URS CERTIFICĂRI

CERTIFICĂM PERFORMANȚA

## Securitatea informațiilor și continuitatea afacerii

# Implementarea standardelor ISO 27001 și ISO 22301 în organizațiile din industria IT

Dragoș Petrescu
Lead Auditor

# Cuprins

# Elemente specifice standardului ISO 27001:2013

## Ce reprezintă standardul ISO 27001:2013 – Securitate informațională?

Pe măsură ce riscurile cu privire la atacuri informatice ce au ca destinație bazele de date, securitatea informațiilor devine o problemă critică, de actualitate, ba chiar iminentă pentru toate organizațiile, indiferent de profilul specific de activitate.
O abordare corespunzătoare trebuie să fie capabilă să prevină atât atacurile externe cât și amenințările interne comune, precum este eroarea umană.

**ISO 27001:2013** este standardul internațional adecvat acestor situații, întrucât furnizează specificațiile, termenii și cerințele unui **Sistem de Management al Securității Informaționale (SMSI)**.
Acesta este un proces sistematic care ia în considerare personalul, procesele și echipamentul pentru a proteja și gestiona securitatea informațiilor pentru organizație.

**Standardul 27001:2013** se concentrează pe protejarea a **3 aspecte principale** care vizează securitatea informațiilor:

**Confidențialitatea:** informația nu trebuie să fie disponibilă sau divulgată către terțe persoane, entități sau procese neautorizate)

**Integritatea:** informația este completă și exactă și este protejată de pierderea integrității morale)

**Disponibilitatea:** informația este accesibilă și se poate utiliza atunci când utilizatorii autorizați au nevoie de aceasta

## De ce optează organizațiile din industria IT pentru implementarea standardului ISO 27001:2013?

1. pentru securizarea informațiilor în toate formele sale (informații digitale, informații arhivate în formă fizică sau stocate online, în serviciul de cloud)

2. sporirea rezistenței în cazul unui atac informatic, prin instalarea unui sistem de software dedicat sau prin implementarea unui sistem de proceduri de lucru pe care personalul trebuie să îl urmeze

3. protejarea activității organizației se referă la protejarea datelor în cazul neatenției pesonalului, care poate periclita informații, sau în cazul procedurilor incomplete, care nu acoperă plaja riscurilor potențiale de pierdere a informațiilor

4. răspunde constant noilor provocări de securitate, întrucât este un sistem care se îmbunătățește

5. „plan-do-check-act”, menit să testeze în mod sistematic posibile soluții, să evalueze rezultatele și să le implementeze pe cele care efectiv funcționează, raportat la situația dată

6. reducerea costurilor cauzate de eventualele pierderi ale informației (SMSI urmărește să evalueze și să trateze riscurile într-un mod eficient, cu asigurarea faptului că organizația își va maximiza rentabilitatea investiției)

## Mai mult decât atât, standardul ISO 27001:2013 vine în sprijinul organizațiilor din industria IT facilitând conformitatea cu cerințele legale specifice:

### GDPR

General Data Protection Regulation (Regulamentul general privind protecția datelor), conform Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE, care, începând cu data de 25 mai 2018, a intrat în vigoare și se aplică în mod direct în toate statele membre ale Uniunii Europene.


### NIS Regulations

Network and Information Systems Regulations (Reglementări privind rețelele și sistemele informaționale), conform Legii nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice, care a intrat în vigoare la data de 12 ianuarie 2019 și transpune Directiva NIS (Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsurile adoptate pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniunea Europeană.

## Cum se implementează standardul ISO 27001:2013 în organizațiile din industria IT?

**ISO/IEC 27001** este împărțit în 11 secțiuni, plus anexa A.
Secțiunile de la 0 la 3 sunt introductive (și nu sunt obligatorii în vederea implementării), la care se adaugă secțiunile de la 4 la 10 (obligatorii).
În consecință, toate cerințele trebuie să fie implementate la nivelul organizației dacă se dorește conformitatea cu **standardul ISO 27001:2013.**

Pe de altă parte, **standardul ISO 27001:2013** cuprinde, în plus, Anexa A, una dintre cele mai cunoscute publicații **ISO**, care prevede 114 posibile puncte de control, de urmărit și implementat.

