# MATRICEA DE AUDIT A RISCURILOR CIBERNETICE

ENCRYPT 4.0

Co-finanțat de programul Eramus+ al Uniunii Europene

*Proiectul ENCRYPT4.0 (2020-1-RO01-KA202-079983) a fost finanțat cu sprijinul Comisiei Europene. Această publicație reflectă doar punctul de vedere al autorilor, iar Comisia nu poate fi trasă la răspundere pentru orice utilizare care ar putea fi făcută informațiilor conținute în aceasta.*

# CUPRINS

# 1. INTRODUCTION

Productivitatea, calitatea și costurile de fabricație pot beneficia de îmbunătățiri dramatice prin conectivitatea crescândă a industriei 4.0, utilizarea calculelor digitale și stocarea datelor în afara site-ului. Cu toate acestea, există riscuri asociate ale întreprinderilor mici și mijlocii (IMM) cu profil de producție, precum potențialitatea concurenților și a adversarilor de a le accesa datele. Atacurile cibernetice sunt din ce în ce mai frecvente și sunt, de obicei, implementate pentru a extrage date confidențiale și / sau private, de a manipula date capturate pentru a provoca efecte nedorite și a distruge activele de capital (Margot Hutchins și Stefanie Robinson, 2015). Atacurile cibernetice pot fi definite ca „atacuri cibernetice, prin intermediul spațiului cibernetic, care vizează utilizarea întreprinderii de către o altă întreprindere a spațiului cibernetic, de a întrerupe, dezactiva, distruge sau controla în mod tendențios un mediu / infrastructură de calcul; ordonarea integrității datelor sau furtul informațiilor controlate ”(Institutul Național pentru Standarde și Tehnologie, 2012, p. B3). Forumul Economic Mondial (2017) prioritizează soluția pentru abordarea riscurilor de inovație-conducere: i) Măsurarea riscului cibernetic și ii) Evaluarea securității cibernetice. În 2019, frauda datelor și atacurile cibernetice au fost identificate de Forumul Economic Mondial drept al patrulea și al cincilea risc cel mai probabil (Forumul Economic Mondial, 2020), în 2020 a identificat probleme legate de spațiul cibernetic, cum ar fi atacurile cibernetice și fraudele de date, cu ajutorul unui top 10 al riscurilor pe termen lung.

**ENCRYPT 4.0 se concentrează pe evaluarea securității cibernetice, prin dezvoltarea Matricei de audit a riscului cibernetic**

Industria manufacturieră are nevoie de instrumente pentru a încorpora riscurile cibernetice în procesele lor existente de gestionare a riscurilor. În acest context, ENCRYPT 4.0 abordează această nevoie identificată, concentrându-se pe evaluarea securității cibernetice, prin dezvoltarea matricei de audit a riscului cibernetic (MARC). MARC este un instrument cuprinzător menit să sprijine managerii IMM-urilor de producție să efectueze o analiză cuprinzătoare a proceselor lor, luând în considerare utilizarea soluțiilor tehnologice inovatoare bazate pe industria 4.0, să identifice riscurile cibernetice și să îi susțină în proiectarea și stabilirea unor controale eficiente în propria întreprindere. MARC va fi dezvoltată luând în considerare expertiza din standardele naționale, UE și mondiale (Anexa A), precum și feedback-ul experților în securitate cibernetică din șase țări europene - Austria, Portugalia, România, Bulgaria, Cipru și Spania.

- Acest document cuprinde a) propunerea de valoare MARC, b) metodologia MARC, c) descrierea categoriilor de matrice de audit al riscului cibernetic, c) pașii pentru efectuarea auditurilor de securitate cibernetică d) referințe bibliografice.

# 2. PROPUNEREA DE VALOARE MARC

**Matricea de audit a riscului cibernetic (MARC)** va permite fabricilor inteligente să realizeze o imagine de ansamblu, sistematică a peisajului lor de risc cibernetic și să creeze un profil precis al riscurilor de amenințări cibernetice. Encrypt 4.0 MARC va permite fabricilor inteligente să efectueze

o analiză consistentă a datelor în timp real și să-și evalueze riscurile cibernetice, pe baza unei matrice specifice și extinse.

Matricea de audit a riscurilor cibernetice va fi un instrument analitic care va sprijini companiile producătoare să identifice, să analizeze, să stabilească prioritatea riscurilor și să stabilească prompt măsuri de protecție. În ultimii ani, una dintre cele mai presante probleme ale lumii digitale este securitatea cibernetică și protecția confidențialității datelor. În 2019, Forumul Economic Mondial (WEF) a clasat atacurile cibernetice printre primele cinci riscuri globale.

În 2020, odată cu pandemia COVID-19, dependența mai mare de conectivitate și infrastructura digitală datorită blocării globale a sporit oportunitățile de intruziune și atacuri cibernetice. În același timp, pentru a maximiza daunele și câștigurile financiare, infractorii cibernetici își mută țintele de la persoane fizice și întreprinderi mici către mari corporații, guverne și infrastructură critică, care joacă un rol crucial în răspunsul la focar (INTERPOL G. S., 2020). „Atacurile cibernetice reprezintă un pericol mai mare pentru democrații și economii decât armele și tancurile” (Juncker, 2017).

Cybersecurity Ventures, principalul cercetător mondial în economia cibernetică globală, a prezis că „daunele globale legate de criminalitatea cibernetică în 2021 vor ajunge la șase trilioane de dolari, ceea ce va reprezenta mai mult decât dezastre naturale într-un an” (Cybersecurity Ventures, 2020). Raportul anual anual oficial privind criminalitatea informatică din 2019 a declarat că „la sfârșitul anului 2016, o companie a fost victima unui atac de ransomware la fiecare 40 de secunde” (Cybersecurity Ventures, 2019) și previziunile sunt că această cifră va crește la fiecare 11 secunde până în 2021.

Atacurile cibernetice asupra infrastructurii critice, clasificate pe al cincilea loc de risc în 2020 de către rețeaua de experți WEF, au devenit noul normal în sectoare precum energia, sănătatea și transporturile. Cu toate acestea, producția suferă de atacuri cibernetice în creștere, așa cum a arătat Raportul de investigații privind încălcarea datelor din 2020, care detaliază 922 de incidente, 381 cu divulgarea datelor confirmate, doar în SUA (Verizon, 2020). Organizațiile care luptă împotriva criminalității cibernetice își unesc forțele iar probabilitatea de detectare și urmărire penală este estimată la 0,05% în Statele Unite, „criminalitatea cibernetică ca serviciu este un model de afaceri în creștere, deoarece sofisticarea tot mai mare a instrumentelor pe Darknet face serviciile rău intenționate mai accesibile și ușor accesibile pentru oricine ”( Forumul Economic Mondial, 2020).

