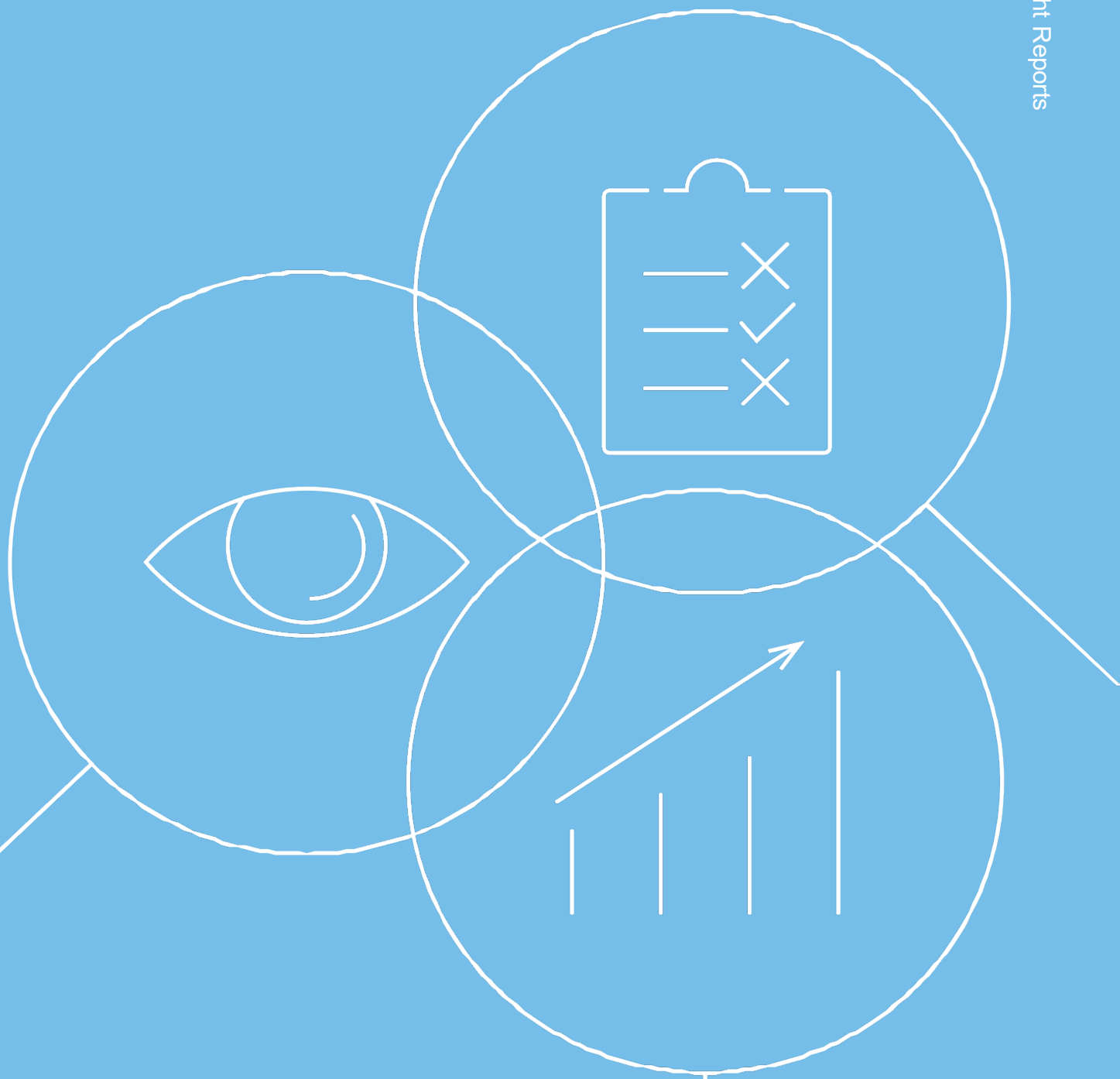


Audit of Enterprise Risk Management

Internal Oversight Reports



IOD Ref: IA 2021-01
March 8, 2022
IOD Audit Engagement



Note: Parts of the original report were withheld or redacted on grounds of information security.

TABLE OF CONTENTS

LIST OF ACRONYMS	3
EXECUTIVE SUMMARY	4
1. BACKGROUND	6
2. ENGAGEMENT OBJECTIVES	8
3. SCOPE AND METHODOLOGY	8
4. ENGAGEMENT RESULTS – OUTCOME(S)	9
5. ENGAGEMENT RESULTS - POSITIVE DEVELOPMENTS	10
6. ENGAGEMENT RESULTS - OBSERVATIONS AND RECOMMENDATIONS	11
(A) IOD SURVEYS	11
(i) IOD Survey on ERM at WIPO	11
(ii) IOD External Survey on ERM with United Nations Representatives of Internal Audit Services (UNRIAS)	11
(B) ERM FRAMEWORK AND POLICY	12
(i) ERM Framework	12
(ii) WIPO Risk Appetite.....	14
(iii) ERM Framework Self-assessment and Improvement mechanisms.....	16
(C) RISK MANAGEMENT GOVERNANCE AND ORGANIZATIONAL STRUCTURE	18
(i) Risk Management Governance System.....	19
(ii) Risk Management Function - Comparison with other Organizations.....	22
(D) PROCESS AND INTEGRATION	24
(i) Risk identification and assessment	24
(ii) Developing Risk Responses.....	26
(iii) Monitoring and Follow-up.....	29
(iv) Statement on Internal Control.....	33
(v) ERM Integration with Results Based Planning.....	34
(E) ERM SYSTEMS AND TOOLS.....	36
(i) Risk Registers.....	37
(ii) Linkage of WIPO Risk Registers with other systems.....	40
(F) RISK CAPABILITIES	40
(i) Staff Risk Awareness	41
(ii) Availability of Risk Information	44
(iii) Data Analytics Project.....	45
(G) RISK CULTURE	47
(i) Transparency and Learning from Lessons	50
TABLE OF RECOMMENDATIONS	52
ANNEXES	54

LIST OF ACRONYMS

AFMS	Administration, Finance and Management Sector
AIMS	Administrative Integrated Management System
BI	Business Intelligence
CMT	Crisis Management Team
COSO	Committee of Sponsoring Organizations
ELC	Entity Level Controls
ELM	Enterprise Learning Management
EPM	Enterprise Performance Management
ERM	Enterprise Risk Management
ESD	Enterprise Solutions Division
HLCM	High Level Committee on Management
HRMD	Human Resources Management Department
IAOC	Independent Advisory Oversight Committee
IIA	Institute of Internal Auditors
IOD	Internal Oversight Division
ISO	International Organization for Standardization
IS	Information Security
IT	Information Technology
JIU	Joint Inspection Unit
MRL	Management Representation Letter
MTSP	Mid-Term Strategic Plan
PMSDS	Performance Management and Staff Development System
PPBD	Program Performance and Budget Division
RAS	Risk Appetite Statement
RBM	Results Based Management
RMG	Risk Management Group
RMM	Reference Maturity Model
SIC	Statement of Internal Control
SRC	Sector Risk Coordinator
UN	United Nations
UNRIAS	United Nations Representatives of Internal Audit Services
WIPO	World Intellectual Property Organization

EXECUTIVE SUMMARY

1. The implementation of efficient and effective risk management benefits organizations by helping them achieve operational and strategic objectives, and increase value and sustainability. The Internal Oversight Division (IOD) conducted an audit of Enterprise Risk Management (ERM) at the World Intellectual Property Organization (WIPO) to among others assess governance and design efficiency and operational effectiveness of risk management controls and practices, and the level of risk maturity of the Organization.
2. As part of the audit procedures, IOD administered an internal survey to selected staff members including, Sector Leads and their Alternates, Directors, Heads and other relevant staff members. IOD also conducted an external benchmarking exercise with the United Nations (UN) System and other International Organizations that make up the United Nations Representatives of Internal Audit Services (UNRIAS) group, to assess the evolution of risk management and capture insights and best practices that can further enhance the WIPO Risk Management framework and practices.
3. The audit including the survey results found that WIPO ERM framework conforms to best practices, and the governance setup generally operates effectively and efficiently. Further, WIPO ERM framework and practices ranked high when benchmarked with other Organizations.
4. The WIPO ERM processes are well established and positively evolving. The Central Risk Team within the Office of the Controller, while limited in resources, has implemented measures and taken consistent actions to support the continued integration of risk management at WIPO. The update of WIPO Risk Management and Internal Controls Manual may help further operationalize current risk management processes. Further, WIPO needs to raise staff awareness about its Risk Appetite Statement to increase integration and understanding of the Organization's risk strategy.
5. IOD recognizes the advanced state of WIPO concerning the implementation of tools to support risk management. However, feedback received from some stakeholders highlights issues on user-friendliness of the system. Considering user feedback in developing enhancements for the tool, supported by a fit-for-purpose training program would benefit the Organization's risk management. IOD also welcomes the initiative of the Office of the Controller to implement a system of self-assessment of its risk management maturity level. The result of the latest self-assessment are coherent with the observations and conclusions made in this audit.
6. The Risk Culture, while being intangible, is a key foundational element of risk management. Similar to the Office of the Controller, IOD highlights the need to further enhance the risk culture of WIPO. For instance, IOD draws attention to untapped opportunities that the Organization could benefit from, by expanding and enhancing the mandate and use of Sector Risk Coordinators (SRCs) as key enablers for enhancing the risk culture and raising risk awareness across the Organization. One such opportunity is the establishment of a community of practice by introducing rotation for the role of SRC, and increased interactions with other focal points such as Financial Closure and Results Based Management (RBM).
7. Further, IOD found that although the Terms of Reference advise that the SRC role be included in the Performance Management and Staff Development System (PMSDS) of designated staff members, this was not always the case, and Sector Leads need to take corrective measures in that regard. In addition, participants to the internal survey highlighted the need to enhance culture and move away from the perception of risk management as a bureaucratic burden by increased regular interactions and conversations on risk.
8. Finally, broadening the focus of Risk Management Group (RMG), including discussions on identifying opportunities and not only risks, and enhancing Sector Leads' knowledge of the

discussions of the RMG, would strongly contribute towards both setting the tone on risk management at the top, and enhancing the risk conversation across the Organization.

9. IOD makes four recommendations and nine points for consideration, covering areas such as, visibility of accountability and risk management frameworks; application of the risk appetite at operational levels; continued integration of risk management; visibility of key project risks; and timeliness of risk information updates. The recommendations and points for consideration made in this report will collectively contribute towards enhancing the operationalization of risk management, and the maturity of the risk culture in WIPO.

1. BACKGROUND

10. The implementation of efficient and effective risk management benefits organizations of any type and size by helping them achieve operational and strategic objectives, and to increase value and sustainability.

11. Risk management continues to garner attention as the world becomes more interconnected, and disruption accelerates across all industries. The adoption of documented risk management as an organization-wide effort has already become a universal norm.

12. The Institute of Internal Auditors (IIA) International Standards for the Professional Practice of Internal Auditing require internal auditors to evaluate the effectiveness and contribute to the improvement of risk management process¹.

13. Furthermore, the UN Joint Inspection Unit (JIU) in its report “Enterprise Risk Management (ERM): approaches and uses in United Nations system organizations”² suggests that “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 target ERM maturity stage. It is also recommended that periodic and independent assessments be made by auditors, individuals tasked with the oversight 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.”³

14. The **WIPO Accountability Framework**⁴ serves as an overarching framework document setting the basis for the functioning of Risk Management and the System of Internal Controls at WIPO. Figure A below depicts the placement of risk management within the WIPO Accountability Framework.

Figure A: WIPO Accountability Framework



Source: Compiled by IOD based on the model provided by WIPO Accountability Framework

¹ Standard 2120 – Risk Management

² JIU/REP/2020/5

³ JIU/REP/2020/5, Periodic review for continuous improvement (benchmark 9)

⁴ WO/PBC/29/4

15. The Figure B below summarizes the components of the WIPO Risk Management Framework within the system of WIPO Main Assurance Frameworks and Processes.

Figure B: Components of WIPO Risk Management Framework within the system of WIPO Main Assurance Frameworks and Processes



Source: Compiled by IOD

16. WIPO Risk Management Framework is guided by the risk appetite noted by Member States in the WIPO Risk Appetite Statement⁵ initially issued in 2014, and subsequently updated in 2019.

17. The WIPO Risk Management Policy⁶ sets out WIPO's approach to managing risks and internal controls in a consistent and business-oriented manner in order to support the achievement of its strategic goals and expected results. As a complementary document to the Risk Management Policy, the Risk and Internal Control Management Manual covers the day-to-day operational details of managing risks and controls at WIPO.

18. Information Security Risk Management and Safety and Security Risk Management, being a part of WIPO ERM, are operated by the Security and Information Assurance Division.

19. Information Security (IS) Risk Management is an element of WIPO Information Security Governance and relates to identification, assessment, remediation and monitoring of risks related to Information Security. IS Risk Management is aligned with ISO/IEC 27001⁷, and is supported by internal guidance such as IS Management System manual, IS Risk Management user guide and IS Risk Management video. IOD conducted an audit of cybersecurity in 2021, which among others, provided comments on the IS Strategy.

20. The Safety and Security Coordination Service provides professional Security Risk Management services to enable secure, safe and resilient delivery of WIPO's mandate. Currently the Safety and Security Coordination Service operates under regulations of WIPO Security Management System⁸, which will be replaced by WIPO Safety and Security Framework (in preparation). The WIPO Security Management System is operationalized

⁵ WO/PBC/29/5

⁶ OI 41/2017

⁷ An international standard on how to manage information security

⁸ IC/23/2009

through Safety and Security Policies and Guidance. In addition, WIPO is part of the UN Security Management System and seeks to align with its policies and procedures. As part of Business continuity and managing related risks, WIPO has established a Crisis Management Team (CMT), and Business Continuity Plans describing what needs to be done to ensure the continuity of critical business and support functions following a disruptive incident (including security incidents).

21. A Business Continuity Coordinator is responsible for supporting business continuity efforts. Beyond crisis management, the CMT also considers post-incident “lessons learned”, to identify evolving gaps and requirements for the continuous strengthening of the Organization's resilience. IOD conducted a Review of WIPO Crisis Management during the Coronavirus Disease 2019 Pandemic that included a more in-depth review of safety and security, business continuity and disaster recovery processes and practices.

22. To avoid duplication, the scope of this engagement excludes an in-depth review of Physical and Information Security and Business Continuity.

23. Finally, systems and tools put in place to support risk management at WIPO include the WIPO ERM system (Acuity STREAM™) as a repository of the entity's risks and risk responses, the Oracle™ Business Intelligence System for data visualization, and MetricStream™ as its IS Governance, Risk and Compliance platform.

2. ENGAGEMENT OBJECTIVES

24. The objectives of this audit were to assess:

- (a) The adequacy of governance surrounding ERM at WIPO;
- (b) The WIPO ERM processes in terms of their design efficiency and operational effectiveness;
- (c) Whether the systems and tools to support the WIPO ERM are fit-for-purpose; and
- (d) The evolution of the risk management culture/maturity and capacities at WIPO.

3. SCOPE AND METHODOLOGY

25. The engagement scope covered the risk management process at WIPO taking into consideration previous audits conducted on related topics.

26. The methodology included interviews with stakeholders, analyses and review of relevant supporting documentation, walkthroughs, benchmarking with best practices and sample testing as applicable, with a view to:

- (a) Assess the adequacy, efficiency and effectiveness of governance and the WIPO risk management process;
- (b) Examine policies, procedures and control activities that will be operational during the performance of audit procedures;
- (c) Assess whether the systems and tools to support the ERM are fit-for-purpose and whether the staff involved in the process know their roles and responsibilities and are receiving sufficient training and guidance to perform their duties concerning risk

management. This also include assessing the Organization’s ability to capture all significant risks on timely basis, and develop effective and efficient responses; and

(d) Verify whether measures have been taken to enhance the risk management culture, maturity, and knowledge of WIPO staff members.

27. Further, IOD carried-out two surveys:

(a) An internal survey of relevant WIPO staff members involved in taking the lead in risk management processes in their respective areas, to get insights and perceptions on Risk Management governance, maturity, culture, processes and tools; and

(b) External benchmarking with UN System and other International Organizations, to enable IOD to assess the evolution of risk management and capture insights and best practices that can further enhance the WIPO Risk Management framework and practices.

28. Among other benchmarks for assessing the WIPO ERM, IOD used The High Level Committee on Management (HLCM) Risk Management Task Force’s Reference Maturity Model (RMM), and the JIU’s nine benchmarks for measuring the maturity of the risk management published in the 2020 Report “Enterprise risk management: approaches and uses in United Nations system organizations” (JIU/REP/2020/5).

29. The Audit Engagement was performed in accordance with the International Standards for the Professional Practice of Internal Auditing (the Standards) issued by the IIA.

4. ENGAGEMENT RESULTS – OUTCOME(S)

30. The objectives and outcomes of the Audit engagement are summarized below.

S/n	Objective(s)	Outcome(s)
(a)	To assess the adequacy of governance surrounding ERM at WIPO.	<ul style="list-style-type: none"> IOD has checked the design and completeness of the WIPO ERM framework. The governance setup was assessed against operating effectiveness and efficiency. One recommendation was made on raising awareness about the Risk Appetite Statement and one recommendation on inclusion of relevant objectives of Sector Risk Coordinators in the PMSDS.
(b)	To assess the WIPO ERM processes in terms of their design efficiency and operational effectiveness.	<ul style="list-style-type: none"> IOD has assessed the design and operating effectiveness of processes such as risk identification and assessment; development of risk responses; monitoring and follow-up; preparation of the Statement of Internal Control; and ERM integration with results based planning. IOD draws attention to the need to ensure that the quality of risks and controls formulation continue to be enhanced through among others, training, and continued awareness raising across the Organization.
(c)	To assess, whether the systems and tools to support the WIPO ERM are fit-for-purpose.	<ul style="list-style-type: none"> IOD recognizes the advanced state of WIPO with regards to the implementation of tools to support risk management. However, feedback received from some stakeholders highlights issues on user-friendliness of the system. Considering user feedback in developing

		enhancements and trainings would benefit the Organization's risk management.
(d)	To assess the evolution of the risk management culture/maturity and capacities at WIPO.	<p><u>Risk Capabilities:</u></p> <ul style="list-style-type: none"> IOD has assessed areas such as risk awareness; availability of risk information and data analytics. The maturity in this area is assessed as "Established" moving towards "Advanced", with planned initiatives of the Office of the Controller, and subsequent implementation of IOD recommendation on developing fit-for-purpose capacity building, and enhancing the community of practice of risk management in WIPO. <p><u>Risk Culture:</u></p> <ul style="list-style-type: none"> Similar to the Office of the Controller, IOD highlights the need to further enhance the risk culture of WIPO towards "advanced". This is also corroborated through the survey results. Recommendations made in this report collectively support the enhancement of the risk culture of WIPO.

5. ENGAGEMENT RESULTS - POSITIVE DEVELOPMENTS

31. IOD notes some positive developments identified during the engagement.

Area	Positive Development
ERM Framework and Governance	<ul style="list-style-type: none"> WIPO has successfully established in place an ERM framework, supported by adequate governance. The completeness of the framework and efficient governance model stand out when benchmarked against other UN system Organizations. IOD has been assigned observer status at the RMG
ERM main processes and their integration	<ul style="list-style-type: none"> WIPO has established an effective identification mechanisms guided through the Risk and Internal Controls Manual. Mitigation actions and controls have been identified to address risks, and tests and validations provide valuable assurance. The Central Risk Team within the Office of the Controller, while limited in resources, has implemented measures and taken consistent actions to support the continued integration of risk management at WIPO by among others, embedding the risk management in the first line through for instance the use of Sector Risk Coordinators.
Risk Capabilities and Risk Culture	<ul style="list-style-type: none"> Interaction with Sector Leads and Senior Management indicate growing focus on risk and opportunities and increased discussions on risk taking at various levels of management.

ERM leadership	<ul style="list-style-type: none"> The Controller, supported by the Risk Assurance and Internal Controls Specialist, co-chairs the UN-Wide HLCM Risk Management Forum.
----------------	---

6. ENGAGEMENT RESULTS - OBSERVATIONS AND RECOMMENDATIONS

32. The following observations, points for consideration and recommendations present opportunities to further reinforce the Risk Management Framework, processes and practices at WIPO.

(A) IOD SURVEYS

(i) IOD Survey on ERM at WIPO

33. As part of the audit procedures, IOD administered an internal survey to selected staff members including Sector Leads and their Alternates, Directors, Heads and other relevant staff members. Around 170 staff members were invited to take the survey, of which 29 per cent participated in the period from September 31 to October 28. The survey aimed at getting insights and perceptions on Risk Management governance, maturity, culture, processes and tools. The full survey result can be found under Annex II. Extracts from the survey are used throughout the report.

Figure C: IOD Internal Survey Statistics



Source: IOD Internal survey data

(ii) IOD External Survey on ERM with United Nations Representatives of Internal Audit Services (UNRIAS)

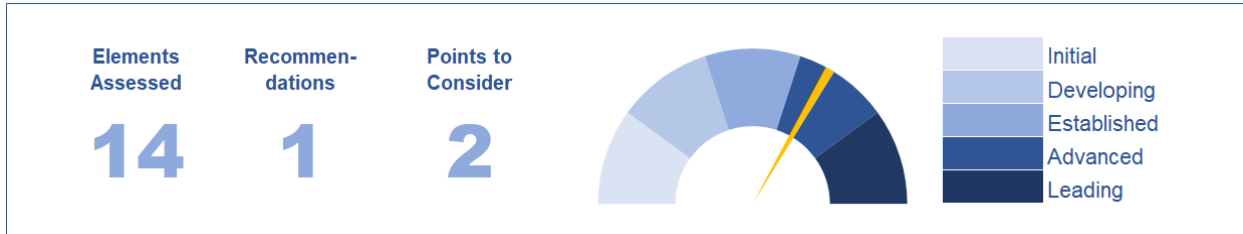
34. In order to assess the evolution of risk management and capture insights and best practices that can further enhance the WIPO Risk Management framework and practices, IOD conducted an external benchmarking exercise between October 8 and 25, 2021, with UN System and other International Organizations that make up the UNRIAS group. The survey was distributed to 59 organizations with 51 per cent response rate.

35. The result of the survey can be found under Annex III of this report, with extracts from the survey used in relevant parts of the report.

(B) ERM FRAMEWORK AND POLICY

36. The Figure below summarizes the results of the assessment of the ERM Framework and Policy.

Figure D: ERM Framework and Policy – Assessment Summary



Source: Gap Analysis Details (Annex XIV)

(i) ERM Framework

37. IOD assessed the staff awareness of ERM framework and obtained perceptions regarding the usefulness and applicability of WIPO ERM in day-to-day operations. Further, IOD has analyzed the components of WIPO ERM Framework and Policy, gathered internal feedback and compared the completeness of ERM Framework elements against external organizations.

i IOD Internal Survey
Fifty-one per cent of respondents⁹ indicated that they were aware of WIPO's accountability and risk management frameworks, against 47 per cent who were somewhat aware.

