AROBS
Transilvania Software

POLITICĂ

Risk Management

(P-GEN-8)

ISTORIE DOCUMENT

VERSIUNE	AUTOR	DESCRIERE	DATA	APROBARE
2.0	RMSI Team	Emitere inițială	17 January 2024	Management Executiv
3.0	RMSI Team	Adaugare detalii de sustainabilitate	25 November 2025	Consiliul de administrare

CONȚINUT

1. SCOP & APLICABILITATE

Această politică descrie procesul și responsabilitățile privind identificarea și evaluarea riscurilor asociate activităților de afaceri și sustenabilității (forța de muncă proprie, lanțul valoric, comunitățile afectate, utilizatorii finali, riscurile financiare, impactul climatic, riscurile geopolitice etc.). Aceasta acoperă acele aspecte pe care organizația le poate controla sau influența, inclusiv dezvoltările planificate sau noi și activitățile modificate. Scopul este de a identifica, analiza, evalua, gestiona, controla și raporta riscurile care apar pe parcursul tuturor activităților companiilor din grup și de a implementa măsuri de control adecvate pentru societatea AROBS Transilvania Software SA si la nivel de Grup.

Politicase aplică persoanelor responsabile de gestionarea riscurilor, evaluarea riscurilor sau implementarea controalelor pentru atenuarea riscurilor, inclusiv șefilor de departamente, coordonatorului de sustenabilitate sau Comitetului de Sustenabilitate (dacă este disponibil), managerilor de proiect și deținătorilor de resurse, atat la nivelul companiei AROBS cat si la nivel de Grup.

Consiliul de Administratie stabilește natura și amploarea riscurilor pe care Societatea este dispusă să și le asume pentru atingerea obiectivelor strategice (apetitul pentru risc) și se asigură că există structuri, politici și proceduri adecvate pentru identificarea, evaluarea, raportarea, gestionarea și monitorizarea riscurilor semnificative și emergente, inclusiv cele legate de durabilitate, securitate cibernetică și utilizarea tehnologiilor digitale. De asemenea, Consiliul trebuie să descrie în raportul anual mecanismele și procesele de administrare a riscurilor.

Consiliul adoptă o politică formală de management a riscurilor care asigură identificarea, măsurarea și raportarea corectă, completă și la timp a riscurilor, implementarea unor măsuri adecvate de control și integrarea riscurilor de mediu și sociale (E&S) în cadrul general de management al riscurilor.

2. DEFINIȚII & ABREVIERI

AROBS – AROBS Transilvania Software SA;
Consiliul- Consiliul de Administratie ;
Grupul – totalitatea companiilor in care Arobs Transilvania Software SA este actionar majoritar;
Resurse - orice valoare pentru organizație.
Risc - efectul incertitudinii asupra obținerii rezultatelor dorite; riscul trebuie privit ca o combinație între probabilitate și impact.
Identificarea Riscului - proces global de analiză și evaluare a riscurilor.
Analiza riscurilor – utilizarea sistematică a informațiilor pentru a identifica sursele și a estima riscul.
Evaluarea riscurilor – procesul de evaluare a riscurilor pe baza criteriilor de risc agreate și a importanței riscului evaluat.
Managementul riscurilor – activități de coordonare pentru a ghida și controla o organizație, luând în considerare riscurile.

Tratare riscurilor - procesul de selecție și implementare a măsurilor pentru atenuarea riscului.
Măsură de securitate (mijloc de control) – un mijloc de abordare a riscului, incluzând politici, proceduri, ghiduri, practici, echipamente, dispozitive, acțiuni sau structuri organizaționale, care pot avea natură administrativă, tehnică, managerială sau juridică.
Risc Inerent - nivelul de risc care există atunci când o amenințare nu este tratată sau abordată.
Risc Rezidual - riscul care rămâne după tratarea riscului.
Amenințare – cauză potențială a unui incident nedorit care ar putea conduce la deteriorarea unui sistem sau a unei organizații.
Vulnerabilitate - slăbiciune a unei resurse sau a unui grup de resurse ori a unei măsuri de securitate, care ar putea fi exploatată de una sau mai multe amenințări.

