SECTIO AUREA®

Webinar: "Directiva NIS si NIS 2 - Abordări Practice"

Vineri, 22 Martie 2024, ora 10. - 12:30

Mădălin Bratu
Director General
Sectio Aurea

Virgil Pascu
Director IT&OT,
RAJA S.A.

Ilie Voinea
CISM,
Auditor Atestat NIS

Ovidiu Cucos
Information Security Officer,
Vienna Insurance Group
Management Service SRL

Agenda

Mădălin Bratu - "Managementul securitatii. Cum sa simplifici ceva ce pare complicat?".

Ilie Voinea - "Directiva NIS 2: Noutăți și impactul asupra operatorilor de servicii esențiale"

Panel Deschis cu Mădălin Bratu și Virgil Pascu - "Decizii strategice de management: Tehnologii, Procese, Oameni, Digitalizare".

Demo - "Digitalizarea implementării cerințelor NIS:
Studiu de caz pentru managementul vulnerabilitatilor prin tehnologiile de la Qualys

Vom incepe la 10:10
Ca sa intre toata audienta.

SECTIO AUREA®

Managementul securitatii.

Cum sa simplifici ceva ce pare complicat?

Madalin Bratu CISM

Director General, Sectio Aurea

+4 0722 154 062

madalin.bratu@phi.ro

www.phi.ro

Webminar
Directiva NIS si NIS 2- Abordări Practice
22 Martie 2024

SECTIO AUREA®

Agenda

Introducere – Sa ne cunoastem

Conditiile primare ale simplificarii managementului securitatii

Simplificarea prin metoda - Usecases pe Directiva NIS

Simplificarea prin digitalizare

SECTIO AUREA®

Sa ne cunoastem

Am petrecut un deceniu lucrând la IBM, unde am contribuit la unele dintre cele mai sofisticate proiecte de servicii din Europa Centrală și de Est.

Am jucat un rol cheie ca Manager Global de Portofoliu pentru Servicii de Securitate Cibernetică la Atos - Eviden, una dintre multinaţionalele de frunte în domeniul securităţii cibernetice, gestionând proiecte globale de securitate cibernetică în domenii precum managementul identităţii și securitatea cloud.

Experiența mea include, de asemenea, contribuţii valoroase la companii locale, cum ar fi Safetech Innovations, una dintre cele mai dinamice firme românești de securitate cibernetică.

Prin Sectio Aurea, ofer servicii unice, flexibile și relevante. Modelul de afaceri, rafinat pe parcursul a aproape 5 ani, se bazează pe un concept inovator - acela al microserviciilor. Sunt însoţit de o echipă atent selecţionată de experţi și voci autoritare în domeniul securităţii cibernetice (CISOs, DPOs, CIOs, arhitecţi), cu care am construit o relație profesională sănătoasă pe parcursul unor proiecte de success.

Auditor Atestat NIS, CISM.

Am servit multi clienti ca si consultant in implementarea Directivei NIS din diverse domenii (companii de apa, bancar, utilitati)

Am participat ca si auditor atestat NIS, la diverse misiuni de audit in medii complexe sau dificile de analizat.

Majoritarea clientilor ma recomanda de la nivel de director general pana la Manageri IT, Manageri de securitate, manageri tehnici.

https://www.phi.ro/testimonials

SECTIΦ 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 General Directiva NIS
seria CLE nr. 8020 din 23.03.2022

ISO 9001 | ISO/IEC 27001 | CERTIFICĂM PERFORMANȚA ISO 14001 SISTEMA CERTIFICARI | IAS ACCREDITED Management Systems Certification Body MSCB-173

Cyber Security Cluster of Excellence


CISO &
DPO
Consultanta Implementare ISMS, Directiva NIS, GDPR
Audit GDPR
Implementare tehnologii Cybersecurity
Audit EBA Guidelines 04/2019, BNR REGIS/SAFIR, CSP SWIFT 2023
Securizare Cloud: Azure, AWS, GCP
Threat Hunting
Audit Directiva NIS, DORA
Security Forensics
Audit Securitate Cloud
SECTIO AUREA®
Monitorizare si raspuns la incidente de Securitate
Red Teaming
Dezvoltare si optimizare SOC
Testare de securitate
Training echipe de SOC
Audit de Securitate
Constientizare Securitate
Campanii de phising

Parteneri tehnologici si solutii disponibile

- SIEM SOAR Threat Intelligence
- XDR, Network Detection and Response, Endpoint Detection and response
- Vulnerability Management
- OT Security
- Deception Technology
- External Attack Surface Management
- Advanced Threat Protection
- Email security, API Security
- Cloud Workload Protection, Cloud-Native Application Protection Platform
- Identity Governance and Administration, Privileged Access Management

SECTIO AUREA®

Conditii de simplificare a managementului securitatii

- Suportul de la Management
- Integrare naturala cu procesele afacerii
- Adaptare la nivelul de maturitate al afacerii
- Digitalizare si automatizare proceselor
- Implementarea ca un process continuu si viu in organizatie
- Cooptarea oamenilor

SECTIO AUREA®

Metode de simplificare

- **Prin abordare**
  - **Abordare top – down**
  - **Analizati intai ce aveti inainte de a incepe ceva**: Servicii esentiale, Procese, Departamente, Stakeholderi, sisteme (aplicatii, arhitecturi, liste de inventar detaliate), Cricitate, Asteptari de business (raportare, disponibilitate, recuperare).
  - **Simplificati procesele si activitatile noi** solicitate de Directiva NIS
- **Prin digitalizare**
  - **Digitalizati** procesele existente / suplimentare

SECTIO AUREA®

Simplificarea prin abordare

SECTIO AUREA®

Guvernanta securitatii

SECTIO AUREA®

Elementele de baza

- Definirea unui politici de securitate
- Alegerea unui singur responsabil NIS
- Definirea canalelor de raportare și feedback
- Stabilirea procesului de acreditare si de audit intern sau autoevaluare
- Definirea indicatorilor de perfomanta a securitatii si de evaluare a conformarii
- Evaluarea conformității cu politica de securitate si cu prevederile legii NIS
- **Identificati de aveti intai.**

SECTIO AUREA®

Inventariati Informația

- **Inventarierea informațiilor:** Primul pas este să se efectueze un inventar al tuturor informațiilor din organizație. Acest lucru ar trebui să includă toate tipurile de informații, indiferent de formatul lor (digital sau analog), și ar trebui să acopere toate domeniile și departamentele organizației.

