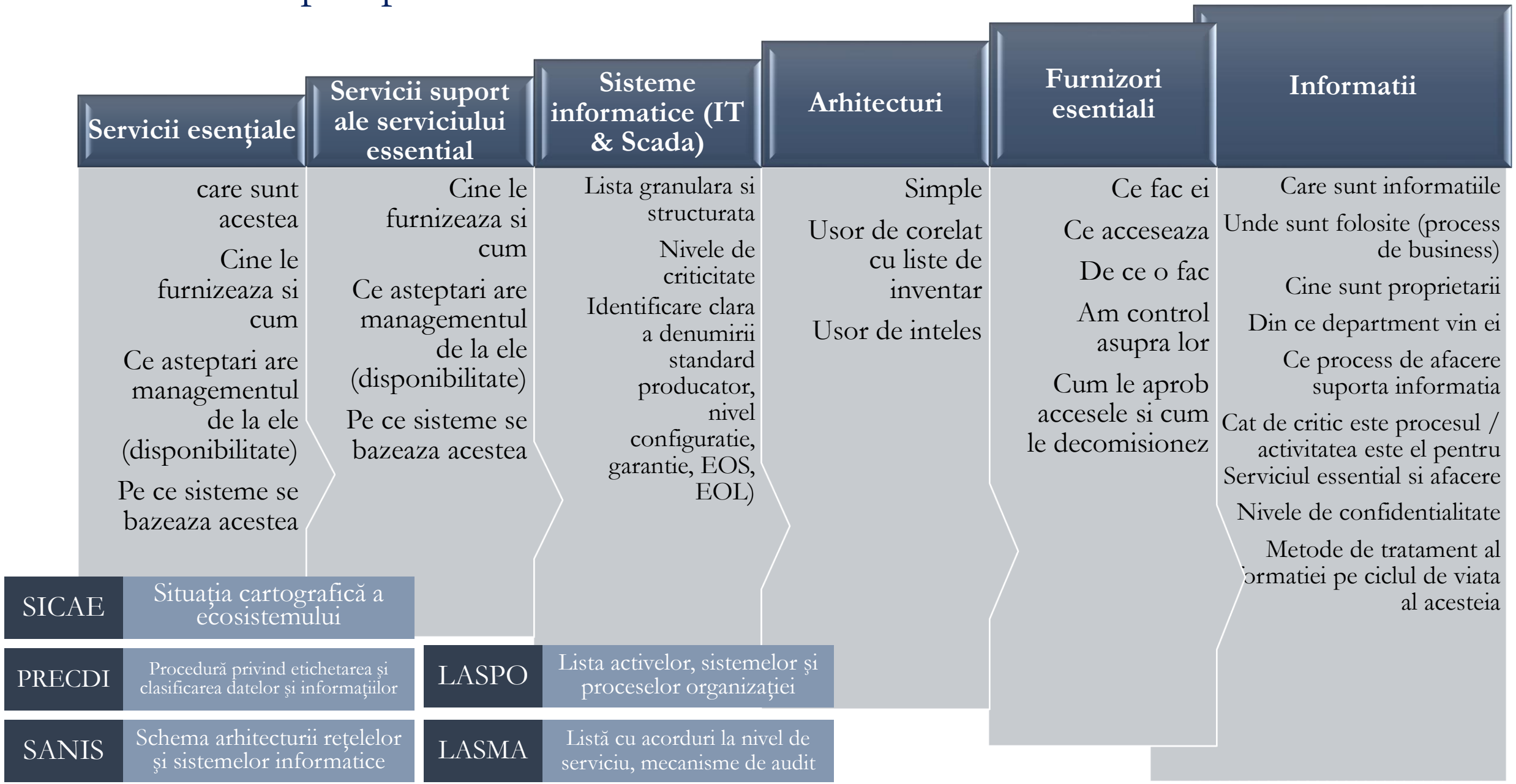
- Constructia de matrici de amenintari si vulnerabilitati
- Identificarea de vulnerabilitati tehnice si de proces
- Analiza de procese operationale
- Identificarea riscurilor majore si propunerea de planuri de mitigare catre Management
- **Management Signoff**

**Implementare Sistem de Management**

- Masuri adecvate administrative, tehnice, fizice
- Modificari tehnice infrastuctura existenta
  - noi tehnologii
  - noi capabilitati
  - reconfigurari tehnice