This is further supported by the 37 per cent of respondents¹⁰ who indicated not knowing where to find relevant risk management and internal controls documentation on the intranet. However, 63 per cent indicate that they know where to find this information.

Finally, 24 per cent respondents¹¹ found the risk management and internal control documentation useful in their day-to-day management or risk, 37 per cent somewhat agreed, 18 per cent somewhat disagreed and another 18 per cent disagreed.

38. Feedback suggests that there are opportunities to increase the visibility of Accountability and Risk Management Frameworks. While more respondents tend to agree with the usefulness of the risk management and internal controls documentation, there is a room for improvement and better alignment with daily operational decision-making.

39. IOD compared the composition of the Risk Management Framework of 30 organizations in its external ERM Survey, and concluded that the WIPO Risk Management Framework was among the most complete in terms of guidance at strategic and operational level.

i IOD External ERM Survey
The survey results indicated that the majority of organizations had set up a Risk Management Framework, but with varied contents. For instance while 87 per cent indicated that their Risk Management Framework includes a risk management policy¹²,

⁹ Annex II, Question 1
¹⁰ Annex II, Question 2
¹¹ Annex II, Question 3
¹² Annex III, Question 2

and 57 per cent had a risk manual, only 40 per cent had an internal control manual, 43 per cent an accountability framework, and 33 per cent had a risk appetite statement.

40. **Framework alignment with the Strategy.** Once strategy is set, the Risk Management Framework should ensure an effective way for management to fulfill its role, knowing that the organization is attuned to risks that can impact strategy and is managing them well.



IOD Internal Survey

Thirty-one per cent of respondents¹³ believe that WIPO's Risk Management Framework is fit-for-purpose and aligned with the strategy and the Results Based Management framework, while 39 per cent somewhat agreed, 16 per cent somewhat disagreed, and 6 per cent disagreed.

Likewise, on whether the risk management system satisfies current requirements, 28 per cent of respondents¹⁴ agreed, 38 per cent somewhat agreed, 13 per cent somewhat disagreed, and 13 per cent disagreed.

41. Some reasons and relevant comments made include:



IOD Internal Survey mentions:

- "Need to first understand the framework".
- "The alignment should probably be reconsidered in view of the new MTSP (Mid-Term Strategic Plan)".
- "The aspects of the framework requiring identification of risk and appropriate mitigation measures are good".
- "The systems for managing and reviewing the identified risks are an administrative burden that do not assist the process".
- "This framework has evolved much over time in listing risks, with many ups and down in quantity depending on who was doing it. It gives sometimes the impression that we reinvent the wheel each year".
- "It's not bad in itself, but I see the risk that the strategy and results based management become too heavily driven by the risk management framework, at the detriment of anything else".
- "The overall use and impact of the framework is unclear. Sometimes it feels like tools that don't really have meaning or impact."

42. WIPO's MTSP 2022-2026 and specifically WIPO Program of Work and Budget for 2022/23 bring on board some structural changes and new terminology. For example, the new Results Framework Chart for the 2022/2023 biennium is framed along the Four Strategic Pillars, Foundation and 16 Expected Results articulated in the MTSP; starting from 2022 work program structure has been streamlined from the current 31 Programs to correspond to the nine Sectors responsible for the implementation of the Program of Work; such terms as "Programs", "Program Managers" and "Senior Management Team" have been replaced by "Departments", "Sector Leads" and "Sector Lead Teams" respectively.

43. However, the current Risk Management Framework documentation reflects the setup and terminology of MTSP 2015-2021. With a new WIPO Program of Work and Budget coming into

¹³ Annex II, Question 4

¹⁴ Annex II, Question 22

force in 2022, the Risk Management Framework documentation would need to be aligned with the new Strategy House and related terminology.



IOD External ERM Survey

Twenty-nine per cent of respondents were of the view that their Risk Management Framework and practices were aligned with the Strategy/Program & Budget objectives/ Work Plans¹⁵, 36 per cent responded that they were somewhat aligned, and 25 per cent indicated that alignment was work in progress.

Point for Consideration

1. There are opportunities to increase the visibility of Accountability and Risk Management frameworks. While more stakeholders tend to agree with the usefulness of the risk management and internal controls documentation, there is a room for improvement and better alignment with operational daily decision-making.

(ii) WIPO Risk Appetite

44. The Risk Appetite Statement is critical in determining the level of risk that an organization is prepared to accept in pursuit of its objectives. The statement is fed by the vision, and in turn informs the strategy and its operationalization. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) states that “The risk appetite is a critical link between forming strategy and realizing performance”¹⁶.

45. The WIPO risk appetite statement, issued in 2014 and last updated in 2019, is a broad description of the amount and types of risk the Organization is willing to accept to achieve its objectives. This helps management make informed risk-based decisions while understating risk exposure.



IOD Internal Survey

While 29 per cent of respondents¹⁷ indicated that they understood and knew how to apply the risk appetite in their decision-making processes, 37 per cent somewhat understood, and 29 per cent were not sure and indicated the need for further guidance.

46. Relevant concerns raised in the feedback from discussions and survey respondents, suggest that lack of understanding is linked to the low awareness of these guidelines, and the academic nature of the available documentation.



IOD Internal Survey mentions:

- “The problem is that awareness of these guidelines is low, so explaining it to colleagues would be time consuming.”
- “It seems academic rather than linked to real operational risks”

47. While respondents and persons interviewed indicated that risk needed to be further integrated into everyday decision-making, they also pointed out that opportunities needed to be regarded with the same seriousness as threats. A number of stakeholders found the

¹⁵ Annex III, Question 20

¹⁶ Risk Appetite – Critical to Success, Committee of Sponsoring Organizations of the Treadway Commission.

¹⁷ Annex II, Question 3

Organization to be too risk averse, and suggested that there was too much focus on impact without “balancing likelihood” – WIPO needs to shift to “Risk aware”.

48. IOD benchmarked WIPO’s Risk Appetite Statement (RAS) with guidance from among others relevant organizations and standards making bodies (i.e. HLCM, COSO, Institute of Risk Management, and Governance Finance Function (UK)). Figure E below represents a summary of areas and topics covered in the analysis of the WIPO RAS.

Figure E: Summary of Benchmarks used in WIPO RAS analysis

Area	Topic - Benchmark	Area	Topic - Benchmark
DESIGN AND IMPLEMENTATION	Articulation and Wording of the Risk Appetite Statement	EFFECTIVENESS OF OPERATIONALIZATION	Communication and reporting*
	Alignment with the Strategy*		Risk Escalation Mechanisms*
	Risk Appetite Scaling: strategic, tactical, operational levels*		
	Risk Taking, Opportunities and Performance*		Revision of the Risk Appetite
	Risk Appetite Metrics*		
	RM Capacity and Maturity and RM Culture		
	Consultations with Stakeholders		

* - suggestions for enhancement developed by IOD. Refer to Annex IV.

49. There is still no unequivocal view on the best content and structure of the Risk Appetite Statement. Compared with publicly available documents, IOD finds the WIPO RAS comprehensive. IOD positively notes that WIPO is among the small group of organizations that indicated to have formulated a Risk Management Statement, in the external survey.



IOD External ERM Survey

Only 33 per cent¹⁸ of respondents have developed a Risk Appetite Statement.

50. Annex IV to the report contains a matrix summarizing IOD’s analysis and suggestions on how WIPO RAS and its application can be further enhanced during its next update. Some potential enhancements are listed below:

- (a) Adding clearer links to WIPO Strategy House in order to demonstrate the alignment with WIPO Strategic Pillars, Expected Results and associated Risks;
- (b) Highlighting the importance of risk taking and exploiting opportunities; and
- (c) Explaining the application of the Risk Appetite at operational levels and explaining the modalities of risk escalation process, including how to measure impact at the level of Sector / Department and Unit.

51. The work on the WIPO new RAS is underway and a draft RAS has been circulated. Comments and observations from IOD have been taken into account in developing the new Statement.

52. Going forward, communication and staff awareness about the RAS need to be enhanced. Further guidance and information on cascading the Risk Appetite down the hierarchy should be

¹⁸ Annex III, question 2

included in the WIPO Risk and Control Manual, to serve both as, a means to understand how the 'top-down' desired risk profile can be compared with the 'bottom-up' reality, and a useful tool in a day-to-day decision making process at all levels of the Organization.

Recommendation

1. The Office of the Controller in collaboration with the Risk Management Group and Sector Risk Coordinators should raise staff awareness about the WIPO Risk Appetite Statement.

(Priority: Medium)

Point for Consideration

2. WIPO would benefit from:
 - (a) Highlighting the importance of risk taking and exploiting opportunities in the RAS;
 - (b) Explaining in the Risk and Internal Controls Manual, the application of the Risk Appetite at operational levels and describing the modalities of risk escalation process, including how to measure impact at the level of Sector/Department/Division/Section and Unit, will help operationalizing the RAS.

(iii) ERM Framework Self-assessment and Improvement mechanisms

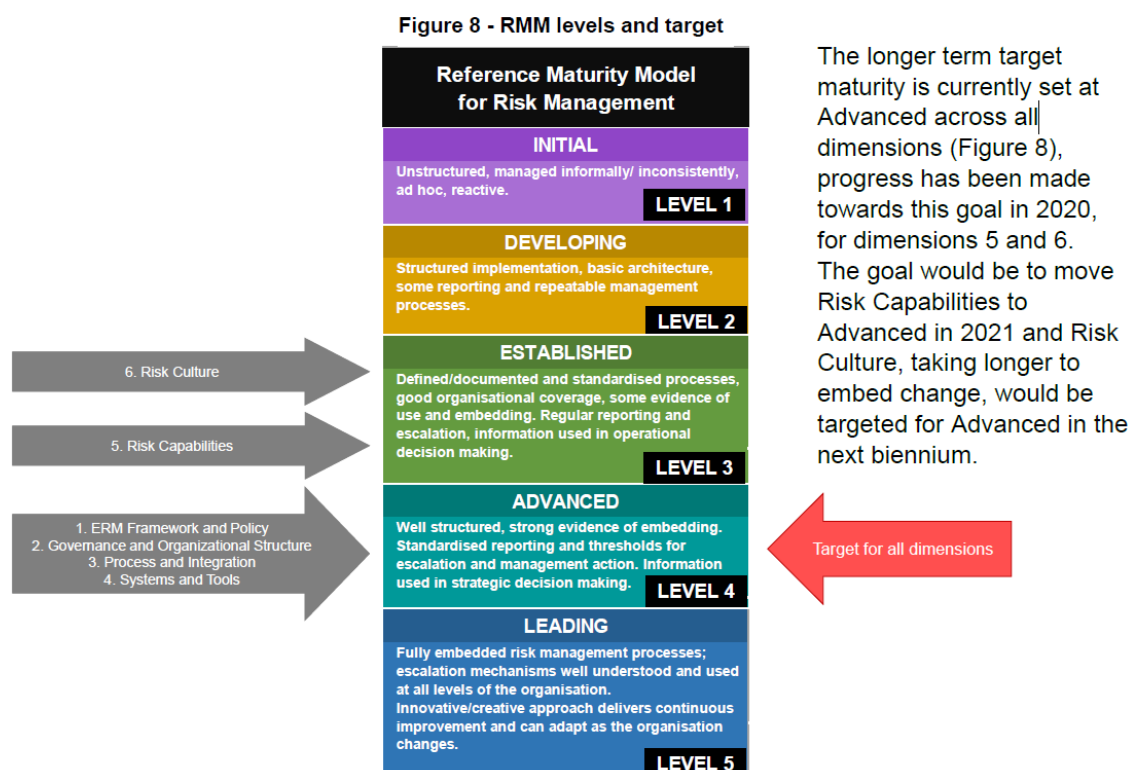
53. WIPO has implemented a system of self-assessment of its Risk Management Maturity level. The model is based on the HLCM Risk Management Task Force's Reference Maturity Model (RMM)¹⁹ as well as the JIU benchmarks²⁰. The Task Force is co-led by WIPO and the World Food Programme and reports to the HLCM.

54. The last self-assessment was performed in 2020 by the Office of the Controller. Figure F below shows the self-assessed and target Risk Management Maturity levels.

¹⁹ HLCM Risk Management Task Force's Reference Maturity Model (RMM) provides a tool for management improvement initiatives in risk management, through a self-assessment of maturity against six dimensions.

²⁰ JIU in its 2020 Report "Enterprise risk management: approaches and uses in United Nations system organizations" (JIU/REP/2020/5) has developed nine benchmarks for measuring the maturity of the Risk Management.

Figure F: Self-assessed and Target Risk Management Maturity at WIPO



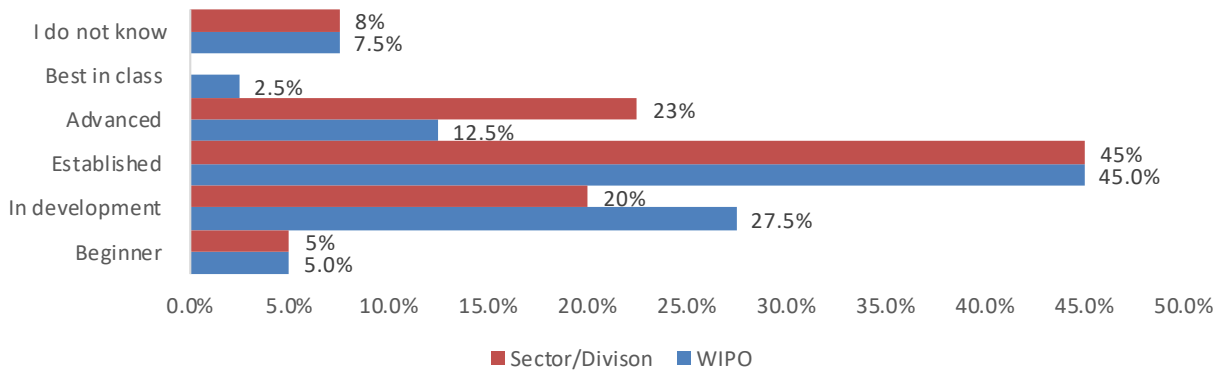
Source: WIPO Annual Risk Management Report 2020

55. WIPO’s longer-term target maturity is currently set at “Advanced” across all dimensions. According to the WIPO Annual Risk Management Report for 2020, the goal would be to move Risk Capabilities to “Advanced” in 2021, while Risk Culture, would be targeted for “Advanced” in the next biennium.

56. IOD collected internal feedback on current Risk Management Maturity at WIPO. Drawing from the HLCM RMM, the survey questioned participants on their perception of the Risk Management Maturity level of their Sector/Division, and that of the Organization as a whole. Note however, that the dimensions were not provided, and IOD only sought a general perception of participants. The levels for assessment were as follows:

- (a) **Beginner** (unstructured and *ad hoc*);
- (b) **In development** (structured, some system, monitoring and reporting in place);
- (c) **Established** (defined framework, evidence of embedding, and information used in operational decision making);
- (d) **Advanced** (well structured, strong evidence of embedding, monitoring, escalation, use of information in strategic decision making); and
- (e) **Best in class** (fully embedded risk management, monitoring and escalation used at all levels of the organization, innovative/creative approach and continuous improvement as environment evolves).

Figure G: Staff perceptions on Risk Management Maturity at Sector/Division versus at Organization Level



57. A comparison of results shows that respondents in two categories rated their Sector/Division at least at the same level as the Organization – Beginner and Established. More respondents found that their Sector/Divisions were more advanced than the Organization. By contrast, more respondents rated WIPO at “In development” compared to their Sector/Division.

58. There is consensus among respondents about the “Established” maturity of Sector/Division and the Organization with 45 per cent rating for both. While two and a half per cent of respondents set the Organization as “Best in Class”, respondents found that their Sector/Divisions were more “Advanced” than the Organization.

59. While acknowledging the limitations and perceptive/subjective nature of this exercise, this does indicate that more work is needed to better communicate and build on the risk culture in the Organization. Recognizing that risk management is “the responsibility of everyone”; however, the onus is on leadership to set the tone and middle management to push that tone further down the line, with a view to enhancing the common understanding of how the organization addresses threats and opportunities, while building a collective risk conscious culture.

60. IOD welcomes the initiative of the Office of the Controller to implement the system of self-assessment of its Risk Management Maturity. Regular self-assessments will make a notable contribution to raising the quality and maturity of risk management at WIPO.

(C) RISK MANAGEMENT GOVERNANCE AND ORGANIZATIONAL STRUCTURE

61. The Figure below summarizes the results of the assessment of the Governance and Organizational structure.

Figure H: Governance and Organizational structure – Assessment Summary

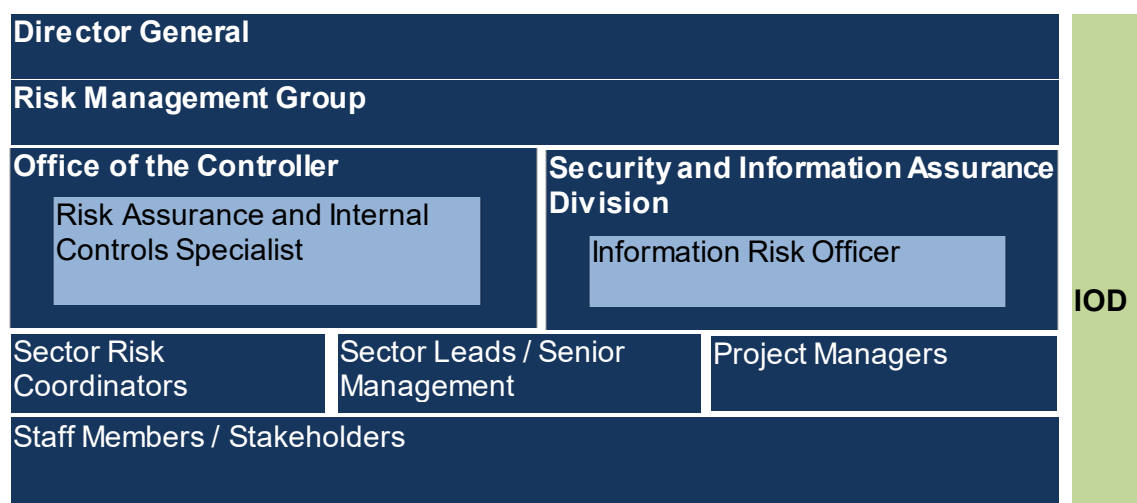


Source: Gap Analysis Details (Annex XIV)

(i) Risk Management Governance System

62. The Risk Management Governance defines the way in which an organization undertakes risk management by providing rules, procedures, and guidance for sound and informed decision-making, and effective allocation of resources. A successful Risk Governance is therefore contingent on how effectively the Board (or similar body) and Management are able to work together in managing risks while achieving goals. Central to this is the Enterprise Risk Management (ERM) framework, which articulates and codifies how an organization approaches and manages risks. The Figure I below depicts the Risk Management Governance setup at WIPO.

Figure I: Elements of Risk Management Governance at WIPO



Source: Compiled by IOD

63. While Risk Management is a shared responsibility of every staff member in the Organization, the ultimate accountability for risk management lies with Senior leadership.

64. The RMG was established in 2014 to promote a culture of responsible and effective financial and risk management in WIPO. The RMG reviews and monitors WIPO’s financial situation and the key risks to the achievement of the Organization’s expected results. It approves the risk strategy and proposes a suitable Organizational risk appetite for approval by Member States. Further, the RMG reviews and confirms key risks at the organizational level. Finally, the RMG endorses the assessment of, and response to all risks within the red zone of the corporate risk scale chart (Annex VII). The Terms of Reference and composition of the RMG is set out by the Director General in an Office Instruction²¹.

65. Among the positive feedback collected on the functioning of the RMG, there are potential areas of enhancement such as the needs to better communicate to and involve Senior leadership that are not members of the RMG. Closer involvement and sharing of information would contribute to enhance the risk management process and enrich the RMG discussions and outcomes. Solutions may include for instance, cascading the RMG communication down through for management briefing, or inviting senior leadership to RMG on a rotational basis.

66. Further it was noted that the RMG discussions have strong emphasis on revenue related risks, whereas there are opportunities to further expand the topics covered.

67. Finally, the RMG meetings may include an additional agenda item on “Identifying Opportunities”, which would focus on opportunities to exploit risks that could generate positive

²¹ OI 33/2016

outcomes that would demonstrate the shift towards for calculated risks taking and set the tone from the top.

68. **The Office of the Controller** – Risk Management as a second line²², is placed under the responsibility of the Office of the Controller, with the objective of providing compliance and oversight in the form of frameworks, policies, tools, and techniques to support risk and compliance management. The Office is responsible for the comprehensive risk reporting and development of the Organization’s risk and internal controls management strategy. Specifically, the Risk Assurance and Internal Control Specialist is part of the Central Risk Team within the Office of the Controller is responsible for among others²³:

- (a) Coordinating the risk and control management processes of the Organization, as well as the ongoing improvement and enhancement of the same;
- (b) Escalating risk management and internal control issues to the RMG;
- (c) Preparing the reporting for the same, and ensuring that organization-level risks are adequately identified and recorded in the risk management system of the Organization; and
- (d) Assessing the design²⁴ and the operating effectiveness²⁵ of controls as recorded.

69. Additionally, there is an Information Risk Officer in the IS Section of the Security and Information Assurance Division, reporting to the Chief Security Officer, and responsible for coordinating Information Security related risks.



IOD Internal Survey

Sixty-three per cent of respondents²⁶ found the Office of the Controller responsive and effective, 23 per cent somewhat agreed, against 8 per cent who somewhat disagreed. Eight per cent never met a member of the central risk team of the Office of the Controller.

70. **Sector Risk Coordinators.** The Office of the Controller has worked with Sectors to identify SRCs. According to the Terms of Reference, 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 ERM system. Further, SRCs coordinate with the organizational unit heads in the Sector, and the central risk management function, located in the Office of the Controller. 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.

71. There are currently 15 SRCs spread among the nine Sectors, and the table below summarizes the number of staff, risks, SRCs and their grades for each Sector.

²² The IA’s Three Lines Model

²³ OI 41/2017 WIPO Risk Management Policy

²⁴ Whether controls are designed appropriately to mitigate the relevant risk(s)

²⁵ Whether controls operate effectively over a period of time so as to actually result in the mitigation of the relevant risk(s)

²⁶ Annex II, Question 14

Table 1: Sectoral Analysis of the number of WIPO staff, risks SRCs and their grades

Sector		Total Number of Employees ²⁷	Total Active Risks ²⁸	Number of SRC	Grade
Administration, Finance and Management Sector		241	59	2	P2 P5
Brands and Designs Sector		189	22	1	P4
Copyright and Creative Industries Sector		49	16	1	D1
Regional and National Development Sector		97	51	1	D1
IP and Innovation Ecosystems Sector		112	15	1	P5
Infrastructure and Platforms Sector		67	10	1	P4
Global Challenges and Partnerships Sector		49	25	1	P5
Patents and Technology Sector		376	18	2	D1 P4
Director General (32)	ODG/Ethics/Ombudsperson	7	5		
	Human Resources Management Department	48	13	2	P5 P3
	Internal Oversight Division	13	8	1	P5
	News and Media Division	9	4	1	D1
	Diplomatic Engagement and Assemblies Affairs Division	24	2	1	D1

Source: Compiled by IOD

72. Although the Terms of Reference indicate that the ideal profile for an SRC is that of a senior professional, two SRCs of grades P2 and P3 may not fall in that category of professionals. However, each staff was coupled with a senior member.

