



Joint Inspection Unit
of the United Nations System

*"Independent
system-wide
inspection, evaluation
and investigation"*

www.unjtu.org

Available only in English

Enterprise risk management: approaches and uses in United Nations system organizations

**Supplementary Papers to Report of the Joint Inspection Unit
(JIU/REP/2020/5)**

Review Highlights

**Appendix I: Enterprise risk management (ERM):
A tool for legislative/governing bodies to
strengthen oversight and accountability**

Prepared by Keiko Kamioka and Eileen A. Cronin



REVIEW OF ENTERPRISE RISK MANAGEMENT: APPROACHES AND USES IN UNITED NATIONS SYSTEM ORGANIZATIONS

Inspectors Keiko Kamioka and Eileen A. Cronin



Background

Enterprise risk management (ERM) has its roots in the private sector and has value in all sectors, including United Nations system entities. United Nations system organizations are exposed to a myriad of risks while delivering on their mandates — from fraud and corruption, reputational risks and cybercrime to risks of a political nature, mismanagement, natural and human-made disasters. In its resolution 61/245, the General Assembly endorsed the adoption of ERM in the United Nations system to enhance governance and oversight.

ERM is an organization-wide process of structured, integrated and systematic identification, analysis, evaluation, treatment and monitoring of risks towards the achievement of organizational objectives. It is fundamentally about managing uncertainty and can include both threats and opportunities.



Objectives & Purpose

The main objective of the present review is to inform legislative/governing bodies and the executive heads of United Nations system organizations about the progress made since the last review (JIU/REP/2010/4), the status of implementation, utilization and integration of ERM practices across all 28 JIU participating organizations, as well as to identify good practices and lessons learned to guide ongoing and future initiatives. It proposes 10 updated benchmarks and assesses the progress of ERM implementation against them.



What the JIU found

1. Adoption of an ERM policy and/or framework is foundational for ERM.

The ERM policy and/or framework needs to be linked to the organization's strategic plan to ensure that it is aligned with management's strategic vision and the organization's goals and objectives. Of the 28 organizations covered in the present review, 25 have adopted an ERM policy and/or framework. Subsequently ten organizations have revised or are currently revising their ERM policy and/or framework. This represents substantive progress since the previous JIU review. Those organizations that have not yet adopted an ERM policy and/or framework are strongly encouraged to do so.

2. Establishing internal organizational structure for ERM is essential.

For successful implementation of ERM, it is essential that each organization establishes its internal organizational structure with clear roles and responsibilities taking into consideration the business model, availability of resources, the particular mandate and the maturity stage of ERM. Most organizations have an ERM unit and/or specific function dedicated to ERM (often called chief risk officer) and a network of risk focal points. Most organizations also have a senior management-level risk committee, which is vital as senior management has the ultimate responsibility for managing risks and achieving strategic goals.

3. "Tone at the top" is crucial for setting a risk culture.

The "tone at the top" is viewed across the participating organizations as the most important driver in setting a risk culture and supporting and empowering staff to advance and integrate ERM within an organization.

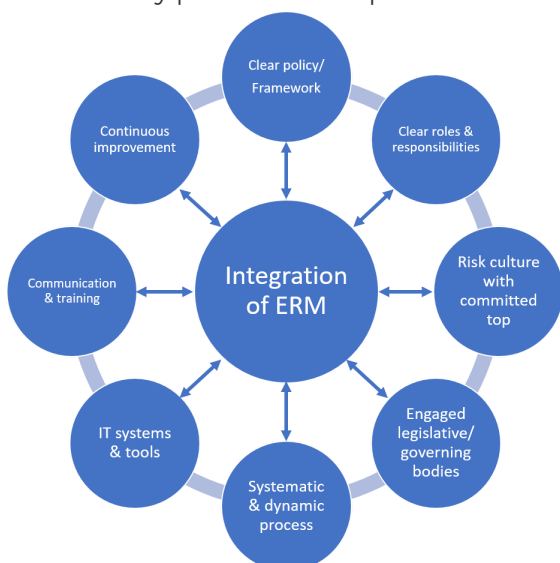
Without appropriate and engaged leadership, ERM could be relegated to a “check the box” exercise. While “tone at the top” regarding ERM has improved over the last decade, more needs to be done in order to further its use and integration. Executive heads must set a tone that supports ERM implementation across the organization, empower staff to sustain it and substantively engage in ERM processes and practices that demonstrates its utility and importance. Each organization needs to have a way to ensure that key risks are escalated to the appropriate levels on a timely basis and that decision makers have the appropriate risk information to make informed decisions.