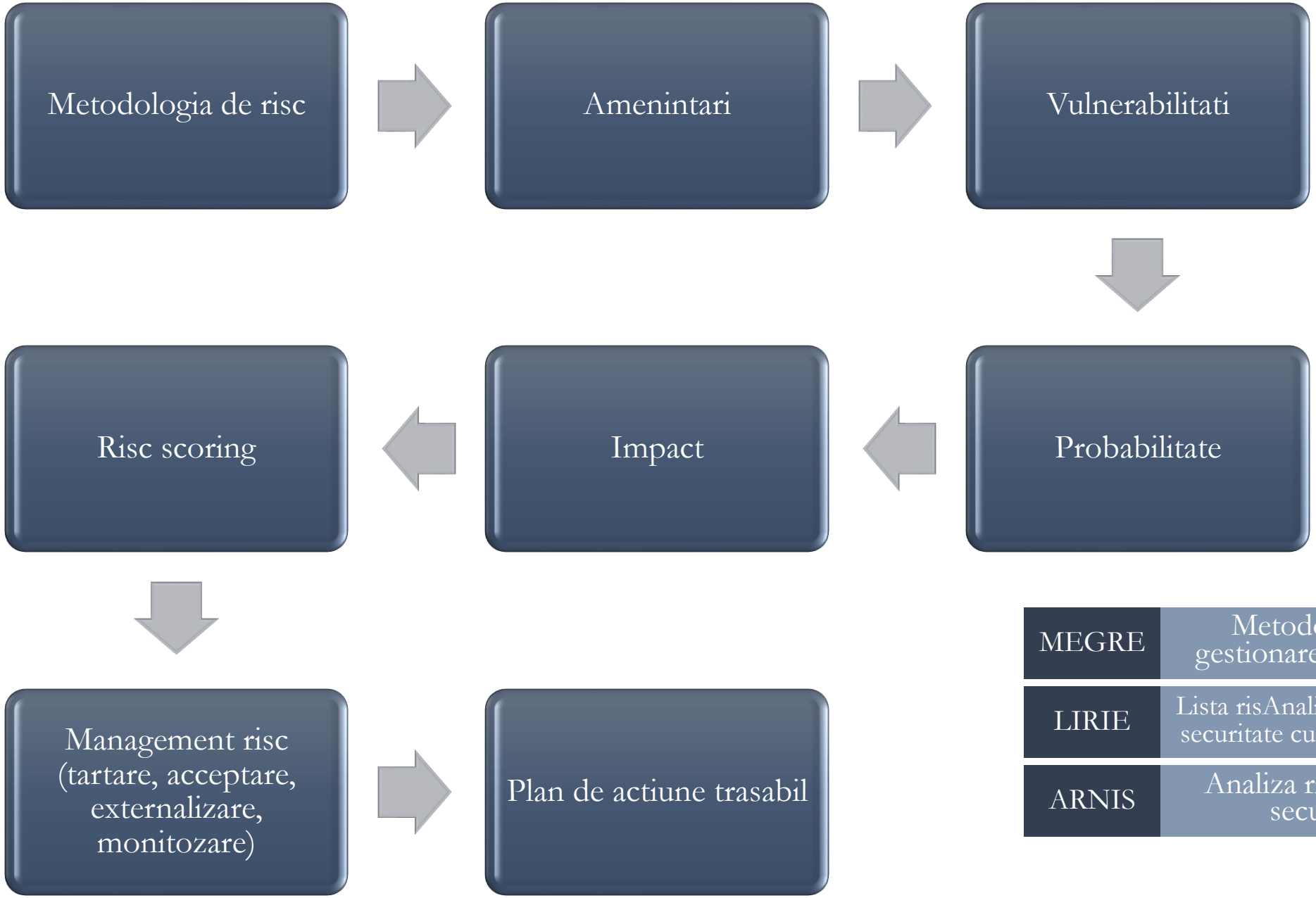
SECTIΦ AUREA

# Primii pasi pana la analiza de risc



SECTIO AUREA

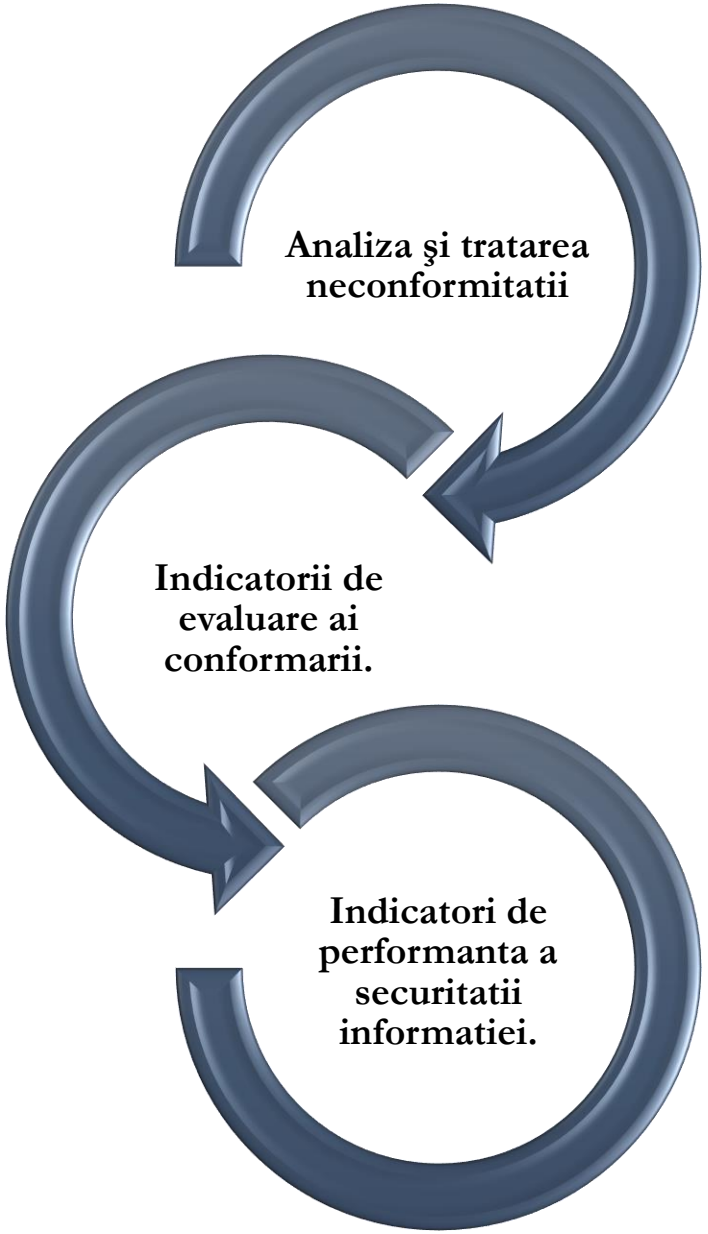
# Analiza de risc




| | |
|---|---|
| MEGRE | Metodologie de gestionare a riscurilor |
| LIRIE | Lista risAnaliza riscurilor de securitate curilor potențiale |
| ARNIS | Analiza riscurilor de securitate |