73. While IOD acknowledges that SRCs are not supposed to identify risks; however, the Terms of Reference indicate that the SRC should have a good understanding of their Sector's work, and the ability to challenge colleagues and support in analyzing risk events.

74. Some Sectors have complex areas and the current approach assumes that the SRCs have sufficient knowledge of specialized areas of their respective Sectors to play their role as outlined by the Terms of Reference and effectively facilitate the risk management process. While other areas have one SRC, the basis for designating two SRCs in some areas is not clear. Discussions with the Central Risk Team of the Office of the Controller indicate that Sectors are free to designate two SRCs. The idea seems to have an SRC for administrative tasks and another SRC for more substantive matters, while also providing back staffing.

75. However, it would be relevant going forward, that there be a more coherent approach for designating SRCs, with regards to grade, experience, suitability, and tasks. Elements such as size of Sectors, number of risks in register, risk maturity of the Sector, among others, should drive the designation process. Further, and to enhance the risk culture, it could be relevant to appropriately mix management and operational staff within the SRC community, and encourage major Sectors to designate at least two staff members of varying experience to among others illustrate the responsibilities at management and operational levels of risk management.

76. Although the Terms of Reference propose a text to be included in the evaluation objectives in the PMSDS of designated SRCs, the review of 10 SRC staff's PMSDS showed that in eight cases, no specific objective has been set regarding their responsibilities and tasks as SRC. While acknowledging that the role of SRC is not a full time position, making SRCs

²⁷ HRMD Business Intelligence Reports - includes regular staff, temporary staff, and non-staff

²⁸ From Risk management Business Intelligence Reports - includes risk acceptance - accepted and not set

accountable would increase commitment, which may in turn have positive effects on the overall enhancement of risk management at WIPO.

77. Discussions with SRCs and the result of the external survey administered to the UNRIAS showed that training of SRCs is a key enabler for enhancing the risk culture and raising the risk awareness of the Organization. The SRCs with the support of the Central Risk Team of the Office of the Controller can facilitate the communication flow among stakeholders and thus influence the larger WIPO community, by creating a critical space for risk discussions and encouraging constructive debates. For instance, interaction between the SRCs and RBM focal points could support better alignment and linkage between risk management, performance management, and the results framework.

78. Going forward, identifying opportunities to better make use of SRCs would require a stock take of the benefits and opportunities resulting from the current use of SRC, subsequently followed by a review of the SRC mandate, role and responsibility. Further, the risk culture at WIPO would also benefit from implementing a process whereby SRCs are changed every three-four years, achieving both stability and rotation, to give the opportunity for other staff members to take on the responsibility. This will also serve to ensure back staffing of SRCs, and contribute to encourage and support an organic and sustained growth of the risk management culture at WIPO.



IOD Internal Survey

- *Fifty-three percent of respondents²⁹ found the SRC effective in their tasks, against 8 per cent who did not find their SRC effective in providing useful advice, support and coordination. Another 8 per cent did not know their SRC.*
- *Thirty-five per cent of respondents³⁰ indicated that the SRC updated risks in the system for their area, 13 per cent indicated that the Central Risk Team of the Office of the Controller performed the updates, while 38 per cent indicated a team member, and 48 per cent designated themselves. In more detail, 38 per cent of respondents³¹ update their risk register once a year, 30 per cent twice a year, 13 per cent respectively do not update, and are unsure. Three per cent update respectively, three, four and at least five times a year.*

79. Finally, while support from SRC and Risk Assurance and Internal Controls Specialist are relevant, updating risks in the system on behalf of Sectors/Divisions is not aligned with the description of their respective roles in the WIPO Risk Management Policy. The current perception that the system is not user-friendly could partly explain reluctance to perform these updates in the system.

(ii) Risk Management Function - Comparison with other Organizations

80. The survey to UNRIAS Organizations indicate that 63 per cent of respondents have established a Risk Management Function of some form³², with 20 per cent indicating that there was only one individual holding a risk related role. Thirteen per cent had no function of any kind (including no individual), and 3 per cent indicated that this was in progress.

81. The number of staff members varied between two and five, with some instances where dedicated staff were between 10 and 20 in the Risk Management Function³³. The most common configurations had two or three staff members. Further, out of the 17 respondents that

²⁹ Annex II, Question 15

³⁰ Annex II, Question 23

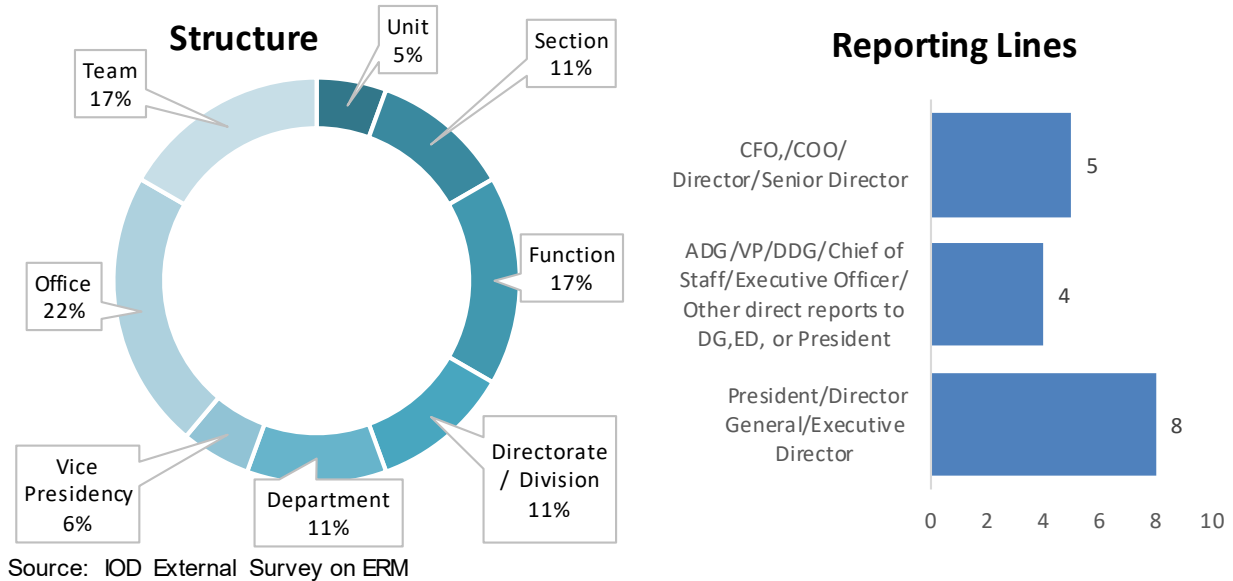
³¹ Annex II, Question 24

³² Annex III, Question 4

³³ Annex III, Question 5

provided clear information on reporting lines, reporting to the Director General/President/Executive Director was the most common, with 47 per cent of instances. Figure J below summarizes the reporting lines and structures of risk management in 17 Organizations.

Figure J: Reporting lines and structures of risk management



Recommendation

2. Sector Leads and relevant Managers should ensure that the PMSDS of designated staff members include objectives related to their role as Sector Risk Coordinators.

(Priority: Medium)

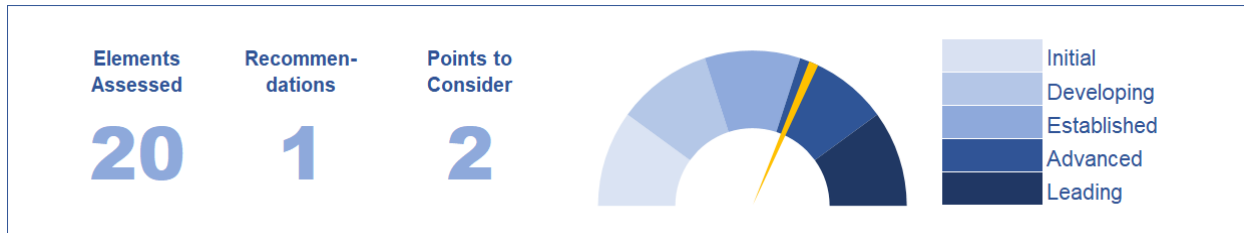
Point for Consideration

3. Enhance Risk Management Framework by:
 - (a) Broadening the focus of RMG discussions and including other elements on the WIPO risk map; including an additional agenda item on “Identifying Opportunities”;
 - (b) Enhancing the Sector Leads’ knowledge of the discussions of the RMG through for instance, inviting a Sector Lead to a RMG, or presenting the results of the RMG meetings to Sector Leads on a regular basis;
 - (c) Developing a coherent and consistent approach for determining membership of SRCs; and
 - (d) Establishing a fixed term (e.g. maximum five years) for SRCs, to enable different staff members to take on the role, and contribute to a community of practice and the growth of the risk management culture at WIPO.

(D) PROCESS AND INTEGRATION

82. The Figure below summarizes the results of the assessment of the risk management process and integration.

Figure K: Risk Management Process and Integration – Assessment Summary



Source: Gap Analysis Details (Annex XIV)

(i) Risk identification and assessment

83. The risk identification and assessment has to be performed by all WIPO staff at three levels of risk hierarchy (Organizational / strategic risks, program risks and project level risks). The aim is to identify the risk events and estimate the likelihood of their occurrence and impact on expected results, if they were to take place.

84. WIPO had 243 organizational and program level risks recorded in the ERM Risk Register as of December 8, 2021. Annex VI to the report provides more details on WIPO risk portfolio.



IOD External ERM Survey

When compared in UNRIAS group organizations, about one third³⁴ were not in a position to determine the total number of risks they have. For the remaining organizations the number of risks ranged from 9 to approximately 1.4 thousand, which indicates a very different approach to the granularity of risks among organizations.

85. Project level risks are not kept in one consolidated register at WIPO as they are recorded in respective Risk Registers of individual projects. Therefore, WIPO has no data on the total number of risks at project level.

86. **Risk Identification.** The risk identification techniques at WIPO among others include brainstorming sessions by subject matter experts, analysis of corporate risk event categorization, analysis of audit information, inputs from risks identified in investigations, events and incidents.

87. One key component of an effective risk and management system and processes, is an ability to adapt to the evolving environment and needs of the Organization and to effectively identify emerging risks.

³⁴ Annex III, Question 15



IOD Internal Survey

While 50 per cent of respondents to IOD Internal survey³⁵ somewhat agreed that the current risk management processes are responsive to changes in their business environment and emerging threats, 20 per cent fully agreed with this affirmation. Further, 23 per cent somewhat disagreed and 8 per cent disagreed.



IOD Internal Survey mention:

Comments of respondents who disagreed and somewhat disagreed that the current risk management processes are responsive to changes in their business environment and emerging threats:

- “There are concrete examples in my area where risks were updated and new risks were identified, as well as the way to deal with them. However, it’s also easy to fall in a bureaucratic routine and not giving all its meaning to the risk management, for many managers. For instance, it’s easy to avoid updating risks/identifying new risks and the mitigation actions.”
- “Risk management becomes a token and limited only to review of the Risk Register. I have regularly noted more senior staff than me have made decisions without considering the risk to the Organization as a whole, because that risk is not on the register. The keeping of a register should not exclude a proper risk-aware approach to everyday operations.”
- “There are many more risks than the ones reported but it would be impossible to report and monitor them all. So in addition to the formal risk management process, prudent daily management of projects and resources is needed as part of the broader risk management strategy.”
- “If the supporting system is too complex to use, and it is, then the process cannot be adapted to our need. That’s my biggest issue at present.”
- “A bit more creative thinking and a simpler risk feedback system would allow us to identify risks a bit better.”

88. WIPO has effectively designed and implemented risk identification processes.

89. **Risk Formulation.** An important element of risk management is a clear articulation of the risks. Leading practices suggest that the risk statement should clearly identify the event or condition, the consequences on associated objectives, and the cause (if such is known). Disciplined use of structured formats can help in describing a risk, producing more effective risk statements, and avoiding weak statements that lead to confusion.



IOD Internal Survey

When questioned on the ability to formulate Risks, Likelihood, Impact and Severity, 47 per cent of IOD Internal Survey respondents³⁶ indicated that they knew how to formulate these concepts, against 43 per cent who indicated that they were somewhat able to do so. Ten percent did not know.

90. Results of the sample based review of the formulation of risks in the ERM and project risks registers are summarized in the Annex XIII. Overall, WIPO risk registers contain

³⁵ Annex II, Question 22

³⁶ Annex II, Question 9

comprehensive risk descriptions which allow informed users to understand recorded risks. Risk registers of some Information Technology (IT) projects could be used as good practices and inspiration for WIPO programs to formulate their risks in the ERM Risk Register. Going forward, quality of registers could be further enhanced by clearer formulation of causes and consequences in risk descriptions of the ERM Risk Register. This will allow better understanding risks.

91. **Risk Assessment.** Risks at WIPO are assessed in terms of impact and likelihood at residual level, e.g. after the effect of risk responses. Organizational and program risks are assessed using the WIPO corporate risk scale. Project risks may use a risk scale customized from the WIPO project risk scale template. Both risk scales are presented in the Annex VII.



IOD Internal Survey

The current risk scale for organizational and program risks was found to be sufficient by 27 per cent of IOD Internal Survey respondents³⁷ and somewhat sufficient by 59 per cent (somewhat agree 37per cent; somewhat disagree 22 per cent). Four percent disagreed and 10 percent indicated other opinions.



IOD Internal Survey mention:

Comments of respondents regarding the current risk scale for organizational and program risks:

- *“There is probably merit for another scale and guidance on assessing risks within each operational area or a project, and defining criteria for when these would need to be escalated to the Enterprise risk scale. Also needs to be tailored for the business at the business level.”*
- *“The views on impact are considerably different depending on whether viewed from a system, program or organizational point of view. However, the significance of that is secondary to the bureaucratic nature of the review process.”*
- *“Different parts of the organization have different risk appetites and profiles, scales should reflect that.”*
- *“Lack proximity information; Risks should reflect the real operational risks.”*

92. The feedback received through the IOD Internal Survey and interviews resonates with observations made in the “Risk Appetite” section of this report: staff members request more guidance on assessing the risk at different levels of the Organization. For example, the current financial thresholds of WIPO corporate risk scale (refer to Annex VII) is difficult to apply in practical decision making. Budgets of different Sectors/Departments/Divisions vary significantly, so the financial impact that could be “noticeable” according to the risk scale, in fact may be “catastrophic” for an area with a smaller budget and *vice-versa*.

93. Furthermore, it is perceived that risks raised by operations and mitigations proposed are not always understood and acknowledged. Suggestions also point to the potential need to distinguish between “Member State” related risks and non-Member State businesses, whereby, different risk profiles and appetites would be set.

(ii) Developing Risk Responses

94. WIPO develops risk responses in the form of mitigating actions and controls. Mitigation actions are intended to reduce the impact or likelihood of risks, and are one-off measures, which have specific objectives and deadlines, and may strengthen controls and/or reduce the

³⁷ Annex II, Question 10

likelihood or impact of the risk event. Controls are designed at various levels of the Organization and are established to ensure reasonable assurance regarding the reliability of reporting; the effectiveness and efficiency of operations; compliance with applicable policies, regulations and rules, and the safeguarding of resources. Controls take various forms, such as the regulations and rules; office instructions and controls in information technology systems. Controls are cross-referenced to the risk that they mitigate.



IOD External ERM Survey

For comparison, only 17 per cent of external survey participants³⁸ had internal controls integrated in their Risk Management system and linked to respective risks.



IOD Internal Survey

Forty-five per cent perceived that the number of mitigating controls/actions recorded in their risk registers were adequate to address the number of risks³⁹, while 36 percent found these mitigations somewhat adequate. Nine percent found that there were too many mitigating actions/controls to address the number of risks.



IOD Internal Survey mention:

Comments of respondents regarding the number of mitigating controls/actions recorded in their risk registers:

- *“It depends on the type.”*
- *“In general the risk register is considered a formality which must have a mitigating action noted against it. This a backwards view of the risk register.”*
- *“I don’t think we recognize enough risks in most projects.”*

95. **Controls.** There were 123 Controls linked to specific risks in WIPO ERM Risk Register as of December 8, 2021; the source of controls is a Control Library that contained 467 controls at that date. Control details are disclosed in the Annex VIII. The Control Library is fed by WIPO programs and Process Maps.

96. WIPO Project Risk Registers normally do not link risks with existing controls; instead there are mitigating actions in place. This is primarily explained by the short-term nature of projects.

97. Controls are categorized as Entity Level Controls (ELC), process level controls, or implementation level controls. The Risk and Internal Control Manager is responsible for ensuring that the controls are recorded in ERM. Each control is assigned to an owner, who is responsible for ensuring that the control description and any related process maps are up to date. Control owners are responsible for ensuring that all relevant control documentation is maintained and accessible for purposes of the control assessments and validation performed by the Risk and Internal Control Manager.

98. **Control design and formulation.** Effective implementation of controls starts with their proper formulation. Internal controls should be documented sufficiently to demonstrate that controls are in place and functioning as intended (e.g. enable another knowledgeable person to test performance of the control).

³⁸ Annex III, Question 7

³⁹ Annex II, Question 11



IOD Internal Survey

Around 51 per cent of IOD Internal Survey respondents⁴⁰ found that 80 per cent (and above) of mitigating actions/controls are efficiently designed and fit-for-purpose. Only two per cent felt that less than 20 per cent were efficiently designed. Nine percent indicated “other”.



IOD Internal Survey mention:

Comments of respondents regarding the design and fit-for-purpose of mitigating actions and controls:

- *“Some are a controls a little too general”*
- *“The nature of the risk management system is such that the risk register itself is not useful for managing the risks.”*
- *“Staff leaving or staff contract issues are a key risk that “mitigating factors” never seem to address in project risks. It is noted, but the problem recurs again and again.*
- *“As many years as I can recall, loss of good qualified staff due to lack of career prospects, and failure to provide adequate (e.g., IT) resources have been identified as risks. This has materialized several time along the years.”*

99. A sample of 70 WIPO Controls (Annex XIII) has been analyzed against the following criteria:

- (a) Clarity;
- (b) Conciseness;
- (c) Control frequency is stated;
- (d) Control type and function are indicated;
- (e) Control owner assigned; and
- (f) Control is addressing the associated risk.

100. IOD recognizes the good efforts of involved staff in designing, maintaining and updating the risk mitigating controls. Going forward, more attention could be paid to clearer and more concise wording of controls aligned with best practices, and better assignment of controls to the risks they intend to address. Respective Program Managers and SRCs are advised to be more proactive in monitoring the quality of control formulations.

101. **Mitigating Actions.** WIPO is actively using mitigating actions to reduce specific risks or strengthen the existing controls. While the utilization of mitigating actions is more common for project-related risks due to their “short-term” effect, UNRIAS survey feedback and information from different industries evidence the usage of this type of risk response.



IOD Internal Survey mention:

- *“Proposed mitigation measures should be accepted when they are not systematic. Random, post facto analysis of controls may be as efficient and less cumbersome and costly from an administrative standpoint than systematic measures. Not moving towards this type of control demonstrate WIPO’s low risk appetite”.*

⁴⁰ Annex II, Question 12

102. ERM Risk register contained 322 mitigating actions linked to risks as of December 8, 2021 (Annex IX). IOD has analyzed a sample of 100 Mitigating Actions (Annex XIII) against the following criteria:

- (a) Clarity;
- (b) Specificity and ability to measure;
- (c) Action owner assigned;
- (d) Action has a deadline;
- (e) Action is addressing the associated risk; and
- (f) One-off measure; not a control.

103. Some mitigating actions could be more specific and measurable. For example, below are several extracts from the Mitigating Action descriptions:

- (a) Provision of an impartial and inclusive environment for...
- (b) Constant and focused interaction with...
- (c) Facilitate discussion by ...
- (d) Ongoing close coordination with...
- (e) Continuous engagement of...

104. Secondly, about 39 per cent of analyzed actions are of “continuous” nature and have more properties of controls rather than “one-off” actions. These activities potentially could render more value if designed and monitored as controls.

105. **Acceptance of Risks.** Accepting the risk without mitigation is also a risk response option, as long as the risk is within the WIPO risk appetite, and subject to the appropriate approvals. The Risk Management and Internal Controls Manual provides guidance on how to accept risks.

(iii) Monitoring and Follow-up

106. Monitoring activities are undertaken throughout the risk management process, assessing the continued existence of risks and the validity of their associated responses (mitigation and control).

107. **Corporate Risk Follow-ups** are undertaken by RMG at a minimum on a quarterly basis, with reporting at least on a semi-annual basis⁴¹. This frequency is in line with the majority of surveyed UNRIAS organizations⁴². IOD has obtained an evidence on extensive analysis of corporate risks by RMG.

108. **Program Risk Follow-up.** According to the WIPO Risk and Internal Control Manual, ERM Risk Register should be assessed regularly for completeness of risk identification and accuracy of assessment. Based on the analysis of ERM Risk Register and conducted interviews, on average programs update and reassess their risks once a year, during the

⁴¹ WIPO Risk and Internal Control Manual

⁴² Annex III, Question 12

Annual Work planning; however, when significant risk arises, it is being recorded as soon as possible.



IOD External ERM Survey

The majority of respondents (86 per cent)⁴³ use risk registers, and indicated that updates of risk registers are mandatory (84 per cent)⁴⁴; with forty-three per cent updating risk registers two-three times per year⁴⁵.

109. **Project risk Follow-up and Escalation.** Project risks require regular monitoring and ongoing oversight since they are particularly susceptible to change. Project Managers define a risk management strategy, based on a template, agreeing the approval, escalation, frequency, risk scale etc. for risk management activities for the duration of the project. Project risks are recorded and updated in the appropriate project documentation, normally Microsoft Excel-based risk registers, with each iteration being retained for audit and review purposes. IOD has verified the regularity of updates of Project Risk Registers.

110. The Risk and Internal Control Manual stipulates that project risk assessment, response and escalation processes are defined in the project risk management strategy and approved by the relevant project board. Projects are run by different Sectors/Departments/Divisions, so the risk escalation criteria and workflow might be applied differently. Through interviews IOD learned that Project Managers not always aware of when and how they would need to escalate risks. In addition there is a perception of unwillingness to “give a project a bad news”, which is not facilitating a project risk escalation even when possibly needed.