4. Legislative/governing bodies must be engaged with ERM.

To fulfil their oversight and accountability roles and responsibilities and to prepare for uncertainties, legislative/governing bodies must be engaged with ERM to ensure that executive heads are setting the appropriate “tone at the top”. Audit and oversight committees can play a key role in implementing and sustaining ERM by conveying technical information and providing advice to senior management and their respective legislative/governing body. Most organizations report that ERM is a regular agenda item in their legislative/governing body meetings, but the depth and level of coverage varies. Legislative/governing bodies should incorporate ERM into their meetings, at least annually, with substantive coverage determined by the organization’s mandate, field network and risk exposure.

5. Integrating ERM is challenging but necessary to realize its full benefit.

Integrated and well-managed ERM practices can produce crucial information, such as on the threats and opportunities that an organization is, or may be, facing, and offer a useful forum to discuss and take decisions on how best each risk should be addressed. In order to support such high-level identification and decision-making related to risks, risk management should be an integral part of an organization’s strategic, operational and programmatic planning and monitoring processes. While most organizations have linked ERM with results-based management and/or their regular strategic planning processes, many of them report that gaps exist between ERM and day-to-day operations. Integration of ERM into strategic, business and operational planning processes requires a strong “tone at the top” with effective communication and active support from senior leaders, as well as targeted investments in key processes and platforms.



6. ERM processes need to be practical, agile and user-friendly.

Not only do ERM processes need to be fit for purpose, based on what is appropriate for each organization, but they also need to be adequately dynamic and agile in order to demonstrate the fundamental objectives and utility of ERM. Many organizations are still in the initial stage of ERM maturity, that is, its implementation, and are striving to integrate it with more simplified and accessible processes. Agile ERM practices that incorporate relevant external or contextual data can encourage its maturity and integration within an organization, as well as, enable it to better respond to threats and crises.

7. Well-designed information technology systems and tools can facilitate better integration of ERM.

Well-designed information technology systems and tools can facilitate better integration of ERM into key operations, as well as capture, record, consolidate and monitor key risks throughout the organization. A comprehensive system, with the relevant tools, should be implemented to track and monitor risks across the organization, ideally as part of an integrated platform linked to other systems, in order to streamline processes. A dialogue among organizations with similar business models is encouraged to exchange experiences and practices regarding ERM platforms and their linkages with other information systems.

8. Training and communication are crucial for integrating ERM.

A comprehensive training and communication plan for ERM is essential for its effective implementation and integration and should be tailored to the size and scope of an organization, as well as its approach to ERM. Training approaches range across the participating organizations from stand-alone ERM training to a more integrated approach. With a variety of approaches to training and communication, inter-agency cooperation and exchanges are encouraged in order to share good practices and lessons learned.

9. Periodic and structured reviews of ERM are necessary for continuous improvement.

The effectiveness of ERM processes, practices and policies needs to be reviewed on a periodic basis to allow for adaptation and continuous improvement as external and internal contexts change. A periodic self-assessment is recommended to review progress over time towards reaching an identified ERM target maturity stage. It is also recommended that periodic and independent assessments be made by auditors, individuals tasked with the evaluation function or other independent advisers on the effectiveness of the ERM policy and its associated processes. Legislative/governing bodies should review and consider the results of such assessments.

10. Inter-agency cooperation and coordination is valuable to further ERM.

Since 2010, ERM has grown in importance and prominence in most participating organizations and the Cross-Functional Task Force on Risk Management of the Chief Executive Board for Coordination has made a valuable contribution to recent progress in this area. There is broad support and appreciation for its work. The Task Force should evolve into a viable mechanism to continue its work in supporting ERM at the level of individual organizations as well as system-wide in the development of ERM policies and practices.



What the JIU Recommends

The JIU makes 4 formal recommendations to the executive heads and the legislative/governing bodies of the United Nations system organizations as well as 21 informal recommendations that provide a roadmap implementing the 10 benchmarks.