- **Alocarea nivelului de secretizare:** După ce a fost efectuat inventarul, fiecărei informații i se va aloca un nivel de secretizare conform procedurii de clasificare a informației. Acest nivel va determina măsurile de protecție care trebuie aplicate informației respective.

- **Implementarea măsurilor tehnice și organizatorice pentru etichetare si flux informatii:** Următorul pas este implementarea măsurilor necesare pentru a aplica etichetele de clasificare la fiecare informație. Aceasta poate include utilizarea unor sisteme de gestionare a informațiilor care permit etichetarea automată a informațiilor în funcție de criteriile stabilite.

- **Protecția suportului informațional:** implementati măsuri de securitate adecvate pentru a proteja suporturile informaționale împotriva divulgării neautorizate. Acestea pot include criptarea datelor, controlul accesului și alte măsuri de securitate fizică și cibernetică. DLP.

- Faceti o situație centralizata a tipurilor de informații pe nivelele de secretizare.

SECTIΦ AUREA®

Inventariati procese, departamente, asseturi IT, OT BIA - Business Impact Analysis).

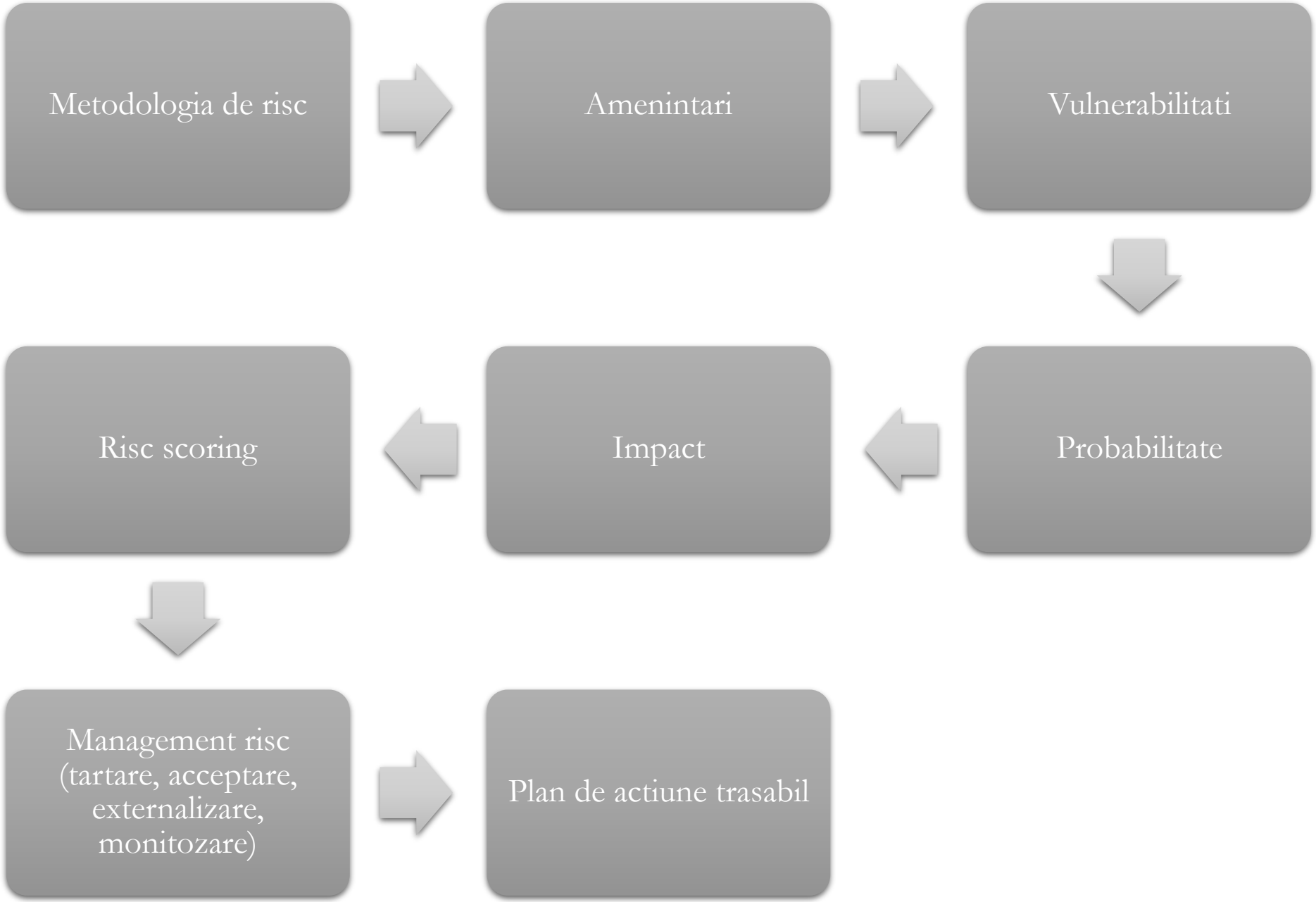
- **Identificarea funcțiilor critice de afaceri**
- **Evaluarea impactului:** După identificarea funcțiilor critice, următorul pas este evaluarea impactului potențial al unei întreruperi. Acest lucru implică evaluarea costurilor directe și indirecte asociate cu întreruperea acestor funcții.
- **Identificarea dependențelor:** Dependențele dintre diverse procese și funcții de afaceri trebuie identificate pentru a înțelege cum o întrerupere poate afecta alte procese.
- **Stabilirea priorităților de recuperare:** Odată ce funcțiile critice, impactul și dependențele au fost identificate, următorul pas este stabilirea priorităților de recuperare.
- Procesele operationale si alocarea de nivele de criticitate, a cerintelor tinta pentru RTO si RPO
- Departamentelor care sustin direct serviciile esentiale in contextul Legii NIS, dar si a departamentelor suport, fara de care furnizarea serviciului esential depind direct.
- Sistemelor si aplicatiilor care sustin procesele de afacere
- Alocati cerintelor de RTO si RPO asupra elementeloe de infrastuctura si aplicatii si definirea nivelelor de criticitate.
- Identificati sistemele care sustin accesul si disponibilitatea sistemelor critice, sau al caror securitate si disponibilitate impacteaza sistemic procesele de business

