Politica de management al riscului (ERM)

Aprobare	**Decizia CA nr. 70 din 19.12.2025**
Responsabil	Comitetul de Audit & Risc
Versiune & dată	V2.0 – 2025-12-19
Revizuire	Anual / la modificarea cadrului normativ

Istoric versiuni	Data	Descriere modificare	Aprobată de
2.0.	19.12.2025	Versiune completată cu obligația de operaționalizare a proceselor unde a existat „explain” în 2025	CA

Conținut

SIMTEL TEAM S.A.
J2010000564406, CUI 26414626
Sediul social: București, sector 6, Splaiul Independenței nr. 319L,
Clădirea Bruxeles (corp B), Intrarea A, Parter
Capital social subscris și vărsat: 1.628.346,2 Lei

Empowering a green future

1. Scopul

Politica de management al riscului stabilește principiile, rolurile și procesele prin care Simtel identifică, evaluează, tratează și monitorizează riscurile, inclusiv ESG șiclimă, securitate cibernetică și IT și utilizarea responsabilă a AI.

2. Domeniul de aplicare

Politica de management al riscului se aplică Simtel și entităților controlate. Vizează toți angajații, administratorii și colaboratorii.

Principii

Această Politică este pregătită în conformitate cu următoarele principii:

a. Prudență și materialitate

Simtel evaluează și tratează riscurile cu ipoteze conservatoare, iar efortul de control îl concentrăm pe expunerile care pot schimba decizii financiare, operaționale sau de guvernanță. Aceasta este unul dintre principiile de bază ale politicii, alături de modelul celor trei linii de apărare, reglementarea acestei Politici și transparența cerută emitenților pe piața de capital.

„**Prudență**" înseamnă că folosim scenariile și a testele de stres care privilegiază ipoteze realiste dar prudente, prin recunoașterea timpurie a semnalelor de deteriorare și prin escaladarea rapidă a abaterilor, în detrimentul optimismului operațional. Această politică leagă prudența de procesele ERM: matrice probabilitate–impact, scenarii, stress-testing, registru de risc actualizat și raportare de incident material în 24–72 de ore, astfel încât consecințele potențiale să fie înțelese înainte de a deveni pierderi efective.

„**Materialitate**" înseamnă că definim explicit ce este „semnificativ" pentru Simtel și prioritizăm acele riscuri. Operațional, materialitatea este ancorată în Declarația de apetit la risc (RAS), care stabilește toleranțe cantitative — de tip variație EBITDA, poziție de cash sau covenanți — și limite calitative, inclusiv toleranță zero la fraudă/mită, breșe majore de securitate sau accidente grave de sănătate și securitate în muncă. Tot în RAS sunt prevăzuți indicatori cheie de risc (KRI) pentru ariile critice ale modelului nostru de afacere: proiecte EPC, risc de contrapartidă, lichiditate, conformare/reglementar, reputație, ESG/climă, cyber/AI.

Simtel aplică prudența în toate evaluările de risc, preferând ipoteze conservatoare și escaladare timpurie, și gestionează materialitatea prin praguri cantitative și calitative definite în RAS, astfel încât resursele de control și raportare să vizeze expunerile cu potențial de a influența deciziile managementului, ale Consiliului și ale investitorilor.

Simtel aplică prudența în toate evaluările de risc, preferând ipoteze conservatoare și escaladare timpurie, și gestionează materialitatea prin praguri cantitative și calitative definite în RAS, astfel încât resursele de control și raportare să vizeze expunerile cu potențial de a influența deciziile managementului, ale Consiliului și ale investitorilor

b. Modelul celor trei linii de apărare

Acest principiu permite gestionarea riscului organizată pe trei niveluri complementare, clar separate ca rol și responsabilitate. Prima linie este managementul operațional: deține riscurile din procesele și proiectele de zi cu zi, implementează controalele primare, menține registrele de risc și raportează abaterile semnificative. Acest rol este al managementului executiv, cu obligația de a ține registrele și de a raporta incidentele majore (inclusiv în fereastra de 24–72 de ore, când impactul este material).

A doua linie este funcția de risc și conformitate: definește cadrul (metodologie, politici, RAS), monitorizează implementarea în prima linie, evaluează constant și consolidează harta riscurilor pentru raportare către structurile de guvernanță. În arhitectura Simtel, rolul este ancorat la Comitetul de Audit & Risc, care „supraveghează cadrul ERM, metodologia, harta riscurilor și controalele cheie", inclusiv pe tematicile ESG, cyber și AI.