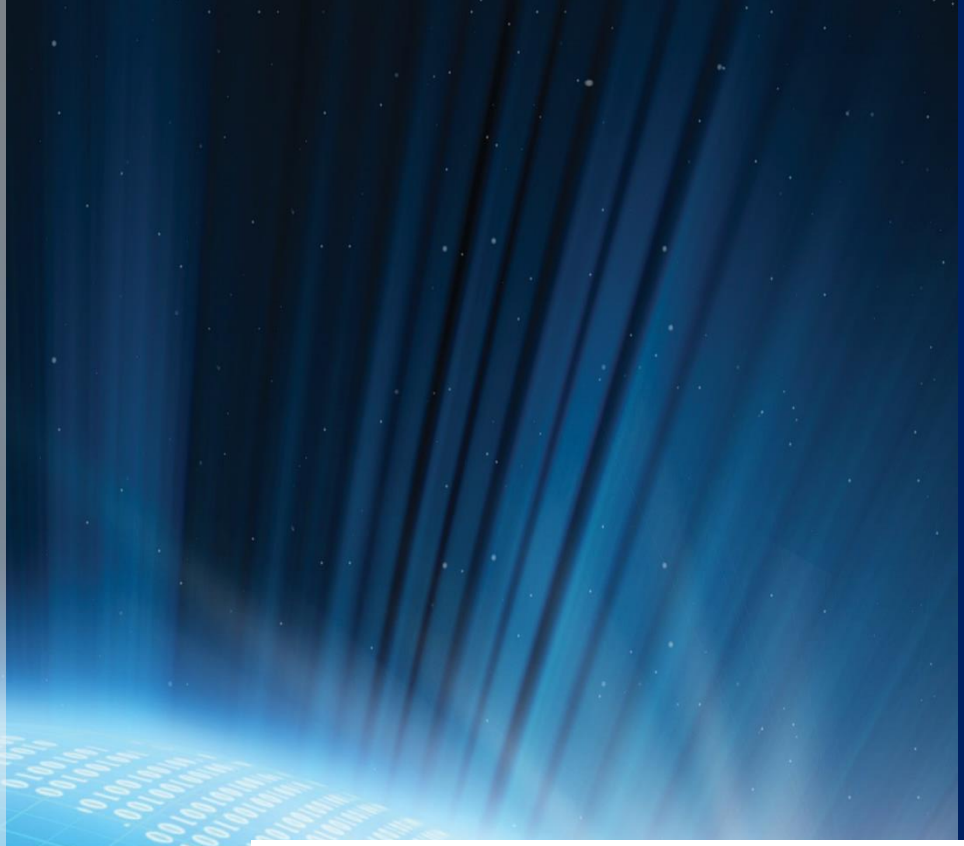
Capacitatea de apărare a IMM-urilor este de obicei mai slabă în comparație cu întreprinderile mai mari și cifrele sugerează că doar 14% dintre IMM-urile afectate își pot recupera singure pierderile. Mai mult, Alianța Națională pentru Securitate Cibernetică afirmă că 60% dintre IMM-urile care suferă un atac cibernetic își pierd afacerea în termen de 6 luni și „producătorii sunt mult mai predispuși la amenințări la adresa securității lor din cauza conectivității în sistemele IT și OT (Tehnologii operaționale) prin Digitalizarea industriei 4.0 ”(Verizon, 2017).

Majoritatea companiilor producătoare, în încercarea lor de a menține un avantaj competitiv, adaptându-se la practicile din industria 4.0, fac eforturi sporadice investind în sisteme de control și consilieri externi, dar le lipsește o abordare integrată a gestionării riscurilor cibernetice. Eforturile lor nu reușesc să abordeze în mod eficient amenințările cibernetice care evoluează rapid, deoarece majoritatea sistemelor de fabricație au fost dezvoltate în mod tradițional pentru a se concentra pe siguranță și performanță ridicată, mai degrabă decât pe securitate. Mai mult, atunci când vine vorba de securitate, producătorii erau preocupați din punct de vedere istoric în principal de asigurarea mediului lor OT, neglijând adesea securitatea IT, „apariția industriei 4.0 introduce noi tehnologii în mediile tradiționale OT și astfel persoanele familiare cu OT care lucrează în astfel de medii trebuie să se adapteze ”(Agenția UE pentru securitate cibernetică, 2019). Angajații folosesc adesea informații potențial conflictuale pentru a descrie sau evalua unele aspecte ale riscului cibernetic.

Matricea de audit al riscului cibernetic (MARC) va contura indicatorii cheie-riscuri care vor fi aplicați cu ușurință datelor în timp real. MARC va permite angajaților nu numai să realizeze o strategie de securitate cibernetică pe termen lung, ci și să efectueze rapid rapoarte zilnice. Acest lucru va arăta nivelurile reale de risc pentru procese la un moment dat, de o importanță crucială în mediul de fabricație, deoarece menținerea producției în desfășurare este esențială și cea mai scurtă perturbare a anumitor procese poate avea un impact ireparabil și poate provoca pierderi financiare imense. Riscurile de securitate din industria prelucrătoare devin din ce în ce mai complexe și evoluează, ceea ce face extrem de importantă dotarea IMM-urilor cu profil de producție cu un instrument analitic adecvat pentru a contura măsurile de precauție care trebuie luate în considerare în fiecare zi în cadrul producției. Spre deosebire de eșecurile proceselor mecanice care pot fi clasificate drept statice, eșecurile de securitate cibernetică sunt dinamice, deoarece se încorporează strâns cu interacțiunile umane.

**Obiectivul principal al MARC** este de a oferi **managerilor din producție** o perspectivă asupra **riscurilor potențiale de securitate cibernetică din sistemele lor** și de a-i sprijini **să adopte o strategie eficientă de reducere a riscurilor**. Deoarece este disponibilă doar o cercetare limitată în domeniul evaluării riscului de securitate cibernetică în sistemele de fabricație, Encrypt 4.0 MARC va reprezenta un instrument inovator menit să fie încorporat în politica de gestionare a riscurilor a companiei de producție

**Matricea de audit a riscului cibernetic va contura indicatorii cheie-riscuri care vor fi aplicați cu ușurință datelor în timp real**

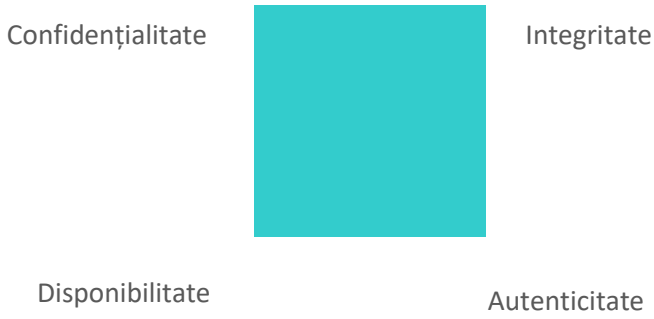


*Obiectivul principal al MARC este de a oferi managerilor din producție o perspectivă asupra riscurilor potențiale de securitate cibernetică din sistemele lor Și de a-i sprijini să adopte o strategie eficientă de reducere a riscurilor.*

**MARC a fost proiectat având în vedere cvartetul CIAD**

# 3. METODOLOGIA MATRICEI DE AUDIT CIBERNIC A RISCURILOR

MARC a fost conceput având în vedere cvartetul CIAD de confidențialitate integritate, autenticitate, disponibilitate. Se măsoară două aspect importante: probabilitatea riscului și impactul riscului., adaptate pentru a răspunde nevoilor specific ale IMM-urilor de producție cu potențialul de a fi ușor modelate și adaptate în cultura organizațională individuală a oricărei companii.




MARC include, de asemenea: i) numărul de riscuri, ii) categoria de risc, iii) sursa de risc, iv) descrierea riscului, v) costurile potențiale asociate cu consecințele riscului, vi) departamentul organizației care ar putea fi afectat, vii) atenuarea / acțiunile implementate anterior, viii) impactul asupra riscului, ix) probabilitatea riscului, x) nivelul general al riscului, xi) declanșatorii, xii) atenuarea / acțiunile care trebuie implementate, xiii) costurile potențiale ale atenuării, xiv) termenul limită, xv) persoana responsabilă cu managementul riscului, xvi) supervizor responsabil cu monitorizarea și xvii) evaluarea eficacității

Mai jos, descrierea principalelor concepte care cuprind matricea de audit al riscului cibernetic:

**Disponibilitate**: Asigurarea accesului la timp și fiabil al informațiilor.

**Autenticitate**: Asigurarea proprietății datelor de a fi autentice și originale, capabile să fie verificate și încredere în validitatea unei transmisii, a unui mesaj sau a inițiatorului de mesaje. (Proiectul Criptare 4.0, 2020).