SECTIO AUREA

# Controlul conformitatii NIS. Indicatori de conformare si performanta

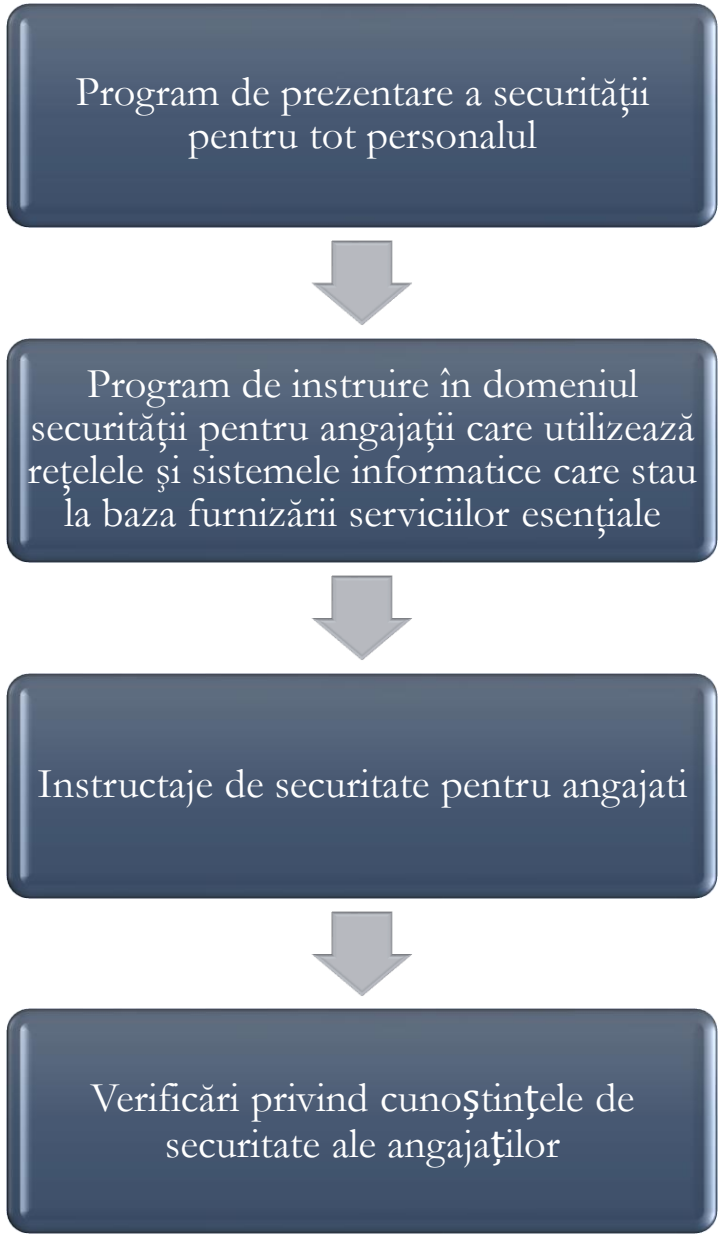



- Identificarea cauzelor si stabilirea actiunilor corective
- Verificarea realizarii actiunilor corective.
- Implementarea acțiunilor corective
- Descrierea activitatii de audit intern.
- Planificarea auditurilor externe NIS.

