IOD GRC Opinion, Building Blocks: Risk Management

Internal Oversight Division

IA-2025-06.B

January 30, 2026

Table of Content

1

Executive Summary

As part of forming an annual opinion on WIPO's Governance**, Risk Management** and Internal Controls for the year ended December 31, 2025, the Internal Oversight Division (IOD) sought to understand the applicable framework, policy and governance structures for Risk Management at WIPO.

Conclusion

The applicable framework, policy and governance structures for Risk Management at WIPO are understood by IOD and summarized in the following pages of this report.	**Understanding Obtained**

Expected Results – as set out in the WIPO Program of Work and Budget for 2024/25. Link.

ERM – Enterprise Risk Management

2

Background:

Risk Management – What is it, and what components did we look at?

Risk Management - A process to identify, assess, manage, and control potential events or situations to provide reasonable assurance regarding the achievement of the organization's objectives. Source: Global Internal Audit Standards

Risk Management Elements were synthesized from the following two documents:

- Reference Maturity Model for Risk Management in the UN System (UN System Chief Executives Board for Coordination)
- Assessing the Risk Management Process, 2nd Edition Global Practice Guide (The Institute of Internal Auditors).

Elements of Risk Management understood by IOD

3

Objectives, Scope, Methodology

Objectives

Obtain an understanding of Risk Management at WIPO.

Scope

Operations in 2025

(Previous periods reviewed for historical insights)

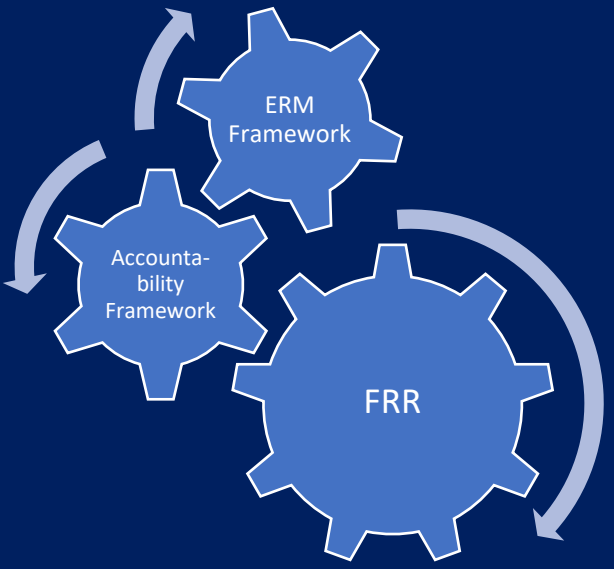
Metho-dology

- Review and analyses of documents
- Inquiries
- Walkthroughs

International Professional Practices Framework® (IPPF)

4.1

ERM Framework and Policy



The ERM Framework is integrated in WIPO strategy setting, planning, decision making and enterprise integrated performance management.

Key Documents defining the Risk Management Framework at WIPO

WIPO Financial Regulations and Rules (FRR)

Regulation 5.1
The Director General shall establish frameworks for Results-Based Management, **Enterprise Risk Management**, and internal controls. These frameworks shall be components of the Organization's accountability framework, providing assurance on performance, results and the effective and economic use of resources to Member States.

WIPO Accountability Framework

The WIPO Accountability Framework provides a comprehensive view of the components that provide assurance of the Organization's system of governance and accountability to its Member States, customers, and other stakeholders. The Framework draws on best practices from the public and private sectors, particularly the Committee of Sponsoring Organizations of the Treadway Commission's (COSO) Internal Control - Integrated Framework. Part of the WIPO Accountability Framework (refer to IOD report IA-2025-06.A2) is tied to the **Risk Management**.

WIPO Risk Management Framework

WIPO Risk Management Policy Office Instruction N° 2/2024

The Policy describes WIPO's approach to managing its risks and controls in a systematic, structured and consistent way in order to support the achievement of the Expected Results, including the strategic and project objectives, within the Strategic Pillars in the WIPO Medium-Term Strategic Plan (MTSP)

WIPO Risk Appetite Statement

Provides guidance on risk strategy, based on the evaluation of opportunities and threats to achieving the Expected Results contained within the Strategic Pillars in the WIPO MTSP.

Reviewed by WIPO Program and Budget Committee at its 34th session in June 2022.

WIPO Risk Handbook

The Handbook provides specific methods, tools and strategies for managing and responding to risks.

