

CISO

Chief Information Security Officer

Manager Securitatea Informației

Ghid de informare

CISO definește strategia și guvernanta IT&C ale organizației, dimensionează resursele necesare și aliniază infrastructura la operațiunile și prioritățile de afaceri.

Cuprins:

Capitolul 1 – Prezentare generală	04
Capitolul 2 – Activități și sarcini specifice	12
Capitolul 3 – Competențe dobândite	20
Capitolul 4 – Metodologia de instruire	28
Capitolul 5 – Certificate și recunoaștere	32
Bonus!	
Tehnici de evaluare a riscului – studii de caz	36
Companii de tehnologia informației și servicii informatice	

Dragi prieteni,

Securitatea informației nu se rezumă la soluțiile achiziționate de o organizație, ci rezultă din deciziile pe care aceasta le ia, din modul în care coordonează și verifică măsurile adoptate și din capacitatea sa de a le îmbunătăți continuu.

Organizațiile moderne depind de informație pentru aproape fiecare decizie, serviciu și relație comercială. Datele, aplicațiile, infrastructura digitală, furnizorii de tehnologie și activitatea angajaților formează un sistem interdependent. Atunci când una dintre aceste componente este compromisă, consecințele nu rămân limitate la departamentul IT. Ele pot afecta operațiunile, veniturile, reputația, conformitatea legală și încrederea clienților.

În acest context, rolul managerului securitatea informației, cunoscut la nivel internațional ca Chief information security officer - CISO, nu poate fi redus la administrarea unor soluții tehnice. CISO este profesionistul care conectează riscul tehnologic cu obiectivele organizației. El trebuie să înțeleagă infrastructura, dar și strategia. Trebuie să poată discuta cu specialiștii tehnici, dar și să prezinte conducerii, într-un limbaj clar, ce riscuri există, ce măsuri sunt necesare și ce resurse trebuie alocate.

Un firewall poate bloca anumite conexiuni. O soluție de autentificare multifactor poate reduce riscul compromiterii conturilor. Un sistem de monitorizare poate genera alerte. Totuși, niciunul dintre aceste instrumente nu poate stabili singur prioritățile organizației, nivelul acceptabil de risc sau modul în care securitatea trebuie integrată în procesele de business. Acestea sunt responsabilități manageriale.

Cursul de specializare, organizat de **RQM Certification „Manager securitatea informației - CISO”** a fost conceput pentru profesioniștii care doresc să treacă de la administrarea fragmentată a problemelor de securitate la o abordare structurată, bazată pe guvernanta, risc, performanță, conformitate și reziliență.

Pe parcursul programului, veți învăța să evaluați infrastructuri și servicii IT&C, să formulați politici, să gestionați riscuri, să coordonați accesul la informații, să monitorizați performanța și conformitatea și să dezvoltați planuri de continuitate și recuperare în caz de dezastru.

Acest ghid prezintă structura programului, activitățile specifice ocupației, competențele care vor fi dezvoltate și modul în care specializarea vă poate sprijini evoluția către un rol managerial în securitatea informației.

Securitatea informației nu devine strategică prin simpla declarare a importanței sale. Ea devine strategică atunci când este transformată într-un sistem coerent de decizii, responsabilități, resurse, controale și rezultate măsurabile.



Ion Iordache

Training and Development Manager, RQM Certification



- ⌚ Policies
- ⌚ Standards
- ⌚ Roles & Responsibilities
- ⌚ Oversight

NETWORK ARCHITECTURE



SECURITY OPERATIONS



COMPLIANCE DASHBOARD

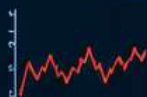
Compliance Status



Frameworks

- ✓ ISO 27001
- ✓ NIST CSF
- ✓ COBIT
- ✓ GDPR
- ✓ PCI DSS

RISK INDICATORS



HIGH
Current Risk Exposure

Threat Level
Vulnerabilities
Incidents (YTD)
Third-Party Risk

HIGH
23
7
MEDIUM

STRATEGIC INITIATIVES

- Zero Trust Architecture
- Cloud Security Enhancement
- Security Awareness Program
- Incident Response Readiness

Progress



RESOURCE ALLOCATION

Budget Distribution



- People 40%
- Technology 30%
- Processes 20%
- Third-Party 10%

Investment Priorities



SECURE
TRUSTED
RESILIENT

CAPITOLUL 1

Prezentare generală

CISO

CHIEF INFORMATION
SECURITY OFFICER

STRATEGIC
GOVERNANCE
RISK
RESILIENCE

ICT STRATEGY
PEOPLE
PROCESS
TECHNOLOGY

Securitatea informației a devenit una dintre condițiile esențiale pentru funcționarea stabilă și credibilă a unei organizații. Datele, aplicațiile, infrastructura digitală, procesele interne și relațiile cu furnizorii formează un ecosistem interdependent, în care o vulnerabilitate aparent locală poate produce efecte asupra continuității activității, conformității, reputației și încrederii clienților.

În acest context, rolul managerului securitatea informației, cunoscut la nivel internațional ca **Chief information security officer – CISO**, depășește cu mult administrarea unor tehnologii sau coordonarea răspunsului la incidente. CISO este profesionistul care transformă informațiile tehnice în decizii manageriale, corelează riscurile cu obiectivele organizației și stabilește modul în care resursele, politicile, oamenii și controalele trebuie integrate într-un sistem coerent de guvernare.

Un CISO eficient trebuie să înțeleagă infrastructura IT&C, dar și contextul de business în care aceasta funcționează. El trebuie să poată evalua riscurile, să definească priorități, să argumenteze investițiile, să coordoneze echipe multidisciplinare și să comunice clar atât cu specialiștii tehnici, cât și cu managementul de vârf. În același timp, trebuie să urmărească performanța sistemelor, respectarea cerințelor legale, eficacitatea politicilor și capacitatea organizației de a răspunde și de a se recupera după incidente.

Programul de specializare „Manager securitatea informației – CISO” dezvoltă aceste competențe într-o manieră structurată și aplicată. Participanții vor aborda guvernarea IT&C, politicile de securitate, controlul accesului, managementul riscurilor, monitorizarea performanței, continuitatea activității și recuperarea în caz de dezastru.

Această specializare pregătește profesioniști capabili să privească securitatea informației nu ca pe o funcție izolată, ci ca pe o responsabilitate strategică, integrată în modul în care organizația decide, operează și se dezvoltă.



Domeniul managementului securitate securității informației

Managementul securității informației operează la intersecția dintre tehnologie, oameni, procese, legislație și strategie organizațională.

Informația nu există izolat. Ea este creată, utilizată, transmisă, stocată și arhivată prin procese organizaționale în care sunt implicați angajați, furnizori, clienți, aplicații, echipamente și servicii externe.

Din acest motiv, securitatea informației nu poate fi administrată eficient exclusiv prin instrumente tehnice.

În esență, CISO este un traducător între limbajul tehnic al vulnerabilităților și limbajul managerial al riscului și performanței.

Un specialist tehnic poate raporta că un server conține o vulnerabilitate critică.

Conducerea organizației trebuie însă să înțeleagă ce proces depinde de acel server, ce servicii pot fi întrerupte, ce date pot fi compromise, ce obligații legale pot fi declanșate și ce costuri poate genera incidentul.