Primii pasi pana la analiza de risc

Servicii esențiale	Servicii suport ale serviciului essential	Sisteme informatice (IT & Scada)	Arhitecturi	Furnizori esentiali	Informatii
care sunt acestea	Cine le furnizeaza si cum	Lista granulara si structurata	Simple	Ce fac ei	Care sunt informatiile
Cine le furnizeaza si cum	Ce asteptari are managementul de la ele (disponibilitate)	Nivele de criticitate	Usor de corelat cu liste de inventar	Ce acceseaza	Unde sunt folosite (process de business)
Ce asteptari are managementul de la ele (disponibilitate)	Pe ce sisteme se bazeaza acestea	Identificare clara a denumirii standard producator, nivel configuratie, garantie, EOS, EOL)	Usor de inteles	De ce o fac	Cine sunt proprietarii
Pe ce sisteme se bazeaza acestea				Am control asupra lor	Din ce department vin ei
				Cum le aprob accesele si cum le decomisionez	Ce process de afacere suporta informatia
					Cat de critic este procesul / activitatea este el pentru Serviciul essential si afacere
					Nivele de confidentialitate
					Metode de tratament al ormatiei pe ciclul de viata al acesteia

SECTIO AUREA®

Analiza de risc



SECTIO AUREA®

Managementul riscurilor furnizorilor de servicii

- **Definiti un flux de lucru** in ceea ce priveste managementul schimbarilor in organizatie, mai ales cele care implica terte parti: de la studiul de fezabilitate, contractare, kick off, acceptanta si executia mentenantei.
- **Analizati contractele cu furnizorii terți**: Examinati fiecare contract în parte pentru a înțelege clar serviciile oferite, nivelurile de serviciu convenite, obligațiile de securitate cibernetică ale furnizorilor și posibilele sancțiuni pentru nerespectarea obligațiilor contractuale.
- **Evaluati responsabilităților tehnice ale furnizorilor**: Aceasta include o revizuire a obligațiilor tehnice ale furnizorilor, verificarea competențelor lor tehnice, evaluarea mecanismelor de securitate pe care le au în vigoare și înțelegerea modului în care acestea contribuie la securitatea generală a organizației.
- **Faceti un raport de riscuri asociate cu furnizorii externi**: care identifică și evaluează riscurile asociate cu fiecare furnizor terț. Acesta va include o listă a riscurilor potențiale identificate și o evaluare a impactului și a probabilității acestora în furnizarea serviciilor esențiale.

SECTIO AUREA®

Protectia, Detectia

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

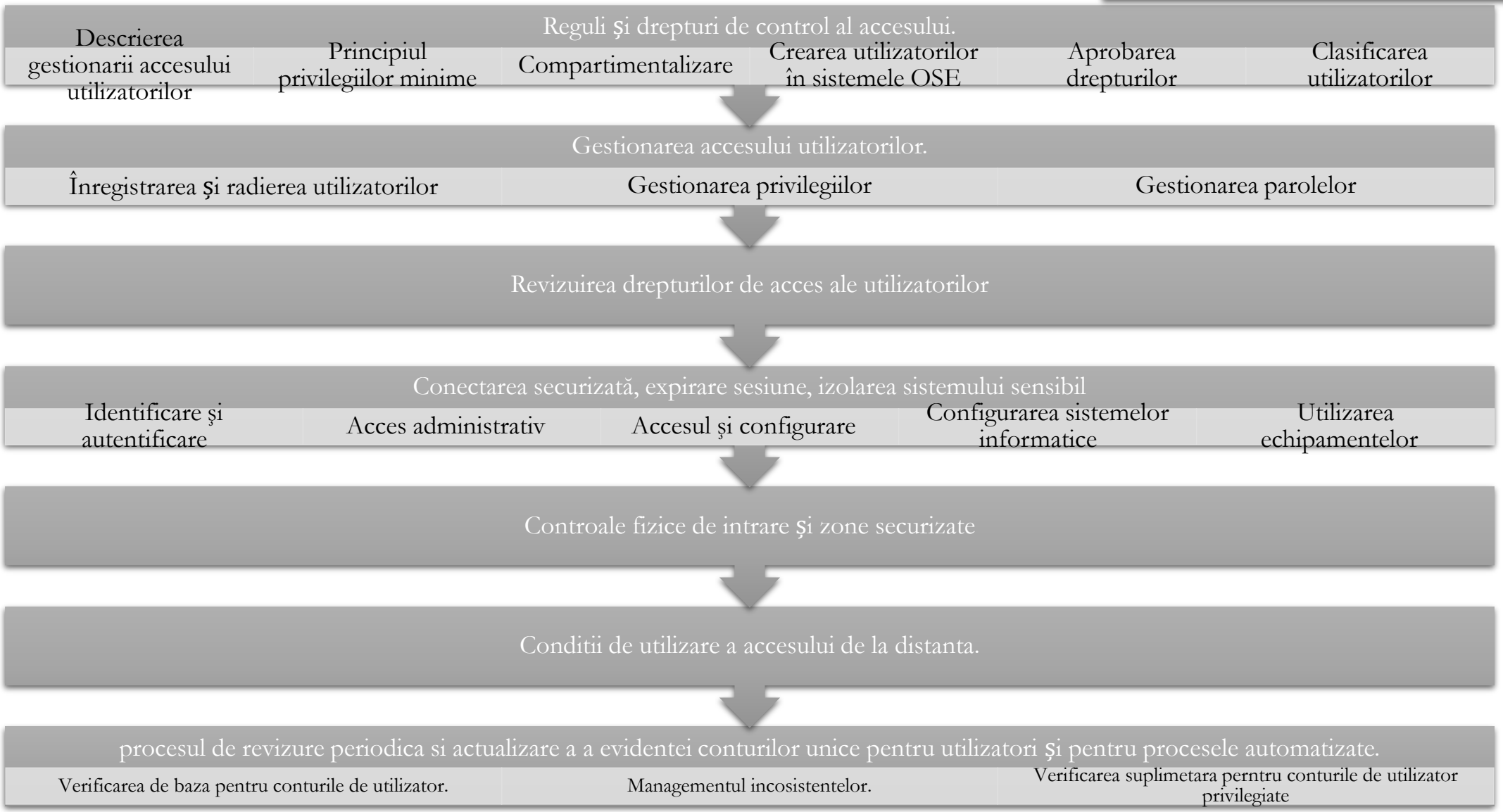
Implementarea de tehnologii (obligatorii)