**Evaluarea securității cibernetice**: Îmbunătățirea mecanismelor de orientare și evaluare a securității cibernetice, inclusiv principii comune pentru evaluările securității cibernetice, un mecanism de punctare bazat pe puncte și pași practici de îmbunătățire, care permit companiilor să evalueze și să îmbunătățească disponibilitatea lor pentru securitate cibernetică (World Economic Forum, 2017).

**Confidențialitate**: Păstrarea restricțiilor (controlate) privind accesul și divulgarea informațiilor, inclusiv mijloace de protejare a confidențialității personale și a informațiilor proprietare.

**Impact**: Impactul potențial evaluat rezultat dintr-un compromis al confidențialității, integrității sau disponibilității unui tip de informație, exprimat ca o valoare *scăzută, moderată* sau *ridicată*.

**Integritate**: Protecția împotriva modificării sau distrugerii necorespunzătoare a informațiilor și include asigurarea nerespectării și autenticității informațiilor.

**Probabilitate**: Un factor ponderat bazat pe o analiză subiectivă a probabilității că o anumită amenințare este capabilă să exploateze o anumită vulnerabilitate sau un set de vulnerabilități.

*Descrieri inspirate din Ghidul pentru efectuarea evaluărilor riscurilor (Institutul Național de Standarde și Tehnologie, 2012).*

# 4. MATRIZA DE AUDIT A RISCURILOR CIBERETICE (MARC)

Encrypt 4.0 MARC reprezintă un instrument cuprinzător destinat sprijinirii managerilor IMM-urilor producătoare pentru a efectua o analiză cuprinzătoare a proceselor lor, luând în considerare utilizarea soluțiilor tehnologice inovatoare bazate pe industria 4.0 și identificarea riscurilor cibernetice și sprijinirea acestora în proiectarea și stabilirea unor controale eficiente în aria lor de activitate.

## 4.1 CATEGORII DE MATRICI DE AUDIT ALE RISCURILOR CIBERETICE

Aceste categorii au fost derivate dintr-o cercetare și analiză efectuată a peste 20 de standarde (anexa A) în domeniul securității informațiilor și protecției datelor, precum și din 12 interviuri aprofundate realizate cu experți în securitate cibernetică din Austria, Portugalia, România, Bulgaria, Cipru și Spania.

**Tabelul 1. Categorii ale matricei de audit a riscurilor cibernetice**

| Categoria de risc | Descrierea categoriei de risc |
|---|---|
| **Resurse umane** | resursele umane ale companiei. Riscurile legate de rolurile și responsabilitățile personalului companiei, luarea deciziilor, gestionarea identităților, controlul accesurilor, sensibilizarea. |
| **Proprietate intelectuală** | Identificarea riscurilor legate de proprietatea intelectuală a companiei. Proprietatea intelectuală include proprietatea industrială, drepturile de autor și drepturile conexe și conferă dreptul la utilizarea exclusivă a informațiilor tehnice, comerciale și industriale respective. Proprietatea industrială își propune să protejeze invențiile, brevetele, mărcile și proiectele acoperite de drepturi exclusive de utilizare, producție și comercializare. |
| **Sisteme de control industrial (SCI)**<br><br>**Securitate** | Securitatea SCI implică păstrarea și securizarea sistemelor de control industrial, precum și a software-ului și hardware-ului necesar care sunt utilizate de sistem. |
| **Produse** | Identificarea riscurilor legate de produse. Apariția acestui tip de risc poate pune în pericol produsele produse de organizație. |
| **Riscuri juridice privind securitatea cibernetică** | Identificarea riscurilor legate de responsabilitățile legale și de reglementare. Apariția acestui tip de risc poate pune în pericol responsabilitățile legale și / sau de reglementare ale organizației. |
| **Atacuri în lanțul de aprovizionare** | Identificarea vulnerabilităților din lanțul de aprovizionare. Organizația trebuie să definească, să evalueze și să gestioneze procesele de gestionare a riscurilor din lanțul de aprovizionare și logistică. Identificarea legăturilor către furnizori cu posturi de securitate slabe. |
| **Tehnologie, TIC și siguranță operațională** | Identificarea riscurilor legate de tehnologie, TIC și operațiunile companiei. Pentru a aborda pericolele care rezultă din insuficiențele funcționale ale funcționalității intenționate, tulburări operaționale sau rateuri rezonabile / erorile colaboratorilor legate de tehnologie, TIC și operațiuni. |
| **Clienți** | Apariția unui anumit risc poate pune în pericol serviciul oferit clienților organizației sau poate compromite datele clienților. |
| **Securitatea cibernetică fizică** | Securitatea cibernetică fizică este protecția sistemelor cibernetice fizice, a dispozitivelor aferente obiectelor de internet, protecția oamenilor, a bunurilor și a bunurilor fizice de acțiuni și evenimente care ar putea provoca daune sau pierderi. |

# 5. AUDITURI DE SIGURANȚĂ CIBERNICE

## 5.1 CE ESTE UN AUDIT DE SIGURANȚĂ CIBERNICĂ?

A patra revoluție industrială sau Industria 4.0 a adus câteva noi tehnologii care leagă lumea fizică și cea digitală a proceselor de afaceri în sistemele inteligente integrate. Acest lucru aduce multe oportunități pentru îmbunătățirea proceselor și a performanței generale, dar și multe noi responsabilități și amenințări. Nivelul mai ridicat de conectivitate între toate sistemele prin Internetul obiectelor, cloud computing și multe alte tehnologii, în afară de multe beneficii, prezintă noi provocări pentru companii legate de securitatea informației, Big Data etc., care este procesată de aceste sisteme integrate. Acesta este motivul pentru care companiile și în special IMM-urile au nevoie de instrumente care să le sprijine în procesul de verificare și analiză a punctelor slabe ale acestora în ceea ce privește securitatea tehnologiilor din industria 4.0 pe care le au în vigoare. Un instrument eficient pentru a pune în aplicare această verificare este conducerea auditului de securitate cibernetică.

*Un audit de securitate cibernetică reprezintă o evaluare a performanței în raport cu specificațiile, standardele, controalele sau liniile directoare.*

Un audit de securitate cibernetică reprezintă o evaluare a performanței în raport cu specificațiile, standardele, controalele sau liniile directoare (CyLumena, 2020). Auditurile de securitate cibernetică se efectuează în mod obișnuit cu o listă de verificare a controalelor (biblioteca de controale) care sunt definite pe baza anumitor standarde de securitate cibernetică (național, internațional, intern pentru companie) și / sau procedurile și / sau politicile companiei. Scopul unui audit de securitate cibernetică este de a ajuta organizațiile să evalueze dacă au instituite mecanisme de securitate adecvate, identificând lacunele de securitate sau validând procedurile și politicile aplicate. Auditurile de securitate cibernetică ajută companiile să verifice ce este în rețeaua lor, ce trebuie protejat și ce lacune există în protecțiile existente, astfel încât să poată aduce îmbunătățiri (Dosal, 2020).