CISO transformă aceste informații într-o decizie fundamentată. El **stabilește contextul, evaluează riscul, propune alternative, estimează resursele necesare și monitorizează implementarea măsurilor aprobate.**

Un exemplu concret

O organizație descoperă că unul dintre furnizorii săi are acces permanent la o aplicație critică. Abordarea strict tehnică ar putea fi schimbarea parolei sau blocarea temporară a contului.

Abordarea managerială presupune mai mult:

- ✓ Clarificarea necesității accesului.
- ✓ Identificarea datelor și proceselor care pot fi afectate.
- ✓ Verificarea contractului și a obligațiilor furnizorului.
- ✓ Evaluarea drepturilor acordate și a trasabilității activităților.
- ✓ Stabilirea unor reguli de autentificare și acces temporar.
- ✓ Revizuirea procesului de atribuire și retragere a drepturilor.
- ✓ Monitorizarea periodică a accesului furnizorilor.

Această perspectivă sistemică diferențiază managementul securității informației de administrarea punctuală a unor tehnologii.

Standardul ocupațional atribuie rolului responsabilități privind strategia IT&C, securitatea sistemelor, coordonarea resurselor, bugetele, furnizorii, personalul și procedurile operaționale și administrative.

Este acest domeniu de activitate pentru tine?

Succesul într-un rol de CISO necesită o combinație echilibrată de înțelegere tehnică, gândire strategică, capacitate analitică și abilități de comunicare.

Programul nu este conceput exclusiv pentru persoanele care configurează echipamente sau administrează rețele. El se adresează profesioniștilor care vor să înțeleagă cum sunt luate, documentate și monitorizate deciziile privind securitatea informației.



Este posibil să coordonezi procese de risc, audit, conformitate, protecția datelor sau continuitate și să ai nevoie de o perspectivă integrată asupra securității informației.

Este posibil să fii manager și să observi că deciziile privind tehnologia, furnizorii și digitalizarea generează riscuri care nu mai pot fi tratate separat de strategia organizației.

Candidatul potrivit pentru acest program:

- ✓ Analizează problemele înainte de a propune soluții.
- ✓ Înțelege că riscul nu poate fi eliminat complet, dar poate fi identificat, evaluat și tratat.
- ✓ Poate colabora atât cu specialiști tehnici, cât și cu persoane fără pregătire tehnică.
- ✓ Este pregătit să argumenteze investițiile în securitate prin impact, priorități și rezultate.
- ✓ Înțelege că securitatea este un proces continuu, nu un proiect cu o dată definitivă de finalizare.
- ✓ Dorește să participe activ la procesele de decizie ale organizației.

Un CISO eficient nu trebuie să execute personal fiecare activitate tehnică. El **trebuie însă să înțeleagă suficient de bine tehnologia, riscul și organizația pentru a formula cerințe corecte, a evalua opțiuni și a coordona specialiștii potriviți.**

Cui se adresează această specializare?

Programul se adresează profesioniștilor care ocupă sau urmăresc să ocupe roluri cu responsabilități privind securitatea informației, tehnologia, riscul și continuitatea organizațională.

- ✓ **Manageri IT și responsabili ai infrastructurii IT&C** - Profesioniști care coordonează sisteme, servicii, proiecte, echipe sau furnizori IT și care doresc să integreze securitatea informației în procesele de management tehnologic.
- ✓ **Responsabili și manageri de securitatea informației** - Persoane care elaborează politici, monitorizează controale, gestionează incidente sau coordonează programe de securitate și doresc să își formalizeze și extindă competențele.
- ✓ **Specialiști în securitate cibernetică** - Analisti, ingineri, arhitecți sau consultanți care doresc să evolueze de la activități predominant tehnice către guvernanta, strategie și leadership.
- ✓ **Responsabili NIS2 și membri ai echipelor de conformitate** - Profesioniști implicați în evaluarea cerințelor de securitate cibernetică, gestionarea riscurilor, raportarea incidentelor și pregătirea documentației de conformitate.
- ✓ **Auditori și specialiști în managementul riscului** - Persoane care evaluează controale, procese și sisteme și care doresc să înțeleagă modul în care constatările trebuie transformate în decizii, planuri de acțiune și măsuri de îmbunătățire.

- ✓ **Responsabili cu protecția datelor** - Specialiști DPO sau persoane implicate în protecția datelor care doresc să aprofundeze relația dintre confidențialitate, securitatea informației, incidente și obligațiile de notificare.
- ✓ **Manageri de continuitate și reziliență** - Profesioniști care elaborează planuri de continuitate, recuperare în caz de dezastru, răspuns la incidente sau comunicare de criză.
- ✓ **Manageri de risc, conformitate, juridic și control intern** - Persoane care trebuie să evalueze impactul riscurilor tehnologice asupra obligațiilor legale, contractuale și organizaționale.
- ✓ **Membri ai conducerii și manageri operaționali** - Factori de decizie care coordonează procese dependente de tehnologie și care doresc să înțeleagă modul în care securitatea informației trebuie integrată în guvernanta organizației.

Recomandare pentru participare

Pentru accesul la instruire, standardul ocupațional recomandă o experiență profesională relevantă de minimum un an în domeniul IT sau digital ori în funcții care implică utilizarea, administrarea sau gestionarea sistemelor informatice și a informațiilor în format electronic.



De ce rolul CISO este unul strategic?

O organizație poate avea tehnologii performante și poate rămâne vulnerabilă dacă nu există responsabilități clare, politici aplicabile, priorități bine definite și mecanisme de verificare.



CISO oferă cadrul managerial prin care securitatea informației este conectată cu:

- ✓ Misiunea și obiectivele organizației.
- ✓ Procesele critice și serviciile esențiale.
- ✓ Nivelul de risc pe care organizația este pregătită să îl accepte.
- ✓ Investițiile în infrastructură și tehnologie.
- ✓ Obligațiile legale, contractuale și sectoriale.
- ✓ Relațiile cu furnizorii și partenerii.
- ✓ Dezvoltarea competențelor angajaților.
- ✓ Continuitatea activității și reziliența organizațională.

Rolul său nu este să blocheze digitalizarea, ci **să contribuie la realizarea ei în condiții controlate.**

Un exemplu concret

O organizație dorește să migreze o aplicație critică în cloud. Beneficiile pot include scalabilitate, disponibilitate și reducerea unor costuri operaționale. Decizia generează însă întrebări privind localizarea datelor, responsabilitățile furnizorului, controlul accesului, backup-ul, monitorizarea, continuitatea și ieșirea din contract.

CISO nu decide automat că migrarea este sigură sau nesigură.

1. Clarifică obiectivele de business.
2. Identifică informațiile și procesele implicate.
3. Evaluează riscurile și obligațiile aplicabile.
4. Definește cerințele de securitate.
5. Analizează furnizorii și opțiunile disponibile.
6. Prezintă managementului alternativele și riscurile reziduale.
7. Monitorizează implementarea și performanța serviciului.

Aceasta este diferența dintre securitatea reactivă și guvernanta securității informației.

Structura programului de formare

Modulul 1. Fundamente digitale, sustenabilitate și coordonare organizațională

Durată: 45 de ore | 3 credite

Participanții învață să utilizeze instrumente digitale pentru colaborare, analiză și raportare, să integreze principiile sustenabilității în deciziile IT&C și să coordoneze echipe care lucrează în medii fizice, hibride sau virtuale.

