ITUCOUNCIL
GENEVA2026
28 April – 8 May 2026 - Geneva, Switzerland

Document C26/INF/11
10 April 2026
English only

Note by the Secretary-General

ASSESS ITU'S RISK MANAGEMENT FRAMEWORK AND SUPPORT IMPLEMENTATION OF AUDIT RECOMMENDATIONS

Purpose

As part of ITU's ongoing efforts to strengthen enterprise risk management (ERM) practices, and as decided by the Risk Management and Internal Controls Task Force (RMIC-TF), ITU conducted an assessment of ITU's Risk Management and Internal Controls Framework, supported by EY. The assessment provided insights into the organization's current risk management and internal controls maturity across key dimensions, including governance, risk management integration, capabilities, and business-level performance, culminating in a roadmap for improvements. Following consultation with IMAC, this final version of the report provides enhanced context to complement Document C26/49 on strengthening risk management and the internal control system.

Action required by the Council

This document is transmitted to the Council **for information**.

International Telecommunication Union (ITU)

Assess ITU's Risk Management Framework and Support Implementation of Audit Recommendations

April 2026

The better the question. The better the answer.
The better the world works.

Building a better working world

Executive Summary

- The International Telecommunication Union (ITU) engaged the EY team to evaluate the effectiveness of its existing risk management framework against internationally recognized standards, including COSO ERM 2017 and ISO 31000:2018. The assessment highlighted some foundational gaps that limit ITU's ability to proactively manage enterprise level risks and align risk-taking with strategic objectives.

- Some of the Key observations indicate that:
  - ITU's current governance structure provides limited strategic oversight, creating potential blind spots in decision making and weakening accountability.
  - Additionally, the absence of a defined risk appetite framework results in inconsistent risk-taking behaviors that may either constrain performance or expose the organization to undue vulnerabilities.
  - The review also identified operational gaps in risk identification, escalation, and tracking processes, increasing the likelihood that emerging risks remain unaddressed until they escalate into operational or compliance issues. The detailed key takeaways in further areas of integration in planning & performance, coordinated Risk management and technology enablement are listed in the detailed report.

- To support ITU's journey toward a more mature and sustainable risk management function, a comprehensive implementation roadmap has been developed. This roadmap outlines the actionable steps required to evolve the current framework into a more proactive, integrated, and resilient risk management capability.

ERM Maturity Assessment – Key Takeaways

	Key Observations	Key Takeaways for Management
Risk Governance	• Risk Management function not positioned for strategic oversight • Risk Management manual not updated • Lack of proactive risk culture and communication	• The current governance structure does not provide strategic oversight, limiting the ability to anticipate and manage enterprise-level risks. This exposes the organization to potential blind spots in decision-making and accountability.
Risk Vision & Appetite	• Risk appetite and tolerance statement to be reviewed and enhanced	• The absence of a robust risk appetite framework means that risk-taking is not consistently aligned with business objectives. This can lead to either excessive caution or unmanaged exposure, impacting growth and resilience.
Risk Management Process	• Gaps in risk identification and assessment process • Inadequate risk monitoring, escalation, and accountability mechanisms	• Gaps in risk identification, escalation, and tracking mechanisms suggest that emerging risks may not be addressed promptly. This reactive approach increases vulnerability to operational disruptions and compliance failures.
Integration in Planning & Performance Management	• Risk management process not embedded into Strategic and Operational planning process • Risk management accountability across three lines of defence is unclear	• Risk management is not integrated into strategic or operational planning, resulting in decisions being made without considering risk implications. This disconnect can lead to resource misallocation and missed opportunities for risk-informed growth. Additionally, unclear accountability across the three lines of defence weakens governance and increases the likelihood of unmanaged or unresolved risks.
Coordinated Risk Management	• Risk prioritization and mitigation process lack holistic impact assessment and cost-effectiveness consideration • Coordination amongst the assurance functions (i.e. Oversight unit, IT services) for Risk Management activities can be enhanced • Absence of Risk Management training and awareness programs	• The lack of coordination across assurance functions and ineffective training programs point to a siloed approach. Without a unified risk culture, the organization struggles to prioritize risks holistically and implement cost-effective mitigations.
Technology Enablement	• Absence of a comprehensive ERM platform leading to fragmented Risk Management activities	• Absence of a comprehensive ERM platform restricts Management to have a consolidated view of ITU's risk profile, ability to monitor risk trends and respond proactively.