Executive Heads of United Nations system organizations are called on to:

1 By the end of 2021, undertake a comprehensive review of their ERM implementation against JIU benchmarks 1 to 9, as outlined in the present report.

2 By the end of 2021, ensure that the Cross-Functional Task Force on Risk Management of the High-level Committee on Management of the Chief Executives Board for Coordination is continued as a viable mechanism to further promote and facilitate inter-agency cooperation, coordination, knowledge-sharing and to explore shared risks associated with United Nations reform efforts.

Legislative/governing bodies of the United Nations system organizations are called on to:

3 Incorporate ERM into their meetings at least annually, with substantive coverage determined by the organization's mandate, field network and risk exposure in order to fulfill their oversight roles and responsibilities.

4 By the end of 2022, request executive heads to report on the outcomes of a comprehensive review of the organization's implementation of ERM against JIU benchmarks 1 to 9, as outlined in the present report.

Also available!

Appendix I: Enterprise risk management (ERM)

A tool for legislative/governing bodies to strengthen oversight and accountability provides comprehensive information to support legislative/governing body members in implementing the report's two relevant recommendations and fulfilling their oversight roles and responsibilities regarding ERM.

This document is available on the JIU website.



Approach & Methodology

In accordance with the JIU internal standards, guidelines and working procedures, the review was conducted using a blend of qualitative and quantitative data collection methods, including:



Desk review of relevant documents and literature, as well as an analysis of the data in the JIU web-based tracking system



65 interviews with 102 stakeholders



4 questionnaires to the 28 participating organizations including those to internal auditors, external auditors and chairs of audit and oversight committees; and one questionnaire to the secretariat of the Chief Executives Board for Coordination



A workshop with 16 entities and an internationally recognized ERM expert



Assessment and update of the 2010 JIU benchmarks by using a variety of sources and with the assistance of the international ERM expert



JIU Reports 2020/2019

[JIU/REP/2020/5](#), Enterprise risk management: approaches and uses in United Nations system organizations

[JIU/REP/2020/4](#), Review of management and administration in the Economic Commission for Latin America and the Caribbean

[JIU/REP/2020/3](#), Common premises in the United Nations system: current practices and future prospects

[JIU/REP/2020/2](#), Policies and platforms in support of learning: towards more coherence, coordination and convergence

[JIU/REP/2020/1](#), Review of the state of the investigation function: progress made in the United Nations system organizations in strengthening the investigation function

[JIU/REP/2019/9](#), Review of contemporary practices in the external outsourcing of services to commercial service providers by United Nations system organizations

[JIU/REP/2019/8](#), Review of staff exchange and similar inter-agency mobility measures in United Nations system organizations

[JIU/REP/2019/7](#), Review of the management and administration of the Joint United Nations Programme on HIV/AIDS (UNAIDS)

[JIU/REP/2019/6](#), Review of audit and oversight committees in the United Nations system

[JIU/REP/2019/5](#), Managing cloud computing services in the United Nations system

[JIU/REP/2019/4](#), Review of change management in United Nations system organizations

[JIU/REP/2019/3](#), Review of the integration of disaster risk reduction in the work of the United Nations system in the context of the 2030 Agenda for Sustainable Development

[JIU/REP/2019/2](#), Review of the United Nations System-wide Action Plan on Gender Equality and the Empowerment of Women

[JIU/REP/2019/1](#), Review of management and administration in the International Civil Aviation Organization (ICAO)

For all reports visit: <https://www.unjiu.org/content/reports>



For further information, please contact jiucommunications@un.org

ABOUT THE JIU

The Joint Inspection Unit is the only independent external oversight body of the United Nations system mandated to conduct evaluations, inspections and investigations system-wide.
Visit the JIU website for more information at www.unjiu.org



JIU
Statute



11
Inspectors



Latest
news



Reports, notes
and management letters



Main
thematic areas



2020
Programme of Work



28 Participating
Organizations



Appendix I to JIU report: Enterprise risk management: approaches and uses in United Nations system organizations (JIU/REP/2020/5)

Enterprise risk management (ERM)

A tool for legislative/governing bodies to strengthen oversight and accountability



This appendix is a supplement to the 2020 JIU report “Enterprise Risk Management: approaches and uses in United Nations system organizations”. The review contains **two recommendations** directed towards legislative/governing body members of United Nations system organizations. The information in this appendix is intended to assist legislative/governing body members in implementing these recommendations and fulfilling their oversight roles and responsibilities in terms of ERM.