Modulul 2. Managementul infrastructurii și resurselor IT&C

Durată: 30 de ore | 2 credite

Sunt analizate componentele infrastructurii, rețelele, arhitecturile centralizate, distribuite și cloud, compatibilitatea tehnologică, monitorizarea calității, achizițiile, bugetele, furnizorii și resursele umane.

Modulul 3. Performanță, conformitate și strategie în IT&C

Durată: 30 de ore | 2 credite

Modulul abordează monitorizarea sistemelor, proceselor și serviciilor, indicatorii de performanță, raportarea incidentelor, cadrul legal, guvernanta IT, strategia de digitalizare, auditul managerial și raportarea către conducere.

Modulul 4. Politici și controlul accesului în securitatea informației

Durată: 30 de ore | 2 credite

Participanții învață să redacteze, implementeze și actualizeze politici de securitate, să definească responsabilități și să coordoneze controlul accesului, autentificarea și gestionarea identităților digitale. Sunt analizate principiile „necesității de a cunoaște” și „privilegiului minim”, sistemele IAM, autentificarea multifactor și ciclul de viață al drepturilor de acces.

Modulul 5. Riscuri, infrastructuri critice și continuitate în securitatea informației

Durată: 45 de ore | 3 credite

Modulul integrează evaluarea și tratarea riscurilor, protecția infrastructurilor critice, securitatea dispozitivelor mobile, munca la distanță, securitatea fizică a infrastructurii digitale, continuitatea activității, recuperarea în caz de dezastru și colaborarea cu autoritățile.

Structura oficială a programului alocă fiecărei competențe cinci ore de pregătire teoretică și zece ore de pregătire practică.

Guvernanță, risc, conformitate și reziliență

Un program conectat la provocările actuale ale organizațiilor

Competențele definite de standardul ocupațional sunt relevante pentru aplicarea principiilor întâlnite în principalele cadre de guvernanță, management al riscului și continuitate.

NIS2 și responsabilitatea conducerii

Directiva NIS2 introduce o perspectivă clară de guvernanță: organismele de conducere ale entităților esențiale și importante trebuie să aprobe măsurile de gestionare a riscurilor de securitate cibernetică și să supravegheze implementarea acestora.

CISO contribuie la acest proces prin evaluarea riscurilor, formularea politicilor, coordonarea controalelor, monitorizarea performanței și raportarea către management.

Participarea la programul de formare nu certifică automat conformitatea unei organizații cu NIS2. Programul dezvoltă însă competențe profesionale care pot susține procesele organizaționale de guvernanță și conformare.

ISO/IEC 27001

ISO/IEC 27001:2022 stabilește cerințele pentru un sistem de management al securității informației și promovează o abordare bazată pe riscuri, care integrează oamenii, politicile, procesele și tehnologia.

Temele programului de formare referitoare la guvernanță, politici, riscuri, monitorizare, audit și îmbunătățire continuă facilitează înțelegerea contextului în care funcționează un astfel de sistem de management.

ISO/IEC 27005

ISO/IEC 27005:2022 oferă îndrumări pentru identificarea, evaluarea și tratarea riscurilor de securitate a informației și susține implementarea unui sistem de management bazat pe ISO/IEC 27001.

ISO 22301

ISO 22301:2019 oferă cadrul internațional pentru managementul continuității activității, pregătirea pentru întreruperi și recuperarea serviciilor și proceselor organizaționale.

Programul de formare include analiza impactului asupra activității, identificarea proceselor critice, planurile de continuitate, recuperarea în caz de dezastru, testarea și documentarea lecțiilor învățate.

COBIT și ITIL

Programa integrează concepte de guvernanță IT, audit managerial, management al serviciilor, performanță, indicatori și îmbunătățire continuă, făcând referire la cadre precum COBIT și ITIL.



CAPITOLUL 2

Activități și sarcini specifice

Activitatea unui **Chief information security officer – CISO** este definită prin **capacitatea de a transforma obiectivele generale ale organizației în măsuri concrete de securitate a informației**. Rolul nu se limitează la reacția în fața incidentelor și nici la supravegherea unor tehnologii. El presupune coordonarea unui ansamblu de activități manageriale, tehnice și organizaționale, prin care informațiile, sistemele și procesele critice sunt protejate într-un mod proporțional cu riscurile identificate.

CISO analizează infrastructura IT&C, monitorizează performanța sistemelor și serviciilor, evaluează riscurile și definește politici aplicabile. În același timp, coordonează controlul accesului, gestionarea identităților, relațiile cu furnizorii, investițiile în tehnologie și activitatea echipelor implicate în securitate. O parte importantă a rolului constă în interpretarea datelor tehnice și operaționale și prezentarea lor într-o formă care permite conducerii să ia decizii informate.

Responsabilitățile sale includ și **pregătirea organizației pentru situații de întrerupere**. Elaborarea și testarea planurilor de continuitate, recuperarea în caz de dezastru, protejarea infrastructurilor critice și coordonarea raportării incidentelor sunt elemente esențiale ale funcției. Aceste activități trebuie realizate în corelare cu cerințele legale, standardele relevante și obiectivele de business.

În practică, **CISO acționează ca punct de legătură între management, specialiștii IT, audit, juridic, resurse umane, achiziții și furnizorii externi**. El nu execută singur toate sarcinile, ci stabilește priorități, atribuie responsabilități, urmărește rezultatele și intervine atunci când riscurile depășesc nivelul acceptat.

Capitolul următor prezintă cele 12 domenii de competență care definesc activitatea ocupațională a managerului securitatea informației și arată modul în care acestea se aplică în situații organizaționale concrete.



Date, colaborare și sustenebilitate

1. Utilizează instrumente digitale pentru analiza și interpretarea datelor

CISO trebuie să poată transforma datele operaționale și tehnice în informații utile pentru decizie.

Activitățile specifice includ:

- ✓ Selectarea instrumentelor digitale pentru comunicare și colaborare.
- ✓ Colectarea și centralizarea datelor din surse multiple.
- ✓ Calcularea și interpretarea indicatorilor de performanță.
- ✓ Crearea rapoartelor vizuale și a tablourilor de bord.
- ✓ Identificarea tendințelor, abaterilor și punctelor critice.
- ✓ Fundamentarea deciziilor pe baza datelor analizate.
- ✓ Monitorizarea digitală a proiectelor, responsabilităților și termenelor.

Exemplu practic: participanții pot construi un tablou de bord pentru monitorizarea incidentelor, a timpilor de răspuns și a stadiului măsurilor corective.

2. Promovează practici sustenabile și eficiente energetic în activitățile IT&C

Deciziile tehnologice produc efecte asupra costurilor, consumului de resurse și impactului de mediu.

CISO contribuie la:

- ✓ Identificarea tehnologiilor cu consum redus de energie.
- ✓ Evaluarea impactului ciclului de viață al echipamentelor.
- ✓ Integrarea criteriilor de sustenabilitate în achiziții.
- ✓ Susținerea utilizării responsabile a resurselor cloud.
- ✓ Elaborarea politicilor pentru un IT&C sustenabil.
- ✓ Reducerea deșeurilor electronice și promovarea reutilizării.
- ✓ Monitorizarea aplicării politicilor de sustenabilitate.