| | |
|---|---|
| IEC | Indicatori de evaluare |
| MEIEC | Metoda de evaluare a indicatorilor de conformitate |
| PRECAS | Procedură privind evaluarea conformităţii NIS şi efectuarea auditului de securitate a reţelelor şi sistemelor informatice |

SECTIO AUREA

# Asigurarea securității personalului

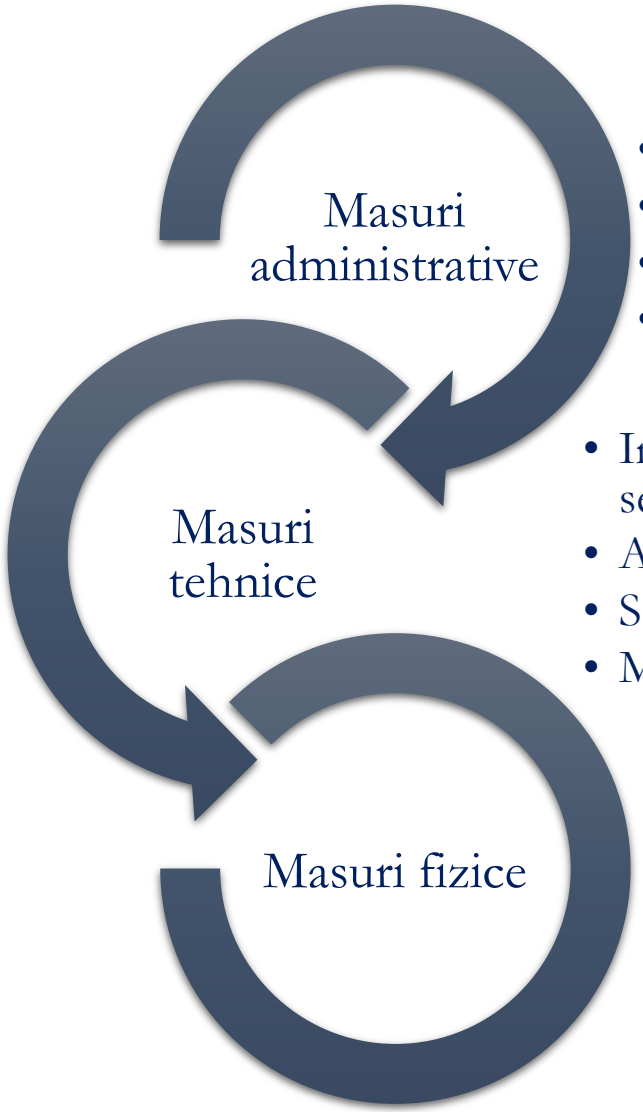


SECTIΦ AUREA

# Care sunt etapele de conformare?

## #2. Protectia serviciilor esentiale.

Rezulta din analiza de risc si din aplicarea de standarde de securitate




- Documentare planuri
- Definirea de proceduri, responsabili, registre
- Programe de training de securitate angajati
- Actualizare continua

- Implementare / configurare sisteme/ solutii securitate
- Administrare, Control access, Mentenanta
- Segregare retele, filtrare
- Mentenanta / actualizare