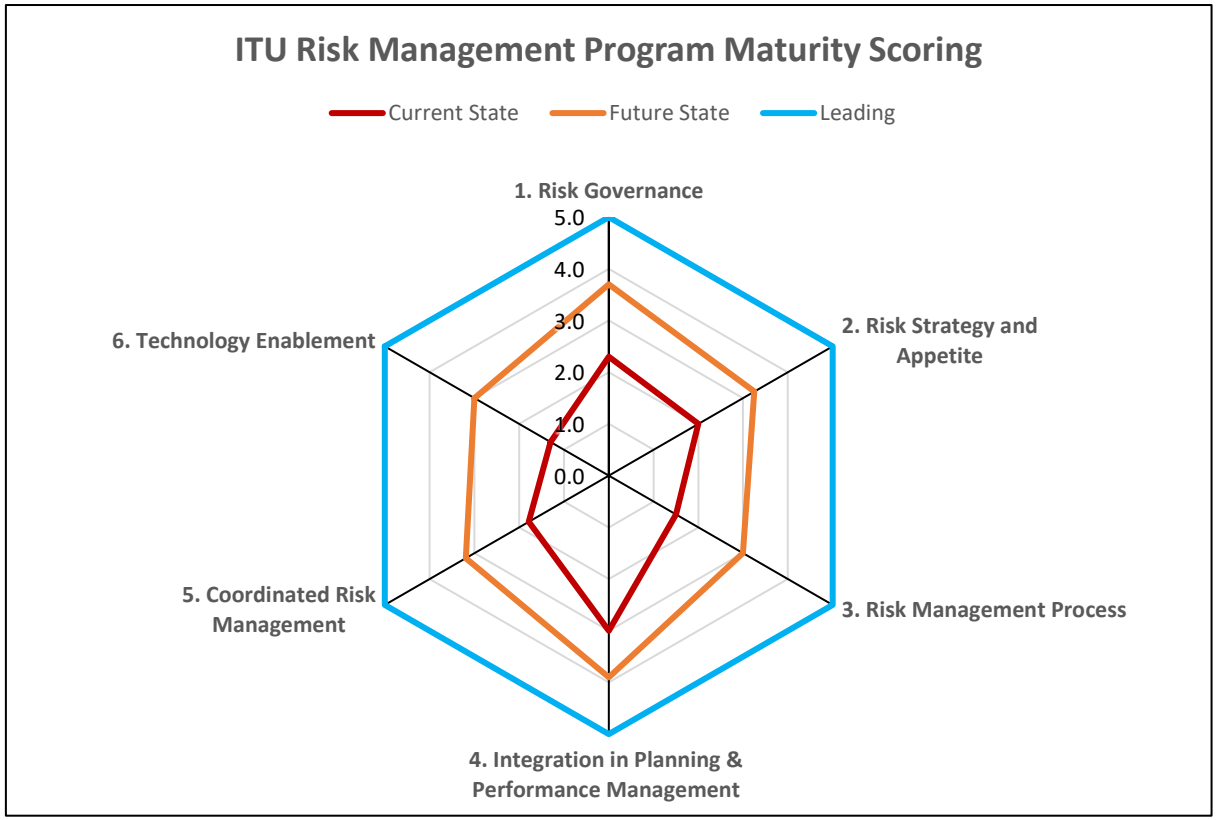
ERM Maturity Assessment Summary

The Maturity diagram depicts ITU's ERM maturity level, as assessed within the context of the six ERM Framework Categories. The overall scoring correlates to an aggregate scale, as defined below:

Maturity Elements*	Current State	Future State	Leading
1. Risk Governance	2.3	3.7	5.0
2. Risk Strategy and Appetite	2.0	3.3	5.0
3. Risk Management Process	1.5	3.0	5.0
4. Integration in Planning & Performance Management	3.0	3.9	5.0
5. Coordinated Risk Management	1.8	3.2	5.0
6. Technology Enablement	1.3	3.0	5.0
Overall	**2.0**	**3.3**	**5.0**

* Maturity elements definitions and details are on slide 8

1. **Basic:** This element is absent/ not evident across the organisation or is inconsistently applied.
2. **Developing:** Methodologies are evolving or are inconsistently applied.
3. **Evolved:** Methodologies are established, understood but still inconsistently applied.
4. **Advanced:** Methodologies are advanced and relatively consistent.
5. **Leading:** Methodologies are reflective of leading practice in design and application.