- Security Information and Event Management(SIEM)
- Managementul Vulnerabilitatilor
- IDS
  - Network Detection and Response (NDR) IT
  - Network Detection and Response (NDR) OT
- TFA
- SIEM
- Sistem de gestionare a activitatilor
- **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®

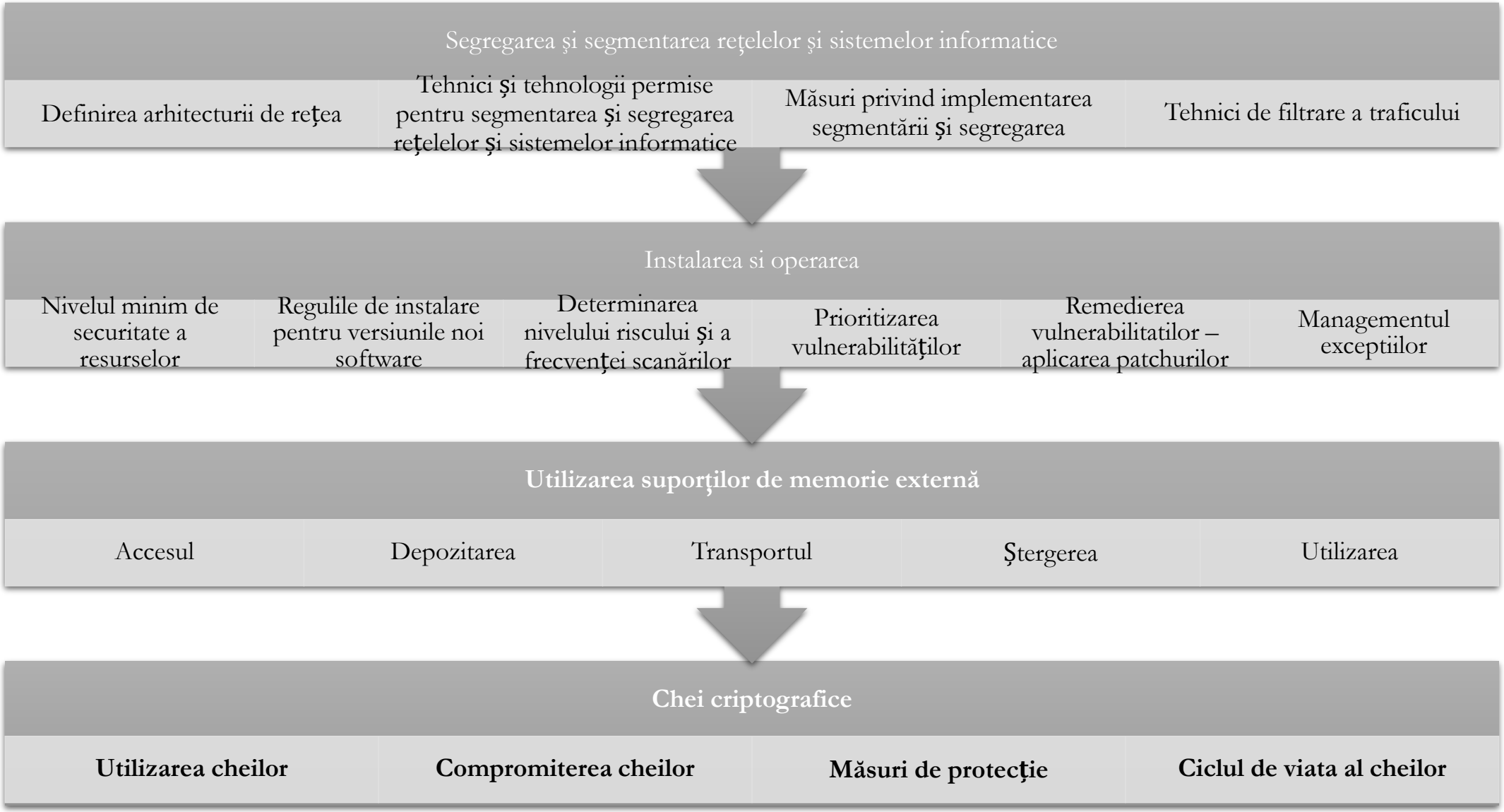
Managementul identitatii si al accesului.