IMSR - Responsabil pentru Sistemul de Management Integrat
PM – Manager de Proiect
HoD – Șef de Department
SC –Coordinator de sustenabilitate
ISMS –Sistem de Management al Securității Informației

3. REFERINȚE

SR ISO/IEC 27001:2022 – Information Security Management System.
ISO/IEC 27005 – Information Security Risk Management. Guidelines.
SR ISO 31000:2009 – Risk management - Principles and guidelines.
SR EN ISO 9001:2015 – Quality Management Systems. Requirements.
SR EN ISO 14001:2015 – Environmental Management Systems. Specifications and guidelines for use.
SR EN ISO 45001:2018 – Occupational Health and Safety Management systems. Specifications and guidelines for use.
CSRD – Corporate Sustainability Reporting Directive

4. DESCRIEREA PROCEDURII

4.1 Stabilirea Contextului Organizațional

Prin stabilirea contextului, compania AROBS definește inclusiv pentru Grup, parametrii interni și externi relevanți care trebuie luați în considerare în procesul de management al riscurilor. Acești parametri trebuie detaliați și analizați din perspectiva domeniului de aplicare al ISMS.

Contextul va fi stabilit și documentat de fiecare dată când este desfășurat procesul de management al riscurilor, fie înainte, fie în timpul colectării informațiilor privind inventarul resurselor informaționale. Documentația de bază trebuie să fie o parte integrantă a analizei riscurilor / registrului de riscuri.

Contextul intern reprezintă mediul intern în care AROBS urmărește să își atingă obiectivele. Contextul intern al AROBS - include, dar nu se limitează la:

- domeniul de aplicare al ISMS

- disponibilitatea în ceea ce privește resursele și cunoștințele (de exemplu: competențe, capital, timp, persoane, procese, sisteme și tehnologii)
- sistemele informaționale, fluxurile de informații, procesele de luare a deciziilor (formale și informale)
- părțile interesate interne
- politicile, procedurile, obiectivele, măsurile, metodologiile și strategiile existente
- percepțiile, valorile, cultura organizațională
- standardele și modelele de referință adoptate de organizație
- structura (autoritate, roluri și responsabilități)

Contextul extern reprezintă mediul extern în care AROBS - urmărește să își atingă obiectivele. Înțelegerea contextului extern este importantă pentru a asigura că părțile interesate, obiectivele și preocupările acestora sunt luate în considerare la elaborarea criteriilor de risc. Contextul extern se bazează pe contextul mai larg al AROBS -, dar include detalii specifice privind cerințele legale și de reglementare, percepțiile părților interesate și alte aspecte de risc specifice domeniului de aplicare al procesului de management al riscurilor.

Aspectele **contextului extern** al AROBS includ, dar nu se limitează la, următoarele:

- mediul cultural, politic, geopolitic, juridic, legislativ, financiar, tehnologic, economic, lanțul valoric, mediul natural și competitiv, atât la nivel internațional, cât și național, regional sau local
- tendințele și elementele cheie care pot avea impact asupra obiectivelor AROBS
- percepțiile și valorile părților interesate externe

Consiliul și Comitetul de Audit trebuie să acorde o atenție constantă riscurilor emergente generate de tehnologia informației și inteligența artificială, inclusiv riscurilor de securitate cibernetică. În acest sens, pe agenda Consiliului trebuie alocat timp pentru analiza riscurilor și oportunităților asociate IA și pentru asigurarea unui nivel adecvat de înțelegere a protecției cibernetice.

4.2 Identificarea Riscurilor

Identificarea riscurilor reprezintă un prim pas esențial în managementul riscurilor, implicând identificarea sistematică, documentarea și descrierea evenimentelor potențiale (amenințări) care ar putea afecta obiectivele AROBS, utilizând metode sau analiza cauzelor principale pentru a crea o listă cuprinzătoare în vederea analizei și controlului ulterior. Aceasta vizează înțelegerea impacturilor potențiale și construirea unor strategii pentru gestionarea proactivă a acestora.

Identificarea riscurilor (logice și fizice) înseamnă determinarea a ceea ce s-ar putea întâmpla pentru a provoca o pierdere sau un eveniment care să afecteze negativ organizația, inclusiv **confidențialitatea, integritatea** și **disponibilitatea** resurselor informaționale, precum și cum, unde și de ce ar putea apărea pierderi.

AROBS identifică riscurile printr-un proces structurat care include evaluări regulate ale operațiunilor interne, implicarea părților interesate de-a lungul lanțului valoric, monitorizarea continuă a factorilor de mediu, sociali, financiari, politici și geopolitici care pot avea impact asupra organizației.

Riscurile associate cu Corporate Sustainability Reporting Directive (CSRD) includ **penalități financiare, prejudicii de reputație, litigii legale și pierderea încrederii** părților interesate ca urmare a neconformității.