### AUDITURI CIBERALE DE SECURITATE VS. EVALUAREA SECURITĂȚII CIBERETICE

Auditurile de securitate cibernetică diferă de evaluările de securitate cibernetică. În timp ce auditul securității cibernetice este orientat pe existența anumitor controale stabilite, evaluarea securității cibernetice vizează evaluarea eficacității acestor controale (Aldorisio, 2020). Evaluările pot include un anumit grad de audit, dar nu întotdeauna. Auditurile de securitate cibernetică, în funcție de obiectiv, ar putea fi aplicate și atunci când o organizație dorește să evalueze conformitatea lor cu anumite legi sau standarde, în acest caz, de obicei, auditul este efectuat de o terță parte externă care are competența necesară. Evaluările securității cibernetice, pe de altă parte, ar putea fi efectuate intern de către persoanele din cadrul organizației care au o bună cunoaștere a infrastructurii de securitate cibernetică..

### AUDITURI DE SECURITATE CIBERNICĂ EXTERNE VS. INTERNE

Auditurile externe sunt efectuate de profesioniști, mai ales atunci când scopul auditului este de a oferi un motiv pentru certificare în conformitate cu anumite standarde de securitate cibernetică și evaluarea conformității cu standardele oficiale, legi etc. care conștientizează procesele companiei și arhitectura de securitate cibernetică. Conform GDPR (GDPR.EU N.d.), fiecare companie are obligația legală de a avea un responsabil desemnat cu protecția datelor, care să fie conștient de gestionarea datelor - ce informații intră și ies din companie, în ce procese sunt utilizate și cum sunt a manageriate. Prin urmare, în funcție de sfera auditului, o alegere naturală pentru efectuarea unui audit intern de securitate cibernetică ar putea fi responsabilul cu protecția datelor desemnat sau o echipă a companiei. În următoarele secțiuni ale acestui document vom prezenta o abordare combinată în vederea realizării unui audit și evaluare internă a securității cibernetice pe baza mai multor categorii menționate anterior, care trebuie luate în considerare în procesul de audit.


## 5.2 CUM SE DESFĂȘURĂ UN AUDIT INTERN DE CIBERSECURITATE?

Scopul acestei secțiuni este de a oferi îndrumări ușor de urmărit pentru conducerea auditului de auto-securitate cibernetică (audit intern de securitate cibernetică) care ar putea servi drept instrument eficient pentru evaluarea securității cibernetice și a datelor în cadrul organizației dvs. și / sau ca pregătire pentru audituri externe de securitate cibernetică (terță parte).

**PASUL 1: Definiți prioritățile de securitate ale organizației dvs. și sfera auditului**

În această etapă, persoana sau echipa desemnată să conducă auditul trebuie să identifice care va fi scopul procesului de audit. Un bun punct de plecare este să enumerăm toate activele cibernetice ale companiei, cum ar fi activele cibernetice asociate cu activele critice, cum ar fi: sistemele de control; Sisteme de achiziție de date; Echipamente de rețea; Platforme hardware pentru mașini virtuale sau stocare; Sisteme secundare sau de suport, cum ar fi scanere de viruși, sisteme HVAC și surse de alimentare neîntreruptibile (UPS) (n.d., Versify Solutions);

Apoi, trebuie să evaluați care sunt activele cibernetice critice (CCA). Conform standardului Critical Infrastructure Protection (CIP), versiunea 4 de către North American Electric Reliability Corporation (NERC) un CCA este „orice dispozitiv care utilizează un protocol rutabil pentru a comunica în afara perimetrului electronic de securitate (ESP), folosește un protocol rutabil dintr-un un centru de control sau este accesibil dial-up. ”(2011, Flick & Morehouse).

În cuvinte mai simple, activele pot varia de la echipamente computerizate la diverse sisteme și informații sensibile despre clienți și companii, documentație internă și sisteme de comunicații.

Odată ce activele cibernetice critice au fost identificate, va trebui să identificați unde se află parametrii critici de securitate și, astfel, să stabiliți ceea ce va fi inclus în domeniul auditului (2019, LeCount). Parametrii și activele de securitate vor varia foarte mult de la o companie la alta, prin urmare acest pas inițial și definirea corectă a sferei auditului sunt de o importanță crucială pentru eficiența procesului de audit. Odată ce sfera auditului este definită, puteți trece la pasul următor - identificarea amenințărilor potențiale.

**PASUL 2: Identificați riscurile și amenințările potențiale**

Pe baza interviurilor aprofundate cu 12 experți în domeniul securității cibernetice, consorțiul ENCRYPT 4.0 a identificat nouă categorii posibile de risc și a întocmit o listă a potențialelor amenințări pe care fiecare dintre aceste categorii le poate reprezenta activelor cibernetice critice. Modelul ENCRYPT implică următoarele nouă categorii de risc care trebuie luate în considerare: (1) Resurse umane; (2) Proprietatea intelectuală; (3) Securitatea sistemelor de control industrial (SCI); (4) Produse; (5) Riscuri juridice privind securitatea cibernetică; (6) Atacuri în lanțul de aprovizionare; (7) Tehnologie, TIC și siguranță operațională; (8) Clienți; (9) Securitate cibernetică fizică. Rețineți că, în funcție de activitățile de afaceri ale organizației dvs., de modelul de afaceri și de sectorul operațional, nu toate categoriile s-ar putea aplica pentru dvs. sau puteți decide că nu aveți active cibernetice critice aparținând acestor categorii. Pentru a face această evaluare consultați Anexa 1 și alegeți categoriile aplicabile organizației dvs. și

amenințările pe care le considerați relevante, în funcție de activele cibernetice esențiale identificate în cadrul companiei dvs.

### PASUL 3: Prioritizați riscurile

La acest pas crucial, trebuie să verificați lista potențialelor amenințări pe care le considerați aplicabile companiei dvs. și conform unui set de criterii pentru a decide care sunt riscurile extrem de probabile și cu un impact advers potențial mai grav. Din acest motiv, consorțiul ENCRYPT 4.0 a elaborat o metodologie de evaluare a riscurilor care ia în considerare următoarele componente:

- Costuri potențiale asociate cu consecințele riscului;
- Departamentul (departamentele) organizației care ar putea fi afectate;
- Impactul potențial;
- Probabilitate - atunci când evaluați probabilitatea, luați în considerare tendințele industriei, încălcările anterioare ale securității;
- Nivelul de risc.

Puteți utiliza direct instrumentul de evaluare a riscului de securitate cibernetică ENCRYPT 4.0 (MARC) dezvoltat pentru a prioriza cu ușurință riscurile potențiale.


### PASUL 4: Auditați măsurile de securitate actuale în vigoare

După ce ați identificat categoriile de riscuri și amenințările aplicabile organizației dvs., următorul pas este să evaluați dacă activele și infrastructura dvs. cibernetică critică sunt vulnerabile la oricare dintre aceste amenințări. În acest scop, trebuie să evaluați protocoalele / procedurile / măsurile de securitate stabilite în ceea ce privește identificarea potențialelor lacune de securitate care necesită soluționare. În tabelul 2, veți găsi câteva întrebări orientative și sfaturi despre cum să evaluați dacă măsurile de securitate în vigoare sunt adecvate, însă depinde și de amenințările pe care le considerați aplicabile în fiecare categorie.