Exemplu practic: compararea a două opțiuni de infrastructură prin cost, securitate, consum energetic, scalabilitate și impact operațional.

Aceste activități sunt prevăzute în primele două competențe ale standardului ocupațional.

Leadership și infrastructură

3. Coordonează activitățile echipelor și gestionează conflictele

Securitatea informației presupune colaborarea dintre IT, management, juridic, resurse umane, audit, achiziții, operațional și furnizori.

CISO trebuie să poată:

- ✓ Planifica, organiza și monitoriza activitatea echipelor.
- ✓ Stabili obiective, responsabilități și termene.
- ✓ Coordona echipe fizice, hibride și virtuale.
- ✓ Delega activitățile în funcție de competențe și experiență.
- ✓ Comunica strategic cu persoane tehnice și non-tehnice.
- ✓ Participa la ședințe și forumuri de decizie.
- ✓ Aplica regulamentele interne și legislația muncii.
- ✓ Gestiona constructiv conflictele și diferențele de opinie.

Exemplu practic: coordonarea unei echipe multidisciplinare după producerea unui incident care afectează simultan sistemele IT, datele personale și activitatea operațională.

4. Evaluează infrastructura IT&C și calitatea sistemelor

CISO nu trebuie să administreze personal fiecare componentă, dar trebuie să înțeleagă arhitectura și dependențele infrastructurii.

Activitățile includ:

- ✓ Identificarea componentelor hardware, software și de rețea.
- ✓ Analizarea arhitecturilor centralizate, distribuite și cloud.
- ✓ Evaluarea compatibilității și interoperabilității sistemelor.
- ✓ Verificarea scalabilității și rezilienței infrastructurii.
- ✓ Aplicarea standardelor și bunelor practici relevante.
- ✓ Utilizarea indicatorilor de disponibilitate, performanță și securitate.
- ✓ Identificarea neconformităților și formularea recomandărilor.
- ✓ Colaborarea cu echipele tehnice pentru aplicarea măsurilor corective.

Exemplu practic: evaluarea unei infrastructuri în care sistemele critice funcționează pe echipamente depășite, fără redundanță și fără o strategie clară de actualizare.

Activitățile sunt detaliate în programa privind coordonarea echipelor și managementul infrastructurii.

Resurse, furnizori și performanță

5. Gestionează achizițiile, bugetele și resursele umane IT&C

Securitatea informației implică decizii privind investițiile, furnizorii și capacitatea organizației de a susține măsurile adoptate.

CISO participă la:

- ✓ Planificarea achizițiilor și bugetelor IT&C.
- ✓ Definirea cerințelor tehnice, funcționale și de securitate.
- ✓ Evaluarea tehnică și financiară a ofertelor.
- ✓ Selectarea și evaluarea furnizorilor.
- ✓ Negocierea și monitorizarea contractelor și acordurilor SLA.
- ✓ Integrarea cerințelor de securitate în documentațiile de achiziție.
- ✓ Monitorizarea execuției bugetare.
- ✓ Realizarea analizelor cost-beneficiu.
- ✓ Planificarea și dezvoltarea resurselor umane IT&C.
- ✓ Coordonarea relațiilor dintre IT, juridic, achiziții, audit și management.

Exemplu practic: evaluarea unei soluții de securitate care oferă funcționalități avansate, dar necesită resurse de operare pe care organizația nu le poate asigura.

6. Monitorizează performanța și conformitatea sistemelor și serviciilor IT&C

Monitorizarea nu se limitează la colectarea alertelor. Datele trebuie interpretate și corelate cu obiectivele organizației.

Activitățile includ:

- ✓ Stabilirea obiectivelor de monitorizare.
- ✓ Definirea indicatorilor și pragurilor critice.
- ✓ Selectarea surselor de date relevante.
- ✓ Analizarea jurnalelor, alertelor, telemetriei și rapoartelor.
- ✓ Evaluarea disponibilității, fiabilității și calității serviciilor.
- ✓ Verificarea conformității cu legislația și politicile interne.
- ✓ Evaluarea impactului incidentelor.
- ✓ Elaborarea rapoartelor pentru management și audit.
- ✓ Stabilirea măsurilor corective și preventive.

Exemplu practic: corelarea unei degradări repetate a serviciului cu obligațiile contractuale, riscurile operaționale și necesitatea unei investiții suplimentare.

Conținutul programului include managementul achizițiilor și furnizorilor, monitorizarea performanței, indicatorii, incidentele și raportarea managerială.

Guvernanta și politici

7. Evaluează nevoile IT&C și coordonează strategia de digitalizare

Tehnologia trebuie selectată și administrată în raport cu obiectivele organizației, nu doar în funcție de tendințele pieței.

CISO contribuie la:

- ✓ Identificarea nevoilor IT&C ale organizației.
- ✓ Analizarea cerințelor proceselor și utilizatorilor.
- ✓ Integrarea cadrelor de guvernanta în planificare.
- ✓ Corelarea investițiilor IT cu strategia generală.
- ✓ Elaborarea strategiei de digitalizare.
- ✓ Definirea obiectivelor, resurselor și indicatorilor.
- ✓ Coordonarea auditului managerial IT&C.
- ✓ Identificarea neconformităților.
- ✓ Monitorizarea implementării strategiei.
- ✓ Documentarea deciziilor și raportarea către management.

Exemplu practic: transformarea unei solicitări generale, precum „avem nevoie de mai multă securitate”, într-un program cu obiective, priorități, termene, responsabilități și indicatori.

8. Definește, implementează și actualizează politicile de securitate

O politică eficientă nu este un document formal păstrat într-un dosar. Ea trebuie să stabilească reguli clare și să fie integrată în activitatea reală.

CISO coordonează:

- ✓ Identificarea domeniilor care necesită politici.
- ✓ Diferențierea dintre strategie, politică, procedură și instrucțiune.
- ✓ Redactarea documentelor de securitate.
- ✓ Consultarea părților interesate.
- ✓ Aprobarea, publicarea și comunicarea politicilor.
- ✓ Integrarea politicilor în procesele organizației.
- ✓ Monitorizarea respectării regulilor.
- ✓ Corelarea politicilor cu gestionarea incidentelor.
- ✓ Revizuirea documentelor după audituri, incidente sau schimbări legislative.
- ✓ Păstrarea trasabilității versiunilor și aprobărilor.

Exemplu practic: actualizarea politicii de lucru la distanță după identificarea unor accesări ale datelor de pe dispozitive personale neadministrare.

Programa tratează guvernanta IT, strategia, auditul managerial, documentarea și ciclul complet al politicilor de securitate.

Identitate, acces și risc

9. Coordonează controlul accesului, autentificarea și gestionarea identității

Accesul la informații trebuie acordat în funcție de responsabilități, justificat, monitorizat și retras atunci când nu mai este necesar.