- Protejarea sistemelor si echipamentelor dpdv fizic
- Control acces fizic

**Indicatori de control principali conform Ordin 1323 din 26 noiembrie 2020**

- Proceduri
- Documente de stare
- Tehnologii

SECTIO AUREA

# Care sunt pasii de conformare? Implementare masuri adecvate.

## Politici / Proceduri

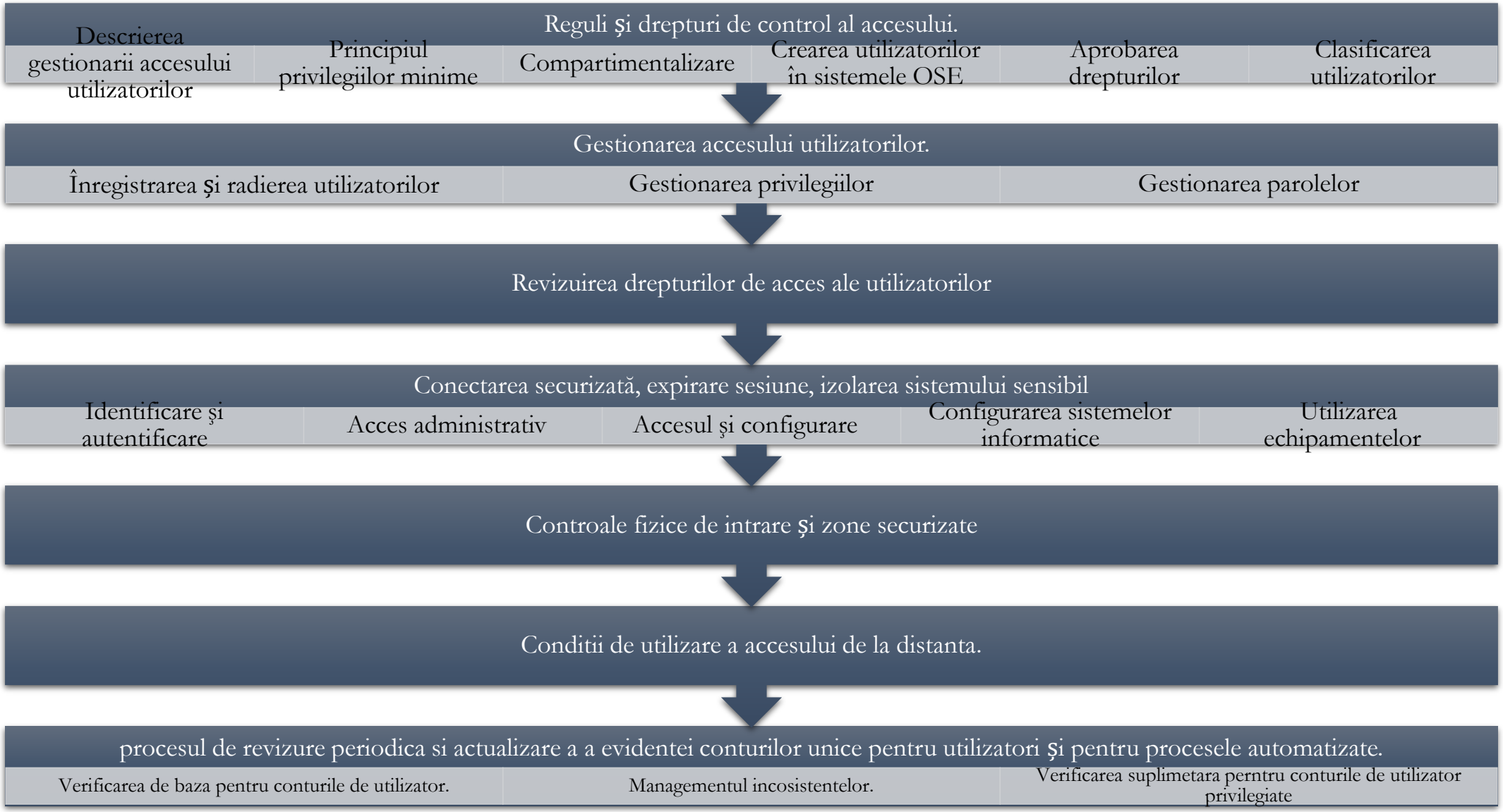
- Proiectarea si actualizarea arhitecturii de reţea si de sistem
- Instalarea si configurarea echipamentelor si sistemelor, interconectarea acestora in condiţii de siguranţa prin segregarea reţelelor, hardening
- Managementul identităţii, autentificării si autorizării
- Controlul accesului administrativ
- Mentenanţa evolutiva si managementul versiunilor
- Controlul accesului fizic la echipamente
- Business continuity planning si Disaster recovery
- Monitorizarea de Securitate si managementul vulnerabilitatilor

## Implementarea de tehnologii (obligatorii)

- Security Information and Event Management(SIEM)
- Managementul Vulnerabilitatilor
- IDS
  - Network Detection and Response (NDR) IT
  - Network Detection and Response (NDR) OT
- TFA
- **Implementarea de tehnologii (ajutatoare)**
  - Asset management (organizarea asseturilor)
  - Service management (implementarea procedurilor)
  - PAM / izolarea si monitorizarea sesiunilor privilegiate
  - Firewall IT / OT
  - Secrets Management

