Sandoz Enterprise Risk Management Framework

SANDOZ

01

Introduction

to our Enterprise Risk Management Framework

At Sandoz we aim to address evolving global uncertainties and risks through our integrated risk management approach that supports our strategic goals. The Enterprise Risk Management (ERM) Framework is underpinned by our internal policies and guidelines, which provide guidance across the organisation to safeguard our commitments and reputation.

By defining principles, processes, and roles under the ERM Framework, we aim at strengthening accountability, fostering transparency, upholding corporate responsibility and executing our business practices with integrity.

Our ERM Framework sets out the key components of the Sandoz Risk Management System, addressing both strategic and operational risk management while reinforcing enterprise resilience organisation-wide. It clarifies responsibilities and information flows across the organisation — from frontline teams to the Board — to enable early risk detection, effective prioritisation and response, and continuous efforts to build a resilient company. This enables sustainable business performance and, most importantly, allows millions of patients worldwide to access affordable medicines.

It applies globally to Sandoz' employees, external workers and third parties acting on its behalf.

SANDOZ

02

Our approach

to building and maintaining an organisation-wide Risk Management System

We operate a structured system that is aligned with the principles of ISO 31000:2018 and the framework of the Committee of Sponsoring Organisations of the Treadway Commission (COSO), both being international standards for risk management. The key principles establish clear role definition, effective communication, an integrated approach to risk management, and a culture of continuous improvement, reinforced by independent assurance from Internal and External Audit.

The ERM Framework was developed in close collaboration with key risk-relevant functions – including Corporate Legal and Compliance, Internal Controls, ESG, HSE, Quality, Data Privacy, Corporate Security, Business Continuity, Information Security, Internal Audit and others. Their input was gathered through one-on-one interviews that helped clarify current practices, interdependencies, and areas for improvement. Supported by subsequent functional alignments and external benchmarking, it now serves as the enterprise risk management framework for Sandoz.

To maintain its relevance and effectiveness, the ERM Framework undergoes continuous improvement and is subject to at least biennial updates. In addition, it provides guidance for individual risk functions to review their operational risk frameworks annually – or more frequently when required – to keep pace with regulatory and organisational changes.

SANDOZ

02 Our approach
to the Risk Management System

Internal risk factors

Risks that originate within the organisation and are shaped by internal decisions, processes, people, culture, and systems under management's direct influence.

External risk factors

Risk factors that rise from the broader environment and are driven by political, economic, social, technological, environmental, and legal forces that shape the organisation's operating landscape and lie outside its control.

Under Sandoz's ERM Framework, we aim to assess both internal factors and external influences that shape our risk profile. By grounding assessments in this comprehensive paradigm, Sandoz enables consistent, forward-looking risk identification, assessment, and decision-making across the organisation.

Internal drivers: product development and portfolio; manufacturing and supply chain topics; financial compliance and management aspects, such as tax, treasury, insurance; commercial execution, such as marketing and selling practices; people and organisation aspects; health, safety and environmental aspects; technology and information security matters; compliance, regulatory and legal aspects.

External drivers: political (government stability, regulatory frameworks, legislative changes, geopolitics); economic (GDP trends, market growth, inflation, interest-rate environment, credit availability, exchange rates); social (demographic shifts, workforce skills, cultural norms, community expectations); technological (emerging technologies and automation, connectivity infrastructure, patent activity, licensing frameworks, data protection); natural environment and legal landscape.*

*These categories highlight major risk factors and are not exhaustive.

03 Components
of the Risk Management System

Strategic Risk Management

Operational Risk Management

Resilience Management

SANDOZ

03 Components
of the Risk Management System

Strategic Risk Management

At Sandoz, we define **Strategic Risk Management** as a regular top-down process for identifying, assessing, and managing significant (material) risks – including both threats and opportunities – that relate to future uncertainty and the achievement of the company's strategic objectives. Defined by the Strategic Risk Management Policy, it supports Sandoz's ability to deliver on its financial and non-financial commitments it discloses externally. Structured through an **annual cycle**, it combines collaboration across Global Risk Units and continuous dialogue with the Sandoz Executive Committee, Audit, Risk & Compliance Committee and the Board.

Strategic Risk Management follows the process steps defined in ISO 31000:2018 and is managed by the Global Risk Unit Coordinators, overseen by the Sandoz Leadership Team, and reviewed by the Board, with material risk summaries disclosed in the Integrated Annual Report. Although designed as a top-down process, all employees are encouraged to raise material risks through established reporting lines, supporting a risk-aware culture and effective enterprise-wide risk management.

SANDOZ

03 Components
of the Risk Management System

Operational Risk Management

Operational Risk Management is a continuous, bottom-up process of identifying, reporting, assessing, mitigating, and monitoring risks arising from day-to-day business activities that may affect execution. It relies on a steady flow of information from designated Risk / Response Coordinators or other trained individuals within global functions or Sandoz Group Entities through established reporting lines to the respective Global Risk and Control Oversight Owner(s) and all the way up to permanent Board Committees – such as Audit, Risk & Compliance Committee, Human Capital & ESG Committee, Science, Innovation & Development Committee – and the Board as appropriate.