CISO coordonează:

- ✓ Definirea politicilor de acces.
- ✓ Aplicarea principiului privilegiului minim.
- ✓ Aplicarea principiului necesității de a cunoaște.
- ✓ Gestionarea ciclului de viață al identităților.
- ✓ Atribuirea, modificarea și revocarea drepturilor.
- ✓ Integrarea soluțiilor IAM.
- ✓ Alegerea metodelor de autentificare.
- ✓ Implementarea autentificării multifactor.
- ✓ Monitorizarea și trasabilitatea accesului.
- ✓ Organizarea revizuirilor periodice ale drepturilor.
- ✓ Instruirea personalului.

Exemplu practic: verificarea drepturilor unui angajat care a schimbat departamentul, dar a păstrat accesul la aplicațiile utilizate în rolul anterior.

10. Evaluează riscurile de securitate informatică

Managementul riscului permite organizației să prioritizeze măsurile în funcție de active, amenințări, vulnerabilități, probabilitate și impact.

Activitățile includ:

- ✓ Stabilirea contextului și a domeniului analizei.
- ✓ Identificarea și clasificarea activelor.
- ✓ Corelarea activelor cu procesele critice.
- ✓ Identificarea amenințărilor și vulnerabilităților.
- ✓ Evaluarea riscurilor prin metode calitative, cantitative sau mixte.
- ✓ Stabilirea pragurilor de acceptabilitate.
- ✓ Prioritizarea riscurilor.
- ✓ Selectarea măsurilor tehnice și organizaționale.
- ✓ Elaborarea planului de tratare.
- ✓ Monitorizarea implementării controalelor.
- ✓ Actualizarea și arhivarea analizei de risc.

Exemplu practic: evaluarea riscului de ransomware pentru un proces critic, luând în considerare backup-ul, accesul privilegiat, segmentarea rețelei, instruirea personalului și capacitatea de recuperare.

Controlul accesului, IAM și evaluarea riscurilor sunt dezvoltate în modulele patru și cinci.

Infrastructuri critice și continuitate

11. Coordonează securitatea infrastructurii critice, a dispozitivelor mobile și a muncii la distanță

Digitalizarea extinde perimetrul organizației dincolo de sediul fizic. Angajații, dispozitivele și datele pot opera din locații și rețele diferite.

CISO coordonează:

- ✓ Identificarea riscurilor asociate mobilității.
- ✓ Elaborarea politicilor BYOD și de lucru la distanță.
- ✓ Stabilirea regulilor pentru utilizarea rețelelor publice.
- ✓ Implementarea accesului securizat prin VPN și MFA.
- ✓ Gestionarea centralizată a dispozitivelor mobile.
- ✓ Protejarea datelor în repaus și în tranzit.
- ✓ Monitorizarea activităților desfășurate la distanță.
- ✓ Integrarea securității fizice și informatice.
- ✓ Protejarea camerelor server, UPS-urilor și nodurilor de comunicații.
- ✓ Gestionarea incidentelor fizice cu impact digital.
- ✓ Auditarea periodică a măsurilor de securitate fizică.

Exemplu practic: gestionarea pierderii unui laptop care conține date sensibile și este utilizat pentru accesarea resurselor organizației.

12. Elaborează și testează planurile de continuitate și recuperare

Continuitatea activității nu înseamnă doar existența unui backup. Organizația trebuie să înțeleagă ce procese trebuie recuperate, în ce ordine, cu ce resurse și în ce interval.

CISO contribuie la:

- ✓ Realizarea analizei impactului asupra activității.
- ✓ Identificarea proceselor și resurselor critice.
- ✓ Stabilirea scenariilor de întrerupere.
- ✓ Elaborarea planurilor de continuitate.
- ✓ Elaborarea planurilor de recuperare în caz de dezastru.
- ✓ Integrarea backup-ului, redundanței și serviciilor de failover.
- ✓ Organizarea simulărilor și testărilor.
- ✓ Documentarea lecțiilor învățate.
- ✓ Actualizarea periodică a planurilor.
- ✓ Raportarea incidentelor către autoritățile competente.
- ✓ Pregătirea documentației pentru audituri și controale.
- ✓ Participarea la inițiative de colaborare în domeniul securității.

Exemplu practic: simularea indisponibilității centrului principal de date și evaluarea capacității de recuperare a serviciilor critice.

Cerințele privind mobilitatea, securitatea fizică, continuitatea, recuperarea și colaborarea cu autoritățile sunt dezvoltate în ultima parte a programei.



STRATEGIC ROADMAP

	Q1	Q2 2025	Q3	Q4	Q4 2026
Business Alignment					
Experience					
Analytics					
Infrastructure					
Security					
Automation					

INFRASTRUCTURE ARCHITECTURE



BUSINESS KPIs

IT Service Availability

99.9%

+0.2% vs last month

Project Delivery

92% On-Time

+5% vs last month

IT Cost Optimization

-12%

vs last quarter

Security Posture

High
Risk Level

ICT GOVERNANCE FRAMEWORK



- Policies & Standards
- Risk & Compliance
- Architecture Review
- Performance & Value



STRATEGIC PRIORITIES

- Customer Centricity
- Operational Excellence
- Innovation & Growth
- Data-Driven Decisions



CAPITOLUL 3

Competențe dobândite

RESOURCE ALLOCATION



RESOURCE PLAN

- People
- Skills
- Budget
- Tools & Platforms
- Partners

• • • **Competența profesională** nu înseamnă doar
• • • acumularea unor cunoștințe, ci capacitatea de a le
• • • utiliza în mod coerent pentru rezolvarea unor situații
reale. În domeniul securității informației, această
• • • diferență este esențială. Un profesionist poate cunoaște
• • • terminologia tehnică, standardele și tipurile de
• • • controale, dar valoarea sa managerială se evidențiază
atunci când poate transforma aceste elemente în decizii,
• • • politici, priorități și rezultate măsurabile.

• • • Programul de specializare „**Manager securitatea
informației – CISO**” urmărește dezvoltarea unui profil
• • • profesional complet, capabil să integreze perspectiva
• • • tehnică, organizațională și strategică. La finalul formării,
absolventul va putea să analizeze date și indicatori, să
• • • evalueze infrastructura IT&C, să identifice riscurile și să
stabilească măsuri proporționale cu impactul acestora.
De asemenea, va putea să contribuie la definirea
strategiei de digitalizare, să coordoneze elaborarea
politicilor de securitate și să monitorizeze aplicarea lor în
procesele organizației.

O componentă importantă a competențelor dobândite
este **capacitatea de comunicare**. CISO trebuie să poată
explica riscurile tehnice într-un limbaj accesibil
conducerii, să argumenteze investițiile și să formuleze
recomandări clare pentru echipele operaționale. În
același timp, trebuie să poată coordona accesul la
informații, relațiile cu furnizorii, răspunsul la incidente și
procesele de continuitate și recuperare.

Competențele dezvoltate prin acest program nu sunt
izolate unele de altele. Ele formează un sistem integrat,
în care analiza riscului susține politica, politica
orientează controlul, monitorizarea verifică eficacitatea,
iar raportarea sprijină decizia managerială.

Capitolul următor prezintă rezultatele concrete ale
învățării și modul în care acestea pot fi aplicate în
activitatea profesională a unui manager al securității
informației.



De la date tehnice la decizii manageriale

La finalul programului, absolventul va putea să:

Transforme datele de securitate în informații utile pentru management

Va putea să selecteze indicatori relevanți, să interpreteze rapoarte și să construiască tablouri de bord care evidențiază riscurile, performanța și progresul măsurilor.

