Risk Management Policy (ERM)

Approval	**Board of Directors Decision no. 70 of 19.12.2025**
Responsible & Date Version	Audit and Risk Committee V2.0 – 2025-12-19
Review	Annually / when the regulatory framework is amended

Version history	Date	Description of the change	Approved by
2.0.	19.12.2025	Completed version with the obligation to operationalize processes where there was "explain" in 2025	CA

Contents

1. Purpose....2
2. Scope....2
Principles....2
a. Prudence and materiality....2
b. The model of the three lines of defense....3
c. CA Approved Risk Appetite (RAS)....4
d. Transparency and compliance with capital market regulations....4
3. Governance and roles....6

SIMTEL TEAM S.A.
J2010000564406, Tax No. 26414626
Registered office: Bucharest, sector 6, Splaiul Independenței nr. 319L, Brussels Building (Building B), Entrance A, Ground Floor
Subscribed and paid-up share capital: 1,628,346.2 Lei

Empowering a green future

4. The ERM process 7
a. Identification 7
b. Rating 7
c. Treatment 8
d. Monitoring and reporting 9
e. Annual Review 9
5. Thematic risks 9
5.1. ESG / climate (transition, regulatory, health & safety, supply chain) 9
5.2. Cyber. IT 11
5.3. AI 12
6. Reporting and transparency 13
7. Implementation and training 14
8. Review 14

1. Purpose

The risk management policy sets out the principles, roles and processes by which Simtel identifies, assesses, treats and monitors risks, including ESG and climate, cybersecurity and IT, and the responsible use of AI.

2. Scope

The risk management policy applies to Simtel and controlled entities. It targets all employees, administrators and collaborators.

Principles

This Policy is prepared in accordance with the following principles:

a. Prudence and materiality

Simtel assesses and treats risks with conservative assumptions, and we focus our control effort on exposures that can change financial, operational or governance decisions. This is one of the basic principles of the policy, along

with the three-line defence, the regulation of this Policy and the transparency required of issuers on the capital market.

"**Prudence**" means that we use scenarios and stress tests that favor realistic but cautious assumptions, by recognizing signs of deterioration early and rapidly escalating deviations, to the detriment of operational optimism. This policy links prudence to ERM processes: probability–impact matrix, scenarios, stress-testing, updated risk register andmaterial incident reporting within24–72 hours, so thatthe potentialconsequencesarenotchosen before they become actual losses.

"**Materiality**" means that we explicitly define what is "significant" to Simtel and prioritize those risks. Operationally, materiality is anchored in the Risk Appetite Statement (RAS), which establishes quantitative tolerances — such as EBITDA variation, cash position or covenants — and qualitative limits, including zero tolerance for fraud/bribery, major security breaches or serious occupational health and safety accidents. Also in the RAS, key risk indicators (KRIs) are provided for the critical areas of our business model: EPC projects, counterparty risk, liquidity, compliance/regulatory, reputation, ESG/climate, cyber/AI.

Simtel applies caution in all risk assessments, preferring conservative assumptions and early escalation, and manages materiality through quantitative and qualitative thresholds defined in the RAS, so that control and reporting resources target exposures with the potential to influence management, Board and investor decisions.

Simtel applies prudence in all risk assessments, preferring conservative assumptions and early escalation, and manages materiality through quantitative and qualitative thresholds defined in the RAS, so that control and reporting resources target exposures with the potential to influence management, Board and investor decisions

b. The model of the three lines of defense

This principle allows for risk management organised on three complementary levels, clearly separated in role and responsibility. The first line is operational management: it owns risks in day-to-day processes and projects, implements primary controls, maintains risk registers and reports significant deviations.

This role belongs to executive management, with the obligation to keep records and report major incidents (including within the 24–72 hour window, when the impact is material).

The second line is the risk and compliance function: it defines the framework (methodology, policies, RAS), monitors the implementation on the front line, constantly assesses and strengthens the risk map for reporting to governance structures. In Simtel's architecture, the role is anchored to the Audit & Risk Committee, which "oversees the ERM framework, methodology, risk map and key controls", including on ESG, cyber and AI topics.

The third line is internal audit: it provides independent assurance to the Board and the Audit & Risk Committee on the effectiveness of the entire system (controls, ERM, governance), based on an annual plan and a risk-based methodology.