A treia linie este auditul intern: furnizează asigurare independentă Consiliului și Comitetului de Audit & Risc asupra eficacității întregului sistem (controale, ERM, guvernanță), pe baza unui plan anual și a unei metodologii bazate pe risc.

Deasupra celor trei linii, supravegherea aparține CA și Comitetului de Audit & Risc astfel: CA aprobă Politica ERM și declarația de apetit la risc, iar Comitetul monitorizează cadrul, indicatorii și controalele, primind rapoartele periodice și incidentele materiale. Astfel se asigură segregarea sarcinilor, independența verificării și o escaladare rapidă atunci când expunerea iese din apetit.

c. Apetit la risc (RAS) aprobat de CA

Declarația conține atât toleranțe cantitative (EBITDA, lichiditate/cash, covenanți), cât și limite calitative de tip „toleranță zero", plus KRI-uri operaționale pentru proiecte EPC, contrapartidă, lichiditate, reglementar, reputație, ESG / climă, cyber / AI. Aceasta se aprobă de CA, este supravegheată de Comitetul de Audit & Risc și se revizuiește anual sau ori de câte ori profilul de risc se schimbă semnificativ.

d. Transparență și conformitate cu reglementările pieței de capital.

Simtel se angajează să raporteze corect, la timp și pe canalele oficiale tot ceea ce este relevant pentru investitori și autorități, și să-și alinieze procedurile interne la regulile BVB / ASF. Acest principiu este unul dintre reperele de bază ale politicii, alături de prudență / materialitate, modelul celor trei linii de apărare și existența unei Declarații de apetit la risc aprobată de CA.

Aplicarea practică pornește din procesul ERM: menținem registre de risc și raportăm periodic către structurile de guvernanță, iar dacă apare un incident material îl escaladăm rapid și îl divulgăm conform legii, cu ritm de reacție deja precizat în Politică (raportare incident major în 24–72 de ore). În plus, includem în raportul anual un rezumat al cadrului ERM și al RAS pentru a asigura transparența față de piață.

La nivelul relației cu investitorii, principiul impune ca informația reglementată și materialele aferente evenimentelor publice să fie publicate bilingv și prompt. Anexa la Politica IR cere ca secțiunea „Investitori" să conțină documentele corporative relevante și rapoartele curente/periodice, precum și ca prezentările să fie publicate în ziua evenimentului; aceeași anexă cere publicare simetrică în română și în engleză și menținerea unei arhive accesibile. Aceste cerințe operaționalizează atât transparența, cât și egalitatea de acces la informație.

Politica de prognoze (Forecast / Guidance) completează principiul pe zona informațiilor sensibile de piață: ghidajele se aprobă în CA și se publică exclusiv prin canalele oficiale BVB și website, iar abaterile materiale față de ghidaj sunt monitorizate și declanșează actualizarea sau retragerea ghidajului, cu păstrarea unei arhive. Această disciplină protejează egalitatea de tratament a investitorilor și calitatea așteptărilor pieței.

În plus, conformitatea cu reglementările pieței de capital este asigurată și prin politici tematice: tranzacțiile cu părți afiliate se fac la „arm's length", cu protecția acționarilor minoritari, trasee de aprobare pe praguri și publicarea tranzacțiilor conform legii, pe baza unui registru RPT; conflictele de interese sunt declarate inițial și anual, actualizate la cinci zile când apar situații noi, cu abținere de la deliberare și raportare / înregistrare formală. Toate acestea sunt cerințe de fond pentru a preveni abuzul de informație și pentru a documenta deciziile în fața investitorilor.

Acest principiu permite ca informația relevantă pentru piață să fie identificată, validată și publicată corect, în timp util și în oglindă română – engleză, pe canalele oficiale, cu procese interne care garantează respectarea BVB/ASF. Politicile de guvernanță previn conflictele, tranzacțiile opace sau divulgările selective.

3. Guvernanță și roluri

Rolurile de guvernanță ale acestei politici sunt împărțite între și constau în:

CA aprobă cadrul de management al riscului (Politica ERM) și Declarația de apetit la risc (RAS), adică pragurile cantitative și limitele calitative în interiorul cărora SImtel își desfășoară activitatea. În practică, CA definește riscul, alocă resurse, validează anual revizuirea RAS și primește periodic tabloul de bord cu

indicatorii-cheie de risc (KRI), astfel încât să poată cere măsuri când apar abateri semnificative. Pentru incidente materiale, CA este informat prin canalele de raportare stabilite (inclusiv ferestre de 24–72h pentru evenimente majore), iar pentru deviații „în afara apetitului" poate solicita corecții și, după caz, ajustarea ghidajului public.