4.2

ERM: Governance Structure

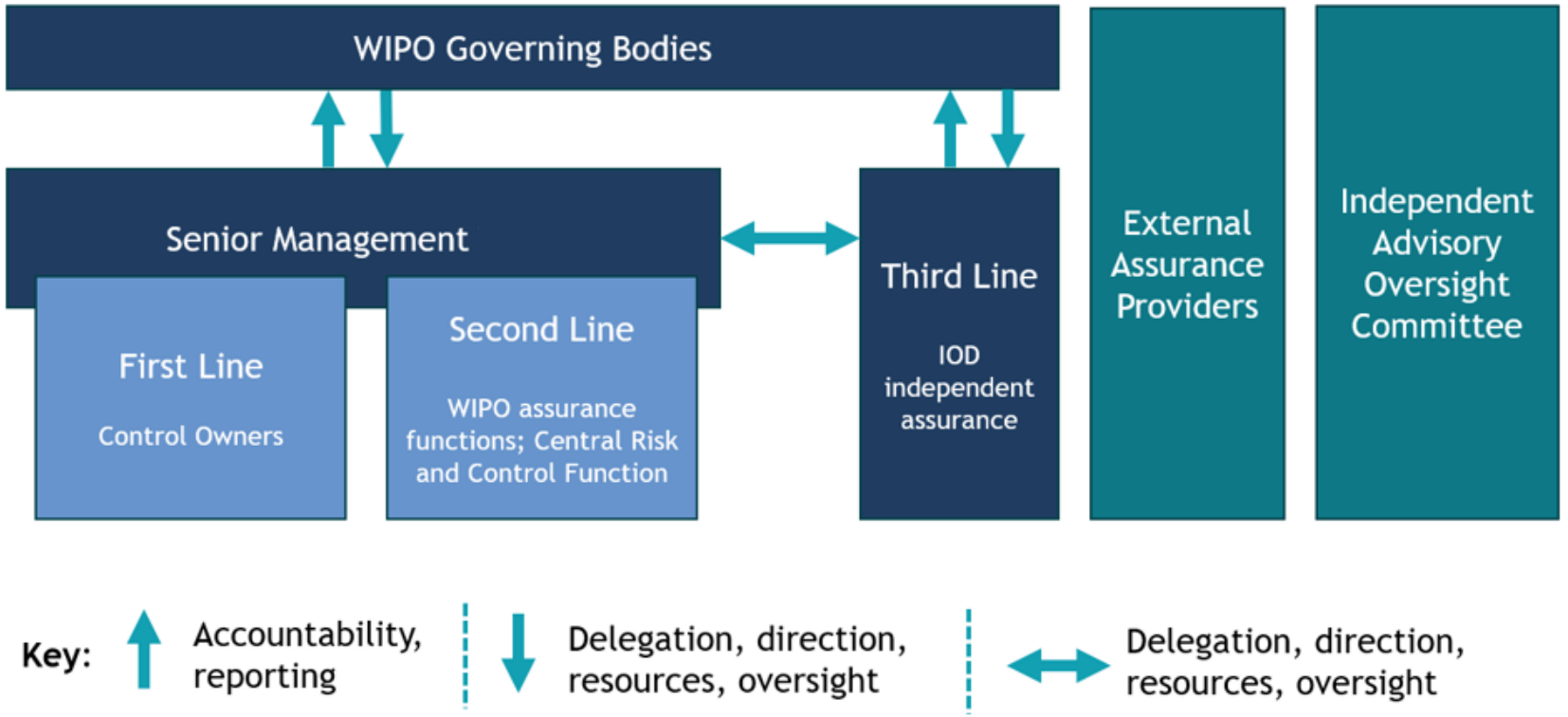
WIPO Governing Bodies - comprise of the WIPO General Assemblies, WIPO Conference, Coordination Committee (CoCo), and Program and Budget Committee (PBC).

First Line roles - (control owners) lead and direct actions (including managing risk) and application of resources to achieve WIPO's expected results. Through the Sector Leads, they maintain a continuous dialogue with Governing Bodies, and report on planned, actual, and expected outcomes linked to the objectives of the organization; and risk. Further, they establish and maintain appropriate structures and processes for the management of operations and risk (including internal control) and ensure compliance with legal, regulatory, and ethical expectations.

Second Line roles - provide complementary expertise, support, monitoring, and challenge related to the management of risk, including:
(a) The development, implementation, and continuous improvement of risk management practices (including internal control) at a process, systems, and entity level. (b) The achievement of risk management objectives. In addition, the Second Line roles provide analysis and reports on the adequacy and effectiveness of risk management (including internal control).