Risk Management Implementation Roadmap

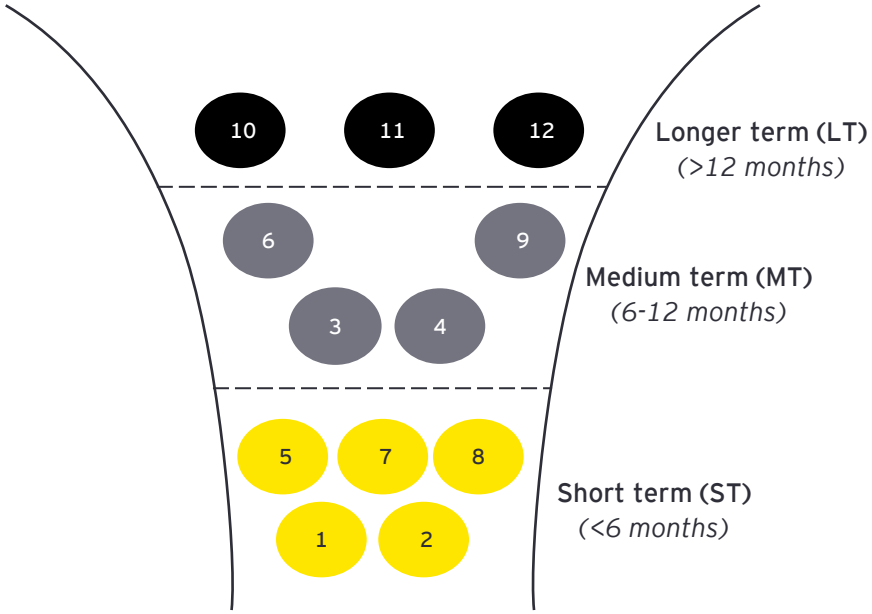
1. Realign Risk Management Reporting and Formalize Governance Structure	2. Revise Risk Management Policy and Manual to Align with Leading Practices	3. Implement Periodic Risk Reviews and Strengthen Risk Culture	4. Update Impact and Assessment Parameters to Ensure Strategic Alignment	5. Redesign Risk Identification and Assessment Process with Standardized Taxonomy	6. Establish Process for Risk Register Updates and KRI Integration
7. Enhance Understanding and Alignment of Risk Strategy with Corporate Objectives	8. Define Roles and Responsibilities Across Three Lines of Defence and Assurance Functions	9. Implement Cost-Effectiveness Evaluation of Risk Mitigation Measures	10. Establish Formal Periodic Review Process for Risk Management Program using KPIs	11. Implement Role-Based Training and Awareness Programs for Risk Management	12. Deploy Centralized ERM Platform for Automation and Real-Time Visibility

Note: *Assumed that the timeframe for implementation of all the recommendations will start April' 2026 onwards.*

Risk Management Implementation Roadmap

Category	#	Recommendation by category	Phase
Risk Governance	1	Reassign the Risk Management/ Manager reporting under the Strategy/ Secretary-General/ Deputy Secretary-General and setup a formal Risk Management Committee (RMC) with clearly defined governance structure, and roles and responsibilities	ST
	2	Revise the Risk Management Policy and Manual to align with leading practices, strategic and operational planning activities and communicate updates across organization	ST
	3	Implement periodic risk reviews and improved reporting for actionable insights; launch initiatives to strengthen the overall risk culture (e.g., leadership communication, risk culture surveys, formalized internal and external communication protocols)	MT
Risk Strategy and Appetite	4	Update impact and assessment parameters to ensure robustness and alignment with strategic priorities; incorporate quantitative measures and control effectiveness for residual risk assessment	MT
Risk Management Process	5	Redesign the risk identification and assessment process to ensure consistency across departments, and develop a comprehensive enterprise risk taxonomy/ universe to standardize risk categorization	ST
	6	Establish a process for regularly updating risk registers with changes to risk drivers, emerging risks, key risk indicators (KRIs), and integrate KRIs with likelihood parameters/ incident reporting for dynamic monitoring and timely escalation of materialized risks to Senior Management/ RMC	MT
Integration in Planning and performance Management	7	Improve understanding and alignment of the risk strategy with corporate objectives across all levels of the organization	ST
	8	Define roles and responsibilities across the Three Lines of Defence and create a coordination mechanism among assurance functions (Ethics, Legal, Information Security)	ST
Coordinated Risk Management	9	Implement the process of evaluating cost-effectiveness of the mitigation measures through comparison with the associated costs, with probable reduction to the risk exposure for informed decision-making	MT
	10	Establish a formal process of periodical review of the Risk Management program. This review should leverage defined KPIs to strengthen accountability and responsibility for Risk Management.	LT
	11	Implement training and awareness program (role-based, scenario-led) to strengthen understanding of Risk Management across the board	LT
Technology Enablement	12	Implement a centralized ERM platform to automate risk identification, assessment, mitigation tracking, and reporting for real-time visibility and data consistency	LT

Prioritized road map



*The underlying assumption is there will be a dedicated and experienced ERM resource to drive the efforts