Inventariati **toate** identităţile si accesele lor în **toate** sistemele informatice



SECTIO AUREA®

Managementul sistemelor

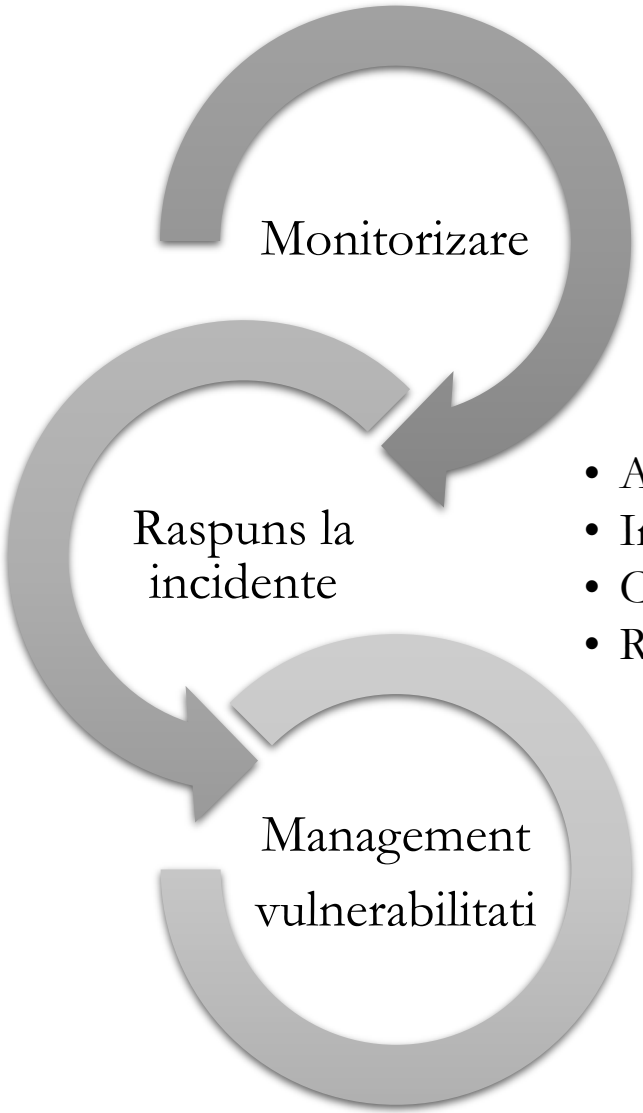


SECTIO AUREA®

Managementul vulnerabilitatilor

- Definiti fluxurile operationale pentru scanarea și detectarea vulnerabilităților dar mai ales
  - Analiza de risc aliniata la cerintele legii
  - Tratarea vulnerabilitatilor
  - Managementul exceptiilor
- Implementati solutii de management al vulnerabilitatilor, nu scanare a lor.
- Implementati solutii specifice pentru mediul OT

Managementul Detectiei



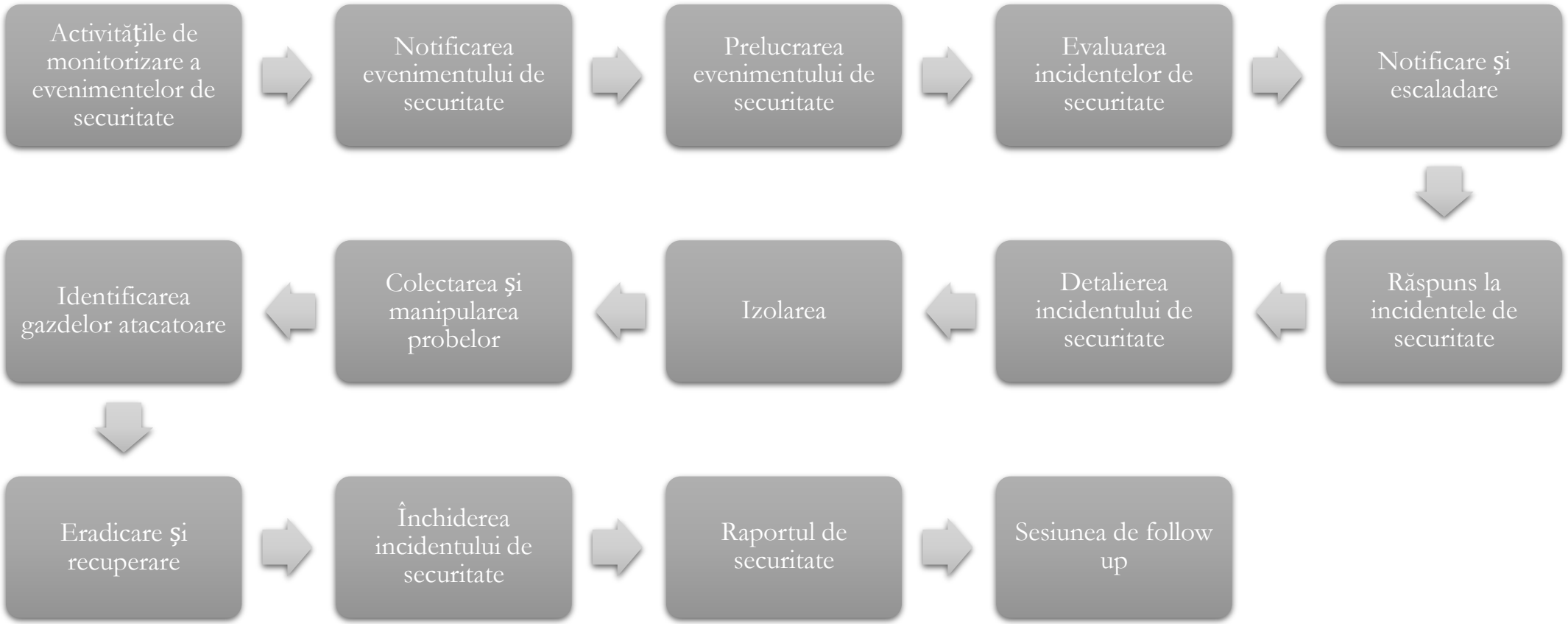
- Sisteme de monitorizare a evenimentelor
- Responsabilitati si organizare specifice unui CERT
- Raportari specifice