**Tabelul 2. Sfaturi despre cum să identificați măsurile de securitate în vigoare**

| No. | Category | Tips on how to audit security measures in place |
|---|---|---|
| 1 | **Resurse umane** | Verificați distribuirea rolurilor și responsabilităților legate de gestionarea și securitatea datelor; securitate cibernetică; controlul sistemului etc.<br><br>Discutați cu angajații din aceste domenii desemnați ca fiind responsabili - întrebați-i cum ar reacționa în anumite situații, ce protocoale de securitate ar implementa, astfel veți putea evalua dacă personalul este conștient și pregătit în cazul realizării anumitor riscuri de securitate cibernetică; dacă au nevoie sau nu de instruire.<br><br>Analizați accidentele și încălcările de securitate din greșelile angajaților și modul în care au fost tratate. Gândiți-vă că se poate face ceva mai mult pentru a reduce în continuare apariția acestei amenințări în viitor. |
| 2 | **Proprietate intelectuală** | Verificați distribuirea rolurilor și responsabilităților legate de gestionarea proprietății intelectuale, precum și a secretelor comerciale etc.<br><br>Intervievează angajații responsabili, revizuiește documentația relevantă privind protecția activelor, cum ar fi brevete, drepturi de autor asupra mărcilor comerciale.<br><br>Cum este păstrată și gestionată această documentație, cine are acces la ea? Au existat incidente în trecut legate de încălcări de informații, lipsă de informații în acest domeniu? Referitor la modul în care au fost tratate, este actualizat protocolul de securitate? |
| 3 | **Securitatea sistemelor de control industrial (SCI)** | Cine are acces la distanță și / sau fizic la SCI?<br><br>Cum se administrează accesul la distanță al SCI? Există controale de securitate, cum ar fi autentificarea puternică, controlul accesului și criptarea pentru a proteja împotriva accesului neautorizat și exploatării acestor sisteme?<br><br>Care sunt măsurile de control al accesului fizic?<br><br>Folosiți firewall-uri sensibile la protocolul SCI pentru a impune controalele de acces la traficul de rețea SCI?<br><br>Aveți instalat un sistem de prevenire a intruziunilor? |
| 4 | **Produse** | În funcție de procesul de fabricație al produselor, trebuie să identificați în ce procese sunt tratate informațiile sensibile și în ce mod sunt gestionate și administrate.<br><br>Există secrete comerciale legate de producția produselor etc.<br><br>Cum se asigură compania că aceste informații sunt gestionate în siguranță? Care este protocolul - roluri și responsabilități, proceduri etc.? |

| | | |
|---|---|---|
| | | Există vreun control al accesului fizic și de la distanță la computere și rețele; sisteme de producție etc.? Cum sunt acestea securizate și controlate? |
| **5** | **Riscuri legale privind securitatea cibernetică** | Există vreun control al accesului fizic și de la distanță la computerele și rețelele companiei? Cum sunt acestea securizate și controlate?<br><br>Cum sunt gestionate și administrate datele legale?<br><br>Serverul este securizat? Cine are acces la aceste informații?<br><br>Au existat încălcări de securitate în trecut? Cum au fost tratate? Există o modalitate de a îmbunătăți protocoalele de securitate pe baza tendințelor / evenimentelor / dezvoltărilor tehnologice recente? |
| **6** | **Atacuri în lanțul de aprovizionare** | Cine are acces la sistemele de management al aprovizionării? Există un acces privilegiat al managementului?<br><br>Cine are acces la date sensibile? Cum este securizat acest acces?<br><br>Aveți implementate Honeytokens?<br><br>Care este nivelul de control al accesului de către furnizorii de servicii? Câți furnizori au acces la software?<br><br>Rețeaua furnizorului este monitorizată pentru vulnerabilități? |
| **7** | **Tehnologie, TIC și siguranță operațională** | Aveți politici stricte de securitate mobilă și de protecție a datelor?<br><br>Sunt toate aplicațiile software și sistemele de operare actualizate?<br><br>Există controale de acces pentru activele critice de securitate cibernetică??<br><br>Monitorizați activitatea conturilor de utilizator, logarea și accesul la rețeaua dvs.?<br><br>Verificați dacă firewall-urile sunt configurate corect, asigurați-vă că aveți criptare de la capăt la altul datele sensibile.<br><br>Aveți stabilite mecanisme pentru a recunoaște și a evita atacurile precum phishing-ul și pharming-ul? |
| **8** | **Clienți** | Cine are acces la date importante despre clienți?<br><br>Aveți copii de rezervă ale datelor și informațiilor importante despre afaceri? |
| **9** | **Securitatea cibernetică fizică** | Cum este gestionată întreținerea echipamentelor și a activelor critice de securitate cibernetică?<br><br>Cine are acces fizic la echipamente și active critice de securitate cibernetică? Cum este securizat accesul? |

### PASUL 5: Setați / actualizați protocoalele de securitate pe baza auditului

La finalizarea PASUL 4, trebuie să aveți lista de amenințări identificate aplicabile organizației dvs., să fiți conștienți de ceea ce faceți deja și ce poate că lipsește și să identificați controale adecvate de securitate a informațiilor pentru a neutraliza sau eradica riscul de amenințare (2020) , LeCount).

Controalele de securitate a informațiilor sunt măsuri luate pentru a reduce riscurile de securitate a informațiilor, cum ar fi încălcarea sistemelor de informații, furtul de date și modificările neautorizate ale informațiilor sau sistemelor digitale (Garcia, 2019). Scopul principal al controalelor de securitate este de a proteja disponibilitatea, confidențialitatea și integritatea datelor și rețelelor în cadrul unei companii. După cum s-a menționat, controalele de securitate sunt de obicei puse în aplicare după o evaluare a riscului de informare sau securitate cibernetică și reprezintă un rezultat dorit al evaluărilor și auditurilor de securitate cibernetică în ceea ce privește soluționarea lacunelor de securitate reale sau potențiale identificate.

În tabelul 3, în conformitate cu modelul de evaluare a riscului de securitate cibernetică ENCRYPT 4.0 bazat pe interviuri cu experți în securitate cibernetică din 6 țări ale UE, am identificat două tipuri de controale - preventive și corective în fiecare dintre cele nouă categorii de risc. Pe baza auditului efectuat în PASUL 4, sunteți deja la curent cu procedurile de securitate cibernetică în vigoare în cadrul organizației dvs. În tabelul 3, puteți găsi câteva sugestii de control preventiv și corectiv pentru fiecare dintre categoriile pe care este posibil să nu le fi avut în vedere în organizația dvs.

**Tabelul 3. Controale preventive și corective de securitate cibernetică**

| Categoria de risc | Măsuri preventive | Măsuri corective |
|---|---|---|
| **Resurse umane** | Stabiliți un program de formare și conștientizare<br><br>Identificați în mod clar gestionarea identităților, autentificarea și controlul acceselor<br><br>Compania are o politică care cuprinde:<br>● Lista software-ului autorizat.<br>● Depozitul software autorizat și registrul de licențe.<br>● Sancțiuni disciplinare asociate nerespectării acestor reglementări.<br><br>Schimbați parolele trimestrial („politica privind parolele puternice”)<br><br>Elaborați soluții de recuperare în caz de dezastru și planuri de continuitate a afacerii | Controlul permisiunilor utilizatorului<br><br>Implementați sistemul de detectare a intruziunilor (SDI) pentru a detecta accesul neautorizat la un computer sau la o rețea<br><br>Schimbați toate parolele după o posibilă încălcare a datelor<br><br>Blocați conturile suspectate de acces neautorizat<br><br>Configurați autentificarea cu doi factori atunci când este posibil, ceea ce va oferi o autentificare cu doi factori |