Un raport eficient nu prezintă doar numărul alertelor. El explică:

- ✓ Ce procese sunt afectate.
- ✓ Care este tendința.
- ✓ Ce praguri au fost depășite.
- ✓ Ce riscuri necesită decizie.
- ✓ Ce măsuri sunt recomandate.
- ✓ Cine este responsabil.
- ✓ Care este termenul de implementare.

Comunice strategic cu diferite categorii de public

Va putea adapta limbajul în funcție de audiență.

- ✓ Echipele tehnice au nevoie de cerințe și specificații clare.
- ✓ Conducerea are nevoie de impact, opțiuni, costuri și riscuri.
- ✓ Angajații au nevoie de reguli inteligibile și exemple practice.

Programul de formare dezvoltă capacitatea de a simplifica limbajul tehnic fără a pierde informațiile esențiale și de a redacta documente argumentate pentru susținerea deciziilor organizaționale.



Guvernanță și strategie

La finalul programului, absolventul va putea să:

Evalueze nevoile tehnologice ale organizației

Va putea analiza infrastructura, aplicațiile, serviciile, procesele și dependențele organizației pentru a identifica nevoile reale de dezvoltare sau îmbunătățire.

Evaluarea nu pornește de la întrebarea „ce tehnologie putem cumpăra?”, ci de la întrebările:

- ✓ Ce obiective trebuie susținute?
- ✓ Ce procese depind de tehnologie?
- ✓ Ce riscuri sunt generate?
- ✓ Ce capacități lipsesc?
- ✓ Ce resurse sunt disponibile?
- ✓ Cum va fi măsurat rezultatul?

Elaboreze și monitorizeze o strategie IT&C

Va putea contribui la o strategie care include:

- ✓ Analiza contextului intern și extern.
- ✓ Viziunea și direcțiile de dezvoltare.
- ✓ Obiective măsurabile.
- ✓ Resurse și responsabilități.
- ✓ Calendarul de implementare.
- ✓ Indicatorii de performanță.
- ✓ Mecanismele de monitorizare și raportare.
- ✓ Măsurile corective.

Utilizeze auditul ca instrument de guvernanță

Auditul nu va fi tratat doar ca o verificare retrospectivă, ci ca o sursă de informații pentru identificarea neconformităților, prioritizarea măsurilor și îmbunătățirea proceselor.



Politici și controlul accesului

La finalul programului, absolventul va putea să:

Elaboreze politici de securitate aplicabile

Va putea diferenția și utiliza corect:

- ✓ Strategia.
- ✓ Politica.
- ✓ Procedura.
- ✓ Instrucțiunea de lucru.
- ✓ Standardul intern.
- ✓ Ghidul de aplicare.

Participantul va putea redacta politici care precizează scopul, domeniul de aplicare, responsabilitățile, regulile, excepțiile, mecanismele de control și consecințele nerespectării.

O politică bună trebuie să fie suficient de clară pentru a fi aplicată, suficient de flexibilă pentru a rămâne relevantă și suficient de precisă pentru a putea fi verificată.

Coordoneze identitățile și drepturile de acces

Va putea evalua modul în care accesul este acordat, modificat, verificat și retras.

Această competență include relația dintre:

- ✓ Management.
- ✓ Resurse umane.
- ✓ Echipele IT.
- ✓ Responsabilii de aplicații.
- ✓ Securitatea informației.
- ✓ Auditul intern.
- ✓ Furnizorii externi.

Absolventul va înțelege că multe incidente nu sunt generate de lipsa unui instrument tehnic, ci de menținerea unor drepturi nejustificate, de atribuirea excesivă a privilegiilor sau de lipsa revizuirilor periodice.



Riscuri și investiții

La finalul programului, absolventul va putea să:

Realizeze o analiză de risc documentată

Va putea:

- ✓ Identifica activele.
- ✓ Stabili valoarea și criticitatea acestora.
- ✓ Identifica amenințările și vulnerabilitățile.
- ✓ Evalua probabilitatea și impactul.
- ✓ Calcula sau atribui scoruri de risc.
- ✓ Compara riscurile cu pragurile de acceptabilitate.
- ✓ Propune opțiuni de tratare.
- ✓ Documenta riscul rezidual.
- ✓ Monitoriza implementarea măsurilor.

Selecteze controale proporționale cu riscul

Nu orice risc justifică aceeași investiție. Măsurile trebuie selectate în funcție de context, impact, costuri, obligații și capacitatea organizației de a le administra.

Va putea analiza controale:

- ✓ Preventive.
- ✓ Detective.
- ✓ Corective.
- ✓ Tehnice.
- ✓ Organizaționale.
- ✓ Fizice.
- ✓ Contractuale.
- ✓ Procedurale.

Fundamenteze investițiile în securitate

Va putea utiliza analiza cost-beneficiu și indicatorii de eficiență pentru a argumenta investițiile.

Scopul nu este să demonstreze că orice măsură de securitate trebuie finanțată, ci să prezinte managementului informații suficiente pentru o decizie responsabilă.

Competența de analiză a riscurilor include redactarea raportului managerial, comunicarea rezultatelor și urmărirea măsurilor.



Monitorizare incidente și conformitate

La finalul programului, absolventul va putea să:

Monitorizeze performanța și securitatea

Va putea defini indicatori pentru:

- ✓ Disponibilitate.
- ✓ Timpi de răspuns.
- ✓ Rate de eroare.
- ✓ Fiabilitate.
- ✓ Respectarea acordurilor SLA.
- ✓ Timpi de remediere.
- ✓ Incidente și neconformități.
- ✓ Implementarea măsurilor corective.

Datele vor fi corelate cu obiectivele și procesele organizației, nu interpretate izolat.

Coordoneze răspunsul managerial la incidente

Va înțelege etapele incidentului și responsabilitățile manageriale privind:

- ✓ Detectarea.
- ✓ Confirmarea.
- ✓ Escaladarea.
- ✓ Limitarea efectelor.
- ✓ Comunicarea.
- ✓ Raportarea.
- ✓ Recuperarea.
- ✓ Analiza post-incident.
- ✓ Stabilirea măsurilor corective.
- ✓ Documentarea lecțiilor învățate.

Evalueze conformitatea

Va putea analiza relația dintre sistemele și procesele organizației și cerințele:

- ✓ Legale.
- ✓ Contractuale.
- ✓ Sectoriale.
- ✓ Organizaționale.
- ✓ Stabilite prin standarde și bune practici.

Cursul nu pregătește un profesionist care urmărește conformitatea doar prin completarea unor liste. El dezvoltă capacitatea de a înțelege scopul cerințelor și de a le integra în procese controlabile și verificabile.



Reziliență și continuitate

La finalul programului, absolventul va putea să:

Protejeze infrastructura digitală în contexte de lucru distribuit

Va putea coordona măsuri pentru:

- ✓ Echipamente mobile.
- ✓ Acces la distanță.
- ✓ Rețele externe.
- ✓ Dispozitive personale.
- ✓ Criptarea datelor.
- ✓ Autentificare.
- ✓ Monitorizarea activităților.
- ✓ Blocarea și ștergerea securizată a dispozitivelor.
- ✓ Gestionarea incidentelor de pierdere sau furt.