AC&R exercită supravegherea tehnică a întregului cadru ERM: validează metodologia (taxonomie de riscuri, matrice probabilitate–impact, scenarii și stress-testing), analizează harta riscurilor și controalele cheie, urmărește funcționarea indicatorilor KRI și escaladează către CA atunci când expunerile ies din apetit.

În mandatul său intră și integrarea tematicilor ESG/climă, cyber/IT și AI în ERM, coordonarea cu AuI, precum și alinierea cu politicile conexe (RPT, Non-Audit, Conflicte de interese, IR/Forecast), astfel încât riscurile de piață de capital să fie gestionate unitar. Comitetul se asigură că există rapoarte periodice (trimestrial/semestrial) și că recomandările sunt închise la termen.

Managementul executiv identifică riscurile din procese și proiecte. Implementează ERM operațional (controale primare, proceduri, instruiri), menține registrele de risc actualizate, monitorizează KRI-urile și raportează imediat incidentele majore pe traseele stabilite. Echipa de management propune și aplică tratamentele de risc (evitare, reducere, transfer prin asigurare, acceptare controlată), pregătește notele de fundamentare atunci când abaterile ar necesita schimbări ale ghidajului / planului, și livrează lunar / trimestrial datele pentru consolidarea hărții de risc și a dashboard-ului către AC.

AuI monitorizează respectarea politicilor și a reglementărilor pieței de capital, provoacă metodologic prima linie, menține documentația (politici, RAS, registre tematice precum RPT și conflicte de interese) și urmărește remedierile. AuI oferă asigurare independentă CA și AC că sistemul de control intern și ERM funcționează: testează designul și eficacitatea controalelor, emite recomandări, stabilește termene de închidere și raportează statutul de follow-up până la remediere. AuI are rutine fixe de raportare către AC (trimestrial) și către CA (cel puțin anual) și sunt parte din mecanismul de escaladare atunci când expunerile ies din limitele aprobate prin RAS.

Empowering a green future

4. Procesul ERM

Procesul de implementare și aplicare a acestei Politici constă în cinci etape, detaliate în continuare.

a. Identificare

Procesul pornește cu ateliere periodice pe fiecare linie de business și funcțiune suport, conduse de „ownerii" de proces/proiect. Înaintea atelierelor, echipa de risc pregătește o scanare PESTEL (politic–economic–social–tehnologic–ecologic–legal) și un rezumat al „lecțiilor învățate" din proiectele încheiate și incidentele apărute în ultimul trimestru.

În EPC, identificarea include și o etapă pre-ofertare în care sunt enumerate riscurile comerciale și operaționale: clauze contractuale asimetrice, riscuri de proiectare, furnizori unici, ferestre de execuție, permise, interdependențe.

Fiecare risc nou este introdus în Registrul de risc cu un profil minim obligatoriu: descriere cauză-eveniment-efect, domeniu (financiar / operațional / ESG / cyber / AI etc.), „owner", legătura cu obiectivele și cu RAS, controale existente, KRI propus, scor inerent, propunere de tratament și data-țintă.

Etapa se încheie cu eliminarea eventualelor dubluri și o mapare pe taxonomia de riscuri a Simtel, astfel încât aceleași tipuri de expuneri să poată fi urmărite comparabil în timp.

b. Evaluare

Fiecare risc este evaluat pe o matrice probabilitate–impact 5×5, cu definiții cantitative și calitative pre-agreate. Probabilitatea este ancorată pe intervale (e.g.: 1 <5%, 2 = 5–20%, 3 = 20–50%, 4 = 50–80%, 5 >80%), iar impactul pe „arii" comparabile: financiar (efect EBITDA / Cash), calendar proiect, H&S, reglementar / MAR, reputațional, date / cyber.

Scorul inerent rezultă din combinație; în paralel, pentru riscurile materiale rulăm scenarii (de bază / nefavorabil / sever) și un stres-test „ce se întâmplă dacă" (de pildă +10% cost materiale, −15% productivitate, întârziere critică a furnizorului, depreciere curs).