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

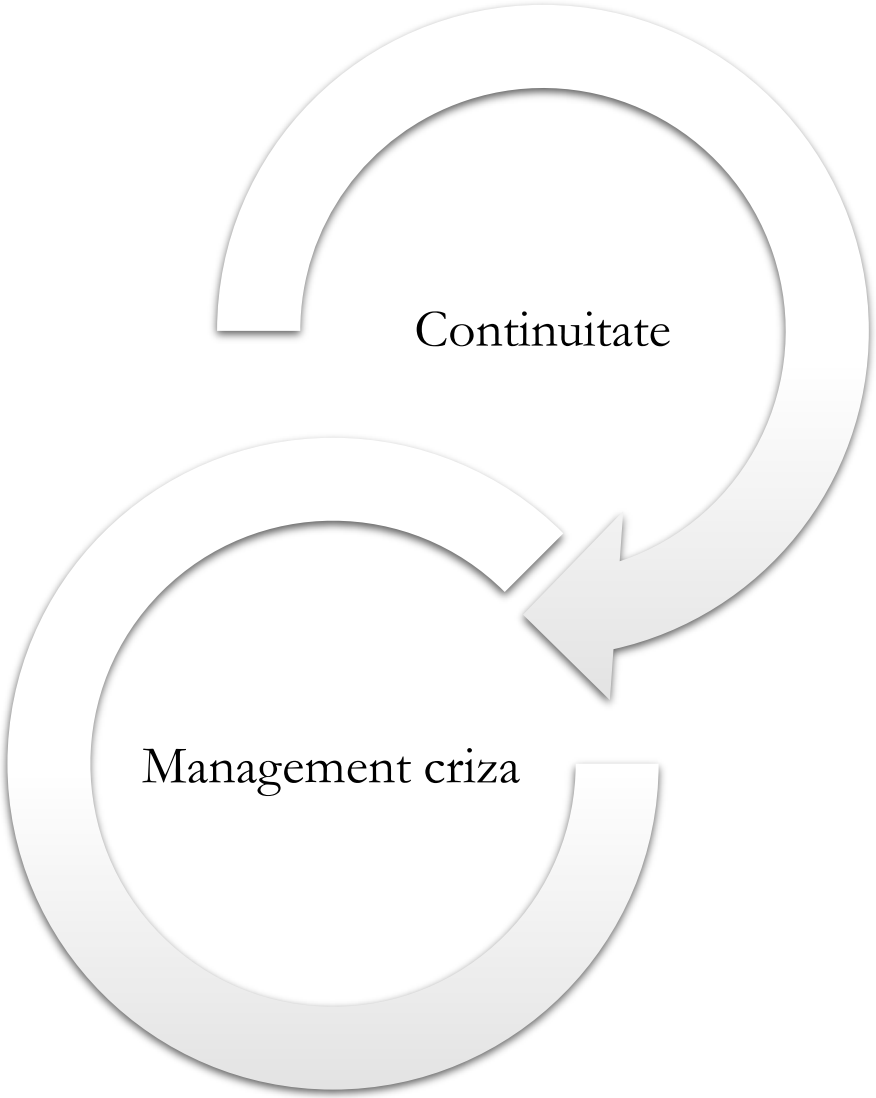
- Tehnologii de scanare
- Informare
- Testare
- Remediere
- Raportare

SECTIO AUREA®

Gestionarea, răspunsul şi analiza incidentelor



Managementul Continuitatii



- 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

SECTIO AUREA®

Simplificarea prin digitalizare

SECTIO AUREA®

Educarea de Securitate - acum

Sesiuni fizice de training

- Sunt greu de organizat
- Impacteaza direct productivitatea angajatilor
- Nu pot fi personalizate

Verificarea cunostintelor pe metode fizice

- Chestionare de intrebari usor de copiat
- Facuta pe hartie, greu de gestionat
- Centralizare si raportare greoaie

Emailuri de security awareness

- Nu se stie daca sunt citite si intelese

SECTIO AUREA®

Educarea de Securitate – To be

Training de Securitate online

- Învăţare Adaptivă: Motorul de alocare a conţinutului dinamic oferă instruire individualizată.
- Automatizare: Instruirea potrivită livrată automat persoanei potrivite la momentul potrivit.
- Personalizare in functie de audienta

Testari de phising inteligente

- Identifică motivul din spatele fiecărui click şi tipul de atacuri la care utilizatorii sunt vulnerabili.
- Instruire ţintită instant pentru utilizatorii compromişi.
- Şabloane de simulare a phishing-ului personalizate şi localizate în limbile preferate ale utilizatorilor.
- Învățare în Timp Real: Pagina de aterizare interactivă dezvăluie indiciile pe care utilizatorul le-a ratat și cum să se îmbunătățească.