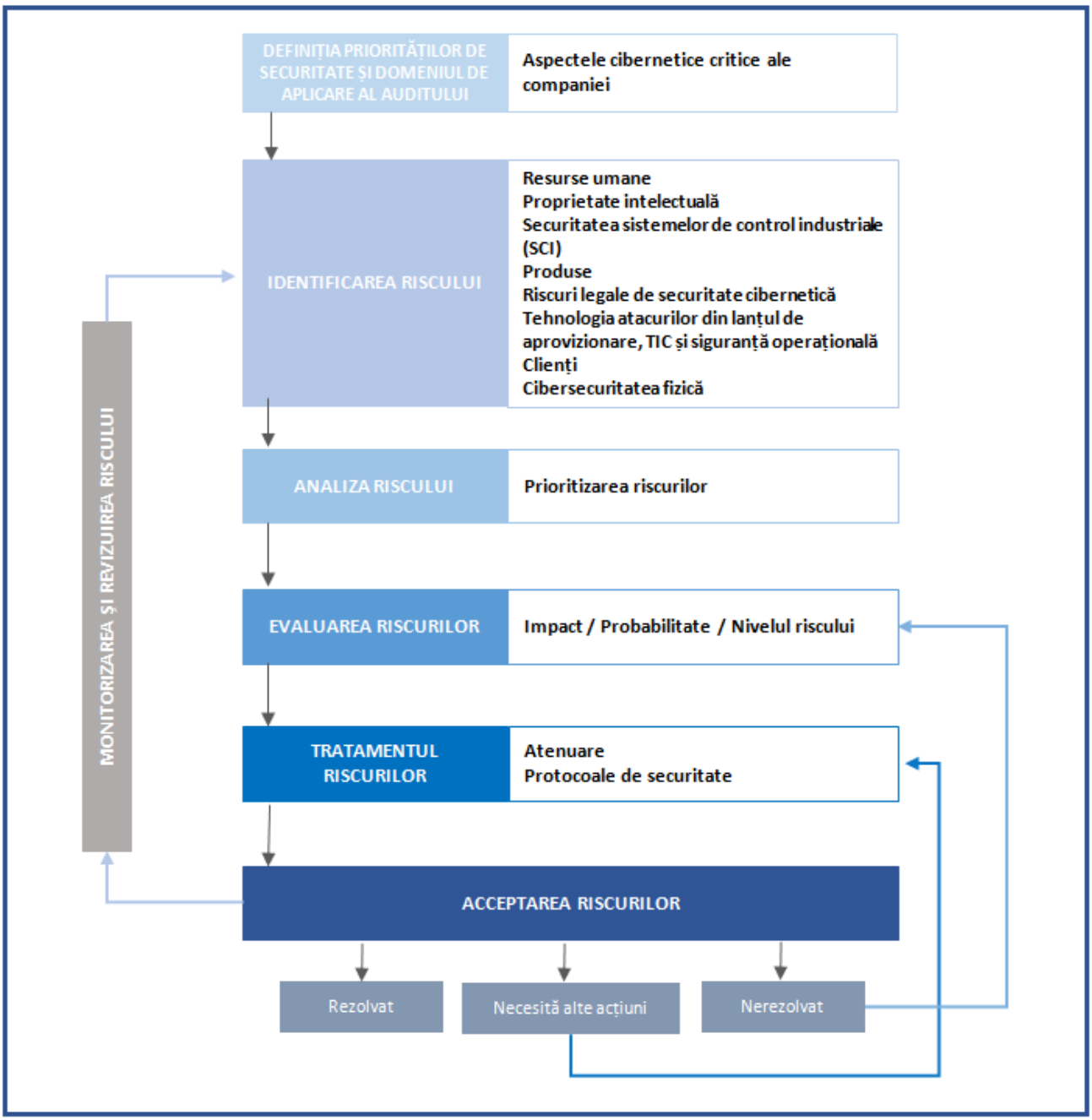
| Categoria de risc | Măsuri preventive | Măsuri corective |
|---|---|---|
| **Proprietate intelectuală** | Politici și responsabilități adecvate privind gestionarea proprietății intelectuale.<br><br>Toate activele aplicabile ar trebui protejate prin brevete înregistrate, drepturi de autor și mărci comerciale.<br><br>Activele relevante ar trebui monitorizate și protejate prin asigurări.<br><br>Dezvoltarea măsurilor, politicilor și responsabilităților privind gestionarea reputației. | Evaluarea periodică și actualizarea politicilor și responsabilităților.<br><br>Dacă nu aveți un brevet înregistrat, trebuie obținute un brevet provizoriu, mărci comerciale și drepturi de autor.<br><br>Evaluarea periodică și actualizarea politicilor și responsabilităților. |
| **Securitatea sistemelor de control industrial (SCI)** | Dezvoltarea de măsuri, politici, responsabilități și răspuns rapid în caz de incidență. | Evaluarea periodică și actualizarea politicilor și responsabilităților. |
| **Produse** | Evaluarea proceselor fluxului de lucru.<br><br>Standardizare și evoluție.<br><br>Controlați accesul fizic la computere și componentele de rețea. | Implementați o abordare stratificată pentru fiecare risc sau cel puțin pentru cei cu potențial ridicat în cazul specific, pentru a beneficia de cel puțin câteva straturi de protecție, indiferent când vine vorba de tehnologii, angajați, procese, clienți etc. |
| **Riscuri legale privind securitatea cibernetică** | Păstrați doar ceea ce aveți nevoie. Inventariați tipul și cantitatea de informații din fișierele dvs. și de pe computerele dvs.<br><br>Date de salvgardare.<br><br>Distrugeți înainte de eliminare.<br><br>Actualizați procedurile.<br><br>Educați / instruiți angajații.<br><br>Controlați utilizarea computerului.<br><br>Securizați toate computerele. | Identificați părțile afectate.<br><br>Anunțați persoanele afectate.<br><br>Căutați un consilier privind legislația. |
| **Atacuri în lanțul de aprovizionare** | Implementați Honeytokens.<br><br>Securizați managementul accesului privilegiat.<br><br>Identificați toate atacurile potențiale din interior.<br><br>Identificați și protejați resursele vulnerabile. | Verificați licențele în toate lanțurile de aprovizionare ale IMM-urilor.<br><br>Stabiliți datele de contact ale întreținerii preventive și corective a utilajelor IMM-urilor din întregul lanț de aprovizionare la nivel regional / local. |

| Categoria de risc | Măsuri preventive | Măsuri corective |
|---|---|---|
| | Minimizați accesul la datele sensibile.<br><br>Trimiteți periodic evaluări ale riscurilor de la terți.<br><br>Monitorizați rețeaua furnizorului pentru vulnerabilități.<br><br>Identificați toate scurgerile de date ale furnizorilor. | |
| **Tehnologie, TIC și siguranță operațională** | Descărcați și instalați actualizări de software pentru sistemele dvs. de operare și aplicații pe măsură ce acestea devin disponibile.<br><br>Sisteme de operare și firmware actualizate.<br><br>Instalați un firewall între internet și LAN.<br><br>Identificați activele critice.<br><br>Conștientizarea securității.<br><br>Backup și recuperare.<br><br>Vulnerabilitate și gestionarea patch-urilor.<br><br>Aplicați controale de acces.<br><br>Utilizați filtrarea conținutului și a listei albe.<br><br>Configurați corect punctele finale, stabiliți procese de răspuns la incidente.<br><br>Folosiți soluții și sisteme de amenințare-informații.<br><br>Firewall-urile configurate corect, politicile stricte de securitate mobilă, criptarea de la un capăt la altul, auditarea înregistrării și autorizarea dispozitivelor pentru accesarea rețelei sunt câteva dintre practicile care reduc amenințările din utilizarea dispozitivelor mobile într-o rețea corporativă.<br><br>Evaluați software-ul în conformitate cu principiile de securitate cibernetică.<br><br>Asigurați-vă că sistemele de operare și toate aplicațiile software sunt actualizate.<br><br>Asigurați-vă că datele sensibile sunt criptate. | Verificați toate termenele limită ale sistemului de operare și ale firmware-ului pe care le aveți în IMM-ul dvs. și supravegheați că toate sunt actualizate.<br><br>Instalați firewall-ul între Internet și LAN.<br><br>Eliminați software-ul ilegal sau nepermis din depozitul software.<br><br>Folosiți standarde pentru toate echipamentele informatice.<br><br>Configurați VPN dacă este necesar să vă conectați din exterior.<br><br>Identificarea și corectarea problemei. Auditarea și actualizarea politicilor și regulilor de securitate. |

