Co-funded by the Erasmus+ Programme of the European Union

# Module de instruire InCyT

| | |
|---|---|
| **Securitatea informațiilor pentru manageri**<br>**Unitatea 4 Săptămâna 7 si 8**<br>**Denumirea unității : Risc cibernetic și rezistență** | |
| ***Activități de învățare*** | ❑ **Webinar** ❑ **Exerciții** ❑ **Workshop** ❑ **Prezentare** ❑ **Alte** |
| ***Responsabil de învățare*** | • Simon Tjoa<br>• Peter Kieseberg |
| ***Obiectivele activității de învățare*** | 1. Participanții cunosc bazele managementului riscului și rezilienței<br>2. Participanții sunt capabili să efectueze analize de impact asupra afacerii și analize de risc<br>3. Din rezultatele analizelor participanții pot deduce contramăsuri și decizii de securitate |
| ***Abilități de dobândit*** | • IS 1, IS 3<br>• MS 1 |
| ***Durata activității de învățare*** | 2 săptămâni<br>• Săptămâna 7 (2 hours)<br>• Săptămâna 8 (2 hours) |
| ***Cerințe de învățare*** | ***Ce e necesar?*** |
| | • Abilități de management de bază<br>• Abilități IT de bază<br>• Abilități de bază de securitate |

## Informații scurte despre modul

| Descriere |
| --- |
| Securitatea perfectă nu este posibilă. Știind acest lucru, este vital să luați decizii informate cum să cheltuiți banii pentru măsurile de securitate corecte. Managementul riscului cibernetic și al rezilienței oferă un set vital de instrumente și tehnici pentru a evalua starea actuală de securitate a unei organizații și pentru a planifica controale pentru a menține riscul de securitate a informațiilor la un nivel acceptabil. |

## Conținutul materialului de învățare

Fără să-ți asumi riscuri, este imposibil să faci afaceri. Prin urmare, managementul riscului și instrumentele și tehnicile corespunzătoare oferă o modalitate sistematică de abordare a riscului. Întrebările precum cât de multă securitate este suficientă sau care contramăsuri ar trebui implementată mai întâi primesc răspuns de managementul riscului. Astfel, managementul riscului este o activitate importantă pentru a permite decizii informate. Standardele importante și cele mai bune practici care abordează acest subiect esențial includ ISO 27005, ISO 31000 sau BSI 200-3.

Înainte de a analiza mai atent procesul de management al riscului, este esențial să definiți termenii esențiali:

- **Vulnerabilitatea:** "Slăbiciune a unui sistem informațional, proceduri de securitate a sistemului, controale interne sau implementare care ar putea fi exploatate sau declanșate de o sursă de amenințare."[1]
- **Control:** "O protecție sau contramăsuri prescrise pentru un sistem informatic sau o organizație concepută pentru a proteja confidențialitatea, integritatea și disponibilitatea informațiilor sale și pentru a îndeplini un set de cerințe de securitate definite."[2]
- **Amenințare:** "Orice circumstanță sau eveniment cu potențialul de a avea un impact negativ asupra operațiunilor organizaționale (inclusiv misiunea, funcțiile, imaginea sau reputația), activele organizaționale, indivizii, alte organizații sau Națiunea printr-un sistem de informații prin acces neautorizat, distrugere, dezvăluire, modificare a informațiilor , și/sau refuzul serviciului."[3]

[1] https://csrc.nist.gov/glossary/term/vulnerability
[2] https://csrc.nist.gov/glossary/term/security_control
[3] https://csrc.nist.gov/glossary/term/threat

- Risc: „O măsură a măsurii în care o entitate este amenințată de o circumstanță sau un eveniment potențial și, de obicei, este o funcție de: (i) impactul negativ sau amploarea prejudiciului, care ar apărea dacă circumstanța sau evenimentul ar avea loc. ; și (ii) probabilitatea apariției."
  „efectul incertitudinii asupra obiectivelor "[4]

Din definiția ISO 31000 („efectul incertitudinii"), putem deduce că riscurile pot avea efecte pozitive și negative. Adesea, dacă riscurile au impact pozitiv, ele sunt denumite oportunități.

Procesul general de management al riscului începe cu domeniul de aplicare, contextul și criteriile. Deoarece nu toate riscurile pentru toate activitățile pot fi analizate, este important să se prioritizeze și să se decidă ce servicii, procese și unități organizaționale ar trebui incluse în evaluare. A avea un domeniu de aplicare adecvat este crucial pentru a asigura rezultate valide, pe de o parte, și efort rezonabil, pe de altă parte. Contextul este mediul intern și extern. Determinarea criteriilor de risc este importantă pentru a asigura un proces repetabil, care să conducă la rezultate comparabile. Criteriile ar trebui definite astfel încât diferitele persoane să poată evalua riscurile într-un mod comun.