Raportare Îmbunătăţită

- Vizibilitate instantă asupra vulnerabilităţii forţei de muncă în faţa atacurilor cibernetice.
- Identifică modele de risc uman în întreaga forţă de muncă.
- Evidenţiază persoanele cu risc înalt şi utilizează acţiunile recomandate de îmbunătăţire pentru a-i ghida şi sprijini mai bine.
- Vizualizează relaţiile de muncă şi de încredere, foloseşte această inteligenţă pentru a te apăra împotriva atacurilor umane laterale.

SECTIΦ AUREA®

Inventarul de IT si OT - ACUM

Liste facute in Microsoft Excel

- Greu de analizat
- De obicei nu sunt actualizate
- Incomplete
- Greu de inteles

Arhitecturi de retea

- Neactualizate
- Incomplete

Inventarul de IT si OT – Digitalizat

CMDB

Gestionează inventarul de hardware, software și centre de date.

Implementeaza in mod detaliata liste de inventar specifice mediului IT si ICS scada, care sunt solicita de catre auditori ca si prima evidenta de audit.

O solutie de managementul vulnerabilitatilor

Scaneaza dinamic toata infrastuctura IT si OT si detecteaza orice schimbare

Identifica versiuni,

Identifica situatii de EOS,

Identifica versiuni ale produselor Software

Identifica configuratii

Procese suplimentare cerute de NIS (selectie, approx. 50 activitati disticte)

- Solicitarile specifice de management incidentelor IT
- Managementul cererilor de access,
- Obtinerea, modificarea, retragerea unui access la un sistem informatic
- Modificarea unui access
- Certificarea unui access
- Revizuirea drepturilor de acces ale utilizatorilor care au acces privilegiat si a conturilor de access normale
- Verificarea cerintelor de securizare minima a infrastucturii critice (security hardening, baselining)
- Activitatile specifice pentru securitatea fizica
- Fluxul alertelor de securitate,
- Activitățile de monitorizare a evenimentelor de securitate,
- Evaluarea, Urmarirea incidentelor de securitate,
- Răspuns la incidentele de securitate,
- Identificare, clasificare, remediere și eliminare a vulnerabilităților, Prioritizarea vulnerabilităților

SECTIΦ AUREA®

Procese suplimentare cerute de NIS – ce se intampla acum

- Impact uman.
  - Departamentele IT sau OT sunt de obicei subdimensionate, sunt depasite daca se respecta procesul (lucrul in XLS, lucrul cu hartii)
- Impact de Securitate si conformare
  - Lipsa de vizibilitate
  - Lipsa de consistenta a implementarii
  - Lipsa de implementare efectiva (boala hartiei neimplementate)
- Impact de productivitate.
  - Resurse umane pretioase sunt allocate pentru sarcini sub capacitatea sau pregatirea lor

SECTIO AUREA®

Procese suplimentare cerute de NIS – digitalizate

- Service desk
  - Digitalizeaza toate procesele anterioare
  - Stabiliste SLAuri
  - Centralizeaza si asigura trasabilitatea unei activitati
- Managementul vulnerabilitatilor
  - Descopera devierile de la security baselines
  - Descopera certificatele digitale
  - Operationalizeaza si digitalizeaza taskurile de aplicare de patch – actualizari
- SIEM de ultima generatie
  - Asigura platforma pentru tratarea incidentelor de Securitate
- SOAR
  - Automatizeaza actiunile repetitive pentru identificarea incidentelor de securitate
- IGA (identity, governance and Administration)
  - Automatizeaza cererile de access,
  - Efectuează recenzii periodice ale accesului utilizatorilor,
  - Detectează și remediază proactiv încălcările segregării sarcinilor (SoD),
  - Gestionează onboarding-ul, durata contractului și offboarding-ul contractorilor,
  - Autentificare unică (SSO) sau multipla pentru aplicațiile on-premises și SaaS