Elaboreze și testeze planuri de continuitate și recuperare

Va putea contribui la:

- ✓ Analiza impactului asupra activității.
- ✓ Identificarea proceselor critice.
- ✓ Stabilirea obiectivelor de recuperare.
- ✓ Definirea rolurilor și responsabilităților.
- ✓ Pregătirea scenariilor de întrerupere.
- ✓ Testarea planurilor.
- ✓ Documentarea rezultatelor.
- ✓ Actualizarea măsurilor.
- ✓ Colaborarea cu autoritățile.

Scopul nu este existența formală a unui plan, ci capacitatea demonstrabilă a organizației de a răspunde și de a se recupera.

Integreze securitatea fizică și securitatea informatică

O cameră server poate fi protejată logic prin parole și autentificare, dar poate rămâne vulnerabilă la acces fizic neautorizat, incendiu, sabotaj, inundație sau întreruperea alimentării electrice.

Va putea identifica aceste interdependențe și coordona măsuri pentru zonele critice, vizitatori, subcontractori, accesul în afara programului și trasabilitatea intrărilor.





CISO TRAINING METHODOLOGY

- 1. STRUCTURED EXPLANATIONS
Concepts, frameworks, standards
- 2. CASE STUDIES
Real-world incidents
- 3. EXERCISES
Practical application
- 4. SIMULATIONS
Tabletop & crisis scenarios
- 5. DEBATES
Challenge assumptions
- 6. RECOMMENDATIONS
Actionable improvements

SolarWinds
NotPetya

Access
Review

Ransomware
Scenario

Risk
Appetite

Roadmap

CISO TRAINING – PRACTICE. ANALYZE. DECIDE.

INCIDENT SCENARIO TIMELINE

- 08:15 Alert: Suspicious activity detected in EDR
- 08:47 Multiple failed logins – VPN
- 09:15 Privilege escalation observed
- 09:42 Data exfiltration attempt blocked
- 10:05 Ransomware note detected on file server
- 10:20 Incident declared – IR Team activated
- 10:45 Executive briefing initiated

RISK MATRIX



ACCESS CONTROL REVIEW



VENDOR RISK SUMMARY

Vendor	Criticality	Risk Level	Due Diligence
Cloud Provider A	Critical	High	✓
MSSP B	High	Medium	✓
Software Vendor C	Medium	Medium	!
Payment Processor D	High	High	!
HR SaaS E	Medium	Low	✓

CONTINUITY & DISASTER RECOVERY



INCIDENT RESPONSE – KEY DECISIONS

- Contain affected systems now?
- Disconnect from network?
- Engage law enforcement?
- Notify customers and regulators?
- Activate BCP / DR site?

DASHBOARD (LIVE)



TABLETOP EXERCISE RANSOMWARE INCIDENT

OBJECTIVE:
Make risk-based decisions under pressure with incomplete information.

TIMEBOX: 60 MINUTES

LEGAL IMPLICATIONS

PUBLIC CONTINUITY

TECHNICAL INVESTIGATION

LEGISLATION

THIRD-PARTY IMPACT

RISK ASSESSMENT

STAKEHOLDER IMPACT

CLIENT EXPANSION PLAN

STAKEHOLDER IMPACT

Stakeholder	Impact	Priority
Customers	High	1
Employees	High	2
Partners	Medium	3
Regulators	High	1
Shareholders	Medium	2

THE ATTACKER CLAIMS TO HAVE EXFILTRATED CUSTOMER DATA. A SAMPLE IS PROVIDED. WHAT IS YOUR RESPONSE?

Decisions Log

CAPITOLUL 4

Metodologia de instruire

Formarea unui **Chief Information Security Officer** nu poate fi realizată exclusiv prin transmiterea unor concepte teoretice.

Rolul presupune analiză, decizie, comunicare, coordonare și capacitatea de a acționa în situații în care informațiile sunt incomplete, timpul este limitat, iar consecințele pot afecta întreaga organizație. Din acest motiv, **metodologia de instruire este construită în jurul aplicării practice a cunoștințelor.**

Fiecare temă este introdusă **prin explicații structurate și exemple relevante, urmate de exerciții, studii de caz, simulări și dezbateri.**

Participanții sunt încurajați să analizeze problemele din mai multe perspective, să formuleze ipoteze, să compare opțiuni și să își argumenteze recomandările. Accentul nu este pus doar pe identificarea unui răspuns corect, ci pe calitatea procesului de analiză și pe capacitatea de a explica decizia adoptată.

Componenta practică ocupă un rol central în arhitectura programului. Cursanții vor lucra cu scenarii privind incidente de securitate, controlul accesului, evaluarea riscurilor, relațiile cu furnizorii, continuitatea activității și recuperarea în caz de dezastru.

Prin **simulări** de tip tabletop, aceștia vor exersa coordonarea echipelor, escaladarea informațiilor, stabilirea priorităților și comunicarea cu managementul.

Instrumentele digitale, platformele de colaborare, dashboard-urile, rapoartele și aplicațiile de management al riscurilor completează procesul de învățare. Participanții vor utiliza aceste resurse nu doar pentru a observa datele, ci pentru a le interpreta și transforma în informații relevante pentru decizie.

Metodologia urmărește dezvoltarea unui profesionist capabil să conecteze teoria cu practica și să aplice principiile securității informației într-un mod coerent, documentat și adaptat contextului organizațional.



Învățare aplicată

Studii de caz și scenarii organizaționale

Conceptele sunt prezentate prin situații care reproduc deciziile și dificultățile întâlnite în organizații.

Exemplele pot include:

- ✓ Un atac ransomware asupra unui proces critic.
- ✓ Compromiterea unui cont privilegiat.

Participanții analizează contextul, identifică informațiile lipsă, evaluează alternative și formulează recomandări.

Simulări de tip tabletop

Participanții primesc un scenariu care evoluează progresiv. Pe parcursul exercițiului apar informații noi, iar echipa trebuie să decidă:

- ✓ Cine coordonează răspunsul.
- ✓ Ce măsuri sunt prioritare.
- ✓ Ce informații trebuie confirmate.
- ✓ Cine trebuie informat.
- ✓ Ce obligații de raportare pot exista.
- ✓ Cum este menținută activitatea.
- ✓ Cum sunt documentate deciziile.

Standardul prevede expuneri, prezentări interactive, dezbateri, studii de caz, demonstrații practice, exerciții, simulări și discuții de grup.

- ✓ Menținerea accesului unui fost angajat.
- ✓ Indisponibilitatea unui furnizor cloud.
- ✓ Pierderea unui dispozitiv mobil.
- ✓ Neîndeplinirea unui acord SLA.
- ✓ Un incident care implică date cu caracter personal.
- ✓ O întrerupere de energie într-o zonă critică.
- ✓ Lipsa testării planului de recuperare.
- ✓ O investiție în securitate care trebuie justificată conducerii.

Instrumente și resurse digitale

Instrumente digitale și simulări

Procesul de formare utilizează resurse care permit participanților să înțeleagă atât funcționarea tehnologiilor, cât și modul în care rezultatele generate de acestea sunt utilizate în deciziile manageriale.