Above the three lines, the supervision belongs to the Board and the Audit & Risk Committee as follows: the Board approves the ERM Policy and the risk appetite statement, and the Board monitors the framework, indicators and controls, receiving periodic reports and material incidents. This ensures segregation of tasks, independence of verification and rapid escalation when exposure runs out of appetite.

c. CA Approved Risk Appetite (RAS)

The statement contains both quantitative tolerances (EBITDA, liquidity/cash, covenants) and "zero tolerance" qualitative limits, plus operational CRI for EPC projects, counterparty, liquidity, regulatory, reputation, ESG/climate, cyber/AI. It is approvedby the Board of Directors , supervised by the Audit & Risk Committee andreviewedannuallyor wheneverthe risk profile changes significantly.

d. Transparency and compliance with capital market regulations.

Simtel is committed to reporting correctly, on time and on official channels everything relevant to investors and authorities, and to align its internal procedures with the BVB / ASF rules. This principle is one of the basic benchmarks of the policy, theprudence/materiality policy, the model of the three lines of application and the existenceof a Risk Appetite Statementapprovedby the Board of Directors.

The practical application starts from the ERM process: we maintain risk registers and report periodically to the governance structures, and if a material incident occurs, we quickly escalate it and disclose it according to the law, with a reaction rate already specified in the Policy (reporting a major incident within 24–72 hours). In addition, we include in the annual report a summary of the ERM framework and the RAS to ensure transparency to the market.

At the level of investor relations, the principle requires that regulated information and materials related to public events be published bilingually and promptly. The Annex to the IR Policy requires that the "Investors" section contain the relevant corporate documents and current/periodic reports, as well as that the presentations be published on the day of the event; The same annex requires symmetrical publication in Romanian and English and the maintenance of an accessible archive. These requirements operationalise both transparency and equal access to information.

The Forecast / Guidance policy completes the principle in the area of sensitive market information: the guidelines are approved in the Board of Directors and published exclusively through the official BVB channels and website, and the material deviations from the guidance are monitored and trigger the update or withdrawal of the guide, with the keeping of an archive. This discipline protects the equal treatment of investors and the quality of market expectations.

In addition, compliance with capital market regulations is also ensured through thematic policies: transactions with related parties are made at "arm's length", with the protection of minority shareholders, threshold approval routes and the publication of transactions according to the law, based on an RPT register; Conflicts of interest are declared initially and annually, updated every five days when new situations arise, with refrains from deliberation and formal reporting/registration. These are all substantive requirements to prevent misuse of information and document decisions in front of investors.

This principle allows market-relevant information to be identified, validated and published correctly, in a timely manner and in a Romanian-English mirror, on official channels, with internal processes that guarantee compliance with BVB/ASF. Governance policies prevent conflicts, opaque transactions, or selective disclosures.

Empowering
a green
future

3. Governance and roles

The governance roles of this policy are divided between and consist of:

The Board approves the Risk Management Framework (ERM Policy) and the Risk Appetite Statement (RAS), i.e. the quantitative thresholds and qualitative limits within which SImtel operates. In practice, the AC defines the risk, allocates resources, validates the RAS review annually and regularly receives the Key Risk Indicators (KRI) scoreboard, so that measures can be requestedwhensignificant deviations occur. For material incidents, the Board of Directors is informed through the established reporting channels (including 24–72h windows for major events), and for deviations "out of appetite" it can request corrections and, as the case may be, the adjustment of the public guidance.

AC&R exercises technical oversight of the entire ERM framework: validates the methodology (risk taxonomy, probability-impact matrix, scenarios and stress-testing), analyses the risk map and key controls, monitors the functioningof the KRI indicators andescalates theCA whenthe exposures come out of appetite.

Themandate includes the integration of ESG/climate, cyber/IT andAI themes intoERM, coordination with AuI, as well as alignment with related policies (TOR, Non-Audit, Conflicts of Interest, IR/Forecast), so that capital market risks are be managed unitarily. The Committee shall ensure that there are regular reports (quarterly/half-yearly) andthat recommendations are finalised.

