Enterprise Risk Management Policy

Group policy

xstreco

Contents

Approved by	The Board of Directors of Xstreco AG
Issued by	Executive management
Issued on	01.09.2026
Version	2.1

1 Introduction

1.1 Purpose and Scope

1.1.1 Purpose of the Policy

This policy sets out how risk is identified, assessed, treated, monitored and reported across the Group, how risks are owned and how they are escalated. It covers strategic, operational, financial, compliance and reputational risk.

1.1.2 Scope and Applicability

This policy applies to all employees, directors, officers, and contractors under Xstreco's direct supervision, working for any Xstreco office or industrial asset directly or indirectly controlled or operated by Xstreco worldwide. Where the Group holds an interest in a joint venture that it does not control or operate, it uses its influence to encourage conduct consistent with this policy.

2 Policy Statement

2.1 Group's Stance on Enterprise Risk Management

Risk must be managed at every level of the Group, within the risk appetite the board sets and reviews, in order to protect its people, its assets and its reputation. This policy requires the board to set the risk appetite, to record it, and to review it at least annually and whenever the Group's activities change materially. Risk management must be integrated into strategic planning, operations and decision-making. Managers are accountable for the risk culture in their areas and for identifying, assessing and escalating the risks arising in them.

2.2 Legal Implications

Article 716a paragraph 1 of the Swiss Code of Obligations makes the overall management of the company, the determination of its organisation, the organisation of its accounting, financial control and financial planning, and the supervision of those entrusted with management, non-transferable duties of the board of directors. Where a company is subject to an ordinary audit, Article 728a requires the auditor to verify that an internal control system exists, and Article 961c requires the management report, which an undertaking subject to ordinary audit must prepare, to give information on the conduct of a risk assessment, subject to the exemption in Article 961d. These provisions apply according to the audit regime and reporting duties to which the Group is subject at the relevant time; the Group applies this policy irrespective of whether they apply to it. In Peru, the Reglamento de Seguridad y Salud Ocupacional en Minería, approved by Decreto Supremo N.° 024-2016-EM, as amended, requires hazard identification, risk assessment and control at mining operations; those requirements are applied through the Health, Safety and Emergency Management Policy and the risk register this policy requires. ISO 31000, COSO Enterprise Risk Management - Integrating with Strategy and Performance and the OECD Guidelines for Multinational Enterprises on Responsible Business Conduct are guidance rather than binding law and provide no basis for certification. Non-compliance with this policy, and the conduct it prohibits, may result in reputational damage, legal penalties, and internal disciplinary action.

3 Key Principles and Guidelines

3.1 Specific Principles or Guidelines

This policy requires the following principles to be applied:

(a) Risk Identification and Classification: Risks must be identified across the strategic, operational, financial, compliance and reputational domains and recorded with both an inherent and a residual rating.

(b) Risk Ownership and Escalation: Each risk must be entered in a risk register, assigned to an accountable owner and escalated according to its severity and potential impact.

(c) Integration into Business Planning: Risk assessment must form part of project planning, investment decisions and operational reviews.

(d) Assurance and Internal Controls: A testing cycle must be set for each risk control and recorded. Controls must be tested for effectiveness on that cycle, and the result of each test must be recorded.

(e) Continuous Improvement and Lessons Learned: Risk events and near misses must be analysed so that controls can be improved and the likelihood of recurrence reduced.

3.2 Examples and Applications

(a) Identifying Operational Risk: Equipment failure interrupts a field programme. The risks arising from equipment failure and from interruption to an activity must be recorded in the risk register and their controls tested on the cycle set for them under section 3.1.

(b) Responding to Regulatory Risk: A new environmental regulation is introduced. Those responsible for the affected activity must update the controls and procedures concerned, taking legal advice where the subject calls for it.

(c) Managing Supply Chain Disruption: A geopolitical event threatens a key supplier. The owner of the risk must identify alternative sources, record the treatment and escalate the risk where it cannot be controlled at their level.

(d) Escalating Reputational Risk: A reputational risk linked to a counterparty is identified. The matter must be escalated to executive management.

4 Roles and Responsibilities

4.1 The Board

Oversight of this policy rests with the board. The board approves this policy and each revision of it.

4.2 Executive Management

Executive management issues this policy, provides the means required to apply it, and is accountable to the board for its application. Where this policy requires a matter to be escalated, it is escalated to executive management.

4.3 Responsibility for This Policy

Responsibility for the day-to-day application of this policy is assigned within the Group. This policy requires that the assignment be recorded in the Schedule of Policy Assignments, an internal document, be kept current, and be made known to those subject to this policy. Where this policy refers to the compliance function, it means the person or persons holding that assignment at the relevant time, whether or not a separate department exists.

4.4 Those Who Direct the Work of Others

Anyone who directs the work of others is responsible for applying this policy in the work they direct, for making those they direct aware of it, and for passing on a concern raised with them.

4.5 Everyone Subject to This Policy

Everyone subject to this policy must comply with it, must raise a concern where they believe it has been or may be breached, and must co-operate with any enquiry into such a concern.

4.6 Counterparties

Counterparties must meet the standards in this policy where their contract with the Group so provides, and may raise a concern through the channels in section 5.1.

4.7 Those Responsible for an Activity

Those responsible for an activity of the Group are responsible for identifying the risks it presents, for recording them, for applying the controls this policy requires, and for escalating a risk they cannot control at their level.