United Nations system organizations are exposed to a myriad of risks while delivering on their mandates — from fraud and corruption, reputational risks and cybercrime to risks of a political nature, mismanagement, natural and human-made disasters. There is no risk-free path to achieving objectives, and uncertainty is a given in all organizations; all United Nations organizations need to be proactive in managing known and unknown risks.

ERM is about managing uncertainty which includes both threats and opportunities. The concept of ERM embodies the notion that risk management cuts across entire organizations. To be effective, ERM should be both comprehensive and customized based on the organizational context and its related objectives.

✓ What is ERM?

Enterprise risk management (ERM) is a process designed to create, protect and enhance both performance and success by managing risks and uncertainty around goals and objectives. ERM should help to ensure an organization is aware of and managing, at a minimum, its most critical risks.

The key benefits of ERM include:

- **Improves** strategic planning and decision-making and their implementation by ensuring a comprehensive and structured understanding of organizational objectives and related risks.
- **Helps** management identify challenges and uncertainties, adapt to meet challenges, prepare for crises and become more resilient and agile.
- **Highlights** common and cross-cutting risks (including opportunities and threats) and improves organization-wide communication and cooperation.
- **Optimizes** resource allocation and protects assets and organizational reputation.
- **Reinforces** accountability and internal control frameworks.
- **Assists** legislative/governing bodies in fulfilling their oversight and accountability roles and responsibilities by anticipating uncertainties and supporting management in risk-informed decision-making.

An organizational risk register is a central repository of all risks and risk information maintained by an organization, which typically includes:

- risk categories;
- risk descriptions;
- risk owners;
- action plans;
- risk status;
- risk likelihood;
- significance levels of risk; and
- other relevant information pertaining to that risk.

It is a communication and monitoring tool that clearly articulates ownership and the sources of risk to enable the management of those risks and uncertainties.

✓ Concepts & terms

- **Risk** is the effect of uncertainty on organizational objectives. It can address, create or result in opportunities and threats. ERM typically includes processes for identifying, assessing, communicating and managing risks.
- Identified and assessed risks are normally recorded in a **risk register**.
- Each risk is assigned to a **risk owner**. Risk owners are typically in supervisory or managerial positions who are best placed to manage a particular risk and have the relevant technical knowledge, available resources and appropriate authority. Risk owners' responsibilities include assessment, review and management of the assigned risk(s) on an ongoing basis.
- **Action plans** provide details on how risks are addressed and managed.
- An organization's risk-taking approach, commonly known as a **risk appetite**, is the aggregate amount, level and type of risk an organization seeks to accept in pursuit of its mission and strategic objectives.
- A **risk appetite statement** is a document that formally articulates the risk appetite of an organisation in different areas (see box below).
- **Risk capacity** refers to the maximum amount and type of risk an organisation is able to support in pursuit of its strategic objectives.
- **Risk tolerance** is defined as the boundary of risk-taking outside of which the organisation is not prepared to venture.

An organizational risk-taking approach: risk appetite

As risk-taking is an organisational necessity, determining an organization's **risk appetite** or **risk-taking approach** is an element of good governance; it facilitates the alignment with stakeholders, the achievement of strategic objectives and decision-making. Risk appetite is a dynamic concept that can be set by, inter alia, strategic, operational, reputational and financial parameters.

The risk appetite or risk-taking approach of an organization must be anchored and supported by its legislative/governing body. As appropriate, the legislative/governing body should be engaged in its development and ongoing advancement. This involvement, for example through the approval and/or endorsement of a **risk appetite statement**, can provide an opportunity to inform legislative/governing body members, including donors, about ERM and the strategic risks to the organization. Furthermore, it can align the secretariat and the legislative/governing body with respect to the level of risk that the organization should/can take based on factors such as its mandate and resource levels, i.e. its **risk tolerance**.