Identificarea riscurilor include: sesiuni de brainstorming privind posibilele riscuri / oportunități, inventarierea activelor informaționale, a amenințărilor și vulnerabilităților aplicabile, a măsurilor de securitate existente, a consecințelor pierderii datelor etc.

Riscurile identificate sunt înregistrate în **Registrul de riscuri** de către responsabilul riscului.

Pentru o abordare adecvată a identificării riscurilor, fiecare responsabil de proces își va identifica propriile riscuri de securitate a informațiilor, cu sprijinul IMSR/SC. Responsabilul de risc va accepta riscurile identificate și evaluate de fiecare responsabil de proces.

4.2.1 Identificarea & evaluarea activelor

AROBS identifică toate activele relevante prin menținerea unui inventar actualizat al tuturor facilităților fizice, sistemelor tehnologice, capitalului uman, resurselor naturale, proprietății intelectuale și relațiilor din lanțul de aprovizionare care influențează performanța de mediu a organizației, impactul social și obligațiile de guvernanță.
Resursele organizației sunt identificate și inventariate de către deținătorul resursei, cu sprijinul responsabilului de activ și al altor părți interesate interne. Următoarele tipuri de resurse sunt luate în considerare în procesul de identificare:

- **Resurse financiare**: numerar, disponibil in conturile bancare, împrumuturi, investiții, capital, linii de credit etc.
- **Informații**: baze de date și fișiere de date (despre companiile din Grup, clienți, angajații companiilor din Grup), contracte și acorduri, documentație de sistem, know-how specializat, instrucțiuni specifice, proceduri operaționale, planuri de continuitate a activității, business intelligence, cunoștințe etc.;
- **Resurse Software**: applicații software, software de sistem
- **Resurse fizice**:, vehicule, stocuri, materii prime, spații de birouri, echipamente IT și de comunicații, medii mobile, echipamente audio, foto și video, alte echipamente;
- **Servicii**: servicii și produse IT și de comunicații, utilități generale (electricitate, aer condiționat, încălzire etc.);
- **Resurse umane:** abilități profesionale, experiență și loialitate;
- **Resurse intangibile / proprietate intelectuală:** precum reputația și imaginea organizației, brevete, mărci, drepturi de autor, secrete comerciale, brand, cultură;
- **Resurse de rețea:** parteneriate, relații cu furnizorii, bază de clienți.

IMSR/SC, împreună cu responsabilii de resurse, înregistrează resursele identificate în **Registrul activelor informaționale (aferent P-GEN-3) și în alte inventare de active**, indicând tipul, formatul, locația și informațiile necesare pentru recuperarea în caz de dezastru. Identificarea resurselor se realizează pentru fiecare proces/departament.

Pentru fiecare resursă identificată este desemnat un responsabil. Acesta este responsabil pentru administrarea, stocarea și securitatea resursei respective.

Resursele identificate sunt evaluate de către responsabilul de activ/risc. Toate resursele informaționale au o anumită valoare pentru AROBS, iar această valoare poate fi măsurată pe baza următoarelor criterii:

- în funcție de impactul compromiterii activului sau al datelor ;
- în funcție de valoarea de inventar, de înlocuire sau de remediere a resursei respective

4.2.2 Identificarea proceselor interne; analiza din partea responsabililor de proces

Pentru identificarea proceselor principale, se analizează organigrama; în **Registrul de riscuri**, principalele departamente și procese sunt abordate corespunzător (de exemplu: IT, HR/Administrativ, Management de proiect / Dezvoltare software, Financiar, Juridic, Achiziții, SC etc.).

Responsabilii de proces au responsabilități în identificarea tuturor surselor semnificative de incertitudine, în principal prin discuții interne.

Pentru evaluări de risc specifice / proiecte

Fiecare Manager de Proiect / Responsabil de Proces va urmări identificarea riscurilor specifice proiectului, riscurilor de sustenabilitate și riscurilor de securitate a informațiilor.

Pentru identificarea riscurilor care decurg din implementarea proiectelor/proceselor, înainte de stabilirea scopului proiectului trebuie definite următoarele:

- rolurile și funcțiile personalului implicat în proiect/process;
- termenii contractuali, dacă este cazul;
- cerințele legale;
- practicile profesionale;
- documentația proiectului/procesului.

Pe baza elementelor enumerate și a interviurilor cu managerii de proiect/deținătorii de proces și partenerii cheie, pot fi identificate etapele critice care afectează securitatea informațiilor.
Pentru fiecare etapă, vor fi luate în considerare cel puțin următoarele vulnerabilități și amenințări:

- infrastructura
- personalul;
- managementul de proiect (costuri, calitate, termene);
- aspectele legale;
- aspectele financiare;
- reputația.