**Organizațiile IT**, împreună cu **consultanții ISO**, compară măsurile implementate anterior publicării anexei A cu cerințele cuprinse în această anexă, ca apoi să implementeze punctele lipsă de control, mai exact:

1. politica firewall
2. conștientizarea personalului
3. monitorizarea riscurilor
4. managementul incidentelor

**Standardul ISO 27001:2013** este proiectat să sprijine organizațiile în administrarea practicilor de securitate într-un mod consecvent și rentabil.
Mai mult, este universal aplicabil, ceea ce înseamnă că poate fi implementat în orice tip de organizație indiferent de domeniul si tipul de activitate, dimensiune, privată sau de stat.

# II. Elemente specifice standardului ISO 22301:2012

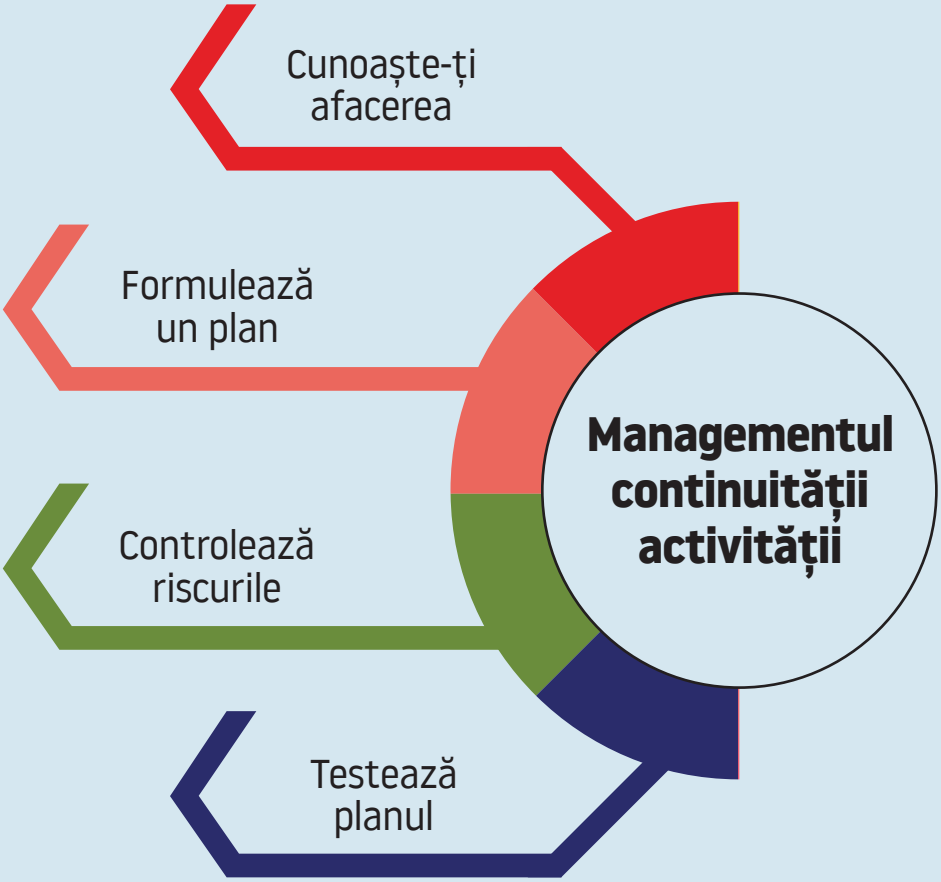
## Ce reprezintă standardul ISO 22301:2012 - Managementul continuității activității?

**Managementul continuității activității**, sau BCM (Business continuity management) este o modalitate de a administra riscurile și expunerea la amenințări prin dezvoltarea unei **strategii** care explică modul în care va funcționa organizația la un nivel acceptabil și prin ce metode se pot restabili procesele critice în cazul perturbării afacerii.

**Standardul ISO 22301:2012** oferă mai mult decât un scut de apărare împotriva atacurilor cibernetice și a breșelor de securitate.

Acest standard este relevant și în cazul:

- dezastrelor naturale
- incendiilor
- defecțiunilor tehnologice
- perturbărilor lanțului de aprovizionare
- protejării reputației etc.