IOD Internal Survey mention:

- *“A Sector Risk coordinator should have a look at some project risk matrices from time to time. The tendency in a project is to downplay the risk. Independent “expert eyes” could be helpful.”*
- *“It is hard to give the project bad news / reality check.”*
- *“The problem is key tech projects are constantly running into the risk of temporary or non-staff resources leaving. This can have severe impacts on a project.”*



IOD Internal Survey

Forty-eight percent of respondents⁴⁶ were aware that significant and relevant project risks needed to be escalated to the corporate risk register. A further 33 per cent were somewhat aware and needed more guidance, against 18 per cent who were not aware and had not received any guidance or information in that regard.

Likewise, 35 per cent of respondents⁴⁷ knew how to escalate project risks to the corporate risk register, and a further 43 per cent somewhat knew how to do so, against 15 per cent who have not, and five per cent who have not been involved in project management. Some comments from respondents indicated that they would be unable to do this on their own, or would contact the Program Manager, the Controller, or the Project Executive.

⁴³ Annex III, Question 10

⁴⁴ Annex III, Question 11

⁴⁵ Annex III, Question 12

⁴⁶ Annex II, Question 17

⁴⁷ Annex II, Question 18

Finally, 30 per cent of respondents⁴⁸ indicate to have escalated project risks to the corporate risk register within the last three years, 10 per cent within four-five years, against 53 per cent who have never escalated such risks. IOD also notes that five per cent indicated that they have not been involved in projects.

111. Given the fact that WIPO constantly runs a number of high-value projects critical to operations, project risk escalation might play an important role and might require a more formalized controlling mechanisms. Potential solutions, among others, could relate to formal inclusion of project risk discussions in the scope of SRC or a centralized project risk repository under a Project Management Office.

112. When compared to other organizations, it appears that the project level risk escalation is not always well covered by available guidance.



IOD External Survey on ERM

On the need to manage project risks, 46 per cent⁴⁹ of participating Organizations indicated that there was no formal process in place to ensure that applicable significant project risks are systematically escalated to the corporate or entity level risk register. Twenty-nine per cent recorded project risks in separate “project” risk registers, compared to 36 per cent that recorded their project risks in respective organizational risk registers.

113. **Follow-up of Controls.** The controls within each Sector Lead’s area of responsibility are (self) assessed in consultation with the Risk and Internal Control Manager, who validates the assessment. Figure L below shows the Control Attributes that are considered in the assessment of effectiveness of controls.

Figure L: Control Attributes used for the assessment of Controls

Control Maturity		Control Type			
Level 0 Non-Existent / Ad-hoc	Level 1 Documented only	Preventive controls		Detective Controls	Directive Controls
Level 2 Partially Deployed	Level 3 Deployed and Reliable	Segregation of duties	Security of Assets & Restricted Access		
Level 4 Measured and Automatic	Level 5 Continuously Improving	Approvals, Authorizations, and Verifications	Training undertaken		
Control Function		Control Priority			
Manual	Automated	Non-Key controls		Key controls	
Frequency of Control Action		Implementation Description			
Annually	Monthly	Narrative on current assessment, identifying any relevant points in considering the assessment.			
Quarterly	Weekly				
Daily	Multiple Times Daily				

Source: WIPO Risk and Internal Controls Manual

114. The results of the control (self) assessment should be formally signed-off by the process owners, demonstrating that they take ownership of the internal control system. This process is performed annually.

⁴⁸ Annex II, Question 19

⁴⁹ Annex III, Question 13



IOD Internal Survey

On the efficiency and effectiveness of the annual control assessment process, 23 per cent of IOD Internal Survey participants⁵⁰ found this process efficient and effective, 40 per cent found it somewhat efficient and effective, while 17 found the process ineffective and inefficient. Note however, that 17 per cent of respondents did not own any controls.

115. Comments include appreciating the value of the annual risk assessment, but also insights on areas of discontent such as:



IOD Internal Survey mentions:

- *“The internal control is also a self-assessment, with the risk of treating the internal control as a mere formality and reducing the effectiveness thereof.”*
- *“The interface is clumsy and the system not designed to support useful management.”*
- *“I do review them for the division. We have too many controls listed, the vast majority of which are not linked to existing risks.”*
- *“I find it too artificial and disconnected from reality”*
- *“More automation is needed.”*

116. IOD has verified the controls validation frequency in the ERM (Annex XIII) and found that the majority have last been updated in November 2021. The assessment and validation of controls take place regardless of whether these controls are linked or not linked to risks.

117. There is a positive increase in the number of evidential documents attached to controls. While 67 and 90 controls had evidential documents attached in ERM in 2019 and 2020 respectively, IOD counted 166 such controls in 2021 (Annex XIII).

118. **Follow-up of Mitigating Actions.** WIPO Risk and Internal Controls manual does not specifically state the frequency of mitigating actions' follow-ups, as well as the role of WIPO risk function in their assessment and validation. The risk function is frequently called on to advise on these matters, and validates the Program of Work and Budget risks and actions as well as those at the critical exposure, or organizational level. SRCs are encouraged to challenge mitigation plans.

119. Based on the analysis of mitigating actions updates, on average they are updated once a year, mainly during the period of the Annual Work planning.

120. Given the high volume of mitigating actions in the ERM Risk Register, it would be beneficial to expand the WIPO Risk and Internal Controls manual with guidance on the frequency of mitigating action follow-ups, and the roles and responsibilities related to their assessment and validation.

121. Finally and going forward, the quality of risks and controls would be further enhanced through staff exposure to among others, effective awareness raising, capacity building and knowledge resources.

⁵⁰ Annex II, Question 13

Recommendation

3. The Office of the Controller should review and update the Risk Manual, including guidance for risk responses, risk escalation (including project risks), and the relationship between risks and controls.

(Priority: Medium)

(iv) Statement on Internal Control

122. The Director General is required to provide an assurance on the operating effectiveness of WIPO's system of internal controls on an annual basis. The requirement stems from the Regulation 5.8 (d) of the Financial Regulations and Rules. This assurance is provided through the "Statement on Internal Control" (SIC) document, which is presented in line with the seven components of WIPO's Accountability Framework, aligned to the COSO framework and Three Lines Model.

123. The SIC is supported by representation letters prepared by Sector Leads of respective Sectors. Annex X to the report provides an SIC preparation flowchart, explaining all main preparation steps and involved actors.

124. IOD analyzed the SIC preparation process and the building blocks of assurance used by Sector Leads to prepare and sign their Representation Letters. Generally, Sector Leads believe to have sufficient assurance information and are feeling comfortable to sign-off their Letters of Representation. The following main sources of assurance have been cited:

- (a) Results of assessments of Entity Level and Process Level Controls;
- (b) Outputs of WIPO RBM System;
- (c) Regular Management Reporting, including RMG reports;
- (d) Information from the Office of the Legal Counsel;
- (e) Business Intelligence (BI) Dashboards; and
- (f) Feedback from External Independent Auditors and IOD.

125. At the same time management noted that the assurance can be further enhanced by adding more visibility on project risks and status.

126. IOD notes that the wording of SIC and Management Representation Letter (MRL) to a large extent is tailored for needs of Financial Reporting. For example, SIC explains the accountability of the Director General for maintaining a system of internal financial control; the wording of MRL states that it is provided in connection with the audit of the financial statements of the WIPO and its Unions for the purpose of expressing an opinion as to whether the financial statements present fairly, in all material respects, the financial position of WIPO in conformity with generally accepted accounting principles applicable to the UN System organizations.

127. While financial controls play an important role, IOD believes that SIC and MRL could add more value if their wording provides assurance over the System of Internal Controls as a whole. Going forward, the Office of the Controller would benefit from engaging with the external auditors, to assess opportunities for expanding the SIC and related management letters to cover the system of internal control as a whole. Finally, IOD points out the need to align the

wording of SIC and MRL with the programmatic structure and terminology of the new Program of Work and Budget for 2022/23, and the MTSP.

Point for Consideration

4. Visibility of key project risks can be further enhanced by considering:
 - (a) Using SRCs to engage with Project Managers in respective Sectors, to identify key project risks that can be escalated at Sector or organizational levels; and
 - (b) Adding a line on awareness of key project risks and related responses in the MRL of respective Sector Leads.

(v) ERM Integration with Results Based Planning

128. Risk Management is an integral part of the development of the Program of Work and Budget.



IOD Internal Survey

Thirty-five percent of respondents⁵¹ were satisfied and somewhat satisfied with the process of identifying risks to be included in the Biennial Program of Work and Budget. However, the 18 per cent respondents who were dissatisfied or somewhat dissatisfied indicated that the process was “too disconnected from the actual work”.

On whether the organizational risks are useful for cross-sectorial work, 43 per cent of respondents⁵² found them somewhat useful, 18 per cent useful, against 23 per cent who did not find it useful. The majority of the 18 per cent respondents who indicated “other”, echoed the sentiment that they did not know or were not part of the process.

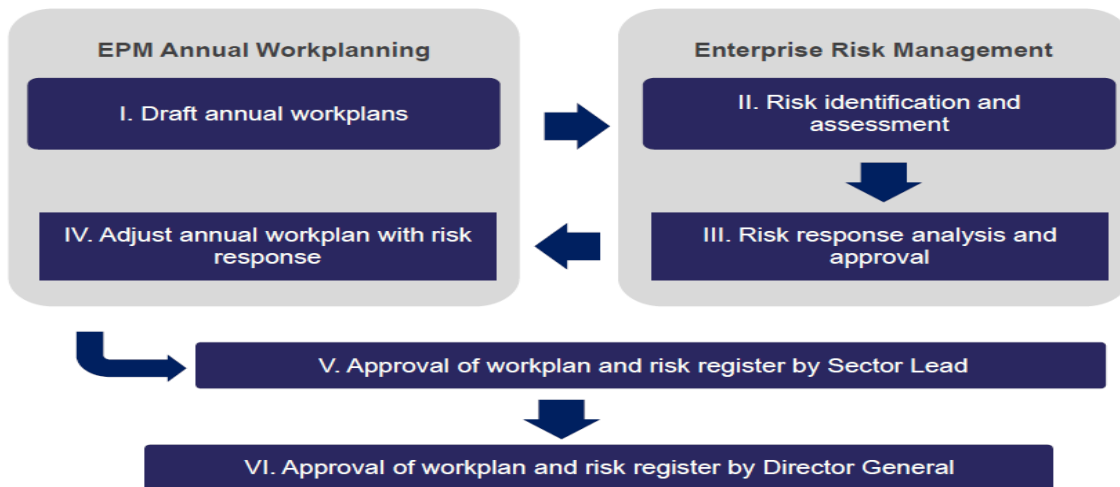
129. **Integration with the Enterprise Performance Management (EPM).** Figure M below illustrates the risk management integration with WIPO Annual Work-planning. The Program Performance and Budget Division (PPBD) has developed a guidance, explaining the process of risk identification, approval and integration of risk responses⁵³ in the Work-planning.

⁵¹ Annex II, Question 28

⁵² Annex II, Question 29

⁵³ According to PPBD guidance, Risk Responses constitute Mitigation plans, Internal Controls or Ways to exploit the opportunity

Figure M: Risk Management Integration with Work-planning

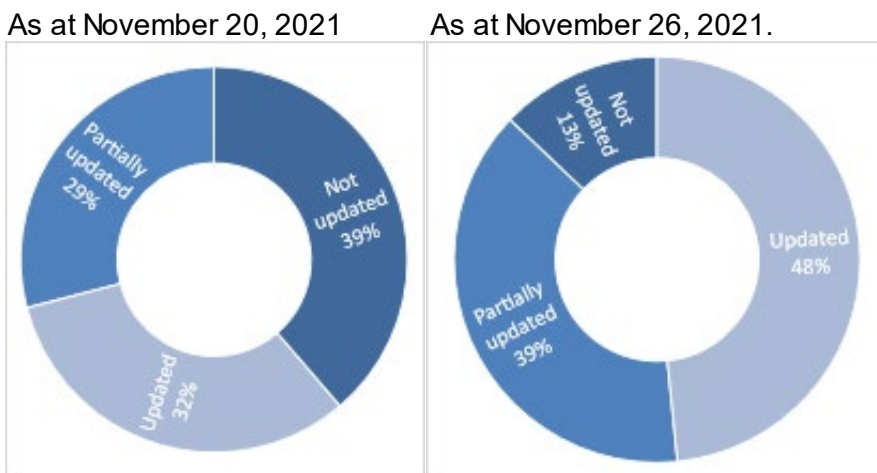


Source: PPBD guidance - Review the Risk Report in BI & Update Risk Registers in ERM

130. When deemed relevant, Sectors record a Risk Response in the Work plan Activity Addition form in EPM. It is under the Sectors’ responsibility to decide whether the Risk Response requires a budget or it may be a contingency.

131. Risks and Risk Response Status Update requires time and effort; therefore, it is important that this process is timely finalized and effectively feeds the Annual Work-planning. The due date for the completion of 2022 WIPO Work plans was set to November 26, 2021⁵⁴. IOD verified the status of Risks and Risk Response update by Programs on November 20, 2021 and November 26, 2021. The details are disclosed in the Annex V and the summary of results is presented in the Figure N.

Figure N: Risks and Risk Response Status Update in ERM by WIPO Programs



Source: ERM Risk Register

132. One third of WIPO Programs have updated their Risks and Risk Response status by November 20, 2021, and almost a half of programs did it by November 26. It is important for Risks and Risk Responses to be updated before the Annual Work-planning deadline to ensure that all significant risks are captured, all necessary Risk Responses are reflected in EPM and

⁵⁴ PPBD, October 25, 2021 email “Launch of 2022 Work-planning”

any necessary changes to the budget are allocated. SRCs are in a good position to facilitate this process.

133. Further, IOD verified the linkage between the Work plan activities in EPM and related risks. While Risks and Risk Responses in the ERM Risk Register can be easily traced back to the expected results of corresponding biennia, the EPM contains no references to associated risks. It would be beneficial to see risks in the EPM for the Work-planning purposes.

134. **Integration with PM SDS.** While Risks and Risk Responses are assigned to specific owners, the performance appraisal system is not linked to their accomplishments in the area of risk management. Linking the risk management to the performance appraisal system of relevant staff would enforce further integration of ERM across the Organization. This observation is in line with observations set out in the 2020 Report of the JIU “Enterprise risk management: approaches and uses in United Nations system organizations”. IOD strongly supports this measure as a means to further support risk management at WIPO.

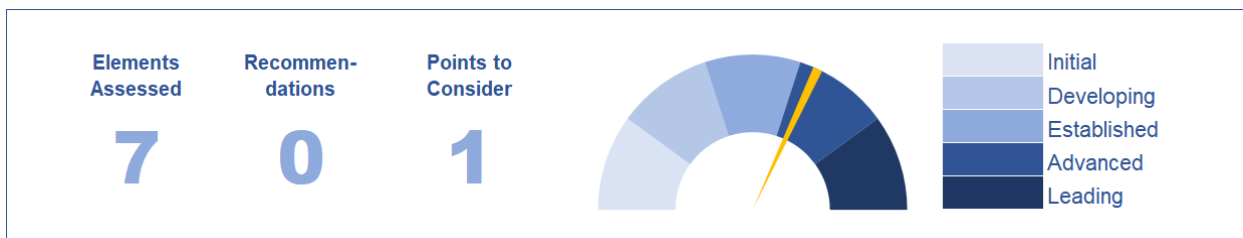
Point for Consideration

5. Sectors to take measures to timely update their risks and risks responses before the deadline for submitting the annual work plans, to among others, ensure that risks related to planned activities are timely captured, and applicable mitigations are budgeted in compliance with relevant PPBD Guidance.

(E) ERM SYSTEMS AND TOOLS

135. The Figure below summarizes the results of the assessment of the ERM Systems and Tools.

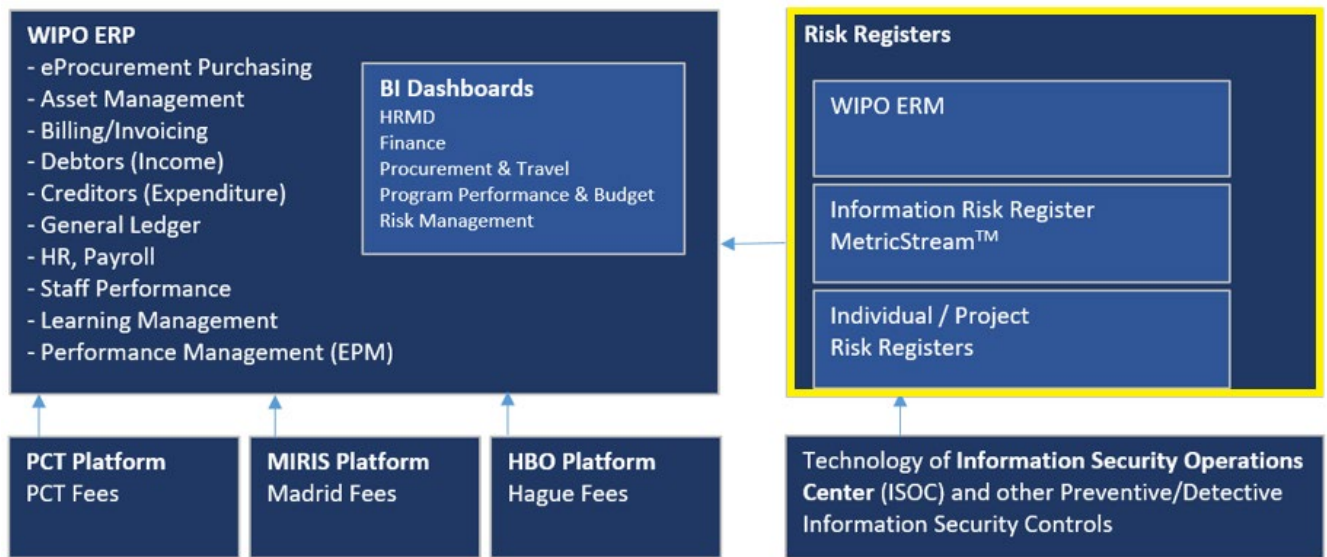
Figure O: ERM Systems and Tools – Assessment Summary



Source: Gap Analysis Details (Annex XIV)

136. Figure P below depicts the collaboration between WIPO Risk Management related systems and other WIPO information systems and tools.

Figure P: WIPO Main Information Systems and Tools



Source: Compiled by IOD from WIPO Platforms, Systems and Tools.

(i) Risk Registers

137. The **WIPO ERM** (Acuity STREAM™) is a repository of the entity’s risks and risk responses. It also includes data on control owners, deployment level of controls, and other relevant information, which makes risk registers a key source of assurance information.



IOD Internal Survey

While 13 per cent of respondents⁵⁵ agree and 20 per cent somewhat agree that WIPO ERM (Acuity STREAM™) is user-friendly and useful, 33 per cent disagree and 15 per cent somewhat disagree with this statement. Twenty per cent of respondents have never used the system.

138. As per feedback received from IOD Internal Survey and IOD meetings with relevant staff, the ERM system is not user-friendly and is too complex, resulting in reluctance to use the tool. Considering that the selected participants include management and risk and control owners, several key issues can be noted such as:

- (a) The need to enhance responsibility and accountability of managers and risk owners in using the system; and
- (b) The importance in identifying the key challenges in the use of the current system.

139. Furthermore, a number of comments support the need to review the adequacy of the current system and encourage use by managers.



IOD Internal Survey mentions:

- “There is a room for using modern, simple and practical digital solutions.” “There is also opportunity to introduce advanced analytics and AI to derive insights into risk evolution and control effectiveness.”
- “Too complex, sophisticated and hard to utilize”

⁵⁵ Annex II, Question 16

- “I would like to point out that the fact that risks are managed through both the BI and the ERM complicate things somewhat.”
- “The current risk management system is very poor; this system is impossible to use; it is user-unfriendly and complicated.”
- “The use of the system and positive real impact is unclear.”
- “I would rather spend my time dealing with the actual risk than feeding the machine, and often time my dealing with the risk allows closing it before it even became an issue worthy of reporting”.

140. IOD analysed the software feedback collected on Gartner peerinsightsTM⁵⁶, and found that Acuity STREAM™ was initially developed as a Cyber-Risk management software, which may have some impact on complexity of the system; on the other hand it allows for more robust analysis of risk information.

141. Figure Q below summarizes the customer experience and rating distribution.

Figure Q: Acuity STREAM™ – Ratings Overview



Source: www.gartner.com



Software reviews on www.gartner.com

- **Favorable Review:** A good solid tool with easy focus on InfoSec, the interface could do with refining. The product met the needs of deployment and the company is easy to deal with going above and beyond in the vendor / supplier relationship.
- **Critical Review:** none
- **Likes:** The creators come from a Cyber Risk background and understand Information Security in context with a maturing environment. The product can mature with the organization and does not have to be overtly process driven. The company is excellent in dealing with support and consultancy
- **Dislikes:** The interface and the User Interface (UI) is quite difficult to get used to, and is not intuitive and reflective of modern Operating Systems. The workflow is clunky compared to other products and the reporting tool is basic.

⁵⁶ Peer Insights is Gartner's peer-driven ratings and reviews platform for enterprise IT solutions and services covering over 300+ technology markets and 3,000 vendors.

142. Furthermore, many staff members have little knowledge on where the system is located and how to run it, which could indicate that communication needs to be enhanced. Some staff members may not make reasonable efforts to better understand the software.

143. Given the high costs of Risk Management software and related implementation and migration efforts, IOD believes that there is room to maximize the value from the existing software, which can be done through raising awareness and educating relevant staff to work with Accuity Stream more efficiently.

144. **WIPO Information Risk Register.** Due to specific operational needs, the IS Section at WIPO is using an automated solution, MetricStream™ (named as a Leader in the 2021 Gartner® Magic Quadrant™ for IT Vendor Risk Management Tools) to manage its Information Security Governance, Risk and Compliance processes⁵⁷. Risks from MetricsStream™ are regularly updated to the ERM at more aggregated level.



IOD Internal Survey mentions:

- *“There is room for improvement and consolidation between various risk management solutions within WIPO”.*

145. Some staff members commented that the centralization of WIPO Risk Registers could enhance the risk management and provide more uniform approach to risks. While IOD understands the benefits and supports the concept of “one-stop-shop” for risks, proper consideration should be given to specific demands of such areas as Cybersecurity and Project risk management. Going forward, WIPO may consider using “native” ERM module of its ERP in case WIPO decides to upgrade or change the existing ERP. This will allow automated embedding of risks into all main WIPO processes such as Performance Management, Budgeting and others.

146. **WIPO Project Risk Registers.** Risks at the level of Projects are captured in separate Project Risk Registers, normally based on Microsoft Excel™, with each iteration being retained for audit and review purposes. If relevant, these risks may also be recorded into the WIPO ERM through the process of escalation.

147. The analysis of a sample of Project Risk Registers shows that overall, records made allow for effective risk identification and mitigation at the level of individual projects. The Office of the Controller’s Intranet page provides a Project Risk Register Excel template with a base risk scale to allow projects to define their own suitable risk impact scale.