Engaging legislative/governing body members in the process of setting a risk appetite can build trust and a broader understanding of an organization's ERM practices.

ERM and fit-for-purpose

The intent behind ERM is to provide a single point of reference in respect of key risks, based on which a legislative/governing body and senior management can discuss and agree on how to manage those risks. Therefore, ERM must be tailored to fit an organization with due consideration given to criteria, which include, but are not limited to, its:

- **Mandate:** Is it an operational or normative/standard-setting organization, or both? What would prevent the organization from fulfilling its mission or mandate and/or remaining relevant?
- **Financial and budget considerations:** How is the organization funded and through what mechanisms? How much of its funding is reliant on a few donors and/or entities?
- **Personnel:** How many staff does the organization have and through what types of staffing mechanisms? What are the demographic staffing patterns?
- **Business model:** How does the organization deliver on its mandate, where and with/to whom? How does it manage its administrative and business operations?
- **Organizational particularities:** What issues does the organization face that others in the United Nations system may not, and what are the implications? How is the organization similar to and different from others, and what makes it distinct or provides it with a competitive advantage?

✓ Roles and responsibilities of legislative/governing bodies in ERM

The 2020 JIU report on ERM (JIU/REP/2020/5) contains **two recommendations** directed to legislative/governing bodies. **The first is to incorporate ERM into their meetings at least annually:**

Recommendation: In order to fulfil their oversight roles and responsibilities, legislative/governing bodies should **incorporate ERM into their meetings at least annually**, with substantive coverage determined by the organization’s mandate, field network and risk exposure.

Incorporating ERM into meetings enables legislative/governing body members to provide oversight on its implementation as well as to hold senior management accountable for setting an appropriate “tone at the top” in order to promote ERM’s integration and effective use, in addition to holding senior management accountable for building ERM and managing their risks. As internal and external forces effect change on and within organizations, United Nations system organizations must adjust and respond swiftly and with agility to deliver on their mandates and remain relevant. Therefore, the legislative/governing body members should be knowledgeable about the ERM processes and policies of an organization and should discuss them at least annually.

Below are some specific aspects of ERM that legislative/governing body members should be aware of in fulfilling their oversight roles and responsibilities:

1. Legislative/governing body and donor interests are important drivers for implementing ERM.

Legislative/governing bodies need to be confident that risks are being identified and managed properly.

At a minimum, legislative/governing body members should know:

- if an organization has a systematic and integrated approach to risk management;
- if there are strategies in place for addressing and managing identified risks, and;
- if a risk-taking approach, such as a risk appetite, has been developed and presented to the legislative/governing body for approval.

A good practice is for legislative/governing body members to be brought onboard or given an orientation on the ERM policies and processes of the organization.

2. ERM provides an opportunity to enhance transparency and establish trust between management and legislative/governing bodies.

Legislative/governing body members can open a dialogue with executive heads on risks – as both threats and as opportunities. Ideally a productive dialogue can:

- build trust between management and legislative/governing bodies;
- open up conversations regarding the opportunities that risk taking may afford;
- be a requirement for funding from donors or act as a guideline for strategic allocation of limited resources to where opportunities and threats are higher;
- provide a sense of reality about programmes and projects operating in dangerous contexts.

3. Legislative/governing bodies need to be engaged with ERM practices at the strategic level.

Whereas senior management should manage the organization’s risks, legislative/governing bodies should exercise oversight of those risks and monitor whether ERM processes are effective.

In exercising their oversight roles and responsibilities, legislative/governing bodies should have a clear view of key strategic and other significant risks (including emerging critical risks) as well as ERM strategies of the organization. Governing bodies may want to inquire about a strategic risk analysis to encourage a focus on strategic-risk identification (as opposed to simply labeling some already identified risks as “strategic”).

Legislative/governing body members should be provided with:

- inventory of key strategic and other significant risks an organization is facing;
- how those risks are being addressed;
- policies and framework documents in relation to ERM;
- risk appetite statement and;

- any recent audits or assessments on the effectiveness of ERM policy and process.

Legislative/governing body members could also discuss with senior management how the organization is considering:

- emerging risks, trends and changes in the organizational context and/or;
- major and potential disruptive risks.