În funcție de tema abordată, pot fi utilizate sau demonstrate:

- ✓ Servere și unități de stocare fizice sau virtuale.
- ✓ Echipamente și arhitecturi de rețea.
- ✓ Firewall-uri.
- ✓ Sisteme de detectare și prevenire a intruziunilor.
- ✓ Soluții de autentificare multifactor.
- ✓ Sisteme de acces biometric.
- ✓ Platforme de management al riscurilor.
- ✓ Soluții de criptare.
- ✓ Instrumente de testare și simulare a vulnerabilităților.
- ✓ Dashboard-uri și instrumente de raportare.
- ✓ Platforme de videoconferință și colaborare.
- ✓ Documente legislative, standarde și protocoale.
- ✓ Fișe de practică și suporturi digitale de curs.

Programa oficială enumeră aceste resurse pentru pregătirea teoretică și practică.



Prelegeri participative

Temele sunt introduse prin explicații structurate, urmate de întrebări, dezbateri și exemple.

Participanții sunt încurajați să coreleze conținutul cu experiența profesională proprie, respectând confidențialitatea informațiilor organizaționale.

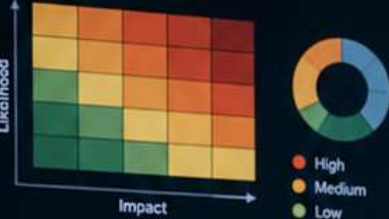
Feedback și învățare progresivă

Exercițiile sunt analizate împreună cu formatorul. Accentul nu este pus doar pe identificarea răspunsului corect, ci pe calitatea raționamentului:

- ✓ Ce informații au fost utilizate?
- ✓ Ce ipoteze au fost formulate?
- ✓ Ce riscuri au fost omise?
- ✓ Cum poate fi justificată recomandarea?
- ✓ Ce efecte secundare poate produce măsura propusă?
- ✓ Cum poate fi monitorizată eficacitatea?



RISK ASSESSMENT



SECURITY POLICIES

- ✓ Access Control
- ✓ Data Protection
- ✓ Acceptable Use
- ✓ Third-Party Risk
- ✓ Compliance

ACCESS CONTROL



INCIDENT RESPONSE



BUSINESS CONTINUITY

Recovery Time Objective: 4h
Recovery Point Objective: 1h
Test Status: Completed

RECOVERY STATUS



GOVERNANCE

- 🏠 Policies
- 📋 Standards
- 👤 Roles & Responsibilities
- 🔍 Audit & Assurance

COMPLIANCE

- ISO 27001
- NIST CSF
- GDPR
- SOX

CISO PROGRAM

- LEADERSHIP
- STRATEGY
- GOVERNANCE
- RISK MANAGEMENT
- RESILIENCE

CAPITOLUL 5

Certificare și recunoaștere

PRACTICAL ASSESSMENT

	✓	✓
STRATEGY & GOVERNANCE	✓	✓
RISK MANAGEMENT	✓	✓
INCIDENT RESPONSE	✓	✓
BUSINESS CONTINUITY	✓	✓
LEADERSHIP & COMMUNICATION	✓	✓

SECURITY STRATEGY



RISK REPORT



Certificarea reprezintă etapa prin care competențele dezvoltate pe parcursul programului sunt evaluate și confirmate în raport cu cerințele standardului ocupațional.

Pentru participant, aceasta nu este doar o formalitate administrativă, ci dovada că poate utiliza cunoștințele dobândite în situații profesionale relevante pentru rolul de manager al securității informației.

Programul de specializare „Manager securitatea informației – Chief information security officer – CISO”, cod COR 133048, este organizat de RQM Certification, furnizor autorizat de Ministerul Muncii, Familiei, Tineretului și Solidarității Sociale pentru desfășurarea acestui program.

Structura formării, conținutul tematic și competențele evaluate sunt stabilite prin standardul ocupațional aprobat de Autoritatea Națională pentru Calificări.

La finalul cursului, participanții susțin un **examen de absolvire**, organizat conform cerințelor aplicabile formării profesionale a adulților. Evaluarea urmărește atât înțelegerea conceptelor, cât și capacitatea de a le aplica. Pot fi analizate situații privind evaluarea riscurilor, elaborarea politicilor, controlul accesului, răspunsul la incidente, continuitatea activității și fundamentarea deciziilor manageriale.

Absolvenții care promovează examenul primesc **certificatul de absolvire** aferent programului de specializare. Documentul atestă competențele profesionale dobândite pentru ocupația de manager securitatea informației.

Recunoașterea profesională oferită de certificare consolidează profilul absolventului și demonstrează parcurgerea unui program structurat, orientat către responsabilități manageriale, guvernanță, risc, conformitate și reziliență organizațională.



Valoarea profesională a specializării

Certificatul atestă dobândirea competențelor profesionale definite prin standardul ocupațional național pentru ocupația „Manager securitatea informației – CISO”.

Standardul poziționează ocupația la nivelul 6 CNC și nivelul 6 EQF. Această raportare facilitează înțelegerea nivelului de complexitate, autonomie și responsabilitate asociat ocupației, fără a echivala automat certificatul cu o certificare internațională separată.

O bază pentru roluri manageriale și conexe

Competențele dezvoltate pot fi relevante pentru roluri precum:

- ✓ Manager securitatea informației.
- ✓ Chief information security officer.
- ✓ Information security manager.
- ✓ Manager sau coordonator de securitate cibernetică.
- ✓ Manager de guvernanță IT.
- ✓ Manager de risc tehnologic.
- ✓ Responsabil NIS2.
- ✓ Manager de conformitate în domeniul IT&C.
- ✓ Manager de continuitate și recuperare.
- ✓ Coordonator al proceselor de gestionare a incidentelor.
- ✓ Manager IT cu responsabilități de securitate.
- ✓ Consultant în guvernanța securității informației.
- ✓ Responsabil pentru politicile și controlul accesului.
- ✓ Coordonator al relației cu furnizorii de servicii IT și securitate.

Denumirea concretă a funcției și condițiile de ocupare depind de structura, domeniul și cerințele fiecărei organizații.

Relația cu certificările internaționale

Certificatul de absolvire pentru ocupația CISO nu înlocuiește certificările individuale emise de organisme precum ISACA, PECB, PeopleCert sau alte organizații internaționale.

De asemenea, **absolvirea cursului nu reprezintă:**

- ✓ Certificarea unei organizații conform ISO/IEC 27001.
- ✓ Certificarea individuală ISO/IEC 27001.
- ✓ Certificarea conformității cu NIS2.
- ✓ O autorizație emisă de DNSC.
- ✓ O certificare tehnică pentru un anumit produs.

Programul oferă, însă, o bază managerială integrată pentru înțelegerea și coordonarea activităților care pot face parte din asemenea inițiative.



TEHNICI DE EVALUARE A RISCULUI

În conformitate cu SR EN IEC 31010:2020 Managementul riscului. Tehnici de evaluare a riscului

STUDII DE CAZ

Companii de tehnologia informației și servicii informatice
[Material didactic]

Autor: Ion Iordache - Consultant de Securitate & Trainer la RQM Certification





✉ office@rqmcert.ro

☎ 0040 737 754 008

☎ 0040 356 173 020

📍 Strada Marginii Nr. 4, Corp A, Ap. 6, Timișoara, România



Chief Information Security Officer

Ion Iordache
www.rqmcert.ro