Integration of Risk Governance Structure: The Three Lines Model Applied at WIPO

WIPO has integrated its risk governance structure (Three Lines Model), applying it across its operations (including WIPO Headquarters, External Offices, and Projects).



Third Line - represented by the Internal Oversight Division (IOD), which maintains primary accountability to WIPO governing bodies and independence from the responsibilities of management. IOD communicates independent and objective assurance and advice to the Senior Management Team and WIPO governing bodies on the adequacy and effectiveness of the governance, risk management, and control processes that impact the achievement of WIPO's objectives and Expected Results. In addition, IOD reports impairments to independence and objectivity to WIPO governing bodies and implements safeguards as required. IOD operates under the WIPO Internal Oversight Charter.

External Assurance Providers - include External Auditors (Terms of Reference Governing External Audit).

The Independent Advisory Oversight Committee (IAOC) - operates as an independent expert advisory and external oversight body, under terms of reference approved by the General Assembly upon recommendation by the PBC. IAOC operates under the Terms of Reference of the WIPO Independent Advisory Oversight Committee.

4.2.1

ERM: Delegation of Authority and RM Functions

While Risk Management is a shared responsibility of every personnel member in the organization, senior leadership is ultimately accountable for it.

IOD – Internal Oversight Division
ICS – Individual Contractor Services
AFMS – Administration and Finance Management Sector

For the details of functions, refer to the next slide.

Hierarchy of functions dealing with Risk Management at WIPO

4.2.2 DETAILS ON KEY WIPO RISK MANAGEMENT FUNCTIONS AND THEIR MAIN RESPONSIBILITIES

Director General

The Director General, being the chief executive of the Organization (WIPO Convention, Article 9) is ultimately responsible for all processes at WIPO, including the Risk Management.

Risk Management Group (RMG)

- Reviews and monitors WIPO's financial situation and the key risks to the achievement of the Organization's expected results.
- Approves the risk strategy and proposes a suitable Organizational risk appetite for approval by Member States.
- Reviews and confirms key risks at the organizational level.
- Endorses the assessment of, and response to significant organizational Risks.
- The Terms of Reference and composition of the RMG is set out by the Director General in Information Circular No 15/2024
- The Director IOD is an observer at the RMG.

Governance, Risk, and Compliance (GRC) Section

- Comprehensive risk reporting and development of the Organization's risk and internal controls management strategy.
- Coordinating and enhancing the risk and control management processes of the Organization.
- Escalating risk management and internal control issues to the RMG.
- Reporting risk information.
- Ensuring that organization-level risks are adequately identified and recorded in the WIPO Enterprise Risk Management (ERM) system.
- Assessing the design and the operating effectiveness of controls.

Risk Officers – Security and Information Assurance Division (SIAD)

The Information Risk Officer from the Information Security Section is responsible for coordinating Information Security related risks.

The Security and Travel Risk Analyst from the Safety and Security Coordination Service is responsible for physical safety and security related risks.

Internal Oversight Division (IOD)

As per WIPO Internal Oversight Charer, the mission of IOD is to provide independent and objective oversight services that enhance WIPO's operations, governance, risk management, and internal controls and support the achievement of the Organization's mission, goals, and objectives.

The Global Internal Audit Standards require Internal Auditors to bring a systematic, disciplined approach to evaluate and improve the effectiveness of governance, risk management, and control processes.

Sector Risk Coordinators (SRCs)

SRCs support the Sector Leads by facilitating an effective risk and internal control management process. They help keep risks and mitigation plans up to date in the Enterprise Risk Management system. Further, SRCs coordinate with the organizational unit heads in the Sector and the GRC section, located in the Planning, Budget, and Risk Management Division. SRCs also assist with risk escalation in line with the risk appetite, analyzing risk events should they occur, and reporting on risks and risk responses. The listing of SRCs is provided on the WIPO Risk Management and Internal Controls Homepage.

Business Continuity Coordinator (BCC)

A Business Continuity Coordinator is responsible for supporting business continuity efforts. Beyond crisis management, the BCC also considers post-incident "lessons learned", to identify evolving gaps and requirements for the continuous strengthening of the Organization's resilience.

Other Personnel

The Risk Management at WIPO is a shared responsibility of every personnel member, meaning that each personnel member is part of the risk management process.

Risks are assigned to responsible "Risk Managers" – usually WIPO Senior Leadership - who manage assigned risks. Organizational and Sector risks are recorded in the WIPO ERM (Enterprise Risk Management) system.