4. Audit and oversight committees can provide a bridge between senior management and legislative/governing bodies.

Audit and oversight committees can play a significant role in various aspects of ERM, including:

- providing expertise typically gleaned from other sectors;
- reviewing relevant action plans and metrics or key risk indicators for top risks;
- contributing to the identification of top risks;
- advising on the top risks facing organizations.

5. Legislative/governing bodies need to hold executive heads accountable for setting the appropriate “tone at the top”

Executive heads must set a tone that supports ERM implementation across the organization, empower staff to sustain it and substantively engage in ERM processes and practices that demonstrate its utility and importance. Legislative/governing bodies should ensure that executive heads and senior management are setting the appropriate “tone at the top” and that it is sustained across the organization and through leadership transitions.

To begin a discussion on *tone at the top*, legislative/governing body members could ask executive heads:

- How does the executive head view ERM and its role in the organization?
- How is ERM being used by senior leaders for strategic decision making and how are key risks escalated?
- Is ERM appropriately tailored for the organization? Is it properly staffed and funded?
- When and how are risk conversations occurring?

✓ The JIU’s ERM benchmarks

The second recommendation directed at legislative/governing bodies is intended to hold JIU participating organizations accountable for having effective ERM policies and practices, as measured by an assessment against JIU benchmarks.

Recommendation: By the end of 2022, legislative/governing bodies of participating organizations should **request executive heads to report on the outcomes of a comprehensive review of the organization’s implementation of ERM** against JIU benchmarks 1 through 9.

The JIU benchmarks

1. Adoption of a systematic and organization-wide risk management policy and/or framework linked to the organization’s strategic plan.
2. Formally defined internal organizational structure for ERM with assigned roles and responsibilities.
3. Risk culture fostered by the “tone at the top” with full commitment from all organizational levels.
4. Legislative/governing body engaged with ERM at the appropriate levels.
5. Integration of risk management with key strategic and operational business processes.
6. Established systematic, coherent and dynamic risk management processes.
7. Effective use of information technology systems and tools for ERM.

8. Communication and training plans to create risk awareness, promote risk policy and establish risk capabilities for the implementation of ERM.
9. Periodic and structured review of effectiveness of ERM implementation for continuous improvement.
10. Inter-agency cooperation and coordination for systematic knowledge sharing and management of common and/or United Nations system-wide risks.

These benchmarks are interrelated and ideally, they serve to point an organization towards good practices and identify gaps that are necessary to address for an effective and integrated ERM.

Integration is key to successful ERM

The JIU benchmarks are interdependent, and as benchmark 5 above conveys, ideally direct an organization towards the integration of ERM. An ERM process that is supported by legislative/governing bodies (as in benchmark 4) increases the chances of successful integration. ERM is also easier to integrate when:

- there is a clear ERM policy and/or framework (as referred to in benchmark 1);
- risk owners understand their roles and responsibilities (as in benchmark 2);
- a committed “tone at the top” (benchmark 3) is reinforced;
- ERM tools and systems are accessible and well-designed (as conveyed in benchmark 7);
- there is effective and consistent communication and training (benchmark 8);
- continuous improvement of ERM is viewed as a dynamic process (as in benchmarks 6 and 9).



Interrelation of JIU benchmarks

As benchmark 9 advocates, legislative/governing bodies may want to request a review or independent assessment of ERM be done periodically, which could include using the JIU benchmarks as a reference framework. Subsequent follow-up by the legislative/governing bodies to understand how gaps are addressed is recommended.

Integration of ERM into strategic, business and operational planning processes requires, as benchmark 3 indicates, a strong “tone at the top”, as well as investments and targeted commitments to update and/or enhance platforms and processes that would embed it into an organization’s planning, decision-making and organizational culture.

To view the full JIU report on ERM, visit: https://www.unjiu.org/sites/www.unjiu.org/files/jiu_rep_2020_5_english.pdf

ABOUT THE JIU

The Joint Inspection Unit is the only independent external oversight body of the United Nations system mandated to conduct evaluations, inspections and investigations system-wide.

Visit the JIU website for more information at www.unjiu.org



JIU Statute




11 Inspectors



Latest news



Reports, notes and management letters



Main thematic areas



2020 Programme of Work



28 Participating Organizations