În EPC, folosim și indicatorii Earned Value pentru a valida dacă ipotezele de program / cost rezistă; sub 0,95 apare abatere semnificativă, iar sub 0,90 intrăm în zona „în afara apetitului".

Empowering a green future

Pentru riscurile de lichiditate și finanțare, stres-testăm covenanții (Net Debt / EBITDA) și DSO / DPO / DIO, astfel încât să putem observa dacă obiectivele definite în RAS se păstrează. Evaluarea consemnează „rezidualul" după tratament propus și marca de conformitate cu RAS: „în apetit", „la limită" sau „în afara apetitului", ceea ce determină escaladarea.

c. Tratament

Decizia urmează arborele clasic: evitare, reducere, transfer, acceptare controlată.

Evitarea înseamnă să nu licitezi, să renegociezi sau să retragi o expunere care contravine flagrant apetitului; în EPC, poate însemna refuzul unei clauze „pay-when-paid" fără protecții sau al unui termen imposibil.

Reducerea înseamnă controale concrete: clauze „back-to-back" cu subcontractorii, plan de management al schimbărilor (change-order discipline), buffer de timp și cost, verificări de calitate, rezervă de risc, diversificare de furnizori, hedging unde e cazul.

Transferul acoperă asigurările (CAR / EAR, răspundere civilă, răspundere profesională), garanții, factoring / credit-asigurare pentru clienți, precum și partajarea riscului prin clauze contractuale.

Acceptarea controlată se aplică doar dacă riscul rămâne „în apetit" după măsuri și are un beneficiu justificat; ea cere o notă de asumare, un „owner" nominal, KRI aferente și revizuire periodică.

Fiecare tratament are obiectiv, responsabil, buget, termen și criteriu de succes; dacă după implementare riscul rămâne „în afara apetitului", măsurile se re-proiectează sau se escaladează către AC&R sau CA.

d. Monitorizarea și raportarea

Registrul de risc se actualizează operațional lunar de către „ownerii" de risc și se consolidează trimestrial, cu un „top 10" pe nivel de intensitate, trendul KRI-urilor și starea acțiunilor.

Raportarea ERM se transmite semestrial către AC&R și include: harta riscurilor, abaterile față de RAS, analize pe teme (ESG, cyber / AI, finanțare / lichiditate), progresul recomandărilor AuI.

Empowering a green future

Incidentele majore – de exemplu, evenimente H&S grave, breșe de securitate, riscuri MAR de divulgare, deviații materiale pe proiecte sau declanșări de covenanți – se raportează și se procesează pe un flux accelerat, în 24–72 de ore de la constatare, cu notificări către AC&R și CA și, după caz, către piață pe canalele oficiale.

Pentru KRI, Simtel folosește praguri color pe modelul semaforizării: „verde" în apetit, „galben" la limită (plan obligatoriu în 30 de zile) și „roșu" în afara apetitului (escaladare imediată). Documentația permite trasabilitatea prin: minute, registre, fișe de risc, transmise în arhiva ERM.

e. Revizuire anuală

La final de an, Simtel evaluează eficacitatea controlului intern și a ERM prin combinarea testelor AuI, a indicatorilor de rezultat (abaterea agregată de la buget / RAS, incidentele, timpii de remediere) și a feedback-ului din „lecții învățate".

Pe baza acestor date, AuI propune actualizarea RAS (de exemplu, ajustarea toleranțelor pe EBITDA / cash sau a limitelor calitative) și, dacă e cazul, revizuirea metodologiei. CA dezbate și, după caz, aprobă modificările, iar un rezumat ERM / RAS va fi inclus în capitolul de guvernanță al Raportului anual.

5. Riscurile tematice

Evenimentele-risc tipice, KRI-uri propuse, praguri / toleranțe și controale cheie avute în vedere sunt definite de trei piloni principali:

5.1. ESG / climă (tranziție, reglementar, sănătate & siguranță, lanț de aprovizionare)

5.1.1. Risc de tranziție climatică

Acest risc vizează creșteri de costuri (energie, CO_2), schimbări de reglementare, acces îngreunat la finanțare dacă intensitatea emisiilor pe proiect rămâne ridicată.

KRI și praguri propuse pentru atenuarea riscului, pot fi:

a) intensitatea emisiilor (tCO_2e/1 mil. RON venit proiect): țintă în scădere YoY;
b) pondere proiecte cu plan de eficiență energetică aprobat: ≥90%;
c) dependență critică de un singur furnizor: ≤20% din cheltuielile relevante.