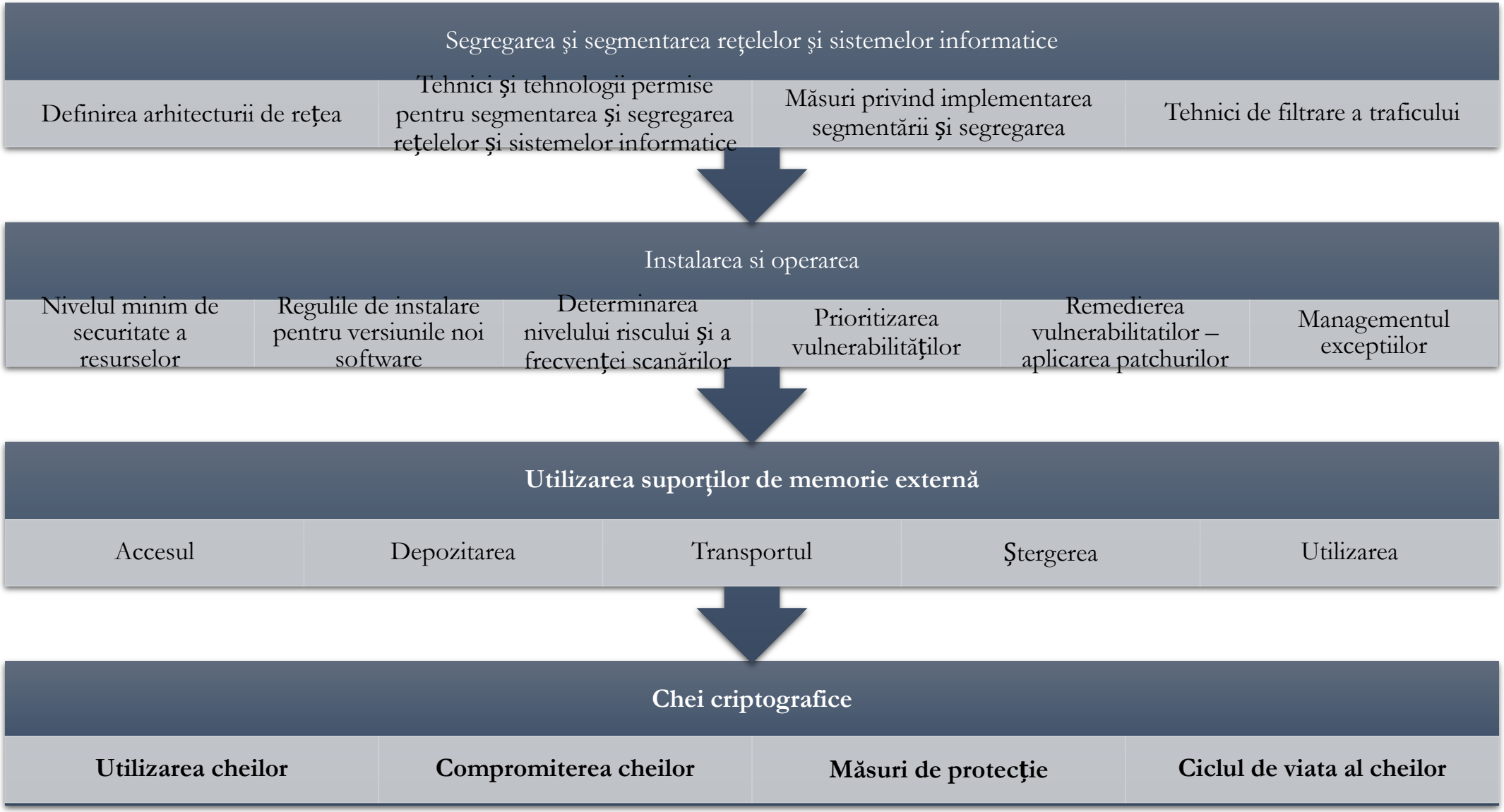
SECTIO AUREA

# Accesul şi securitatea resurselor şi informaţiilor
# Lucrul la distanţă
# Revizuirea acceselor



SECTIO AUREA

# Managementul sistemelor

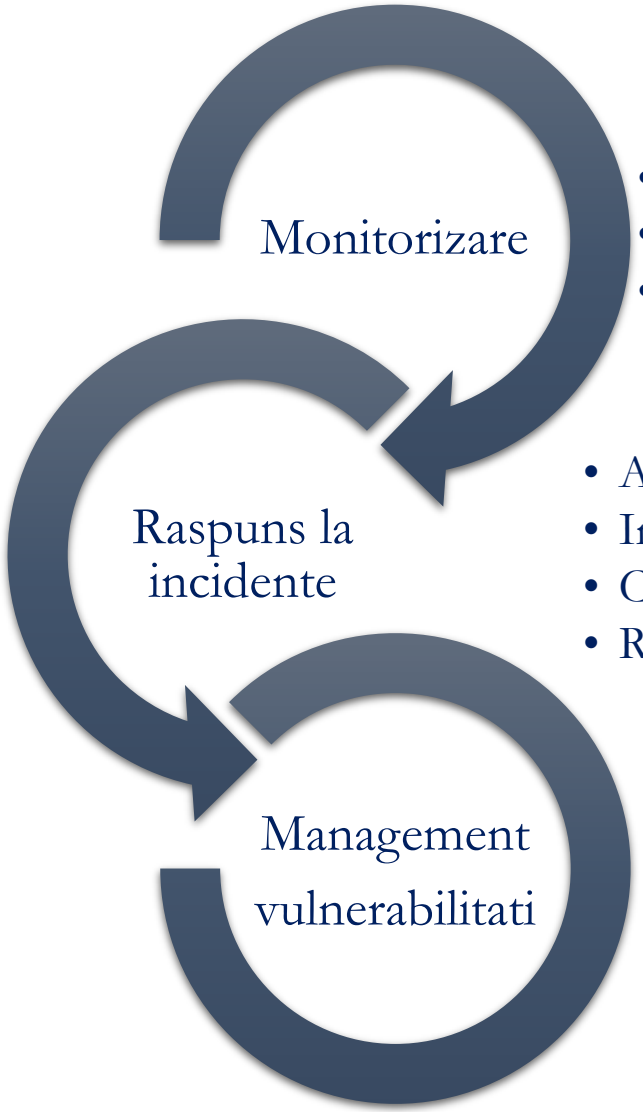


SECTIΦ AUREA

# Care sunt etapele de conformare?

## #3. Monitorizarea si raspunsul la incidente.

Este esentiala pentru demonstrarea respectarii legii




- Sisteme de monitorizare a evenimentelor
- Responsabilitati si organizare specifice unui CERT
- Raportari specifice