Indiferent de metodologia de proiect/proces utilizată, etapele critice ale proiectului/procesului vor fi încadrate în:

- definirea proiectului/procesului (concept, cerințe și arhitectură, proiectare detaliată, planificare, succesiunea activităților, responsabilități și controale, execuția sarcinilor etc.)

- implementare;
- testare și integrare (integrare, testare, verificare, validare, mentenanță etc.).

4.2.3 Analizarea vulnerabilităților și amenințărilor

Amenințările apar accidental, fie în mod natural, fie deliberat (intenționat). Pentru fiecare proces principal/departament, vulnerabilitățile și amenințările sunt identificate în contextul AROBS, luând în considerare măsurile de securitate existente (a se vedea Registrul de Riscuri). Analiza riscurilor include doar vulnerabilitățile și amenințările posibile și probabile, excluzând amenințările și vulnerabilitățile ipotetice care nu pot fi exploatate în contextul AROBS.

La definirea vulnerabilităților și amenințărilor sunt utilizate cataloagele disponibile **(Anexa 1 – Vulnerabilități, riscuri și amenințări) privind vulnerabilitățile și amenințările** la adresa securității informațiilor, calității proceselor, managementului de proiect, resurselor umane etc.

Etapa inițială de identificare a vulnerabilităților și amenințărilor presupune colaborarea dintre responsabilul de proces și IMSR. Aceștia vor indica vulnerabilitățile și amenințările specifice ariei de responsabilitate. IMSR va completa și corecta lista vulnerabilităților și amenințărilor pe baza cunoștințelor globale ale AROBS.

4.3 Analiza/evaluarea riscurilor

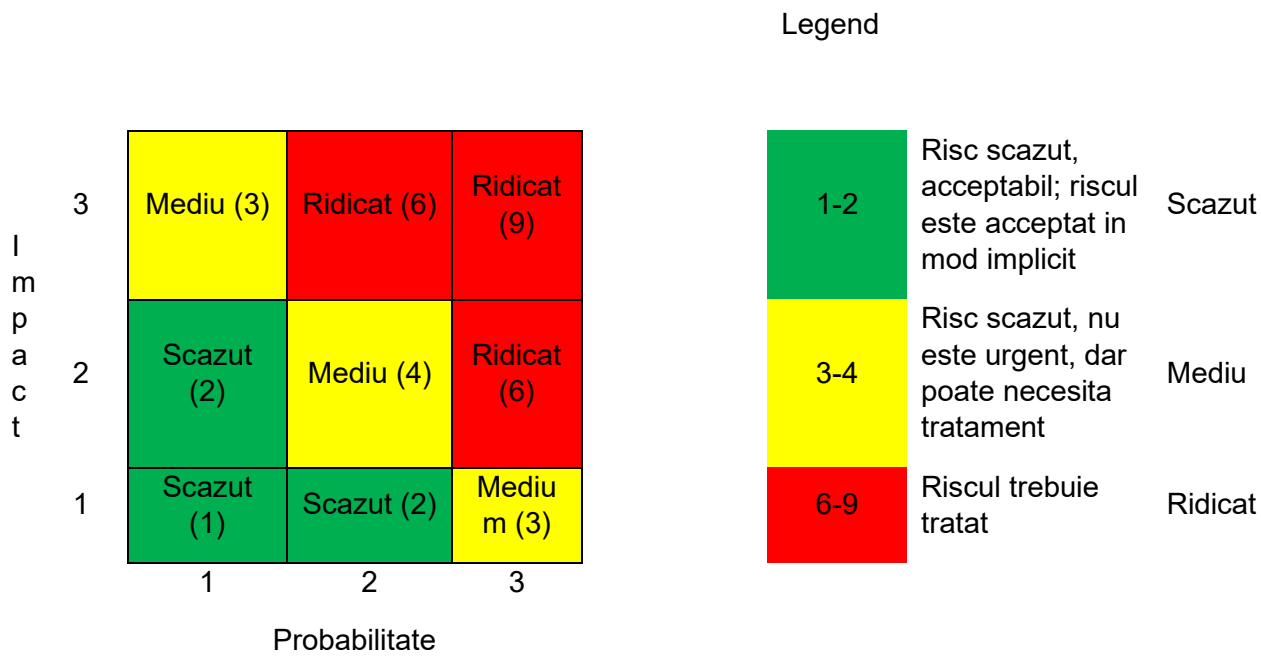
Analiza riscurilor se referă la înțelegerea riscului, a cauzelor posibile, a surselor de risc, dacă riscul este negativ sau pozitiv, care sunt consecințele posibile și care ar fi probabilitatea de apariție. Analiza riscurilor implică evaluarea prin metode calitative și/sau cantitative pentru a determina riscurile asociate unui proces și unei resurse.