Controale-cheie aplicate de Simtel: bugetarea scenariilor de cost energie/CO_2, criterii „low-carbon" în achiziții, clauze contractuale pentru eficiență la operare.

5.1.2. Risc reglementar ESG / raportare

Riscul de nerespectare a cerintelor de raportare ESG (ESRS, GRI acolo unde se aplica, Regulamentul Taxonomiei UE) include: intarzierea publicării informațiilor, inconsistente intre raportul de sustenabilitate si website, absenta trasabilității datelor si constatari de audit privind calitatea informațiilor raportate. Impactul poate include sanctiuni ASF, deteriorarea ratingului ESG si pierderea accesului la instrumente de finantare verde (green bonds, credite legate de sustenabilitate).

KRI & praguri definite pentru gestionarea acestui risc pot fi: acoperire controale de raportare ESG: 100%; deviații de calendar: 0; constatări de audit privind trasabilitatea datelor ESG: 0 „majore".

Controlul riscului se realizează de proprietarii de indicatori ESG pe fiecare temă, traseu de auditabilitate a datelor, aliniere cu IR / website pentru publicare bilingvă și arhivare.

5.1.3. Sănătate & siguranță (H&S)

5.1.4. Riscul H&S cuprinde accidentele de munca pe santier si in spatiile de lucru, opririle de lucru dispuse de ITM sau de clienti, penalitatile contractuale si reputationale asociate, precum si riscul de răspundere penala a reprezentantilor Companiei in cazul fatalitaților sau accidentelor grave. Contextul EPC, cu santiere active si subcontractori multipli, genereaza expuneri H&S semnificative care necesita controale robuste si monitorizare continua.

Riscul accidentelor pe șantier, opririlor de lucru, penalităților și este indicat de KRI cu praguri de: zero fatalități, rata incidentelor care necesită îngrijiri

medicale ≤ 0,8, rata incidentelor care reduc capacitatea de muncă ≤ 0,25, incidente H&S majore = 0.

Aceste riscuri pot fi controlate prin permise de lucru, induction, audit H&S pe șantier, managementul contractorilor.

5.1.5. Lanțul de aprovizionare

Riscurile aferente lantului de aprovizionare includ: neconformitati etice sau H&S la furnizori (munca fortata, munca copiilor, incalcari ale drepturilor omului), întârzieri critice cu impact asupra termenelor de executie EPC, calitate slaba a materialelor sau lucrarilor executate de subcontractori care erodeaza marja proiectului si expun Compania la reclamatii in garantie. Directiva CSDD (Corporate Sustainability Due Diligence Directive) impune obligații extinse de due diligence in lantul de aprovizionare pentru companiile listate.

Principalii KRI și praguri: Furnizorii critici validați ESG & H&S: ≥95%; timp mediu de închidere neconformități furnizor: ≤30 zile; refacerea lucrărilor din cauza furnizorilor: ≤1% din valoarea proiectului.

Controlul riscului asociat lanțului de aprovizionare se face prin implementarea fără excepții a codului de conduită al furnizorilor, realizarea de due diligence și reglementări contractuale ale drepturilor de audit și de reziliere, realizarea unor planuri de continuitate de tip ”dual sourcing”, în scenariile fezabile, unde riscul se materializează.

5.2. Cyber. IT

5.2.1. Breșe de securitate. Confidențialitate

Pentru prevenirea acestor riscuri, Simtel a implementat următoarele controale: EDR pe toate endpoint-urile, MFA obligatoriu, least privilege cu revizuire lunară conturi privilegiate, DLP, criptare la repaus / în tranzit, jurnalizare centrală și playbook de răspuns la incidente. Riscul poate proveni din scurgeri de Date cu caracter personal și PI, ransomware, acces neautorizat la sisteme.Pentru aceste riscuri, Simtel a stabilit KRI și praguri, după cum urmează: remediere patch-uri critice ≤ 7 zile, „high” ≤ 30 zile; rata de click la phishing <5%; incidente DLP „majore” = 0.

Pentru prevenirea acestor riscuri, Simtel a implementat următoarele controale: EDR pe toate endpoint-urile, MFA obligatoriu, least privilege cu revizuire lunară conturi privilegiate, DLP, criptare la repaus / în tranzit, jurnalizare centrală și playbook de răspuns la incidente.