148. The Project files (and respective Project Risk Registers) are stored in different locations on WIPO network and are maintained by respective Project Managers. While basic data on IT-related projects is kept by the Senior Information and Communication Technology Portfolio Management Officer, non-IT project files have no such point of coordination, leaving project management “silos based” or “decentralized”.

149. Amongst other benefits, centralized way of storing and managing projects and related risk registers provide:

- (a) Consistency of the project risk management approach;
- (b) Identification of cross-cutting project risks or concentrations of specific risks which need to be escalated or would require the attention of Project Board or RMG;

⁵⁷ These include annual ISO 27001 Information Risk Assessments, Service Provider Risk Assessments, Policy/standards exception management, Certification and Accreditation Assessments, Vulnerability Management, Information Security Incident Management among others

- (c) More complete risk identification and effective application of lessons learned based on similar projects; and
- (d) Easier reporting, providing a “helicopter view” over the status of all projects and their risks, which would be useful for RMG discussions.

150. WIPO would benefit from centralization of the Project Risk Management by, for example, expanding the role of the current Project Management Officer, or establishing a Project Management Office with relevant roles and responsibilities. This recommendation, which is still pending, was issued by IOD in its Audit of Project Management in 2016 (IA 2016-04), and reiterated in the report on the audit of the Hague Platform Project (IA 2021- 02). The Administration, Finance and Management Sector (AFMS) has recently confirmed its commitment to implementing this recommendation during the course of the year.

(ii) Linkage of WIPO Risk Registers with other systems

151. WIPO ERM Risk Register and Information Risk Register (MetricStream™) used by the Safety and Information Assurance Division are off-the-shelf stand-alone applications. While the integration of risk and risk response data with main WIPO systems is an ongoing process (please refer to the “ERM Integration with Results based planning” section of the report), currently there are no automated linkage with these systems and risk registers.

152. While IOD recognizes benefits of automated linkage of risk data, maintaining the right balance between the implementation costs and benefits gained is relevant.

Point for Consideration

6. The value from the existing ERM software can be maximized by among others:

- (a) Enhancing the responsibility and accountability of managers and risk owners in using the system;
- (b) Identifying the key challenges in the use of the current system and finding cost-effective solutions; and
- (c) Raising awareness and educating relevant staff to work with Acuity STREAM™ more efficiently.

(F) RISK CAPABILITIES

153. The Figure below summarizes the results of the assessment of the WIPO Risk Capabilities.

Figure R: Risk Capabilities – Assessment Summary



Source: Gap Analysis Details (Annex XIV)

(i) Staff Risk Awareness

154. Risk awareness is the acknowledgement of risks. It can have a large effect on how risks are managed and how decisions are made. By increasing the risk knowledge and awareness of the staff and stakeholders involved, the organization can leverage its risk responses to a much greater extent and have a higher chance of succeeding in achieving its objectives.



IOD Internal Survey

While 24 per cent of respondents⁵⁸ were aware of different risk management and internal control trainings available in the WIPO Enterprise Learning Management (ELM) system, 43 per cent were somewhat aware and 33 per cent were unaware.

In more detail, 43 per cent of respondents⁵⁹ indicated that they have been provided with adequate training, 24 per cent were somewhat in agreement, against 14 per cent somewhat disagreed and 18 per cent disagreed.

Furthermore, 24 per cent of respondents⁶⁰ have been trained at least once in the last two years, 27 per cent have not, 39 per cent have been trained more than two years ago, and 10 per cent have never attended a training.

155. Survey participants recognized the different levels of risk maturity across Sectors and Divisions, and the need to raise more awareness about risk management, while implementing a more user-friendly tool that offers useful information to management – numerous comments pointed to the system as a significant inhibitor.

156. Finally, there is some call for a short compulsory risk management training once a year, online, and covering varied topics, to avoid long cumbersome sessions, which would result in less buy-in from staff. Furthermore, these trainings could also be a means to obtain insights and feedback from staff on key threats and opportunities to feed WIPO's risk landscape.

157. Results of IOD Internal Survey are comparable to the IOD External ERM survey feedback.



IOD External ERM Survey

Forty eight per cent of respondents⁶¹ indicate not having a formal risk management training, and out of the 31 per cent that had a training course, 40 per cent highlighted that the training was mandatory for designated staff members only.

158. IOD has analyzed ELM trainings related to Risk Management and Internal Controls in the period from January 2019 to November 2021. The following trainings were identified in the ELM:

- (a) ELM-1061 - HRMD: Spot the Risks;
- (b) ELM-1756 - HRMD: Spot the Risks;
- (c) ELM-1959 - HRMD: LinkedIn: Risk Taking for Leaders;
- (d) ELM-2206 - IT: Blended Learning: Management of Risks (MOR);

⁵⁸ Annex II, Question 6

⁵⁹ Annex II, Question 7

⁶⁰ Annex II, Question 8

⁶¹ Annex III, Question 8

- (e) ELM-2224 - IT: Blended Learning: Management of Risks (MoR);
- (f) ELM-2345 - HRMD: LinkedIn: Project Management Foundations: Risk;
- (g) ELM-674 - Risk Management Briefing;
- (h) ELM-675 - HRMD: Risk Management Training ;
- (i) ELM-683 - Risk Management Training - Desk-to-desk training; and
- (j) RM module - Project Management training sessions.

159. Results of the analysis disclosed in the table below.

Table 2: Number of participants in Risk Management and Internal Controls related trainings (a-i) during the period from January 2019 to November 2021 by sector / office

SECTOR / WIPO OFFICE	Trainings										Total
	(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)	(i)	(j)	
AFMS	22	17								7	46
BDS	12	5								8	25
CCIS	2	1									3
GCP	1	1									2
IP and IES	5	1									6
IPS	1	1									2
PTS	26	18		1	1					6	52
RND	3	1	1			1				7	13
Sector of the DG	9	5								6	20
WIPO Algeria Office											-
WIPO Brazil Office	1										1
WIPO China Office											-
WIPO Japan Office											-
WIPO New York Office											-
WIPO Nigeria Office											-
WIPO Office Russian Federation	2	1									3
WIPO Singapore Office	2										2
Grand Total	86	51	1	1	1	1	-	-	-	34	175

Source: Performance and Development Section. **Please note** that ELM mandatory trainings on Fraud and Ethics have been excluded from the analysis due to their mandatory nature and indirect relation to Risk Management and Internal Controls.

160. Out of 10 ELM Risk and internal control related trainings only three – (a), (b) and (j) had relatively active attendance – 86, 51 and 34 participants respectively. More detailed analysis of these two trainings revealed that trainings (a) and (b) are 10 minutes self-paced eLearning in a “game” environment, which is useful but can be considered only as a “complementary” learning material.

161. Four out of eight ELM trainings have been attended only by one staff member and three ELM trainings have not been attended at all in last three years. This raises questions about staff awareness and popularity of ELM trainings in the Risk Management and Internal Controls domain. Going forward, it would be beneficial to better communicate on, and monitor Risk Management and Internal Controls trainings.

162. Further, there is a rather low participation of WIPO offices in Risk Management and Internal Controls related ELM trainings. Five WIPO External Offices did not take part in the aforementioned ELM trainings in the last three years.

163. In addition, IOD has analyzed participation in Risk Management and Internal Controls related trainings from the perspective of their grade and Sector. Results are summarized in the table below.

Table 3: Number of participants in Risk Management and Internal Controls related trainings during the period from January 2019 to November 2021 depending on Sector and grade

Grade	AFMS	BDS	CCIS	GCPS	IP and IES	IPS	PTS	RNDS	Sector of the DG	Brazil Office	Russia Office	Singapore Office	Total
D2	1												1
D1	1	3		1			1				1		7
P5	6	3			1			2	1		2		15
P4	6	6			1		9	4	2	1		1	30
P3	9	3			1		16	2	2				33
P2	2	3	1		1				4				11
G7	4		2				5		1				12
G6	5	3			2		8		3			1	22
G5	2	1					8	1	1				13
G4	2							2	6				10
Non-staff	7	3		1		2	5	2					20
Total	45	25	3	2	6	2	52	13	20	1	3	2	174

Source: Performance and Development Section. **Please note** that ELM mandatory trainings on Fraud and Ethics have been excluded from the analysis due to their mandatory nature and indirect relation to Risk Management and Internal Controls.

164. The analysis shows that the most “popular” participant profile is a P3-P4 grade staff member. Senior Management (P5 and above) participation is rather low. Potentially this can be explained by the content of trainings, not tailored for the senior leadership.

165. Discussions with the Office of the Controller indicate that fraud risk awareness was the main focus of risk management training between 2019 and 2020. As of October 26, 2021, around 97 per cent of staff had completed the fraud risk training. Since 2016, the Office of the Controller adopted a one-to-one risk coaching strategy, working closely with Senior Managers to address their needs rather than through classroom training. Internal Controls training has also been switched to one-to-one mode during the annual control assessment exercises with control owners.

166. The Office of the Controller continued to run risk management training as a module of the Project Management in an RBM environment training course. Some staff members were last trained in November 2019. The next planned risk management related training is envisaged for 2022 as a module at the Workshop on the Revised Development Agenda Implementation Cycle. Going forward, the development of a dedicated risk management training course is planned for 2023.

167. While IOD appreciates the efforts of the Office of the Controller to provide focused one-to-one guiding sessions to risk and control owners, and acknowledges that some staff members take individual initiatives to attend risk management training provided by third parties, however, collected feedback and analysis of existing trainings, point to the need for additional efforts in this area.

168. Going forward, adopting a hybrid approach which provides class room but tailored training addressed to the different needs of operational staff, risk owners, Directors, and Sector Leads would better support risk maturity. As per staff feedback, trainings may represent series of practical workshops including insights and feedback from staff, which could serve to further enhance the components of the Risk Management Framework

Recommendation

4. The Office of the Controller in coordination with the Internal Training Program of the WIPO Academy, should further raise risk management and internal controls awareness by introducing updated training offerings to address the needs of staff members at different levels and relationships and responsibilities towards Risk Management and Internal Controls.

(Priority: Medium)

(ii) Availability of Risk Information

169. Risk reporting is a means to demonstrate the value that the risk function brings to an organization. Qualitative and timely risk reporting allow for proactive risk management – to identify and escalate issues before they materialize. Robust risk reporting among others provides the following benefits:

- (a) Embeds risk management into leadership, decision making, oversight and business operations;
- (b) Uses retrospective results to learn and predict business risks before they materialize;
- (c) Provides assurance to the management and stakeholders; and
- (d) Highlights areas of concern and promotes continuous improvement.

170. **Risk Reports and BI Dashboards** – As part of supporting the Organization in effectively managing risks and integrating risks in making informed decisions, WIPO has established risk reports and dashboards. Sector/Divisions are encouraged to regularly run risk reports to support their operational and decision-making processes.



IOD Internal Survey

Thirty-eight per cent of survey respondents⁶² indicate that they run risk reports two-three times a year, 30 per cent once a year, and five per cent at least four times a year. However, 28 per cent do not run risk reports, some of which indicated that they request for, or receive extracts.

Thirty per cent of respondents⁶³ indicated that the current content and quality of risk reports are relevant and suitable to support risks management in their Sector/Program/Division. A further 35 per cent somewhat agreed, against 15 per cent that somewhat or fully disagreed. Eighteen per cent indicated that they do not receive reports.

171. Survey respondents and interviews held with relevant stakeholders indicate that there is a need for easier access to available risk reporting. “Enterprise Risk” and “Business Intelligence” buttons are placed on the front page of the New WIPO Administrative Integrated Management System (AIMS) portal, which should make users’ access to the risk reporting more intuitive. To further improve the access to the risk information, additional button on the “Quick-links” could

⁶² Annex II, Question 20

⁶³ Annex II, Question 21

bring the user to the “Risk and Response” BI Risk Dashboard, showing all Risks / Controls / Actions related to that specific user.



IOD Internal Survey mentions:

- *“The ERM software is extremely unfriendly and the risks are set up in a manner that is only relevant to showing that something is being done, not for being in the slightest useful in actively managing the process. Consequently, the reports are only looked at when updates are required.”*
- *“I receive a register of risks 1x a year and review for controls.”*
- *“I think about my risks, but do not run reports and I would not know how to do it.”*

172. **RMG Risk Reports** are prepared on a quarterly basis and contain valuable analysis of internal and external risk information. Among others, the standard agenda includes the following topics:

- (a) Economic and Filing Highlights;
- (b) Financial Highlights;
- (c) Cyber Risk;
- (d) Safety and Security Risk;
- (e) Global Risk Landscape; and
- (f) WIPO Portfolio Overview.

173. The Office of the Controller issues and shares with the RMG and the Independent Advisory Oversight Committee (IAOC), a WIPO Annual Risk Management Report that provides a high-level overview of changes in the Organization’s risk portfolio during the period, and informs on progress in strengthening the Risk Management and Internal Control framework.

174. **IAOC Sessions – Risk Management and Internal Controls Agenda Item.** Risk Management and Internal Control are a regular IAOC meeting agenda item. The Office of the Controller presents the current state of play in the area of Risk Management and Internal Controls enhancements made, status of recommendations issued by IOD, JIU and External Auditors and other relevant related issues.

Point for Consideration

7. The Enterprise Solutions Division should consider adding a button “My Risks” in the Quick-links of the new AIMS Portal. The button should take the user to the “Risk and Response” BI Risk Dashboard, showing all Risks / Controls / Actions related to that specific user.

(iii) Data Analytics Project

175. Increasing business dynamics and growing velocity and emergence of risk among others, have resulted in increased use of data analytics and related techniques to maintain awareness of, and rapid response to evolving risks.











176. The Office of the Controller developed a Roadmap to Maturity of Data Analytics for Internal Controls and Process streamlining 2018– 2024 (Annex XI). The Roadmap contained

activities required to implement the Positive Assurance through Data Analytics for Internal Controls in four main areas: Procure-to-Pay (P2P), Hire-to-Retire (H2R), Financial processes (FIN), Plan-to-Evaluate (P2E).

177. The document was further complemented in 2021 by “Strengthening and Streamlining Internal Controls through the use of Data Analytics” Strategy and Roadmap, which included more detailed implementation steps as well as a Medium Term Strategy with possible future directions towards implementation of preventive analytics and a Data Analytics Maturity Framework (Annex XII). According to a performed self-assessment, the current maturity level of WIPO in that area is set at “Initial”.

178. Figure S below indicates main milestones set in the Strategy and Roadmap document, as well as the stage of completion of the Data Analytics Project.

Figure S: Planned Data Analytics implementation activities – status December 2021

2018	Business requirements defined for key controls for proof of concept (PoC)	
2019	Control metrics developed in OBIEE and migrated to production.	
2020	Prioritize and analyze processes for control analytics	
	Business requirements defined for Procure to Pay (P2P) control metrics	
2021	Establish a foundational internal controls data analytics environment	
	Define business requirements for Hire to Retire (H2R) control metrics.	
	Initiate process simplification review for P2P and H2R.	
2022	Develop control metrics for P2P and H2R and migrate to production.	
	Consider process simplifications for P2P and H2R.	
2023	Define business requirements and develop control metrics for Financial processes, including income and treasury (FIN) and Plan to Evaluate (P2E)	
	Initiate/consider process simplification review for FIN and P2E.	

Source: Office of the Controller

179. Comparison of the plan with the current status highlights a delay in activities planned for 2021. The establishment of a foundational internal controls data analytics environment involves setting up a data lake and procuring a BI solution that fits in with the WIPO system and data architecture. This project, managed by the Enterprise Solutions Division, is currently underway and estimated to be completed by mid-2022.

180. Concerning the other two tasks envisaged for 2021, namely, Define business requirements for Hire to Retire (H2R) control metrics and, Initiate process simplification review for P2P and H2R – they were strategically put on-hold while the business requirements fully were captured and the BI solution identified.

181. While acknowledging that the implementation of Data Analytics of Internal Controls involves collaborative efforts of multiple Divisions such as Information and Communication Technology Department, Enterprise Solutions Division (ESD) and Department for Economics and Data Analytics, and recognizing that some deliverables may create dependencies, it is however relevant that other non-dependent tasks be carried out to optimize efficiency and timelines among others.

182. Given the importance of the Data Analytics for Internal Controls and also increased interest from other internal and external stakeholders, it would be beneficial to formalize the

work as a separate project and allocate dedicated resources to secure the successful implementation of the Roadmap.

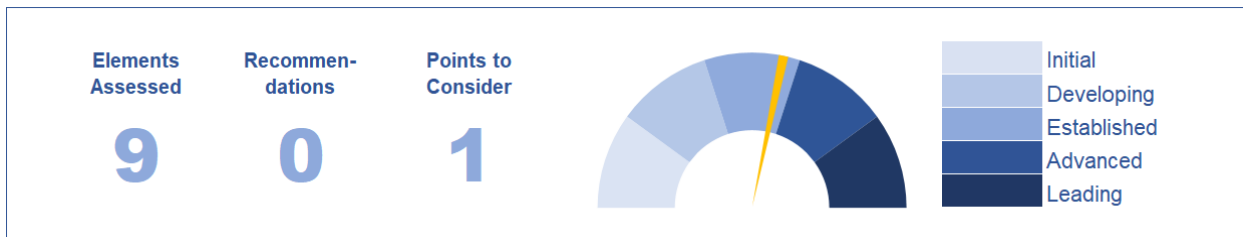
Point for Consideration

8. Formalizing of Data Analytics for Internal Controls as a project and allocate dedicated resources to secure the transparent and efficient implementation of the Roadmap.

(G) RISK CULTURE

183. The Figure below summarizes the results of the assessment of the Risk Culture at WIPO.

Figure T: Risk Culture – Assessment Summary



Source: Gap Analysis Details (Annex XIV)

184. The Risk Management Association⁶⁴ defines Risk Culture as the “set of encouraged and acceptable behaviors, discussions, decisions and attitudes toward taking and managing risk within an institution.” For the risk management framework to be effective, it needs to be accompanied by mechanisms to set the tone of the Organization, define a common understanding of risk with attributes for driving a risk conscious culture where both threats and opportunities are managed.

185. The Risk Culture is a part of the organizational Control Environment; it is therefore overarching, cross-cutting and pervasive and has a role to play in each aspect of Risk Management. A Risk Culture element was frequently mentioned by WIPO staff, which highlights the importance and relevance of the subject in particular its role in enhancing the risk maturity of an Organization.

186. On measures and practices put in place (or to be put in place) to enhance risk management, risk culture and understanding across the Organizations that participated in the WIPO Survey to UNRIAS, and in particular at senior level, the recurring themes and topics summarized below, highlight among others, the need to enhance management accountability, discussions on risks at high levels (tone at the top), raising risk awareness, and capacity building.

⁶⁴ Risk Management Association <https://www.rmahq.org>

Figure U: Summary of Mentions – Enhancing the Culture. IOD External Survey on ERM



Source: IOD External Survey on ERM

187. Furthermore, effective Tone at the Top is a prerequisite to a commitment to continuous improvement that is essential for risk management to function effectively, and for the risk culture to evolve.

188. IOD notes the positive comments from WIPO Sectors regarding the importance of the Risk Management and Internal Controls, including the tone set by the Director General on the need to take calculated risks to better serve users of WIPO services.

189. IOD highlights the importance of cascading the abovementioned message further down the hierarchy, supported by a series of initiatives highlighted in this report, to among others, address the current perception that WIPO is “Risk Averse”.



IOD Internal Survey

Twenty-five per cent of respondents⁶⁵ felt that a risk management culture is effectively embedded in their Sector/Division, and 45 per cent were somewhat of the same opinion, against 15 per cent who somewhat disagreed and eight per cent who disagreed. However, only five per cent of respondents⁶⁶ agreed that the current risk culture encourages taking risks, 18 per cent somewhat agreed, against 70 per cent who somewhat disagreed and disagreed (35 per cent somewhat disagree and 35 per cent somewhat disagreed).



IOD Internal Survey mentions:

- *“The culture for taking calculated risks is present in some parts of the business, but not prevalent.”*
- *“Actually, there is a disconnection between the risk management and the Organization's hyper-reluctance to the taking of risks. This is a question of overall policy; the risk management process in the Organization is not at stake”.*
- *“Whilst the new administration encourages us to embark on innovative projects and initiatives, the nature of the Organization and our rules and procedures require prudent management of our resources and cognizance of our reputation”.*

⁶⁵ Annex II, Question 31

⁶⁶ Annex II, Question 30

- *“This is a risk averse organization as a rule for several reasons including being a part of the UN system. Yet we need risks to keep up with the industry and the corporate sector”.*
- *Having a more risk-friendly culture would be beneficial in my view”.*
- *“There is a culture of fear of failure, making it difficult to take steps forward”.*
- *“WIPO has a zero risk appetite - Management culture does not encourage it”.*
- *“Our division has very strong controls over key risks in place. Sometimes too many - in that, trying new or innovative things can be problematic and challenge the culture”.*
- *“We are generally discouraged from registering risks relating to insufficient human resources.*
- *“Risks can be rejected or rewritten”*

190. To properly push the tone from the top further down the line, there must be an appropriate Buy-in from Management, who supports the value of collective risk conscious culture, and is committed and understands the importance and benefits of risk management.

191. The majority of participants to the IOD internal survey were P5 and/or D grade, which correlates with IOD’s expectations of staff members who should take the lead on risk management at operational level. However, IOD also notes the minimal participation of leadership, who are accountable for setting the tone.



IOD Internal Survey

Further, 50 per cent of respondents⁶⁷ indicated that they took part in the organizational risk management process because they are obliged to, against 43 per cent who participate in the process because they consider it useful. Other comments include “because it is both useful and required”.



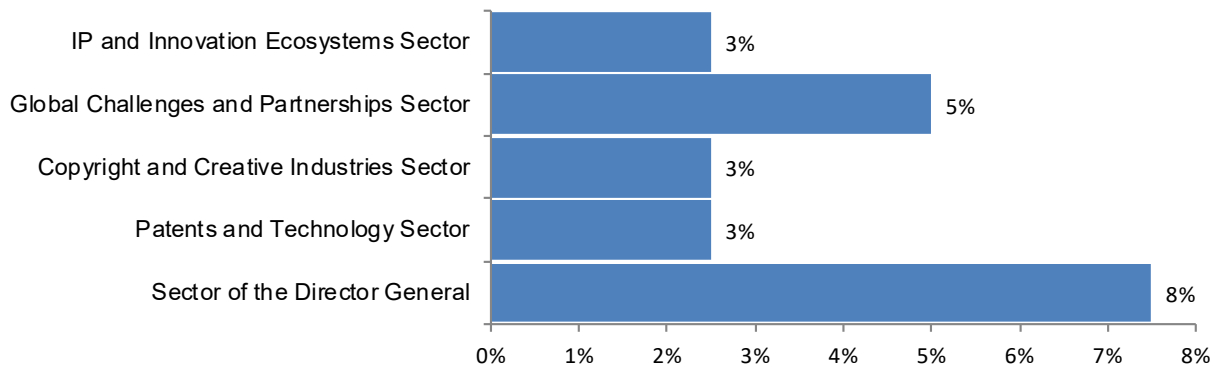
IOD Internal Survey mentions:

- *“Tendency to consider the risk management as just a formal bureaucratic tool”.*
- *“We do not bother dealing with the risk management system because it is too much bureaucracy”.*

192. A relevant number of participants to this survey are members of AFMS, which can be explained by their proximity to risk management. However, IOD would reiterate the need for risk management to be the concern of all Sectors of the Organization. The significantly low participation from other Sectors illustrates the low interest, commitment and potentially low understanding of risk management among key stakeholders responsible for among others setting the tone and driving the risk conscious culture. Specifically, IOD highlighted the following Sectors with less than 10 per cent participation that need to better engage and contribute to enhancing the risk management culture.