5 Reporting and Monitoring

5.1 Reporting Mechanisms

5.1.1 Internal Reporting

A concern under this policy may be raised with a line manager, with any member of executive management, or with the compliance function. A concern may also be raised through the web reporting form at xstreco.com/report, by writing to compliance@xstreco.com or codeofconduct@xstreco.com, both of which reach the compliance function, or by telephone on +41 41 562 32 90, asking for the compliance function. Retaliation against a person who raises a concern in good faith is prohibited.

5.1.2 External Reporting

A person who is not employed by the Group may raise a concern through the web reporting form at xstreco.com/report, by writing to compliance@xstreco.com or codeofconduct@xstreco.com, by telephone on +41 41 562 32 90, or by post, marked 'Confidential - Compliance', to the address at the end of this document. A concern may be raised in English or in Spanish. A name and contact details are not required, and a concern raised without them is assessed in the same way. The Group's website provider records basic technical data with every submission, so a report made through the form is not technically anonymous, and a call is not anonymous; a report sent by post can be.

5.2 Monitoring Procedures

This policy requires that its application be kept under review, and that a record sufficient to show how it has been applied be kept. In particular, this policy requires:

(a) that compliance with this policy be reviewed on the cycle stated in section 8;

(b) that concerns raised under this policy, and the way in which each was resolved, be recorded;

(c) that the risk this policy addresses be reassessed whenever the Group's activities change materially;

(d) that matters which are unresolved, which recur, or which are systemic be escalated to executive management and, where the law requires it or it is otherwise appropriate, to the competent authorities;

(e) that those subject to this policy be able to demonstrate, from the records kept, that its requirements were met.

The means used to meet these requirements are proportionate to the size of the Group and to the scale and nature of its activities at the time, and are extended as those change.

6 Training and Awareness

6.1 Awareness on Appointment

This policy requires that everyone subject to it be made aware of it on appointment and be given the instruction needed to apply it in their role. The form and the depth of that instruction are proportionate to the role.

6.2 Continuing Awareness

This policy requires that awareness of it be refreshed on the cycle stated in section 8, and whenever the policy is revised or an event makes it necessary, and that those in roles carrying greater exposure to the risk this policy addresses receive instruction appropriate to that exposure.

7 Compliance and Consequences

7.1 Reporting Non-Compliance

Everyone subject to this policy must report suspected violations, as must counterparties where their contract with the Group so provides. The identity of the person making a report is treated as confidential and is not disclosed except where disclosure is required by law or is necessary for the enquiry, and then only to the extent necessary. Retaliation against a person who reports in good faith is prohibited.

7.2 Consequences of Non-Compliance

Violations may result in disciplinary action, including termination of employment or contract, and may trigger legal proceedings.

8 Review and Revision

8.1 Review Frequency

8.1.1 Review Cycle

This policy is reviewed at least once in every two calendar years.

8.1.2 Event-Triggered Review

A review is carried out, whether or not one is due under the cycle, whenever a change in the law, a material change in the Group's activities, or an event arising under this policy makes one necessary.

8.1.3 Conduct and Outcome of the Review

The review is carried out by the holder of the responsibility described in section 4.3. Its outcome is submitted to the board, and any revision resulting from it is approved by the board before issue.

8.2 Revision History

8.2.1 Version 2.1 - 01.09.2026

Approved by the board and issued by executive management following a scheduled review of the suite. The amendments are editorial and clarifying; the policy positions stated in version 2.0 are unchanged.

8.2.2 Version 2.0 - 01.01.2026

Approved by the board and issued by executive management, replacing the first issue.

8.2.3 Version 1.0 - 02.06.2025

First issue.

8.2.4 Superseded Versions

Superseded versions are retained. Each revision is communicated to those subject to this policy.

9 Appendices

9.1 Glossary of Terms

(a) Risk Appetite: The amount and type of risk the Group is prepared to accept in pursuit of its objectives.

(b) Residual Risk: The risk that remains once the controls and mitigation applied to it are taken into account.

(c) Control Effectiveness: The degree to which a control reduces risk to an acceptable level.

(d) Inherent Risk: The level of risk before any controls or mitigation are applied.

(e) Risk Register: The record in which risks, their owners and their treatment plans are documented and tracked.

9.2 Related Legislation

9.2.1 Local Legislation

In Switzerland, Article 716a paragraph 1 of the Code of Obligations (non-transferable duties of the board of directors, including the organisation of the accounting, financial control and financial planning), Article 728a (verification by the auditor, in an ordinary audit, that an internal control system exists) and Article 961c (information in the management report on the conduct of a risk assessment), subject to Article 961d. In Peru, the Reglamento de Seguridad y Salud Ocupacional en Minería, approved by Decreto Supremo N.° 024-2016-EM, as amended, which requires hazard identification, risk assessment and control at mining operations.

9.2.2 International Standards and Frameworks

(a) ISO 31000:2018: Guidance on the management of risk. It provides no basis for certification.

(b) COSO Enterprise Risk Management - Integrating with Strategy and Performance (2017): Guidance on enterprise risk management.

(c) OECD Guidelines for Multinational Enterprises on Responsible Business Conduct: Recommendations addressed to enterprises, including on risk-based due diligence.

"Xstreco's policies set the standards that govern how the Group conducts its activities and how that conduct is assessed."

Xstreco AG
General-Guisan-Strasse 6
CH-6300 Zug
Switzerland

Email info@xstreco.com
Web xstreco.com