Exemplele de criterii includ criterii de impact (de exemplu, scăzut, mediu, ridicat) pentru diferite dimensiuni, cum ar fi financiar, reputație sau sănătate.

În cele ce urmează, este prezentat un exemplu de OCTAVE Allegro privind reputația și impactul clienților:

| Allegro Worksheet 1 | RISK MEASUREMENT CRITERIA – REPUTATION AND CUSTOMER CONFIDENCE | | |
|---|---|---|---|
| Impact Area | Low | Moderate | High |
| Reputation | Reputation is minimally affected; little or no effort or expense is required to recover. | Reputation is damaged, and some effort and expense is required to recover. | Reputation is irrevocably destroyed or damaged. |
| Customer Loss | Less than _____% reduction in customers due to loss of confidence | _____to _____% reduction in customers due to loss of confidence | More than _____% reduction in customers due to loss of confidence |
| Other: | | | |

*Figura 1: Criterii de măsurare pentru reputație* [5]

[4] https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en
[5] https://resources.sei.cmu.edu/asset_files/technicalreport/2007_005_001_14885.pdf

După definirea criteriilor de risc și a domeniului de aplicare, primul pas este identificarea riscurilor. Identificarea riscurilor este crucială, deoarece pot fi evaluate doar acele riscuri care sunt identificate. Prin urmare, este logic să comparăm amenințările identificate cu listele de amenințări ale ISO 27005, MEHARI sau alte bune practici sau standarde.

Există diverse tehnici de identificare a riscurilor, cum ar fi brainstorming, tehnica Delphi, analiza modului de eșec și a efectelor (FMEA) sau studii de pericol și operabilitate (HAZOP).

În următoarea etapă a analizei riscului, se obține o mai bună înțelegere a riscurilor identificate. Prin urmare, se determină probabilitatea/frecvența de apariție și impactul/consecințele. Pentru a determina consecințele, este important să se definească un mod sistematic în care sunt evaluate impacturile. Adesea, o măsură calitativă (de exemplu, scăzută, medie, ridicată) este mai ușor de utilizat decât măsurile cantitative.

Riscurile sunt adesea vizualizate într-o așa-numită matrice de risc, care evidențiază riscul folosind probabilitatea și impactul ca axe.

| Probability | Harm severity | | | |
|---|---|---|---|---|
| | Minor | Marginal | Critical | Catastrophic |
| Certain | High | High | Very high | Very high |
| Likely | Medium | High | High | Very high |
| Possible | Low | Medium | High | Very high |
| Unlikely | Low | Medium | Medium | High |
| Rare | Low | Low | Medium | Medium |
| Eliminated | Eliminated | | | |

*Figura 2: Matricea de risc [Sursa Wikipedia][6]*

În pasul următor, riscurile sunt evaluate. Aceasta înseamnă că rezultatele pasului anterior sunt luate în considerare pentru a decide dacă ar trebui luate măsuri. În plus, are loc o prioritizare a riscurilor.

În continuare, se determină una dintre cele patru strategii principale de abordare a riscurilor:

- Acceptarea riscului: documentați și monitorizați riscul dacă riscul se încadrează în apetitul pentru risc al organizației
- Transferul de risc: riscuri de împărțire (de exemplu, asigurări, asocieri în participațiune)
- Evitarea riscurilor: eliminați sursa de risc (de exemplu, golul de aer)

[6] https://en.wikipedia.org/wiki/Risk_matrix

- Reducerea riscurilor: reduceți impactul sau probabilitatea de apariție (de exemplu, controlul accesului)

După determinarea măsurilor, se evaluează dacă riscul rezidual este acceptabil sau dacă trebuie luate măsuri suplimentare.

Ca activități de sprijin pe lângă procesul principal de evaluare a riscurilor, au loc comunicarea riscurilor (adică comunicarea cu părțile interesate relevante), monitorizarea riscurilor și raportarea riscurilor.

Deoarece nu toate riscurile pot fi luate în considerare, spre deosebire de managementul riscurilor, continuitatea afacerii și reziliența se concentrează pe activitățile critice în loc de riscurile individuale. În acest fel, este posibil să vă pregătiți pentru riscuri necunoscute și cu probabilitate scăzută/impact ridicat.

Pentru asigurarea unui program eficient de continuitate a afacerii, sprijinul managementului de vârf este vital. Un artefact important care evidențiază importanța managementului continuității afacerii este politica de continuitate a afacerii. În acest document, acceptarea managementului este exprimată formal. În plus, documentul evidențiază sfera și obiectivele activităților de continuitate a activității, rolurile și responsabilitățile importante (de exemplu, managerul continuității afacerii), precum și cadrul operațional utilizat pentru realizarea programului. Trebuie subliniat că domeniul de aplicare nu ar trebui să fie prea larg pentru a se asigura că complexitatea analizei, precum și efortul nu devin prea mari.