⁶⁷ Annex II, Question 26

Figure V: Significantly Low Participations



Source: IOD Internal survey data

193. Going forward, Sector leadership, Management, and staff members of the Organization should engage with the Office of the Controller to address their needs and make suggestions on challenges and opportunities that would enable an enhanced risk conscious culture to grow across the Organization. Furthermore, there is also a need to align regulations, rules, procedures and practices with an environment that encourages taking risks. Failing to consider this alignment will result in bottlenecks, frustrations, and increase of the risk of failure and overall discouragement.



IOD External ERM Survey

Overall, risk culture and practices vary across organizations, with a number of similarities noted. Nevertheless, a majority agree that **continuous engagement top down and across the organization** led by senior management supported by clear accountability, effective communication and training, are relevant elements to enhance the risk management culture.

(i) Transparency and Learning from Lessons

194. Risk transparency creates a more robust risk culture within an organization, and enables relevant information to flow faster, to among others, reduce organizational “blind spots”. Therefore, it is very important to create an atmosphere of openness and effective information exchange.



IOD Internal Survey

IOD notes that while 58 per cent and 15 per cent of respondents⁶⁸ respectively agreed and somewhat agreed that they do not feel pressured not to record certain risks such as risks with potentially significant monetary impacts, there is however, 13 per cent and 15 per cent respectively who somewhat agree and agree to have felt such pressures.

195. Some collected feedback suggests that situations of reluctance to recognize certain risks do occur. The following was mentioned as potential causes:

- (a) There may be a pressure not to report political risks. The risk register is widely available to staff, and politically sensitive risks may create more of a problem than they solve;

⁶⁸ Annex II, Question 27

(b) Sometimes risks like “not enough human / financial resources” are not accepted just because they had to be taken into account during the work plan preparation; therefore, such risks add little quality to the risk register, and just overload it; and

(c) It could also be risk immaturity on the part of the person pressurizing against reporting the risk. Sometimes people feel if they acknowledge that something may fail, that may happen, or that it may reflect badly on them.

196. While IOD recognizes the importance of “Need to know” principle, it cannot be a reason for not disclosing the risk information. Risk information in WIPO risk registers must be as complete as possible to enable an effective management of risks and opportunities. Shifting from the perception of “blame and fear to fail culture” to a more risk aware culture supported by the right mindset, awareness raising, capacity building initiatives, and encouraging learning from mistakes, would serve the risk culture of the Organization. Where appropriate, calculated risk taking within the Risk Appetite should be encouraged to promote innovative solutions and gain the competitive edge.

Point for Consideration

9. Develop initiatives to enhance the risk management culture, such as:

(a) Taking measures to further enhance the tone at the top on risk management, raise risk management commitment, and capacity building; and

(b) Putting in place processes and practices to encourage and support calculated risk taking.

ACKNOWLEDGMENT

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

Prepared by: Dainis Reinieks, Senior Internal Auditor.

Reviewed by: Alain Garba, Head, Internal Audit Section.

Approved by: Rajesh Singh, Director IOD.

TABLE OF RECOMMENDATIONS

No.	Recommendations	Priority	Person(s) Responsible	Other Stakeholder	Management Comments and Action Plan	Deadline
1.	The Office of the Controller in collaboration with the Risk Management Group and Sector Risk Coordinators should raise staff awareness about the WIPO Risk Appetite Statement.	Medium	Assistant Controller, Risk Assurance and Internal Controls Specialist	Director, Program Planning and Finance (Controller)	OC has shared the draft revised WIPO Risk Appetite Statement with RMG and SRCs, and invited comment. Through Sector Leads, OC has requested broad-based input on the RAS and received feedback from across the Organization. <i>Implementation action: Out reach process leading up to the presentation of the Risk Appetite Statement to the PBC</i>	31.07.2022 (after the Assemblies)
2.	Sector Leads and Relevant Managers should ensure that the PMSDS of designated staff members include objectives related to their role as Sector Risk Coordinators.	Medium	Assistant Controller, Risk Assurance and Internal Controls Specialist	Director, Program Planning and Finance (Controller)	In an email to Sector Leads, the Controller has reminded that “the Joint Inspection Unit’s advice that the risk management responsibilities of Sector Leads, Directors and Sector Risk Coordinators should be reflected in their PMSDS to ensure commitment and accountability.” Further follow up is proposed in collaboration with HRMD, after HRMD’s review of objectives in PMSDS. <i>Implementation action: Inclusion of risk management as a standard organizational competence.</i>	31.03.2023 (for 2023 PMSDS)

No.	Recommendations	Priority	Person(s) Responsible	Other Stake holder	Management Comments and Action Plan	Deadline
3.	The Office of the Controller should review and update the Risk Manual, including guidance for risk responses, risk escalation (including project risks), and the relationship between risks and controls.	Medium	Assistant Controller, Risk Assurance and Internal Controls Specialist	Director, Program Planning and Finance (Controller)	OC recognizes that the risk manual would benefit from an update and proposes to do so during the 2022/23 biennium. <i>Implementation action: Issuing of a revised Risk Manual.</i>	31.12.2023 (Updates to be finalized in 2023)
4.	The Office of the Controller in coordination with the Internal Training Program of the WIPO Academy, should further raise risk management and internal controls awareness by introducing updated training offerings to address the needs of staff members at different levels and relationships and responsibilities towards Risk Management and Internal Controls.	Medium	Assistant Controller, Risk Assurance and Internal Controls Specialist	Director, Program Planning and Finance (Controller)	OC recognizes that risk management and internal controls awareness would benefit from being raised further. OC has in their 2022 work-plan to undertake a scoping exercise in order to present updated training offerings in 2023. These offerings will align with efficient ways of learning using new technology and media tools. <i>Implementation action: Availability of a variety of training offerings that address staff needs at different levels.</i>	31.12.2023 (Scoping in 2022 and offerings in 2023)

ANNEXES

<u>Annex I.</u>	Risk Rating and Priority of Recommendations
<u>Annex II.</u>	IOD Survey on Enterprise Risk Management at WIPO
<u>Annex III.</u>	IOD External Survey on Enterprise Risk Management (UNRIAS)
<u>Annex IV.</u>	Analysis of WIPO Risk Appetite Statement Based on Guidance from Recognized Organizations
<u>Annex V.</u>	Risks and Risk Response Status Update in ERM
<u>Annex VI.</u>	Annex withheld
<u>Annex VII.</u>	WIPO Corporate and Project Risk Scale
<u>Annex VIII.</u>	WIPO Controls by Process
<u>Annex IX.</u>	Mitigation Actions Details
<u>Annex X.</u>	Annex withheld
<u>Annex XI.</u>	Annex withheld
<u>Annex XII.</u>	Annex withheld
<u>Annex XIII.</u>	Analysis of Risks, Controls and Mitigating Actions
<u>Annex XIV.</u>	Gap Analysis Details

ANNEX I: RISK RATING AND PRIORITY OF RECOMMENDATIONS

The risk ratings in the tables below are driven by the combination of likelihood of occurrence of events and the financial impact or harm to the Organization’s reputation, which may result if the risks materialize. The ratings for recommendations are based on the control environment assessed during the engagement.

Table I.1: Effectiveness of Risks/ Controls and Residual Risk Rating

		Compound Risk Rating (Likelihood x Impact)		
		Low	Medium	High
Control Effectiveness	Low	Low	Medium	High
	Medium	Low	Medium	High
	High	Low	Low	Medium

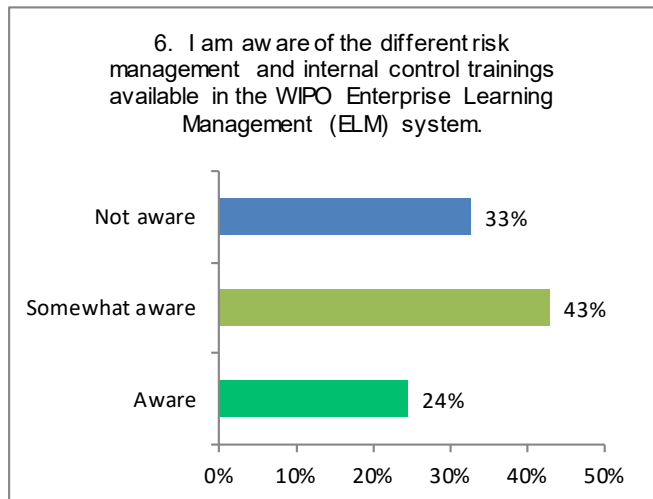
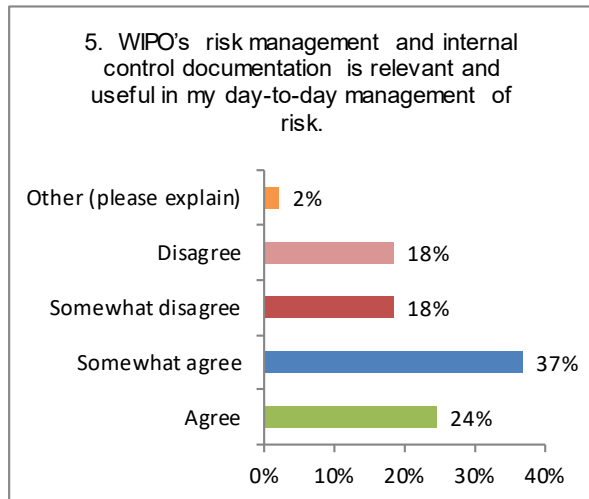
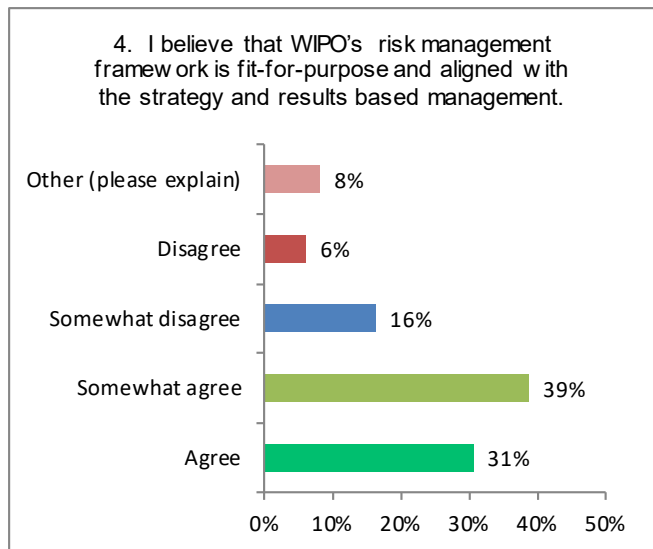
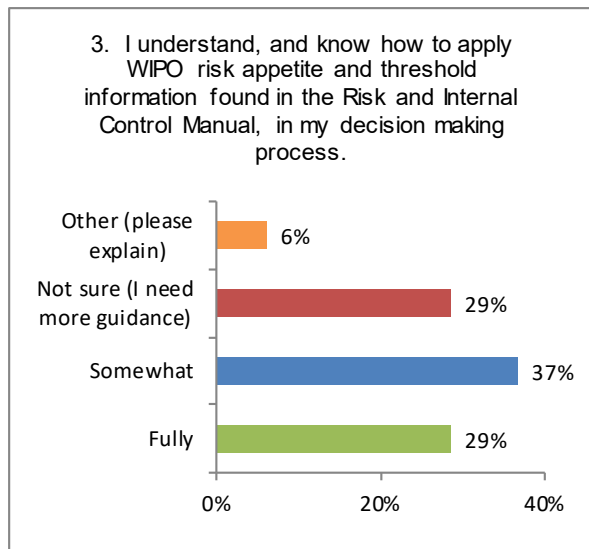
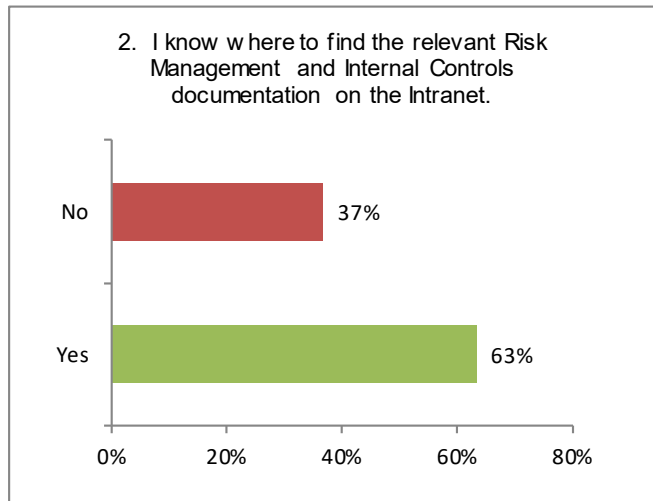
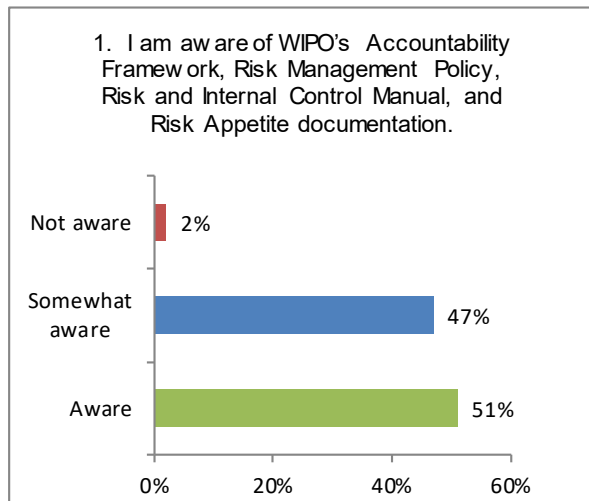
Table I.2: Priority of Recommendations

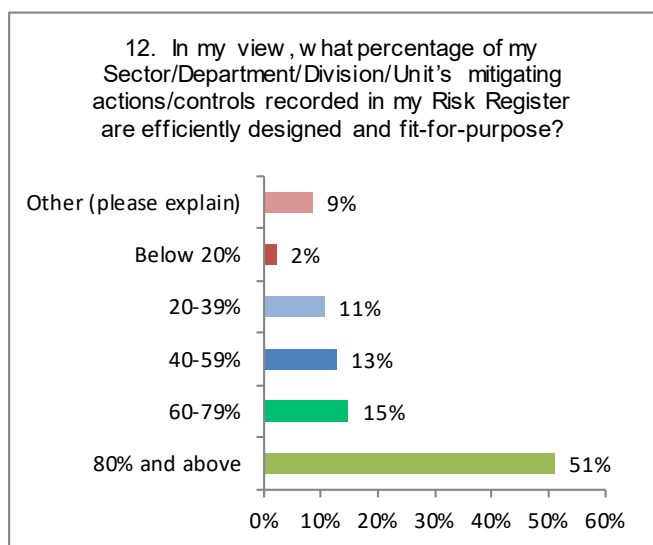
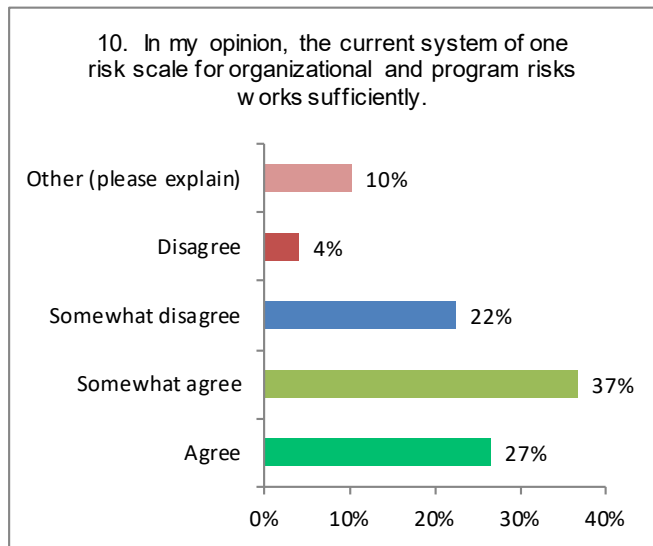
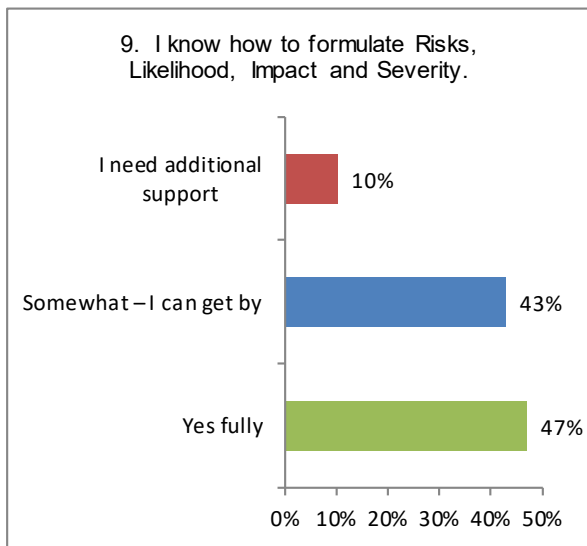
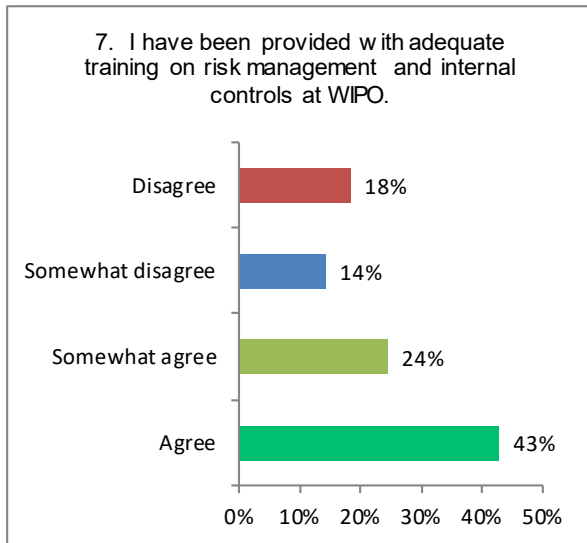
Priority of Recommendations	Residual Risk Rating
Requires Urgent Management Attention	High
Requires Management Attention	Medium
Routine in Nature	Low

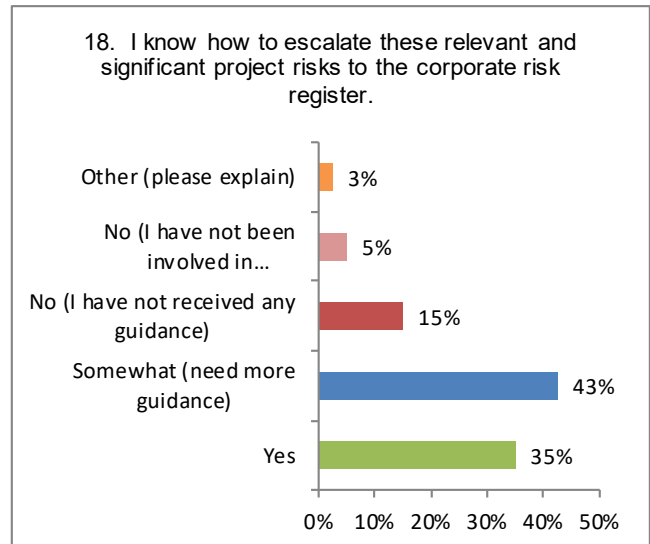
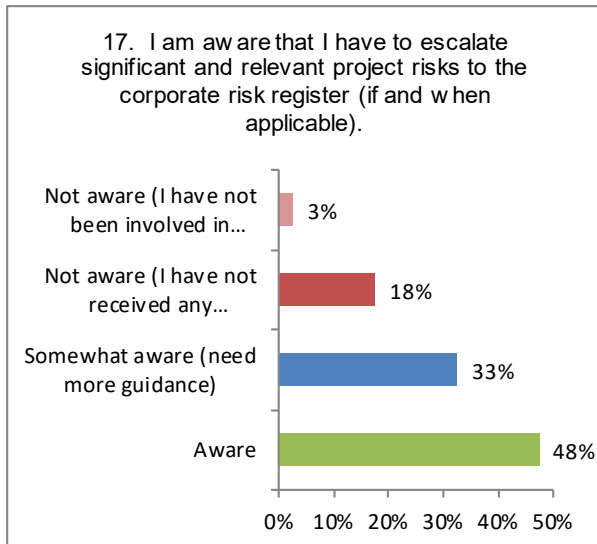
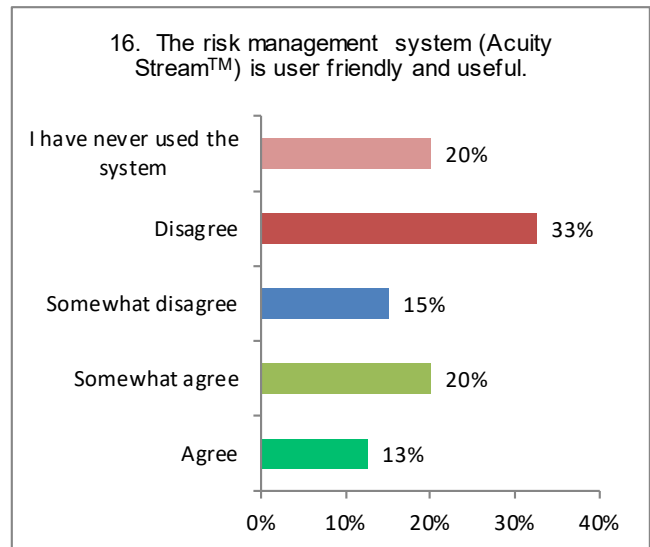
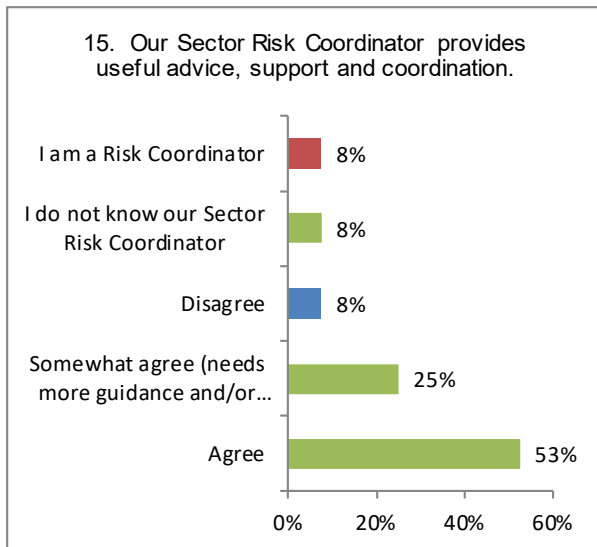
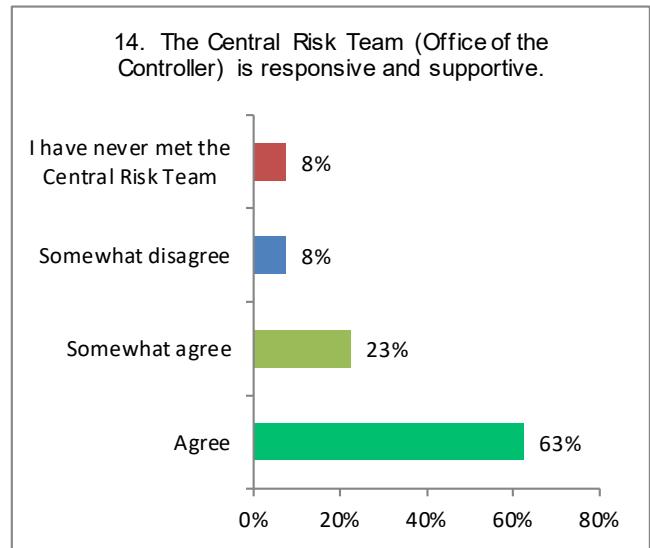
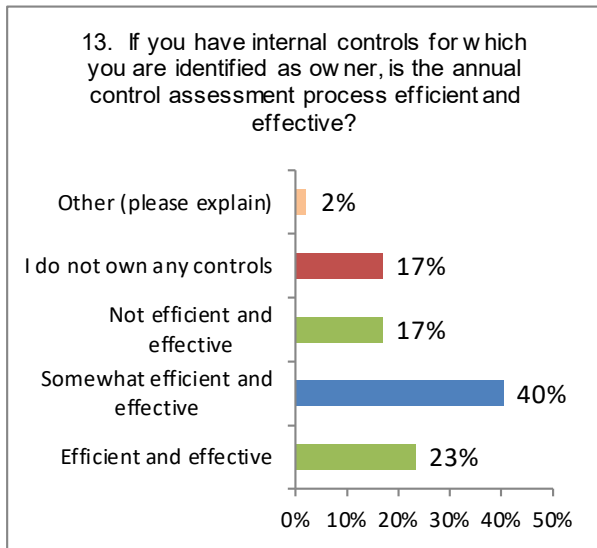
Points for Consideration (PFC) - When relevant, IOD may issue PFCs which are suggestions that are not formally tracked by IOD but merit management attention. PFCs relate to issues that taken either individually or in combination do not significantly affect the result of the engagement, but can, in addition to formal recommendations, present opportunities to add further value.