Executive management identifies risks in processes and projects. Implements operational ERM (primary controls, procedures, trainings), keeps risk registers up to date, monitors KRIs and immediately reports major incidents on established routes. The management team proposes andapplies the risk treatments (avoidance, reduction, transfer by insurance, controlled acceptance), preparesthe substantiation notes whendeviations would require changesofthe guidance/plan, and delivers monthly/quarterly data for strengthening the risk map and dashboard.cetre AC.

The AuI monitors compliance with capital market policies and regulations, methodologically challenges the front line, maintains documentation (policies, RAS, thematic registers such as TOR and conflicts of interest) and tracks

remedies. The AuI provides independent assurance to the CA and CA that the internal control system and ERM is working: it tests the design and effectiveness of controls, issues recommendations, sets deadlines for closure and reports the follow-up status to remediation. It has fixed reporting routines forCA (quarterly) andCA(at leastannually) andis part of the escalation mechanism whenexposures go beyond the limits approved by the RAS.

4. The ERM process

The process of implementing and enforcing this Policy consists of five steps, detailed below.

a. Identification

The process starts with periodic workshops on each line of business and support function, led by the "owners" of the process/project. Before the workshops, the risk team prepares a PESTEL scan (political-economic-social-technological-ecological-legal) and a summary of the "lessons learned" from the completed projects and incidents that occurred in the last quarter.

In the EPC, the identification also includes a pre-bidding stage in which commercial and operational risks are listed: asymmetric contractual clauses, design risks, single suppliers, execution windows, permits, interdependencies.

Each new risk is entered in the Risk Register with a mandatory minimum profile: cause-event-effect description, domain (financial/operational/ESG/cyber/AI, etc.), "owner", linkto the objectives andRAS, existing controls, proposed KRI, inherent score, treatment proposal anddate.int.

Thetask ends with the elimination of possible duplications anda mapping on Simtel's risk taxonomy, so thatthoseand types of exposures can be tracked comparably over time.

b. Rating

Each risk is assessed on a 5×5 probability–impact matrix, with pre-agreed quantitative and qualitative definitions. The probability is anchoredon intervals (e.g.: 1 <5%, 2 = 5–20%, 3 = 20–50%, 4 = 50–80%, 5 >80%), and the impact on comparable "areas": financial (EBITDA / Cash effect), project calendar, H&S, regulatory / MAR, reputation, data / cyber.

The inherent score resultsfrom the combination; At the same time, for material risks, there are scenarios (basic / unfavorable / severe) and a stress-test "what if" (e.g. +10% material cost, −15% productivity, critical supplier delay, exchange rate depreciation).

In EPC, we also use Earned Value indicators to validate whether program/cost assumptions hold up; below 0.95 there is a significant deviation, and below 0.90 we enter the "outside appetite" area.

For liquidity and funding risks, stress test m covenance(Net Debt / EBITDA) and DSO / DPO / DIO, so that we can see if the objectives defined in the RAS can beachieved. The assessment recordsthe 'residual' afterthe proposed treatment and the SAR compliance mark: 'in appetite', 'on the edge' or 'out of appetite', which causes escalation.

c. Treatment

The decision follows the classic tree: avoidance, reduction, transfer, controlled acceptance.

Avoidance means not bidding, renegotiating or withdrawing an exposure that flagrantly contravenes appetite; in EPC, it can mean denying a pay-when-paid clause oran impossible term.

Reduction means concrete controls: back-to-back clauses with subcontractors, change-order disciplines, time and cost buffering,quality checks, risk buffering, supplier diversification, hedging where there is the case.

The transfer covers insurance (CAR/EAR, liability, professional liability), guarantees, factoring/credit-insurance for customers, as well as risk sharing through contractual clauses.

Controlled acceptance only applies ifthe risk of losing an appetite after the meal hasa justified benefit; it requires an assumption note, a nominal "owner", the related KRI andperiodic review.

Each treatment has an objective, accountable, budget, deadline and criterion for success; if after implementation the risk remains "out of appetite", the measures are re-projected or escalatedto includeAC&R or CA.

d. Monitoring and reporting

The risk register is updated operationally monthly by the risk "owners" and is consolidated quarterly, with a "top 10" on the level of intensity, the trend of the KRIs andthe stateof the actions.