4.3

ERM Process and Integration

The Process ensures that risks and opportunities that may affect organizational results are effectively identified, assessed, and responded to, communicated, and monitored as per the ERM framework.

Integration ensures that the interaction/interlinkages with related risk sub-processes or other organizational processes are clearly established.

ERM – Enterprise Risk Management
HQ – Headquarters

ERM process and its integration in Internal Controls and Planning

ERM Process

- WIPO has implemented a systematic risk management process with methodology (go to slide 4.1), which is regularly reviewed and assessed (for example: update of the Risk Handbook in 2025; Risk Appetite Statement in 2024; Internal Audit of Risk Management in 2022: IA 2021-01).
- The ERM Process is equally applicable across WIPO operations (HQ, External Offices, and projects).

Integration with internal controls

- WIPO risks are maintained in the dedicated ERM system. Risks are linked to internal controls and mitigating actions.
- Controls and mitigating actions for all key processes are documented, assessed, assigned ownership, and control criteria are established to measure the control effectiveness and subsequent residual risk assessments (refer to Risk Handbook for details).

Integration with planning

- Results-based planning is linked to risk management. The WIPO Program of Work and Budget includes key risks critical to WIPO. This ensures that resources for mitigation planning are incorporated and budgeted for.

4.4

ERM Systems and Tools

Systems and Tools are the IT components used to record, analyze, integrate, and communicate/report on risk information.

Risk Managers and Sector Risk Coordinators can access the ERM system through the WIPO AIMS Portal to record risk information.

The Internal Oversight Division has read-only WIPO ERM and BI Analytics access. The information from Cherwell ISMS is accessible to IOD by request.

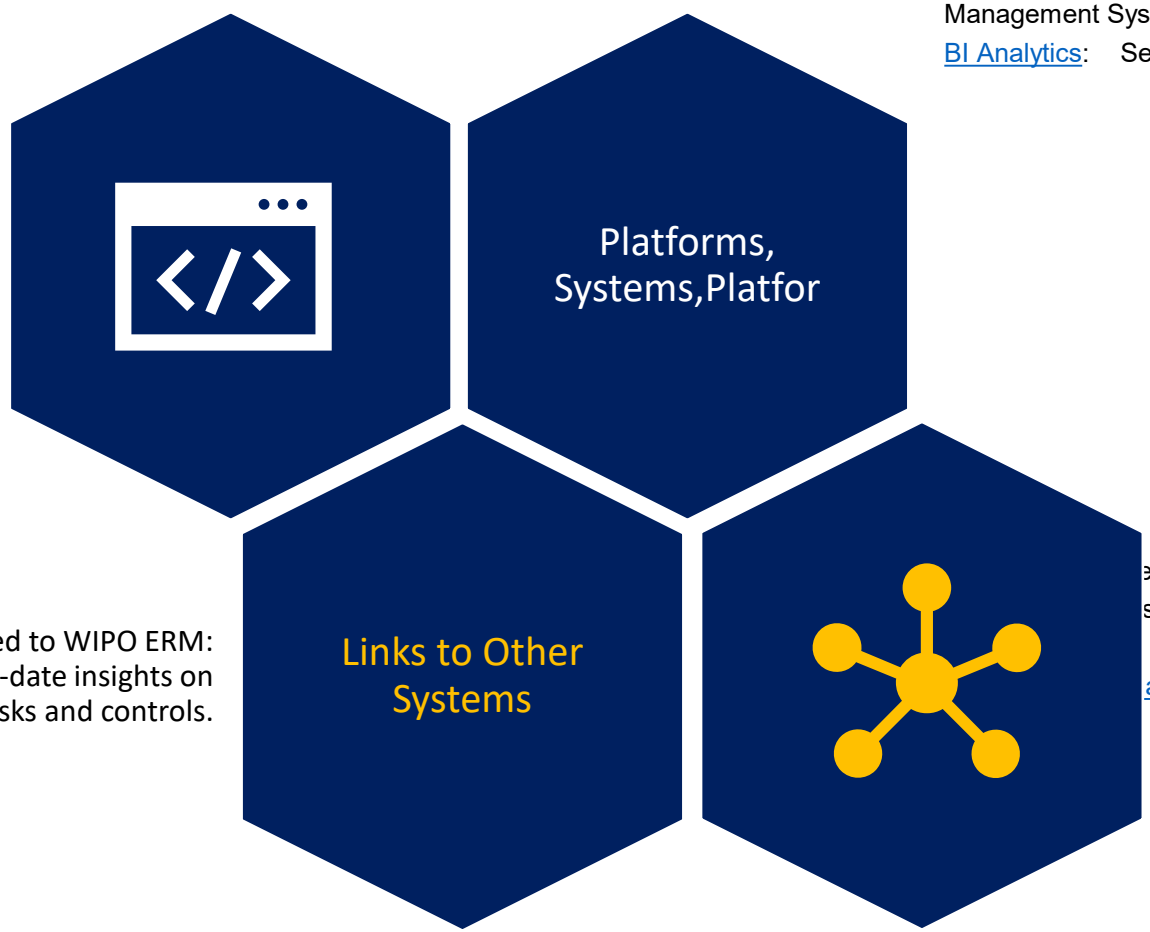
ERM – Enterprise Risk Management
ISMS – Information Security Management System
BI – Business Intelligence