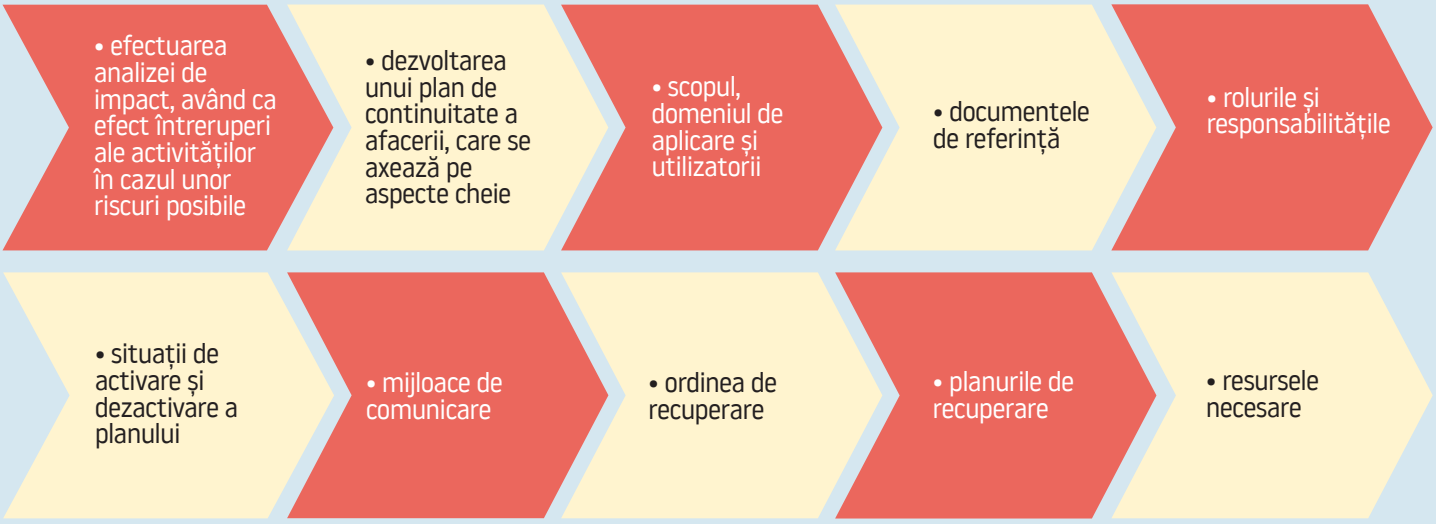
## De ce optează organizațiile din industria IT pentru implementarea standardului ISO 22301:2012?

**Obiectivul** principal al organizațiilor care aleg să implementeze **standardul ISO 22301** este de a se asigura că sunt capabile să își **continue activitatea fără întrerupere.**
Astfel, luând în considerare atât amenințările provenite din mediul intern, cât și cele din mediul extern, organizațiile IT continuă să livreze serviciile specifice, chiar și în urma unui eveniment major.

## Cum se implementează standardul ISO 22301:2012 în organizațiile din industria IT?

Împreună cu consultanții ISO, organizațiile IT aleg o abordare care pornește de la efectuarea unei analize de risc: organizația trebuie să determine riscurile actuale, cât și riscurile viitoare.

Totodată se determină perioadele de nefuncționare acceptabile pentru organizație și punctele critice predispuse la deformare în cazul perioadelor de nefuncționare îndelungate.



# Concluzii

În concordanță cu standardul **ISO 27001:2013**, standardul **ISO 22301:2012** este neutru din punct de vedere al modului de implementare, ceea ce înseamnă că se poate aplica oricărei organizații, indiferent de dimensiune sau domeniu de activitate.
În raport cu cele de mai sus, implementarea prezentelor standarde este dezirabilă pentru orice organizație care dorește să limiteze timpul de stopare a activității în caz de incidente neprevăzute și să își mențină capacitatea de a acționa rapid în aceste situații, totodată menținând controlul asupra efectelor nedorite.
Standardele **ISO 27001:2013**, respectiv **ISO 22301:2012** au capacitatea de a crește operativitatea și reputația organizației, întrucât funcțiile critice ale organizației continuă să activeze, păstrându-și rolul de actor important pe piață.