| Categoria de risc | Măsuri preventive | Măsuri corective |
|---|---|---|
| | Folosiți software de protecție a datelor.<br><br>Monitorizați periodic activitatea conturilor de utilizator.<br><br>Gestionați setările de confidențialitate pentru aplicațiile mobile.<br><br>Aplicați controale stricte ale dispozitivelor pentru datele amovibile.<br><br>Stabiliți mecanisme de recunoaștere și evitare a atacurilor precum phishing-ul și pharming-ul.<br><br>Operare bazată pe politici și reguli de securitate. | |
| **Clienți** | Faceți copii de rezervă ale datelor și informațiilor importante despre afaceri. | Configurați autentificarea cu doi factori atunci când este posibil, ceea ce va oferi o autentificare cu doi factori.<br><br>Blocați conturile suspectate de acces neautorizat.<br><br>Blocați adresele IP ale actorilor suspectați de amenințare pe baza activităților detectate. |
| **Securitatea cibernetică fizică** | Implementarea unui plan de siguranță în caz de incendii, inundații, furturi, pierderi …<br><br>Opriți toate instrumentele sau echipamentele care nu sunt utilizate.<br><br>Să aveți o sursă de alimentare neîntreruptibilă de rezervă sau să obțineți o a doua sursă de energie de urgență.<br><br>Verificați periodic toate dispozitivele.<br><br>Faceți copii de rezervă.<br><br>Să aveți, de preferință, toate datele găzduite în cloud. | În incintă, urmăriți siguranța clădirilor și puneți în aplicare măsuri anti-incendiu.<br><br>Să aveți o baterie de rezervă pentru computer sau sau să obțineți o a doua sursă de energie de urgență.<br><br>Să faceți o „copie de securitate”.<br><br>Instalați un comutator de siguranță.<br><br>Înlocuiți sau remediați dispozitivele deteriorate sau afectate. |

## PREZENTARE GRAFICĂ A PROCESULUI CU AJUTORUL MARC

Este prezentată o imagine grafică de ansamblu a procesului de audit utilizând ca instrument Encrypt 4.0 MARC care prezintă măsurile corespunzătoare care trebuie luate de persoana responsabilă în IMM-urile producătoare pentru a efectua o analiză cuprinzătoare a proceselor lor, identificând riscurile cibernetice și susținându-le în proiectarea și stabilirea unor controale eficiente în funcție de natura progresivă a atacului cibernetic.




Encrypt 4.0 MARC este un proces sistematic, continuu. Este un proces ciclic care, odată ce a identificat, analizat, examinat, evaluat, abordat și acceptat riscurile, trebuie să efectueze un proces de monitorizare și revizuire a riscurilor. În cazul în care problema persistă, va trebui să aplicați acțiuni complementare suplimentare pentru a rezolva problema și, pentru aceasta, va trebui să reveniți la etapa anterioară a tratamentului de risc. Și dacă problema rămâne nerezolvată, va trebui să reevaluați riscul.

# 6. PROIECT ȘI PARTENERIAT

ENCRYPT 4.0

*Inițiativă comună de dezvoltare a forței de muncă cibernetice pentru a permite industriei europene să depășească lipsa de profesioniști în domeniul securității cibernetice*

Proiectul ENCRYPT4.0 (2020-1-RO01-KA202-079983) își propune să permită managementului IMM-urilor producătoare să adopte o abordare proactivă față de securitatea cibernetică, sprijinindu-le în procesul de analiză, identificare și abordare a riscurilor și amenințărilor cibernetice aplicabile organizației lor. Promovează învățarea interactivă bazată pe proiecte în ceea ce privește stimularea abilităților și competențelor în materie de securitate cibernetică ale angajaților IMM-urilor sau / și profesioniștilor în domeniul securității cibernetice.

"George Emil Palade" University of Medicine, Pharmacy, Sciences and Technology of Târgu Mureș - Romania

Project coordinator

European Center for Quality Ltd., Consulting company - Bulgary

Instituto de Soldadura e Qualidade, Technological institution - Portugal

Avantalia, technology-based SME - Spain

FH Joanneum, University of Applied Sciencies - Austria

PCX Management, Computers & Information Systems Ltd. - Cyprus

# REFERINȚE BIBLIOGRAFICE

Aldorisio, J., 2020. Best Practices for Cybersecurity Auditing [a Step-by-Step Checklist]. Security Scorecard. Retrieved from https://securityscorecard.com/blog/best-practices-for-a-cybersecurity-audit

Cybersecurity Ventures. (2019). *Cybersecurity Ventures Official Annual Cybercrime Report.* Retrieved from https://cybersecurityventures.com/annual-cybercrime-report-2019/

Cybersecurity Ventures. (2020). *Cybersecurity Ventures Official Annual Cybercrime Report.* Retrieved from https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

EU Agency for Cybersecurity. (2019). *Industry 4.0 Cybersecurity: Challenges & recommendations.*

European Union Agency for Cybersecurity. (2015). *Information security and privacy standards for SMEs - Recommendations to improve the adoption of information security and privacy standards in small and medium enterprises.* ENISA. doi: 10.2824/829076

Juncker, C. P.-C. (2017). Retrieved from https://www.europarl.europa.eu/RegData/etudes/ATAG/2019/637980/EPRS_ATA(2019)637980_EN.pdf

Margot Hutchins, R. B., & Stefanie Robinson, J. S. (2015). Framework for Identifying Cybersecurity Risks in. *U.S. Department of Energy*, 17.

National Institute for Standards and Technology. (2012). *Guide for Conducting Risk Assessments.* Gaithersburg: Special Publication 800-30.

Verizon. (2017). *Verizon Data Breach Investigations Report.* Retrieved from https://www.verizondigitalmedia.com/blog/2017-verizon-data-breach-investigations-report/

Verizon. (2020). *Manufacturing*. Retrieved from Verizon: https://enterprise.verizon.com/resources/reports/dbir/2020/data-breach-statistics-by-industry/manufacturing-data-breaches/

World Economic Forum . (2017). *Innovation-Driven Ciber-risk to Costumer Data in Financial Services.* Cologny/Geneva.