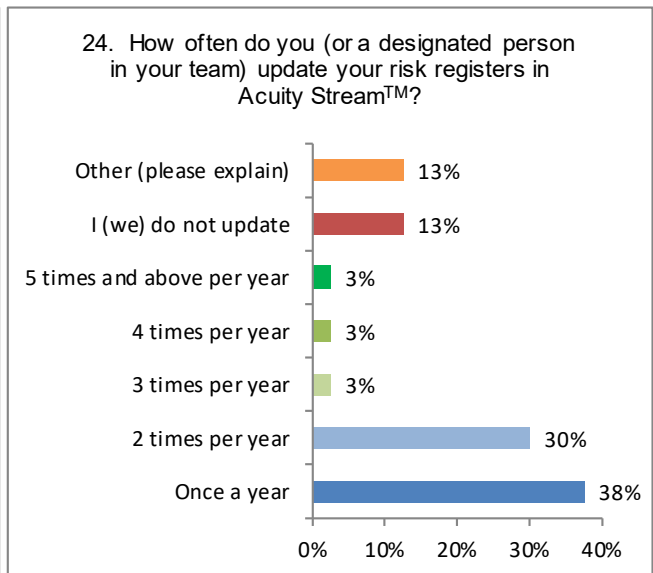
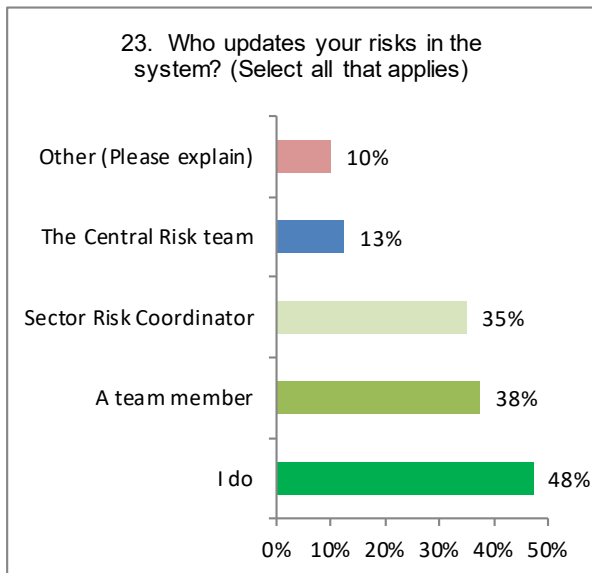
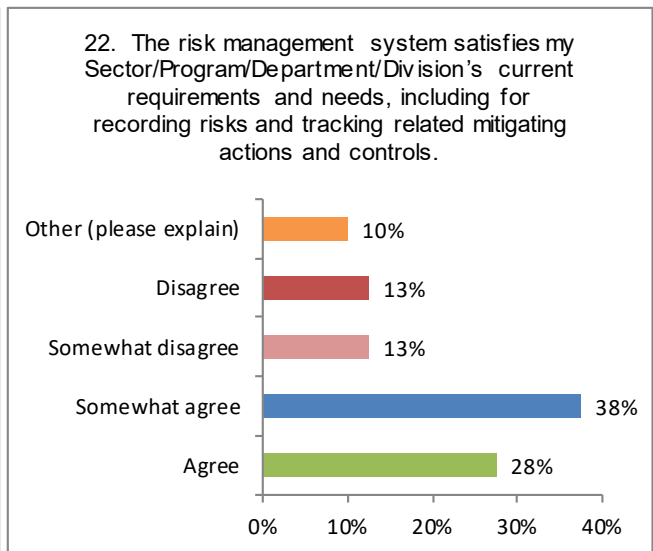
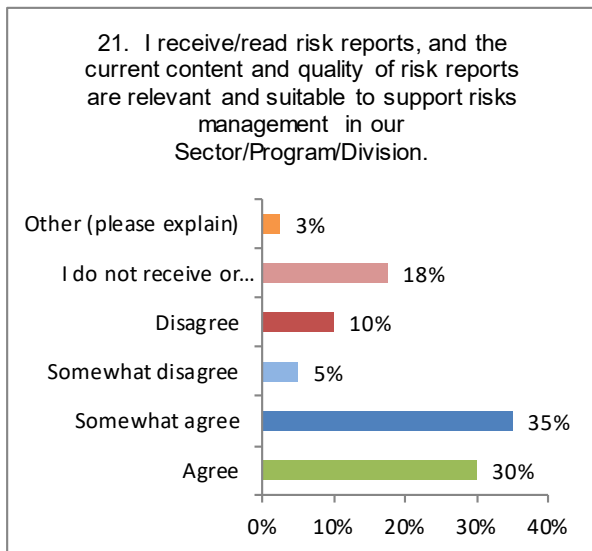
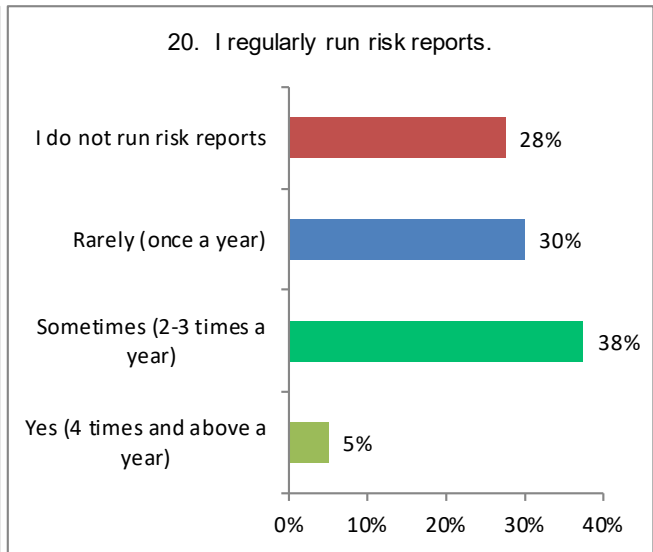
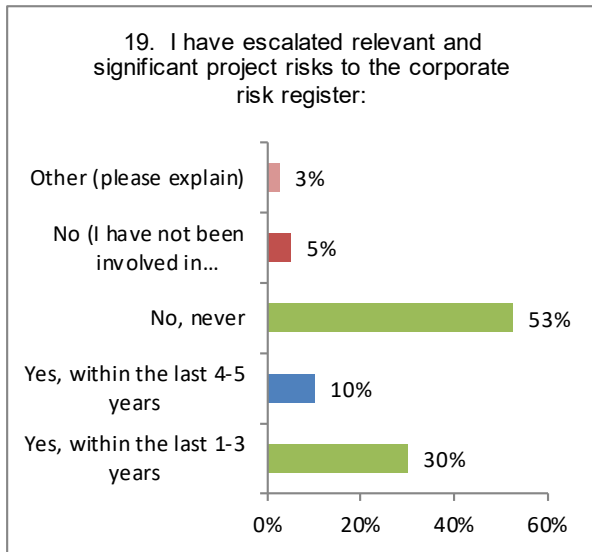
[Annex II follows]

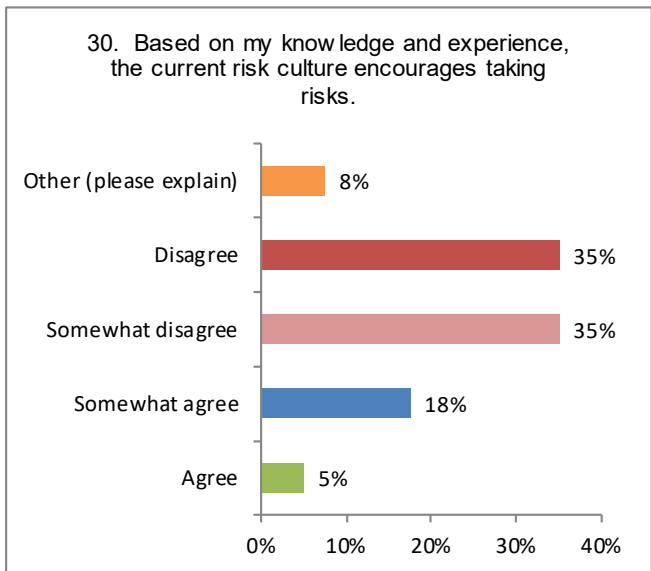
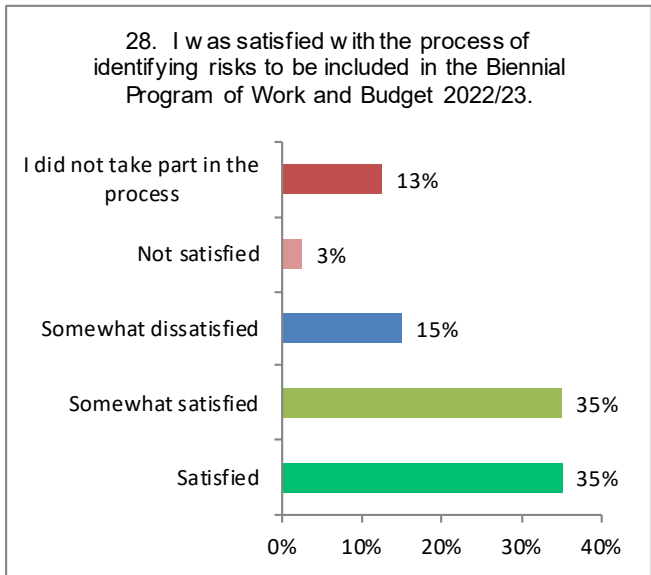
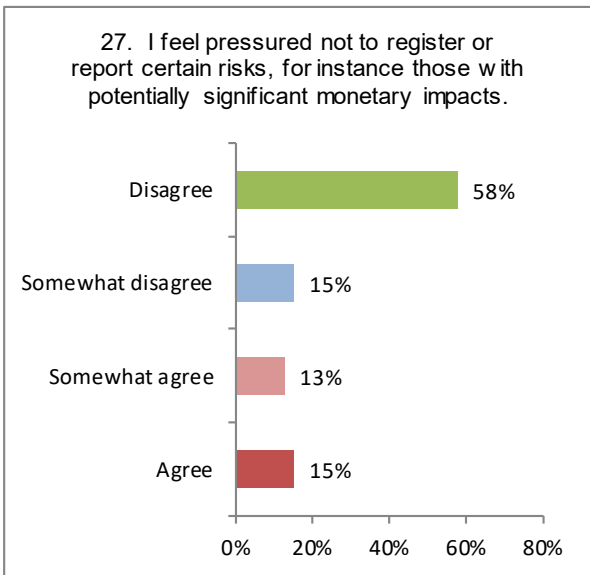
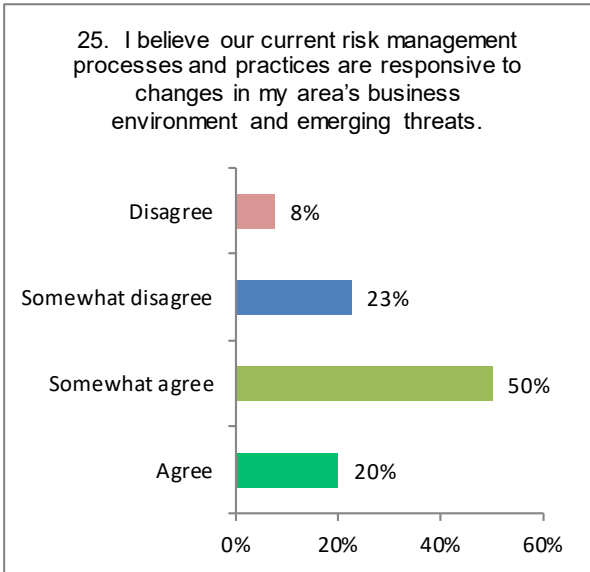
ANNEX II: IOD SURVEY ON ENTERPRISE RISK MANAGEMENT AT WIPO

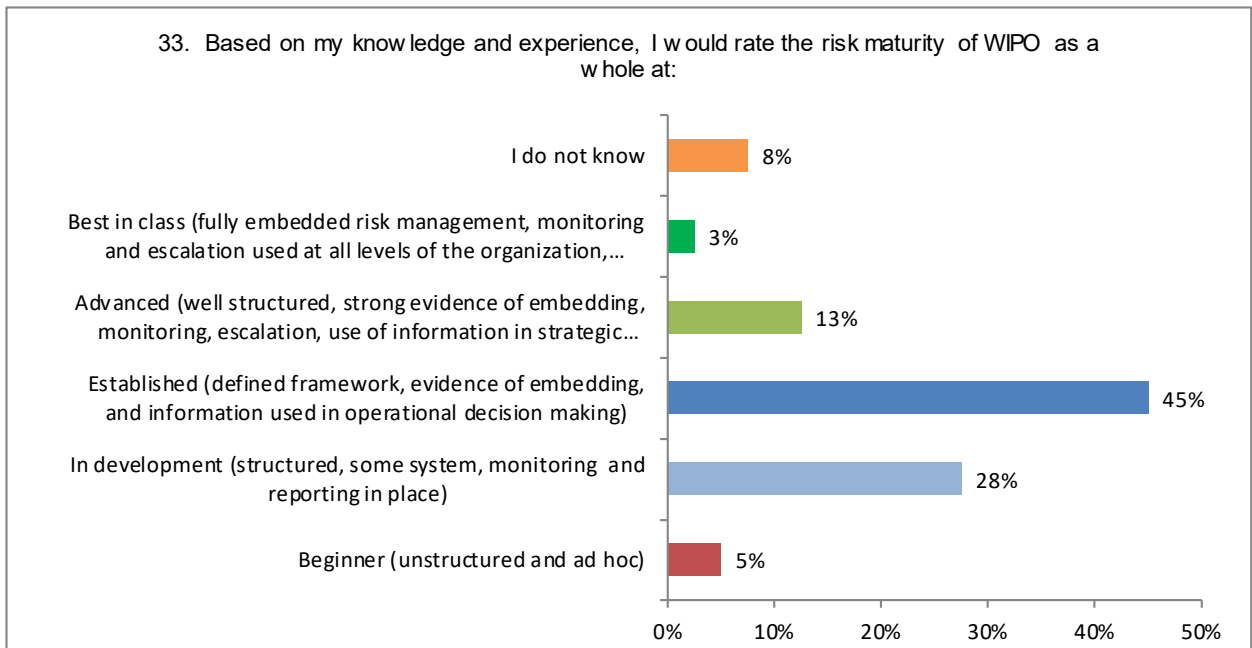
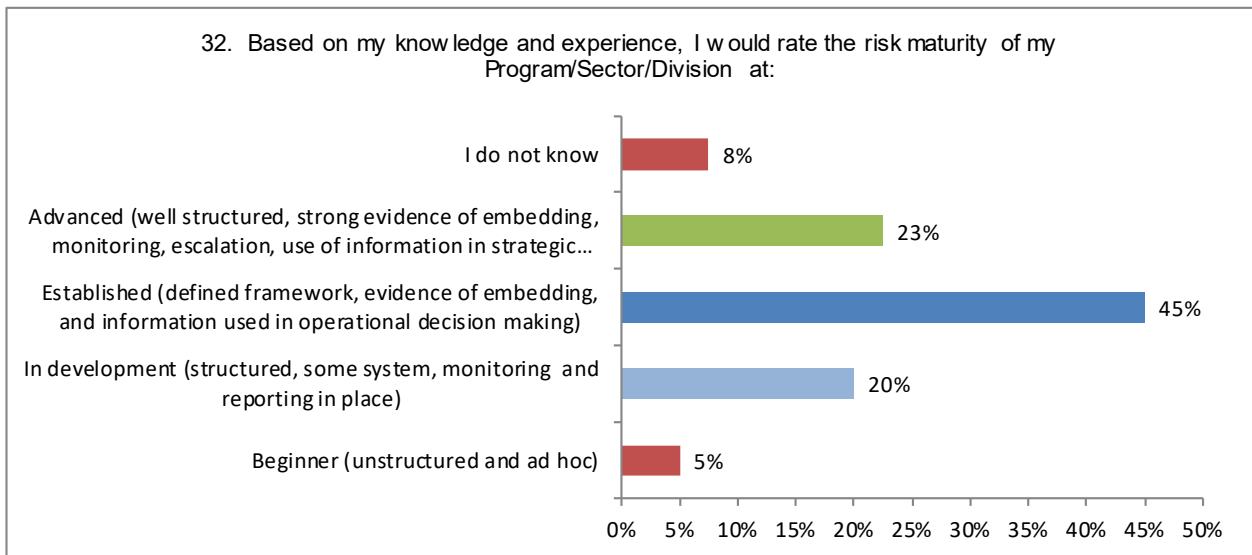
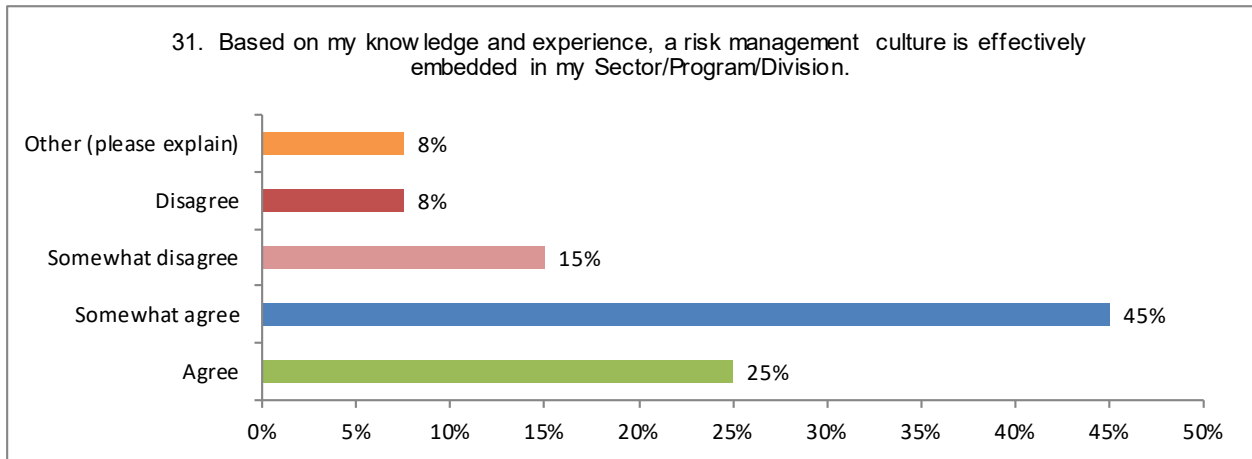