Established global risk-related structures or processes – such as Corporate Governance & Swiss Law, Internal Controls (MCS), External Controls (TPRM) and Global Insurance – are essential in supporting designated Global Risk and Control Oversight Owners and, in certain situations, directly supporting Risk Owners across the organisation in delivering exposure control, compliance, reliable reporting, and balance sheet protection.

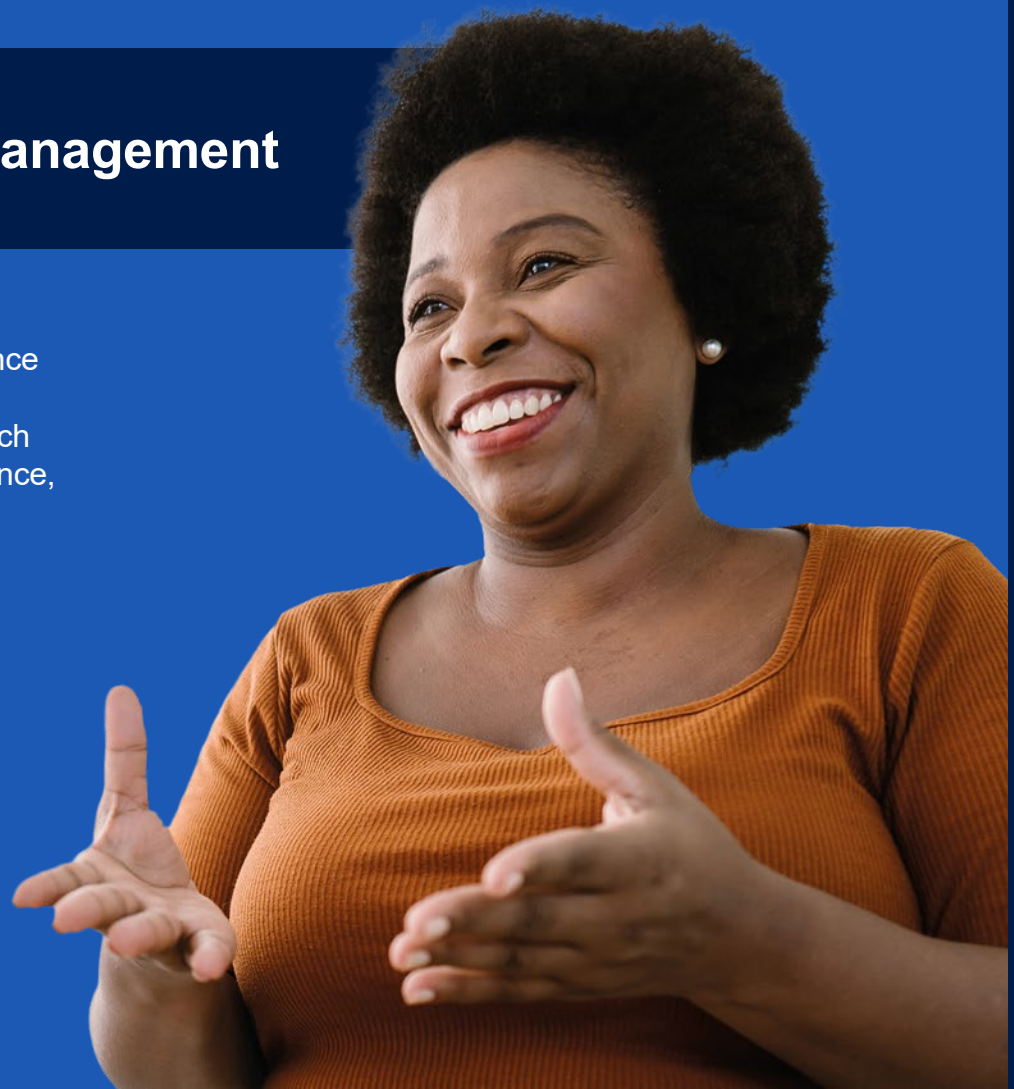
The Operational Risk Management Guideline serves as the foundation for ORM and provides guidance on the expected roles and remits:
(1) Global Risk and Control Oversight Owners in embedding recommendations in their respective risk management frameworks, (2) Group Entities, (3) Line Management, (4) Employees, (5) Third parties.
Sandoz requires employees, external workers and third parties acting on its behalf to comply with applicable laws, regulations, and Sandoz's established policies and procedures. They should escalate incidents, breaches, adverse events, and control failures internally in accordance with established policies and procedures – normally to the Global Risk and Control Oversight Owner and their teams – and, where applicable, report them timely to the authorities.

SANDOZ

03 Components
of the Risk Management System

Resilience Management

Sandoz's commitment to organisational resilience and sustainable performance is anchored in its Business Continuity Management System, which is aligned with the Information Security, Resilience, and Compliance framework to ensure a coordinated and comprehensive approach.