- Analizarea evenimentelor
- Investigarea incidentelor
- Comunicare si cooperare
- Raportare

- Tehnologii de scanare
- Informare
- Testare
- Remediere
- Raportare

**Indicatori de control principali conform Ordin 1323 din 26 noiembrie 2020**

| Proceduri | | |
|---|---|---|
| Identificare | Escaladare | Raportare |
| Oameni | | |
| Tehnologii | | |

SECTIO AUREA

# Care sunt pasii de conformare?
# #3. Monitorizare nivel de Securitate

Implementarea interna sau externalizare

## Nivel 1: DETECTIE

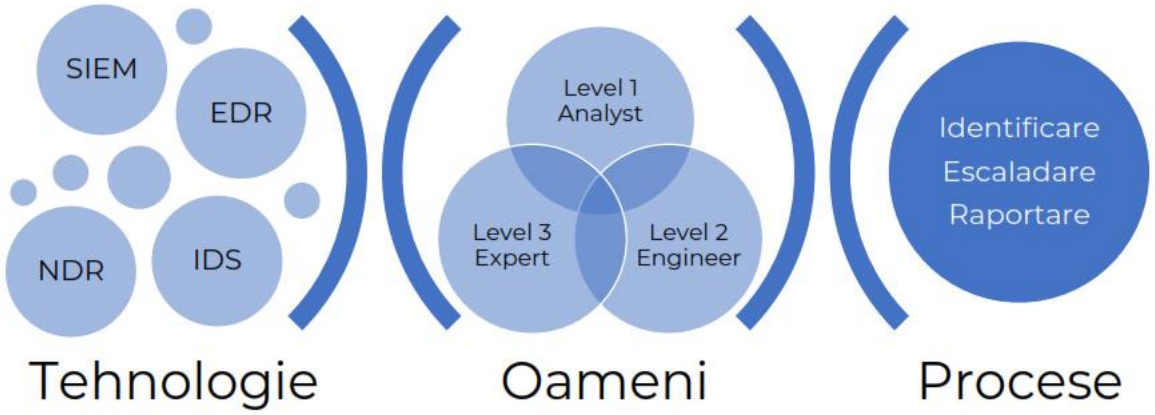
- Monitorizare si analiza evenimente de securitate
- Detectie incidente de securitate
- Management vulnerabilitati