Pentru fiecare risc identificat se stabilește o probabilitate de apariție și un impact, pe o scară de la 1 la 3, conform detaliilor din **Registrul de riscuri**.

4.4 Evaluarea riscurilor

Evaluarea riscurilor reprezintă compararea nivelurilor de risc estimate cu criteriile implicite de acceptare a riscului. Aceasta permite clasificarea și prioritizarea riscurilor.

Pe baza valorii resursei informaționale, a nivelului de probabilitate și a nivelului de impact, valoarea riscului este determinată în conformitate cu următorul tabel:



AROBS a stabilit un nivel minim acceptabil al riscului de 2 (verde). Pentru riscurile cu valori între 3 și 4 (galben), măsurile de tratament vor fi determinate la fiecare caz în parte. Riscurile cu valori între 6 și 9 (roșu) trebuie tratate obligatoriu.

4.5 Tratarea riscurilor

Opțiunile de tratare a riscurilor sunt alese în funcție de rezultatele evaluării riscurilor, costul estimat al implementării și beneficiile acestor opțiuni. Opțiunile de tratament sunt identificate și stabilite împreună cu responsabilul resursei, IMSR și alte părți interesate.

Sunt luate in considerare patru opțiuni posibile pentru gestionarea riscurilor:

- evitarea riscurilor
- reducerea riscurilor
- transferul riscurilor
- acceptarea riscurilor

Cele patru opțiuni nu se exclude una pe alta. În unele cazuri, utilizarea unei combinații de opțiuni, cum ar fi reducerea riscului, atenuarea și transferul riscurilor sau asumarea riscurilor reziduale, poate aduce avantaje considerabile pentru AROBS

a) **Reducerea riscului (modificarea probabilității/impactului)**

Nivelul riscului trebuie redus prin selectarea măsurilor astfel încât riscul rezidual să devină acceptabil (scăderea probabilității sau impactului riscului). Această selecție va lua în considerare criteriile de acceptare a riscurilor, adăugarea de backup-uri, îmbunătățirea securității, instruirea personalului sau proiectarea echipamentelor de protecție (dacă este cazul) pentru a reduce severitatea, făcând acest proces o parte esențială a gestionării amenințărilor prin controlul daunelor potențiale înainte ca acestea să escaladeze.

b) **Evitarea riscurilor (prin decizia de a nu începe sau a nu continua activitatea care generează riscul)**

Activitatea sau condiția care conduce la risc trebuie evitată. Atunci când riscurile identificate sau costurile de implementare a managementului riscurilor sunt considerate prea mari, iar opțiunile depășesc beneficiile, se poate lua decizia completă de evitare a riscului prin retragerea din activitatea sau setul de activități planificate sau prin schimbarea condițiilor de operare ale activității.

c) **Transferul riscurilor**

Aceasta implică decizia de a distribui anumite riscuri către alte părți externe. Transferul riscurilor poate crea riscuri noi sau poate modifica riscurile deja identificat. Așadar, măsuri suplimentare de management al riscurilor pot fi necesare. Transferul se poate realiza prin asigurări care acoperă consecințele materializării riscului.

d) **Aceptarea riscurilor**

Decizia de a accepta/reține riscurile fără acțiuni suplimentare trebuie luată conform evaluării riscului. Dacă nivelul riscului se încadrează în criteriile de acceptare a riscurilor – de obicei pentru riscuri cu impact redus sau când costurile tratării riscului depășesc beneficiile, documentându-l ca risc rezidual –, nu mai este necesară implementarea unor măsuri suplimentare și riscul poate fi asumat.

4.5.1 Planul de tartare a riscurilor

Planul de tratare a riscurilor trebuie definit astfel încât să identifice clar ordinea priorităților pentru implementarea managementului riscurilor și durata tratării.

Planul de management al riscurilor este coordonat de IMSR/SC împreună cu alte funcții din cadrul AROBS, în funcție de natura riscului.