World Economic Forum. (2020). *The Global Risks Report.*

World Economic Forum. (2020). *Wild Wide Web - Consequences of Digital Fragmentation*. Retrieved from World Economic Forum: https://reports.weforum.org/global-risks-report-2020/wild-wide-web/

# ANEXA A - COLECȚIA STANDARDELOR EXISTENTE PENTRU RISCURILE DE SIGURANȚĂ CIBERNICĂ

| | STANDARDE PENTRU PROTECȚIA DATELOR ȘI A SIGURANȚEI CIBERNETICE |
|---|---|
| **Securitatea informațiilor (Industrie transversală)** | ISO/IEC 27001:2018 Information security management systems – Requirements |
| | ISO/IEC 27002:2018 Code of practice for information security controls |
| | ISO/IEC 27003:2017 Information security management systems guidance |
| | ISO/IEC 27004:2016Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation |
| | International Organisation for Standardisation and International Electrotechnical Commission |
| | ISO/IEC 27014:2013 Governance of information security |
| | ISO/IEC TR 27016:2014 Information security management - Organisational economics |
| | ISO/IEC 27032:2012 Guidelines for information security |
| | ISO/IEC 27033-1:2015 Network security - Part 1: Overview and concepts |
| | ISO/IEC 27033-2:2012 Network security - Part 2: Guidelines for the design and implementation of network security |
| | ISO/IEC 27033-3:2010 Network security - Part 3: Reference networking scenarios - Threats, design techniques and control issues |
| | ISO/IEC 27033-4:2014 Network security - Part 4: Securing communications between networks using security gateways |
| | ISO/IEC 27033-5:2013 Network security - Part 5: Securing communications across networks using Virtual Private Networks (VPNs) |
| | ISO/IEC 27033-6:2016 Network security - Part 6: Securing wireless IP network access |
| | ISO/IEC 27034-1:2011 Application security - Part 1: Overview and concepts |
| | ISO/IEC 27039:2015 Selection, deployment and operations of intrusion detection systems (IDPS) |
| | ISO/IEC 27040:2015 Storage security |
| | CSA Cloud Controls Matrix |
| | BSI PAS 555:2013 Cybersecurity risk. Governance and management. Specification |
| | PCI Data Security Standard |
| | ISF The Standard of Good Practice for Information Security |
| | UK Gov. Security policy framework |
| | UK Gov. Cyber essentials scheme |
| | ETSI GS ISI 001 Part 1: A full set of operational indicators for organisations to use to benchmark their security posture |
| | ETSI TR 103 305 Critical Security Controls for Effective Cyber Defence |
| | BSI 100-1 Information Security Management Systems (ISMS) |
| | BSI 100-2: IT-Grundschutz Methodology |
| | BSI 200-1 Information Security Management Systems (ISMS) |

| | |
|---|---|
| | BSI 200-2: IT-Grundschutz Methodology |
| | ISO/IEC 15408-1:2009 Evaluation criteria for IT security - Part 1: Introduction and general model |
| | ISO/IEC 15408-2:2008 Evaluation criteria for IT security - Part 2: Security functional components |
| | ISO/IEC 15408-3:2008 Evaluation criteria for IT security - Part 3: Security assurance components |
| | ISO/IEC 19790:2012 Security requirements for cryptographic modules |
| | ISO/IEC 27006:2015 Requirements for bodies providing audit and certification of information security management systems |
| | ISO/IEC 27007:2017 Guidelines for information security management systems auditing |
| | ISO/IEC 27014:2020 Governance of information security |
| | ISO/IEC 27017:2015: Code of practice for information security controls based on ISO/IEC 27002 for cloud services |
| | ISO/IEC 29147:2018: Vulnerability disclosure |
| | ISO/IEC 30111:2019: Vulnerability handling processes |
| | OENORM A 7700-3:201910 Web Applications - Part 3: Security requirements |
| | ISO/IEC 27701:2019Security techniques- Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines |
| | ISO/IEC TS 27100:2020Information technology -Cybersecurity- Overview and concepts |

| | **STANDARDE PENTRU PROTECȚIA DATELOR ȘI A SIGURANȚEI CIBERNETICE** |
|---|---|
| **Managementul riscurilor** | ISO/TR 31004:2013 Risk management - Guidance for the implementation of ISO 31000 |
| | ISO/IEC 27005:2016 Information security risk management |
| | ISO/IEC 31000 Risk management - Risk assessment techniques |
| | IEC 31010:2009 Risk management - Risk assessment techniques |
| | BSI BIP 0076 Information security risk management. Handbook for ISO/IEC 27001 |
| | BSI 100-3: Risk Analysis based on IT-Grundschutz |
| | BSI 200-3: Risk Analysis based on IT-Grundschutz |
| | ISO/IEC 27005:2018 Information security risk management |
| | ISO/IEC 27102:2019Information security management — Guidelines for cyber-insurance |

| | **STANDARDE PENTRU PROTECȚIA DATELOR ȘI A SIGURANȚEI CIBERNETICE** |
|---|---|
| **Managementul continuității activității** | ISO 22301:2012 Business continuity management systems – Requirements |
| | ISO 22313:2012 Business continuity management systems – Guidance |
| | ISO/IEC 27031:2011 Guidelines for information and communication technology readiness for business continuity |
| | 100-4: Business Continuity Management |
| | OENORM A 7700-4:201910 Web Applications - Part 4: Requirements for secure operations |

| | STANDARDE PENTRU PROTECȚIA DATELOR ȘI A SIGURANȚEI CIBERNETICE |
|---|---|
| **Protecția datelor și confidențialitatea** | ISO/IEC 27018:2014 Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors |
| | ISO/IEC 29100:2011 Privacy framework |
| | ISO/IEC 29101:2013 Privacy architecture framework |
| | BSI BS 10012:2009 Data protection. Specification for a personal information management system |
| | CEN CWA 16113:2010 Personal Data Protection Good Practices |
| | OEVE/OENORM 17529:2020: Data protection and privacy by design and by default |
| | OENORM A 7700-2:201912 Web Applications - Part 2: Data protection requirements |
| | ISO/IEC 27018:2019: Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors |
| | ISO/IEC 29134:2017: Guidelines for privacy impact assessment |
| | ÖNORM EN 419231:2019 11 01: Protection profile for trustworthy systems supporting time stamping |
| | ÖNORM EN 419241-1:2019 03 15: Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements |
| | ÖNORM EN 419241-2:2019 06 01: Trustworthy Systems Supporting Server Signing - Part 2: Protection profile for QSCD for Server Signing |

| | **STANDARDE PENTRU PROTECȚIA DATELOR ȘI A SIGURANȚEI CIBERNETICE** |
|---|---|
| **Gestionarea incidentelor** | ISO/PAS 22399:2007 Societal security - Guideline for incident preparedness and operational continuity management |
| | ISO/IEC 27036-2:2014 Information security for supplier relationships - Part 2: Requirements |
| | ISO/IEC 27036-3:2013 Information security for supplier relationships - Part 3: Guidelines for information and communication technology supply chain security |
| | ISO/IEC 27035-1:2016 Information security incident management — Part 1: Principles of incident management |
| | ISO/IEC 27035-1:2016 Information security incident management — Part 2: Guidelines to plan and prepare for incident response |

| | **STANDARDE PENTRU PROTECȚIA DATELOR ȘI A SIGURANȚEI CIBERNETICE** |
|---|---|
| **Managementul terță parte** | ISO/IEC 27036-1:2014 Information security for supplier relationships - Part 1: Overview and concepts |
| | ISO/IEC 27035:2011 Information security incident management |
| | ISO/IEC 27037:2012 Guidelines for identification, collection, acquisition and preservation of digital evidence |

| | **STANDARDE PENTRU PROTECȚIA DATELOR ȘI A SIGURANȚEI CIBERNETICE** |
|---|---|
| **Securitate industrială** | OVE EN IEC 62443-4-1:2018 11 01: Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements |
| | OVE EN IEC 62443-4-2:2020 01 01: Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components |
| | OVE IEC TS 62351-100-1:2020 06 01 |