Overview of WIPO Key Risk Management Tools and Systems

WIPO ERM: Acuity

Information Security Specific Risk Management System: Cherwell ISMS

BI Analytics: See the screensh



ent Dashboard
s Audit Dashboard

agement Template

BI Dashboards are linked to WIPO ERM: Acuity , ensuring up-to-date insights on risks and controls.

4.5

Risk Capabilities

Risk Capabilities are the skills, abilities, knowledge, and capacity that an organization must possess to effectively manage risks.

Risk Management Self-paced eLearning and other trainings:

- ACAD/HRMD: Introduction to Risk Management (ELM-3193-1)
- ACAD/HRMD: Risk Management for Decision Makers (ELM-3194-1)
- COSO Internal Control Certificate course.

WIPO Risk Management Training Materials

•ERM Training Tutorials

- ERM – Add Risk, Risk Assessment and Risk Response
- ERM – Closing a Risk or Risk Response
- ERM – How Do You Accept a Risk?
- ERM - You need a Risk Report

Elements of Risk Management assessed by IOD

- The WIPO Core Values and Organizational Competencies emphasize effective behaviors such as taking measured risks and learning from failure.
- The Risk Management Policy states that risk management is a shared responsibility across the organization—both Management and Personnel are accountable.
- The Risk Management Training Program includes various RM training courses and tutorials (see examples on the left side of the slide).

- WIPO has multiple functions that are explicitly involved in risk management processes. Refer to Slide 4.2.2.
- The WIPO Program of Work and Budget includes key risks critical to WIPO. This ensures that resources for mitigation planning are incorporated and budgeted for.

- Dynamic Business Intelligence (BI) dashboards provide access to current and historical views of WIPO's risks.
- WIPO risks are regularly reported through:
  - Risk Management Group reports
  - Annual and quarterly risk reports of the Governance, Risk, and Compliance section
  - WIPO Annual Reports

4.6

Risk Culture

Risk Culture is the set of shared values, beliefs, knowledge, attitudes, and understanding about risk that shape how individuals and groups within the organization behave when managing risk.

Key Elements of Risk Management Culture at WIPO

- "High standards of governance and risk management are key to our success." (The Report of the Director General to the Assemblies of WIPO)
- Risk management is integrated in WIPO Medium Term Strategic Plan (MTSP)

- Published, easy-to-find Risk Management Policy, Risk Appetite Statement, and other guidance on Risk Management and Internal Controls Homepage.
- Business Intelligence (BI) dashboards provide current and historical views of WIPO's risks.

- Sector Risk Coordinators meet regularly with relevant Sectors to update risks and capture risk management successes and failures.

- "Risk Management is an Organization-wide responsibility, supported by continuous learning and training (WIPO Risk Management Policy)

- The WIPO Risk Appetite Statement is used for strategic decision-making.
- WIPO risks are dynamically updated, including the inputs of the WIPO Risk Management Group.

WIPO Risk Management Principles (WIPO Risk Management Policy)

a) It is an **Organization-wide responsibility**, supported by continuous learning and training. Both Management and Personnel share accountability.

b) The **calculated risk taking in pursuit of Expected Results is encouraged**, based on reliable information, prioritization, materiality, and in line with the risk appetite statement.

c) It is an **integrated and iterative process** embedded in all aspects of WIPO's business processes, including annual and biennial Results-Based management cycles.

d) Risks are **communicated promptly, transparently, and consistently** across the Organization.

Acknowledgement

IOD wishes to thank all relevant colleagues for their assistance, cooperation, and interest during this assignment.

Consolidated by: Dainis Reinieks, Acting Head, Internal Audit Section

Reviewed and approved by: Julie Nyang'aya, Director, IOD.