După stabilirea și implementarea planului de management al riscurilor, trebuie determinate riscurile reziduale. Acest proces implică actualizarea sau reiterația evaluării riscurilor, luând în considerare efectele așteptate ale tratării propuse. Dacă riscurile reziduale nu îndeplinesc criteriile de acceptare ale organizației, poate fi necesară o nouă iterație a managementului riscurilor înainte de a se trece la acceptare.

Note:
Indiferent de opțiunile de tratare a riscurilor și de rezultatele obținute după implementarea măsurilor de tratament, monitorizarea și reevaluarea riscurilor se realizează periodic **(anual)**, inclusiv pentru riscurile reziduale acceptate, **sau ori de câte ori apare o schimbare în contextul intern sau extern al organizației** care ar putea modifica natura și nivelul riscului.

Consiliul, asistat de Comitetul de Audit, evaluează cel puțin anual adecvarea și eficacitatea cadrului de administrare a riscurilor și a sistemului de control intern al Societății. Evaluarea include eficacitatea funcției de audit intern, gradul de adecvare a proceselor de management al riscurilor și conformității, rapoartele de control intern și capacitatea managementului de a răspunde deficiențelor identificate, precum și transmiterea concluziilor către Consiliu.

4.6 Acceptarea riscurilor

Deținătorul riscului, cu sprijinul IMSR, are responsabilitatea de a revizui, analiza și confirma riscurile înregistrate de responsabilii de proces în **Registrul de riscuri**, concentrându-se pe aspecte precum Planul de tratare a riscurilor, alte date recurente pentru revizuirea riscurilor etc.

4.7 Comunicarea riscurilor

Responsabilii de proces au responsabilitatea de a informa IMSR/SC ori de câte ori actualizează **Registrul de riscuri.**

În plus, IMSR/SC are responsabilitatea de a informa conducerea superioară cu privire la riscuri, dacă este necesar, după evaluarea impactului în cadrul procesului de business.

Note:
Se acordă o atenție deosebită riscurilor etichetate cu galben (mediu) și roșu (ridicat).

Responsabilul de risc trebuie sa revizuiască, analizeze și confirme riscurile înregistrate de responsabilii de proces în **Registrul de riscuri**, concentrându-se pe aspecte precum Planul de tratare a riscurilor, alte date recurente pentru revizuirea riscurilor etc.

4.8 Monitorizarea & revizuirea riscurilor

Această etapă reprezintă monitorizarea și revizuirea sistemului de management al riscurilor și a oricăror modificări care l-ar putea afecta (de exemplu, schimbări ale resurselor, impactului, amenințărilor, vulnerabilităților și/sau probabilității de apariție, acțiuni întreprinse ca urmare a analizelor interne).

Monitorizarea și revizuirea au loc simultan pe parcursul procesului de management al riscurilor. Monitorizarea și revizuirea sunt realizate de către responsabilul de proces împreună cu

responsabilul de risc, cu sprijinul IMSR/SC. IMSR/SC va coordona monitorizarea și revizuirea globală la nivelul AROBS - prin:

- observarea schimbărilor semnificative în contextul intern și extern;
- monitorizarea incidenței materializării riscurilor în incidente de securitate a informațiilor

Evaluările riscurilor trebuie efectuate cel puțin anual sau ori de câte ori apare una dintre următoarele situații:

- modificări ale politicii de securitate care afectează metodologia de evaluare a riscurilor;
- schimbări ale standardelor de referință (benchmarking) care influențează managementul riscurilor;
- modificări majore ale sistemelor existente (de exemplu, domeniul de aplicare);
- schimbări majore, neașteptate sau neplanificate în conducerea superioară;
- modificări semnificative ale facilităților sau schimbarea locației acestora;
- introducerea de noi resurse în IMS;
- modificări necesare ale valorilor resurselor, de exemplu din cauza unor cerințe de afaceri diferite;
- apariția unor amenințări noi, fie din interiorul AROBS GROUP, fie din exterior, care nu au fost încă evaluate (schimbări în peisajul amenințărilor);
- posibilitatea apariției unor vulnerabilități noi sau crescute care să permită exploatarea lor de către amenințări;
- expunerea unor vulnerabilități cunoscute la amenințări noi;
- modificarea impactului în sensul creșterii expunerii la risc;
- apariția unui incident de securitate sau identificarea, în urma unui audit, a necesității unei reevaluări.

5. ÎNREGISTRĂRI & ANEXE

Annex 1 – Baza de date de Vulnerabilități, riscuri și amenințări

Registru de Riscuri

AROBS
Transilvania Software