The ERM reporting is sent every six months toAC&R andincludes: risk map, deviations from RAS, analysis by topic (ESG, cyber / AI, finance/ liquidity), progress of the AuI recommendations.

Major incidents – e.g. serious H&S events, security breaches, MAR risks of disclosure, material deviationson projects or triggers of covenants – are reported and processed on an accelerated basis, within 24–72 hours of detection, with notifications to AC&R and CA and, where appropriate, to the market on official channels.

For KRI, Simtel uses color thresholds on the traffic light model: "green" in appetite, "yellow" at the limit (mandatory plan in 30 days) and "red" outside the appetite (immediate escalation). The documentation allows traceability through: minutes, registers, risk sheets, transmitted to the ERM archive.

e. Annual Review

At the end of the year, Simtel assesses the effectiveness of internal control and ERM by combining AuI tests, result indicators (aggregate deviation from budget/RAS, incidents, remediation times) and feedback from "lessons learned".

Based on this data, the AuI proposes to update the RAS (e.g. adjust the toleranceson EBITDA/cash or qualitative limits) and, if necessary, revise the methodology. The Board shall discuss and, where appropriate, approve the amendments, and an ERM/RAS summary will be included inthe governance chapter of the Annual Report.

5. Thematic risks

The typical risk events, proposed KRIs, thresholds/tolerances andkey controls envisaged are defined by three main pillars:

5.1. ESG / climate (transition, regulatory, health & safety, supply chain)

Empowering a green future

5.1.1. Climate transition risk

This risk concerns cost increases (energy, CO_2),regulatory changes, difficult access to financedue to the emission intensity per project ishigh.

KRI and proposed risk mitigation thresholds can be:

a) emission intensity (tCO_2e/1 mln. RON project income): inten sceter YoY;
b) share of projects with an approved energy efficiency plan : ≥90%;
c) critical dependency on a single supplier: ≤20% of relevant expenses.

Key controls applied by Simtel: budgeting of energy/CO_2 cost scenarios, low-carbon procurement criteria, contractual clauses for operational efficiency.

5.1.2. ESG regulatory risk / reporting

The risk of non-compliance with ESG reporting requirements (ESRS, GRI where applicable, the EU Taxonomy Regulation) includes: delay in the publication of information, inconsistencies between the sustainability report and the website, lack of data traceability and audit findings on the quality of the reported information. The impact can include ASF sanctions, deterioration of the ESG rating and loss of access to green financing instruments (green bonds, sustainability-related loans).

KRI & thresholds defined for managing this risk can be: coverage of ESG reporting controls: 100%; calendar deviations: 0; audit findings on the traceability of ESG data: 0 'major'.

Risk control is performed by ESG indicator owners on each topic, data auditability pathway, alignment with IR/website for bilingual publication and archiving.

5.1.3. Health & Safety (H&S)

H&S's risk includes accidents at work on site and in workspaces, work stoppages ordered by ITM or customers, associated contractual and reputational penalties, as well as the risk of criminal liability of the Company's representatives in the event of fatalities or serious accidents. The EPC

context, with active sites and multiple subcontractors, generates significant H&S exposures that require robust controls and continuous monitoring.

The risk of accidents on site, work stoppages, penalties and is indicated by the KRI with thresholds of: zero fatalities, rate of incidents requiring medical attention ≤ 0.8, rate of incidents reducing work capacity ≤ 0.25, major H&S incidents = 0.

These risks can be controlled through work permits, induction, H&S on-site audit, contractor management.

5.1.4. Supply chain

Supply chain risks include: ethical or H&S non-compliances at suppliers (forced labor, child labor, human rights violations), critical delays impacting EPC lead times, poor quality of materials or work performed by subcontractors that erode the project's margin and expose the Company to warranty claims. The Corporate Sustainability Due Diligence Directive (CSDD) imposes extensive supply chain due diligence obligations for listed companies.

Key KRIs and thresholds: Critical suppliers validated ESG&H&S: ≥95%; average closure time supplier non-conformities: ≤30 days;re-completion of workdue to suppliers: ≤1% of the project value.

The control of the risk associated with the supply chain is done by implementing without exceptions the code of conduct of suppliers, conducting due diligence and contractual regulations of audit and termination rights, carrying out "dual sourcing" continuity plans, in feasible scenarios, where the risk materializes.