To safeguard resilience and reputation, and in addition to the routine escalation processes and mandatory incident reporting through established reporting lines, two mechanisms apply company-wide to ensure adherence to applicable regulations:

Mandatory Crisis Escalation

This mechanism activates crisis response and informs relevant governance structures under the Crisis Management Framework. It includes where applicable, the escalation of crisis events from site or country Crisis Management Teams to the Global Crisis Management Team, in accordance with the Crisis Management Handbook. The Global Crisis Management Team, in turn, communicates relevant information to the Disclosure Committee, in line with the Ad Hoc Policy, as deemed necessary.

Escalation via the Whistleblower programme

The whistleblower programme at Sandoz, namely the SpeakUp programme, enables employees and third parties to (anonymously) report misconduct without fear of retaliation. Whistleblowing serves as a vital safeguard by surfacing issues early and highlighting potential threats to Sandoz's culture of integrity, enabling appropriate governance and management responses that support sustainable performance, reputation, and stakeholder trust.

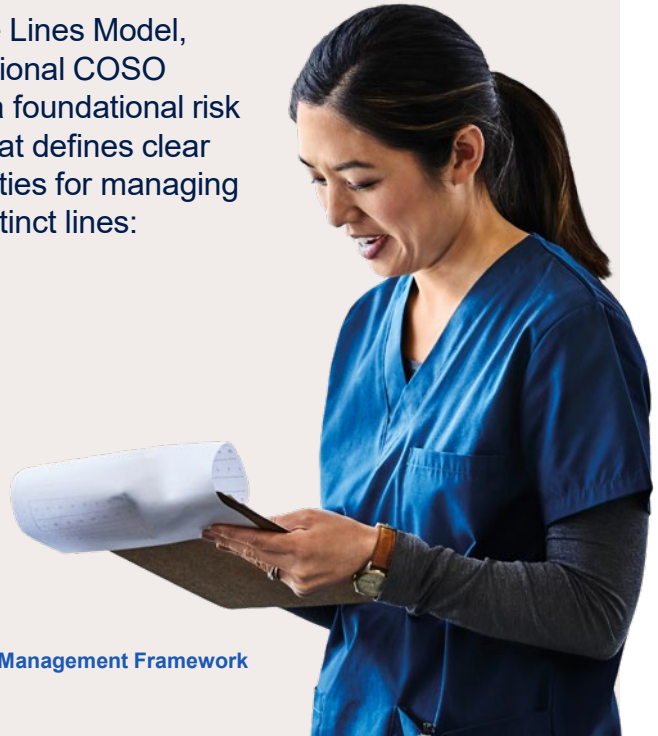
SANDOZ

04

Risk governance

grounded in the Three Lines Model

At Sandoz, the Three Lines Model, based on the international COSO standard, serves as a foundational risk governance model that defines clear roles and responsibilities for managing risks across three distinct lines:



First Line
Risk Owners

The First Line is formed by front line and employees, who are directly responsible for managing, executing processes and activities that generate risk. Their primary role is to achieve business objectives through risk-informed decisions. They are the ones who are responsible for identifying, assessing, and proactively managing risks.

Second Line
Risk and Control Oversight

The Second Line comprises risk management and control functions. These functions provide expertise, policies, and tools to enable the First Line to manage risks consistently and effectively including the coordination of risk management and response through Risk Coordinators and Response Coordinators. They hold oversight responsibilities for specific risk areas and apply ongoing monitoring to ensure that risk exposure remains within boundaries aligned with Board expectations, Executive Committee's and regulatory requirements. In addition, the Second Line tracks the evolving regulatory landscape and conducts proactive horizon scanning to identify emerging risks, thereby maintaining organisational responsiveness and preparedness.

Third Line
Risk Assurance

The Third Line is fulfilled by the internal audit function, which operates independently from the First and Second Lines and delivers impartial evaluation of governance, risk management, and controls effectiveness.

SANDOZ

04 Risk governance
grounded in the Three Lines Model

Sandoz AG Board of Directors & Permanent Committees (ARCC, HC&ESGC, SIDC)

Sandoz Executive Committee (SLT)

General Counsel and Chief Compliance Officer

External assurance

1st Line	2nd Line	3rd Line
Day-to-day business and risk ownership	Functional risk management support	Internal assurance
• **Line management (Risk Unit Head/ Risk Owner/ Action Plan Owner)** Group Global Functions, Group Affiliates	• **Chief Integrity Officer* and ERM function** • **Global Risk Unit Coordinator (SRM)** • **Risk and Control Oversight Owner (ORM)** • **Risk / Response Coordinator (ORM)** Legal and Compliance functions including Regulatory, ISRM, HSE, Sustainability	• **Internal Audit*** • **Other internal audit functions**

External Audit

Business Process Owner | Technical System Owner

Responsible for identifying, assessing, managing and reporting risks

Implement processes and procedures

Provide expertise, policies and tools to support the first line in managing risks

Have oversight responsibilities for specific risk areas

Monitor the evolving regulatory landscape

Deliver impartial evaluation of governance, risk management, and controls effectiveness

*Holds a dotted reporting line to the chair of the Audit, Risk and Compliance Committee (ARCC) | SRM - Strategic Risk Management | ORM - Operational Risk Management | HC&ESGC – Human Capital & ESG Committee | SIDC – Science, Innovation & Development Committee

SANDOZ