5.2.2. Indisponibilitatea sistemelor

Riscul constă în căderi ale sistemelor critice (ERP, email, SCADA), întreruperi de proiect / facturare. Pentru prevenirea acestor riscuri, Simtel a implementat politici care să asigure KRI și praguri pentru: disponibilitate servicii critice ≥99,5%; RTO conform cu clasificarea; test anual DR cu rezultate „satisfăcător" sau mai bine.

Controlul măsurilor implementate se realizează prin arhitectură redundantă, backup testat, patch / upgrade planificat, capacitate monitorizată, SLA contractual cu furnizorii cloud.

5.2.3. Integritatea datelor

Riscurile pot fi cauzate de date de proiect alterate, versiuni concurente, raportări eronate. Pentru prevenirea acestor riscuri, Simtel a stabilit KRI și praguri, precum: rate de reconciliere = 100% la checkpoint-uri; excepții de integritate „majore" = 0; conformitate „segregation of duties" în ERP ≥95%.

Controlul acestor măsuri se realizează prin guvernanța master data.

Simtel raportează incidentele materiale pe fluxul accelerat în 24–72h (AC&R/CA și, după caz, piața), conform procesului din politică.

5.3. AI

5.3.1. Acuratețe / robustețe

Riscul principal in aceasta categorie consta in incarcarea (upload) neautorizata de materiale care constituie IP sau secret comercial al Simtel sau al tertilor (clienti, subcontractori, parteneri) in instrumente AI publice sau neaprobate, cu potential de scurgere de informații confidentiale. Riscuri conexe includ: utilizarea unor modele AI cu grad redus de acuratete in procese decizionale, generarea de rezultate incorecte in estimarile de cost/program EPC si aparitia de erori in documentatia tehnica. Riscurile pot deriva din încărcarea (upload) neautorizată de materiale care constituie IP

sau secret comercial al Simtel sau al unor terți, în instrumente AI publice, apariția unor scurgeri de date etc.

Pentru prevenirea acestui tip de risc, Simtel a stabilit KRI & praguri: incidente de exfiltrare AI = 0; „shadow AI" detectat = 0; acoperire training AI pentru personal cheie = 100%.

Controlul măsurilor de prevenire este realizat prin interdicția de a folosi IP în servicii neaprobate, clasificarea datelor, gateway AI cu filtrare, termeni contractuali cu furnizori (SCC/DPAs), log audit pentru solicitări.

5.3.2. Bias / echitate

Riscurile pot deriva din rezultate discriminatorii (HR, scoring furnizori / parteneri), risc reputațional și legal. Simtel gestionează aceste riscuri prin următorii KRI și praguri: toate modelele „decizionale" trec prin checklist bias / echitate = 100%; incidente confirmate de bias = 0.

Controlul măsurilor se face prin: seturi de test pentru bias, revizuire legal / HR pentru procese sensibile, documentație a datelor de antrenare și a limitărilor.

5.3.3. Confidențialitate și IP

Riscurile asociate confidențialității și IP generate de utilizarea AI pot consta în generarea unor materiale cu licențe neclare, folosirea conținutului protejat fără drept, pierderea IP intern, respectiv încărcarea neautorizată de IP sau secret comercial în instrumente AI publice, scurgeri de date.

Pentru preîntâmpinarea riscurilor, Simtel a introdus KRI și praguri: folosirea numai a materialelor generate prin AI cu licență, 0 notificări în legătură cu IP, interdicția de a trimite IP în servicii neaprobate.

Controlul măsurilor se realizează prin ghid de folosire a materialelor generate, verificări de licență, consultarea provenienței conținutului, acolo unde este disponibil, stocarea internă a materialelor sensibile, gateway AI cu filtrare, termeni contractuali cu furnizori (DPA, SCC) etc.

Empowering
a green
future

6. Raportare și transparență

Sumare ale cadrului ERM și RAS vor fi incluse în raportul de activitate anual al Simtel. Societatea va divulga incidentele materiale conform legii și reglementărilor BVB / ASF.

7. Implementare și training

Societatea organizează anual training pentru management și personalul – cheie. Periodic și în acord cu RAS vor fi definiți indicatori – cheie de conformitate ai acestei politici și vor fi integrați în obiectivele manageriale.

8. Revizuire

Politica se revizuiește anual sau când intervin schimbări semnificative în profilul de risc.