Pentru a înțelege efectele întreruperilor de servicii asupra afacerii și pentru a avea o bază bună pentru planificarea măsurilor de redresare, se efectuează analize de impact asupra afacerii. Este instrumentul central în cadrul procesului de continuitate a afacerii și surprinde relevanța/semnificația produselor/serviciilor. Pe lângă criticitatea produselor/serviciilor, dependențele acestora sunt determinate și evaluate.

Cifrele cheie importante, care sunt utilizate atunci când se efectuează o analiză de impact asupra afacerii includ:

- **MAO (maximum acceptable outage):** „timpul necesar pentru ca efectele negative […], care pot apărea ca urmare a nefurnizării unui produs/serviciu sau a desfășurării unei activități […], să devină inacceptabile”[7]
- **RTO (recovery time objective):** “perioada de timp care urmează unui incident […] în care un produs și serviciu […] sau o activitate […] este reluată sau resursele […] sunt recuperate”[8]

[7] MAO, https://www.iso.org/obp/ui#iso:std:iso:22300:ed-3:v1:en
[8] RTO, https://www.iso.org/obp/ui#iso:std:iso:22300:ed-3:v1:en

- **RPO (recovery point objective):** "punctul în care informațiile [...] utilizate de o activitate [...] sunt restaurate pentru a permite activității să funcționeze la reluare"[9]

În primul pas, sunt identificate produsele și serviciile cele mai critice sau esențiale. După identificare, se evaluează ce daune ar apărea în timp dacă un anumit produs sau servicii este întrerupt sau întrerupt.

Figura următoare arată cum impactul în timp ar putea fi captat într-o foaie de calcul.

| Assessment Period / Damage Category | 1 Hour(s) | 2 Hour(s) | 4 Hour(s) | 8 Hour(s) | 24 Hour(s) | 48 Hour(s) | 96 Hour(s) | 168 Hour(s) | 240 Hour(s) | 720 Hour(s) |
|---|---|---|---|---|---|---|---|---|---|---|
| Financial | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 3 | 4 | 4 |
| Health & Safety | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 3 | 4 | 4 |
| Legal, Regulatory & Contractual | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 2 | 2 | 2 |
| Brand and Reputation | 0 | 0 | 0 | 1 | 1 | 1 | 2 | 4 | 4 | 4 |
| Environmental | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Rational for the assessment (Description) Verbal Description of Implications | | | | | | | | | | |

În plus, studiile de analiză a impactului asupra afacerii de care depind procesele, activitățile și serviciile relevante. În acest fel, pot fi determinate cifre cheie importante, cum ar fi obiectivul de timp de recuperare, obiectivul punctului de recuperare și întreruperea maximă acceptabilă.

După cunoașterea criticității proceselor, serviciilor și resurselor, se elaborează strategii de continuitate a afacerii. Strategiile includ, printre altele, diversificarea (de exemplu, activități în locuri separate geografic), replicarea (de exemplu, copierea datelor pentru a le recupera pe alt site) sau subcontractarea (de exemplu, utilizarea serviciilor terților).

Pe baza strategiilor sunt scrise planuri de continuitate a afacerii, care sprijina organizatiile sa reactioneze eficient in urma unui incident. Pentru a fi utilizabil în situații de mare presiune este vital ca planurile să fie scrise în consecință. Aceasta înseamnă că planurile ar trebui să conțină doar acele informații care sunt relevante în timpul gestionării unui incident. În plus, informațiile ar trebui să fie rapid de înțeles. Astfel, ar trebui utilizate liste de verificare clare și orientate spre acțiune.

[9] RPO, https://www.iso.org/obp/ui#iso:std:iso:22300:ed-3:v1:en

Planurile tipice de continuitate a afacerii conțin informații despre scopul, domeniul de aplicare, structura de gestionare a incidentelor, roluri și responsabilități, activarea planului, aranjamentele de recuperare și detalii de contact.

Pentru a repeta și a verifica adecvarea planurilor se folosesc diferite tipuri de exerciții. Acestea pot fi fie exerciții bazate pe discuții, cum ar fi verificări de birou sau exerciții de masă, fie exerciții tehnice, cum ar fi testarea restabilirii anumitor sisteme.

## Întrebări:

Consultați documentele Word

## Atasamente:

Consultați fișierele Powerpoint și Video

## Referințe:


- ISO 22301:2019, Security and resilience — Business continuity management systems — Requirements
- ISO 22313:2020, Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301
- ISO/TS 22317:2021, Security and resilience — Business continuity management systems — Guidelines for business impact analysis
- ISO/TS 22331:2018, Security and resilience — Business continuity management systems — Guidelines for business continuity strategy
- ISO/TS 22332:2021, Security and resilience — Business continuity management systems — Guidelines for developing business continuity plans and procedures
- ISO 31000:2018, Risk management — Guidelines, https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en
- IEC 31010:2019, Risk management — Risk assessment techniques