## Nivel 2: RASPUNS

- Analiza si investigare incidente de securitate
- Raspuns si actiuni corective

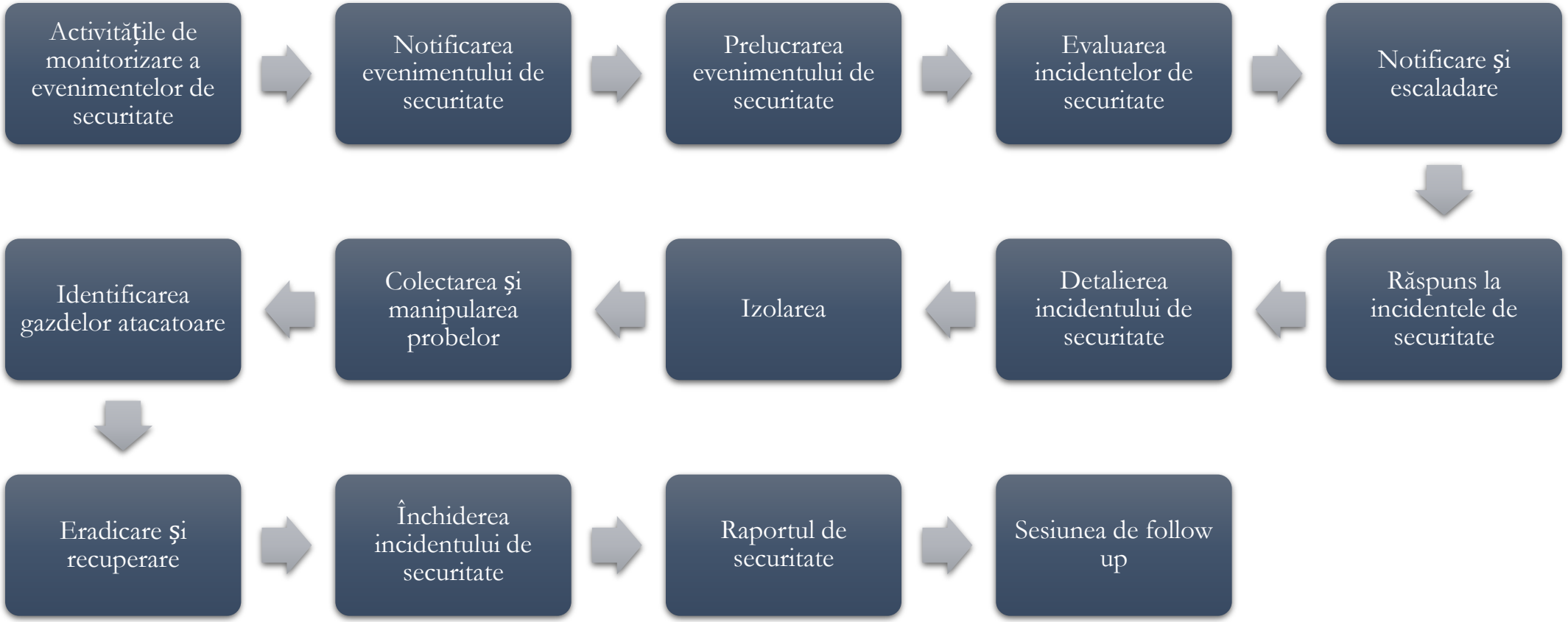
## Nivel 3: AVANSAT

- Security Forensics
- Threat-hunting



SECTIO AUREA

# Gestionarea, răspunsul şi analiza incidentelor



SECTIO AUREA

# Care sunt etapele de conformare?

## #4. Rezilienta.


- Plan de continuitate
- Plan de recuperare in caz de dezastru
- Testare si actualizare

- Analiza evenimente
- Escaladarea incidentelor
- Gestionarea situatiilor de criza
- Testari de Disaster Recovery, exercitii si simulari
- Comunicare si cooperare
- Raportare

Indicatori de control principali conform
Ordin 1323 din 26 noiembrie 2020

Proceduri

Documente de stare

Tehnologii


Recomandari
Lectii invatate

SECTIΦ AUREA

# Recomandari - Recap

## Obtineti sprijinul Managementului.

- Fara acest lucru orice initiativa va fi sortita eseculi.

## Alegeti un standard / cadru aplicabil

- din Decizia nr. 88/2020 a CERT: ISO/IEC 27001:2013 , NIST CSF

## Porniti de la lucrurile simple

- Enumerati procesele de afaceri, serviciile esentiale, componentele IT de care depind acestea
- Definiti Criticitarea procesului si indicatori esentiali
- Faceti un inventar complet al asseturilor
- Alocati responsabili / custodians si mapati pe procesele de business.
- Care sunt cele mai critice asseturi.
- Documentati configuratiile existente si parametrizarile, situatia garantiei, EOL, EOS, SLAurile furnizorilor de servicii
- Documentati minimal procedurile de baza de lucru asupra ITului (ce se face adhoc de obicei), de la achizitie, operare, securizare, decomisionare, backup samd.

## Continuati cu analiza riscurilor de Securitate

- Mapati toate amenintarile de Securitate
  - Identificati vulnerabilitatile reale de Securitate la care sunt expuse asseturile
  - Calculati impactul si probabilitatea ca o vulnerabilitate sa fie exploatata
  - Prioritizati cele mai importante riscuri, definiti metodele de tratament ale acestora cu managementul.

## Definiti si agreati cu managementul un roadmap

SECTIO AUREA

# Care sunt cele mai dese greseli si cum le poti evita?

- Lipsa suportul de management duce la esec
- Cand construiti livrabile incercati sa simplificati
  - Exemple gresite
    - Liste de inventar neclare, incomplete, necorelate cu scheme de arhiectura
    - Neprioritizarea proceselor, asseturilor duce la lipsa de focus.
    - Proceduri complicate si nealiniate la cultura organizatiei. Ele trebuie sa se muleze pe organizatie si nu viceversa
- Lipsa de digitalizare
  - NIS creaza incarcarea oamenilor cu sarcini si activitati suplimentare
  - Folositi unelte software care digitalizeaza activitatile si le automatizarea
    - CMDB
    - Service desk
  - NIS schimba major si creaza o modalitate mai organizata de coordonare a activiattilor zilnice in IT. Nu lasati hartiile asa cum sunt, caci si picati audit, dar nu creati structura in companie.

# SECTIΦ AUREA Ce optiuni tehnice interesante avem

- SIEM
  - Wazuh
- IDS:
  - Snort, ntopng, PFSense, OpenSense
- Vulnerability Management
  - OpenVas
- CMDB, managementul activitatilor
  - GPLI
- Managementul identitati, secretelor: HashiCorp Vault

# Resurse utile

Guidelines on assessing DSP and OES compliance to the NISD security requirements Information Security Audit and Self – Assessment/ Management Frameworks

https://www.enisa.europa.eu/publications/guidelines-on-assessing-dsp-security-and-oes-compliance-with-the-nisd-security-requirements

NIS Cooperation Group

https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group

https://dnsc.ro/

https://www.nist.gov/cyberframework

https://csrc.nist.gov/Projects/risk-management

SECTIΦ
AUREA

SECTIΦ
AUREA


Madalin Bratu

+4 0722 154 062

madalin.bratu@phi.ro

www.phi.ro