SECTIO AUREA®

Madalin Bratu CISM

Director General

+4 0722 154 062

madalin.bratu@phi.ro

www.phi.ro

SECTIO AUREA®

Introducere Directiva Europeana NIS si Legea 362/2018

12 ianuarie 2019

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

Scop

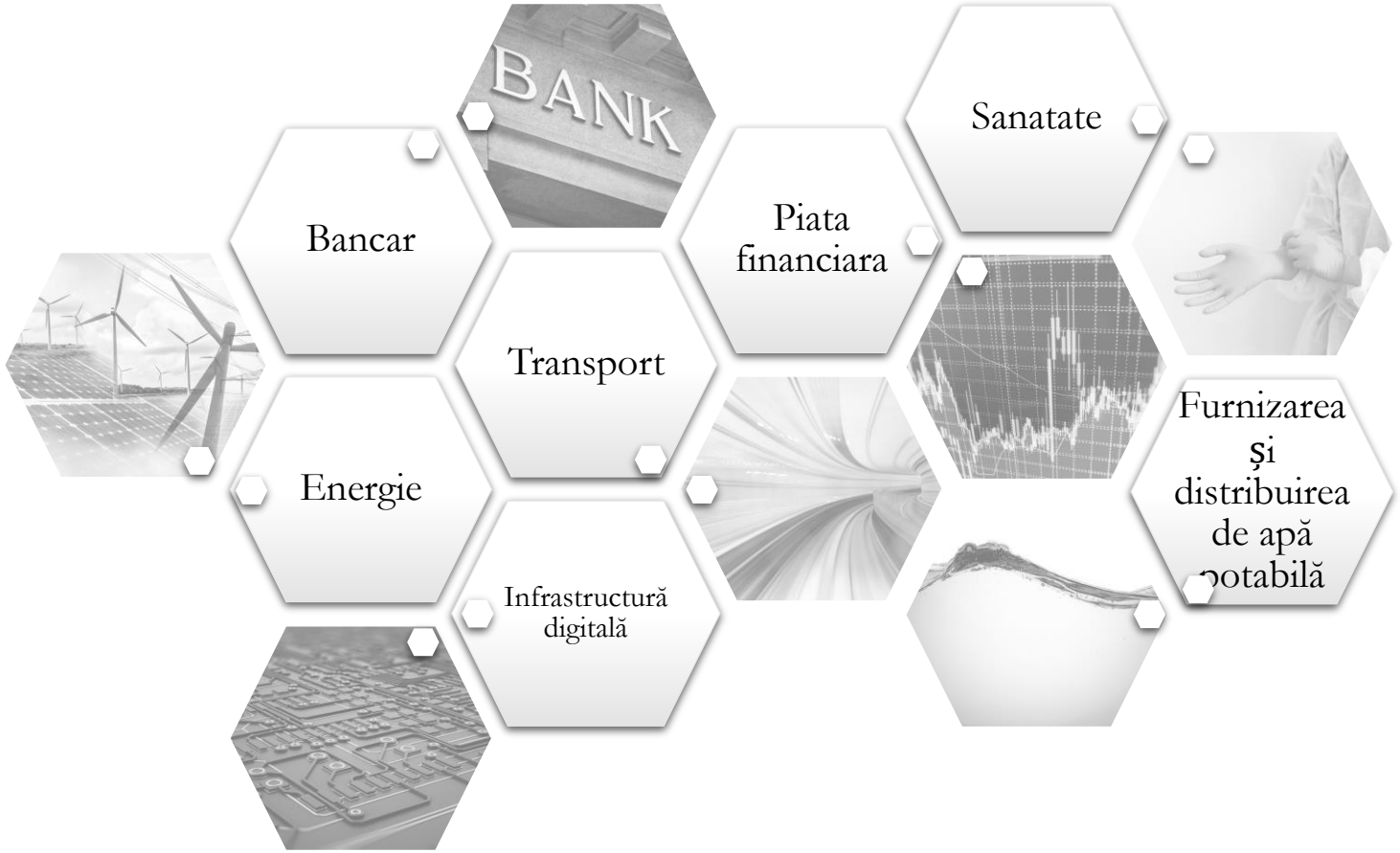
Atingerea un standard comun ridicat pentru securitatea reţelelor şi informaţiilor în toate statele membre ale Uniunii care oferă servicii esenţiale pentru societate.

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

Vi se adreseaza Directiva NIS?

Da

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



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

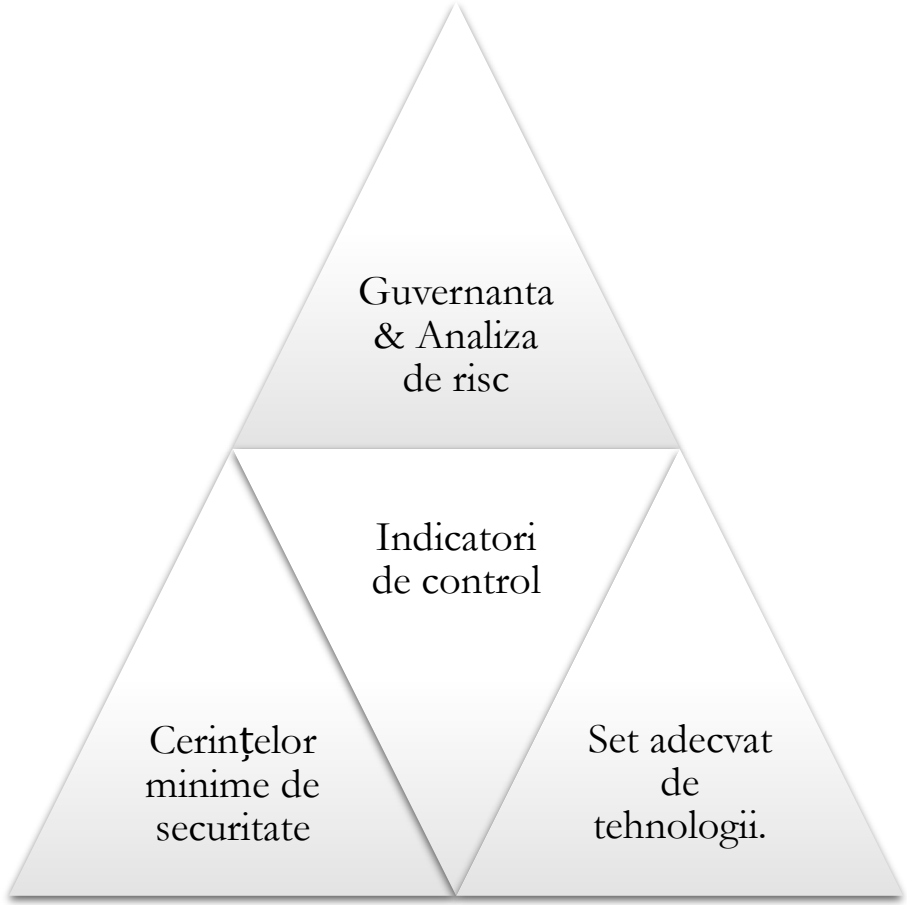
- Implementeaza cerintele directive in Romania

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?

Guvernanță

- Managementul riscurilor
- Politici de securitate la nivelul organizațional
  - Elaborare corecta
  - Implementare reala

Protecție

- Securitatea rețelelor și sistemelor informatice
- Administrarea și mentinerea resurselor
- Controlul accesul la rețelele și sistemele informatice

Sistem de management al securitatii

Apărare cibernetică

- Managementului incidentelor de securitate
- Detectarea și tratarea incidentelor de securitate

Reziliență

- Managementul continuității serviciilor esențiale
- Gestionarea mai buna a situațiilor de criză, în special a incidentelor de securitate

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 Raspuns la incidente Management vulnerabilitati Testarea recuperarii in caz de dezastru