5.2. Cyber. IT

5.2.1. Security breaches. Privacy

To prevent these risks, Simtel has implemented the following controls: EDR on all endpoints, mandatory MFA, least privilege with monthly reviewof privileged accounts, DLP, encryption at rest/in transit, central logging and incident response playbook. The risk can come from leaks of Personal Data and PI, ransomware, unauthorized access to systems. For these risks, Simtel has set KRI and thresholds as follows: critical patch remediation ≤ 7 days, "high" ≤ 30 days; phishing click-through rate <5%; "Major" DLP incident = 0.

To prevent these risks, Simtel has implemented the following controls: EDR on all endpoints, mandatory MFA, least privilege with monthly reviewof privileged accounts, DLP, encryption at rest/intransit, central logging and incident response playbook.

5.2.2. Unavailability of systems

The risk lies in critical system failures (ERP, email, SCADA), project / billing interruptions. To prevent these risks, Simtel has implemented policies to ensure KRI and thresholds for: availability of critical services ≥99.5%; RTO according to classification; annual DR test with "satisfactory" results or better.

The control of the implemented measures is carried out through redundant architecture, tested backup, planned patch / upgrade, monitored capacity, contractual SLA with cloud providers.

5.2.3. Data integrity

Risks can be caused by altered project data, concurrent versions, erroneous reporting. To prevent these risks, Simtel has set KRI and thresholds, such as: reconciliation rates = 100% at checkpoints; "major" integrity exceptions = 0; "segregation of duties" compliance withERP ≥95%.

The control of these measures is carried out through master data governance.

Simtel reports material incidents on the accelerated flow within 24–72h (AC&R/CA and, where applicable, the market), according to the policy process.

5.3. AI

5.3.1. Accuracy/robustness

The main risk in this category consists of the unauthorized upload of materials that constitute IP or trade secret of Simtel or third parties (customers, subcontractors, partners) in public or unapproved AI tools, with the potential to leak confidential information. Related risks include: the use of low-accuracy AI models in decision-making processes, the generation of incorrect results in EPC cost/program estimates, and the occurrence of errors in technical documentation. Risks may arise from the unauthorized uploading of material that constitutes an IP or trade secret of Simtel or third parties, in public AI tools, the occurrence of data leaks, etc.

To prevent this type of risk, Simtel has set KRI & thresholds: AI exfiltration incidents = 0; "shadow AI" detected = 0; AI training coverage for key personnel = 100%.

The control of prevention measures is achieved by prohibiting the use of IP in unapproved services, data classification, AI gateway with filtering, contractual terms with suppliers (SCCs/DPAs), audit log for requests.

5.3.2. Bias / fairness

Risks can derive from discriminatory results (HR, supplier/partner scoring), reputational and legal risk. Simtel manages these risks through the following KRIs and thresholds: all "decision-making" models go through the bias / fairness checklist = 100%; Confirmed bias incidents = 0.

The control of the measures is done through: test sets for bias, legal/HR review for sensitive processes, documentation of training data and limitations.

5.3.3. Privacy and IP

The risks associated with privacy and IP generated by the use of AI can consist of the generation of materials with unclear licenses, the use of protected content without rights, the loss of internal IP, or unauthorized uploading of IP or trade secret in public AI tools, data leaks.

To prevent risks, Simtel has introduced KRI and thresholds: using only licensed AI-generated materials, 0 IP notifications, prohibiting sending IP in unapproved services.

The control of the measures is carried out through a guide for the use of the generated materials, license checks, consultation of the origin of the content, where available, internal storage of sensitive materials, AI gateway with filtering, contractual terms with suppliers (DPA, SCC) etc.

6. Reporting and transparency

Summaries of the ERM and RAS framework will be included in Simtel's annual activity report. The Company will disclose material incidents in accordance with the law and regulations of BVB / ASF.

Empowering
a green
future

7. Implementation and training

The company organizes annual training for management and key personnel. Periodically, and in agreement with the SAR, key indicators of compliance of this policy will be defined and will be integrated into the managerial objectives.

8. Review

The policy is reviewed annually or when there are significant changes in the risk profile.