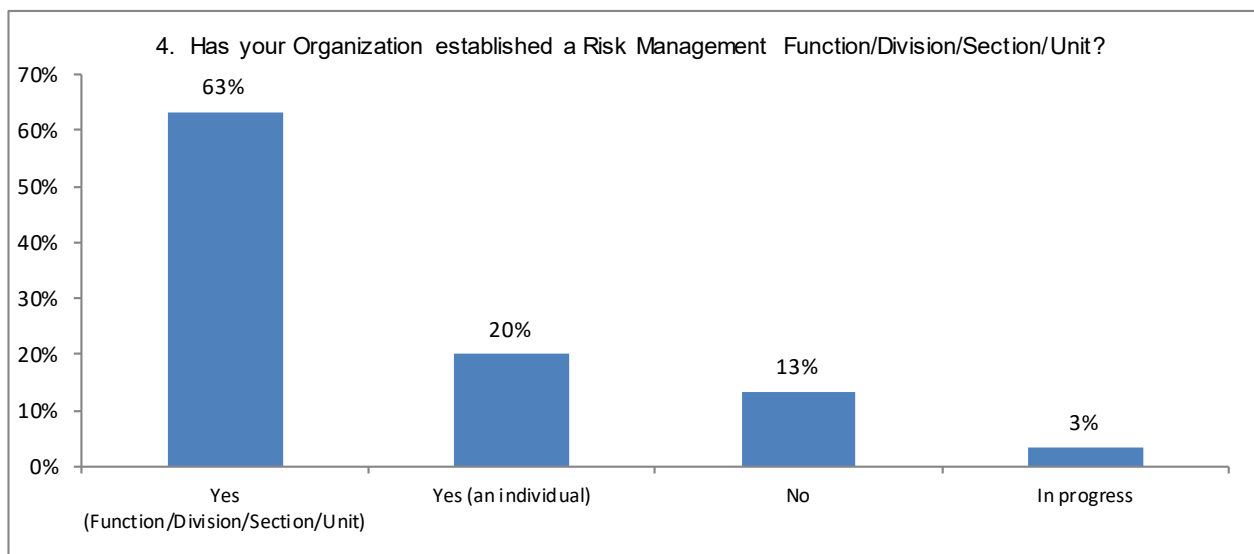
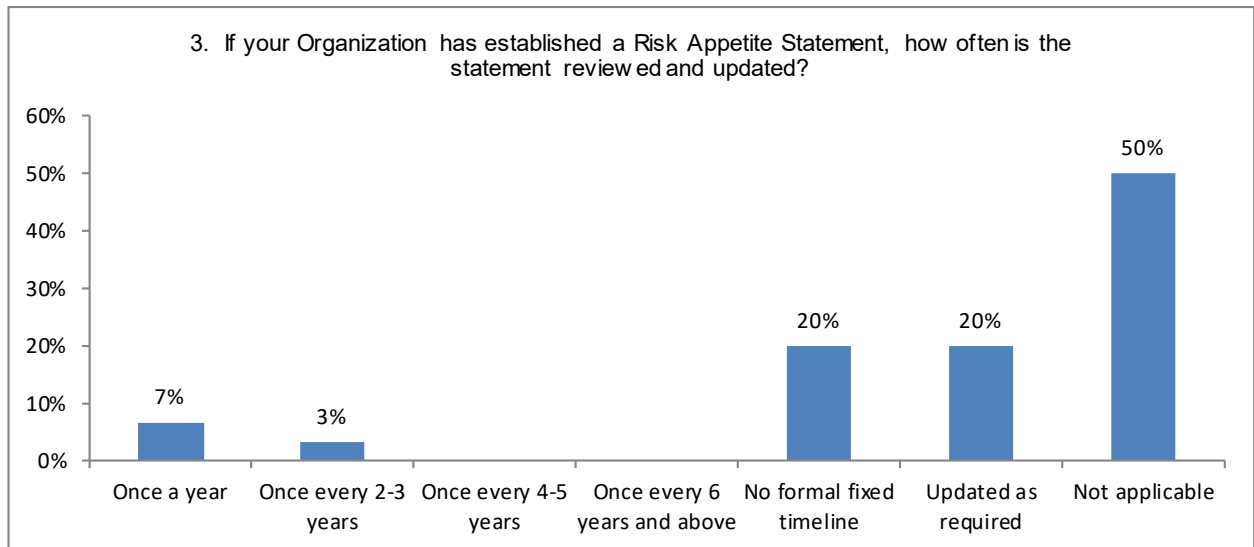
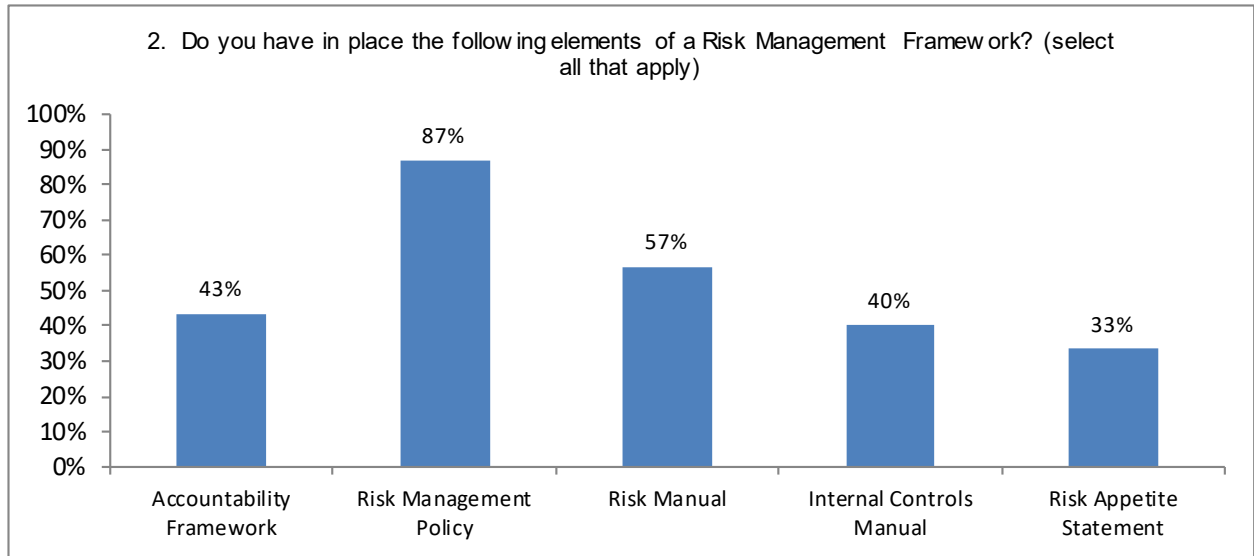




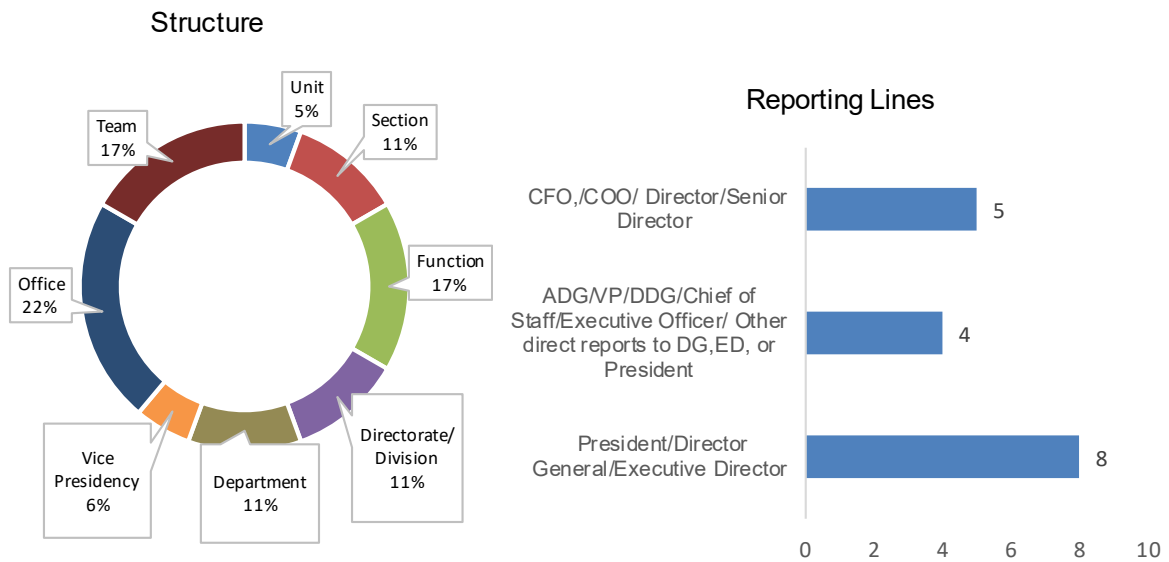
[Annex III follows]

ANNEX III: IOD EXTERNAL SURVEY ON ENTERPRISE RISK MANAGEMENT (UNRIAS)

Question 1. Organization – 30 participating Organizations responded to the Survey

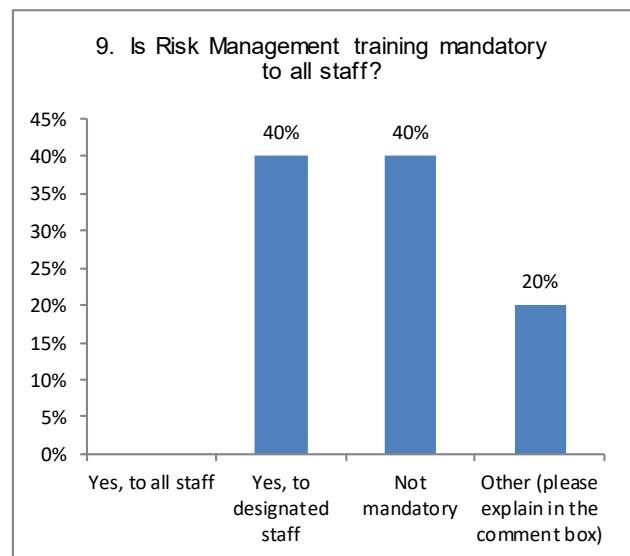
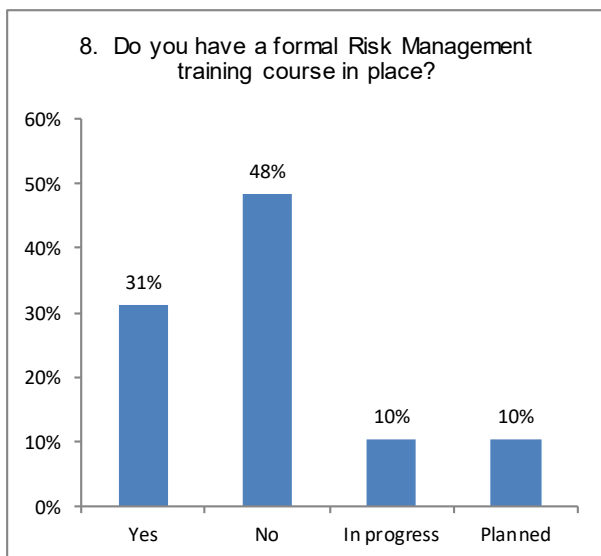
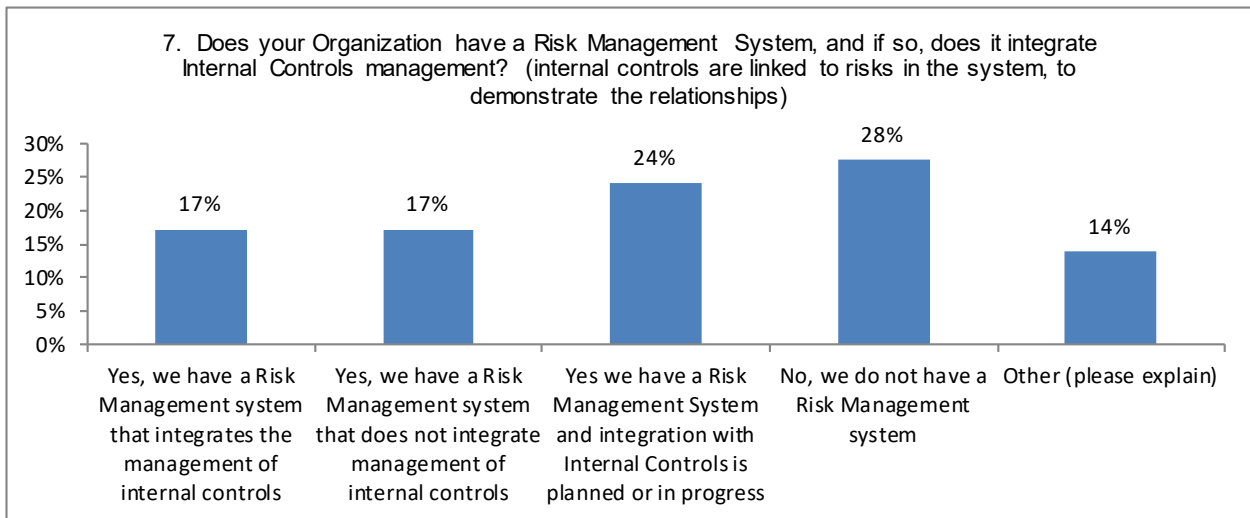
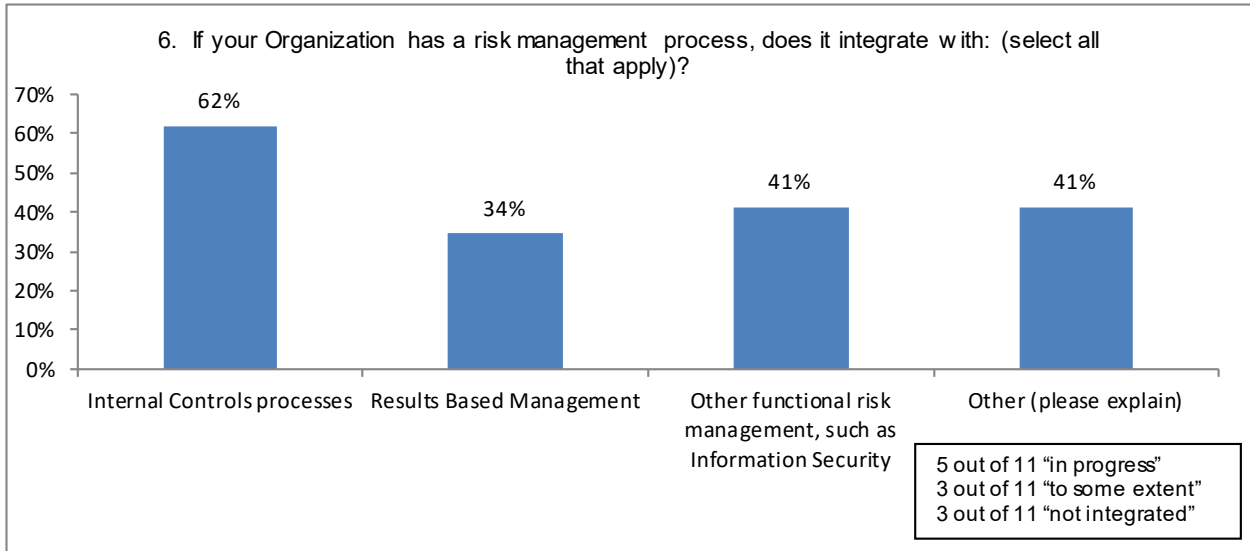


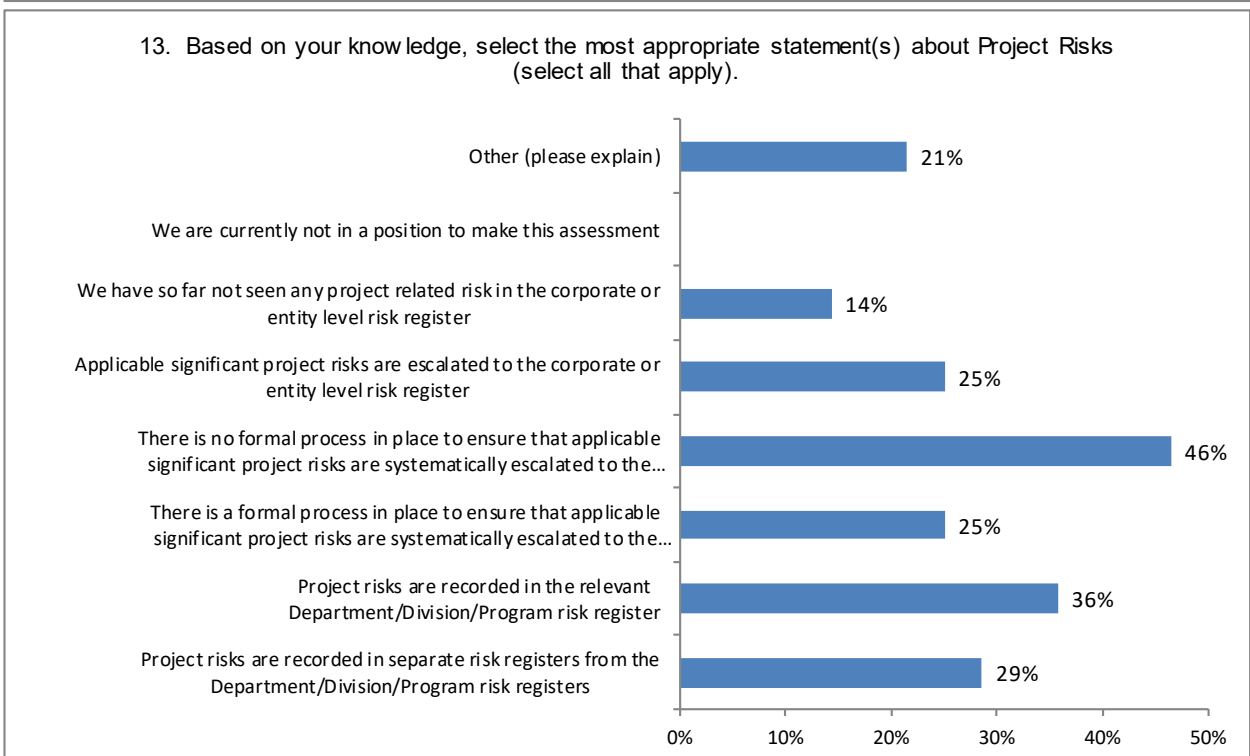
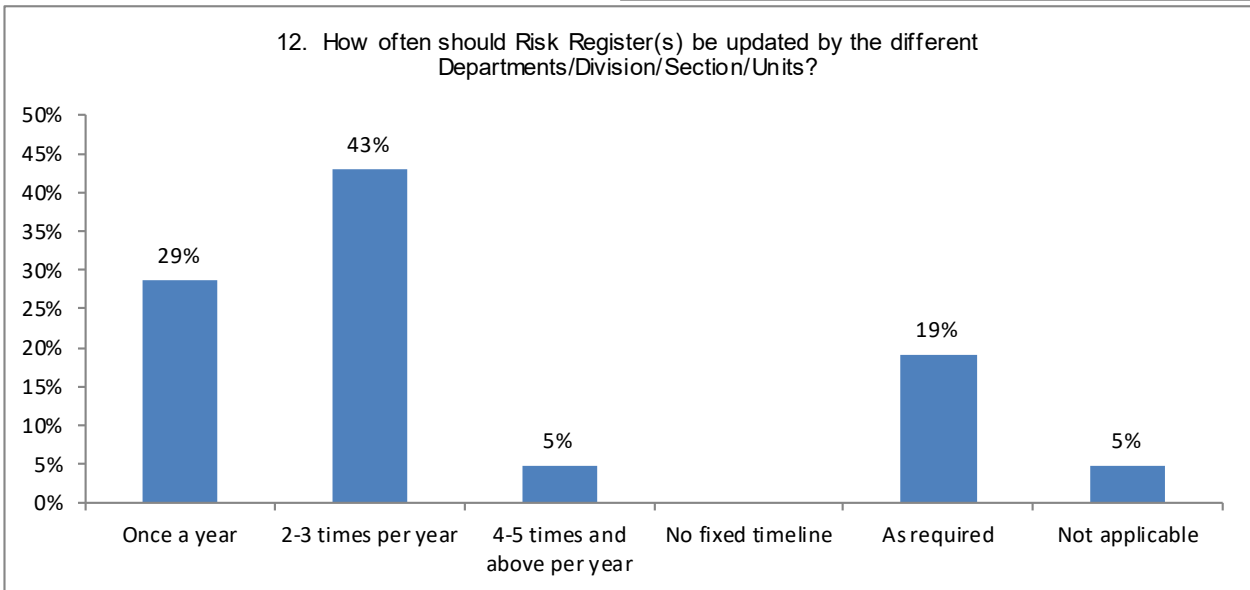
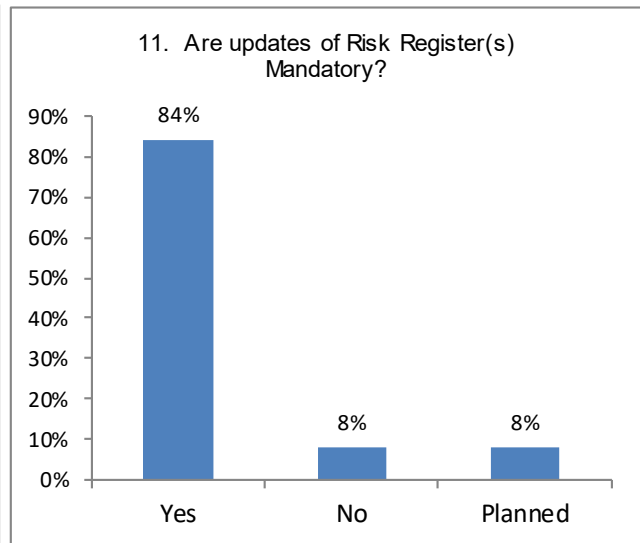
Question 5: If your Organization has established a Risk Management Function/Division/Section/Unit, what is the structure (risk specialists, risk officers, head, etc.) and reporting line, and how many staff members make up the Team?

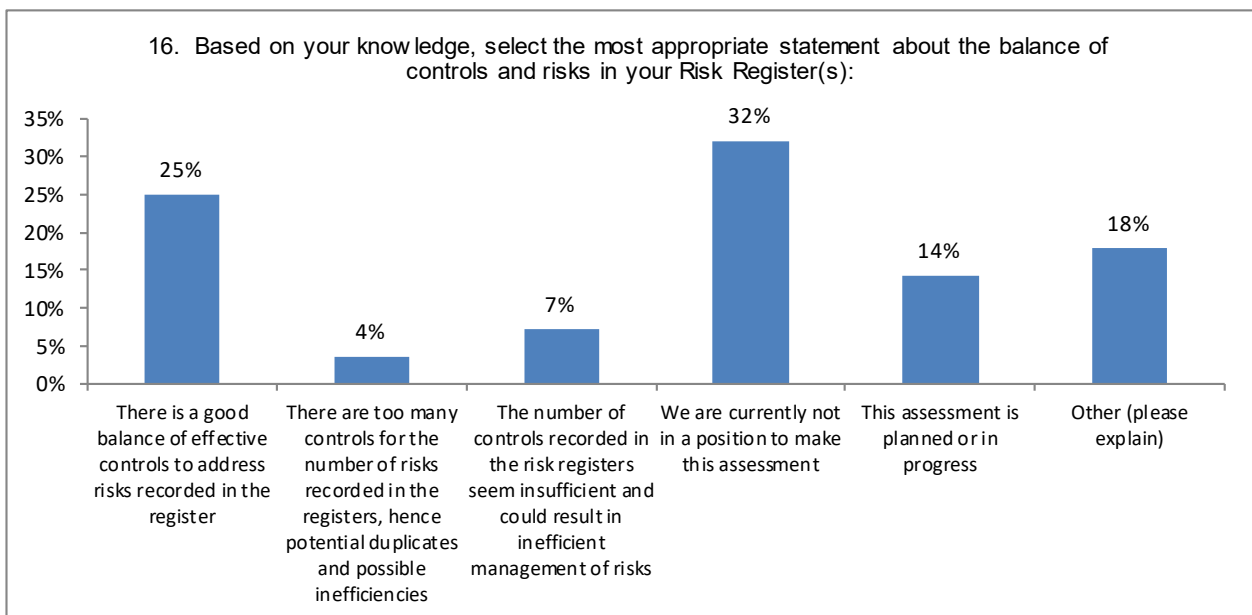
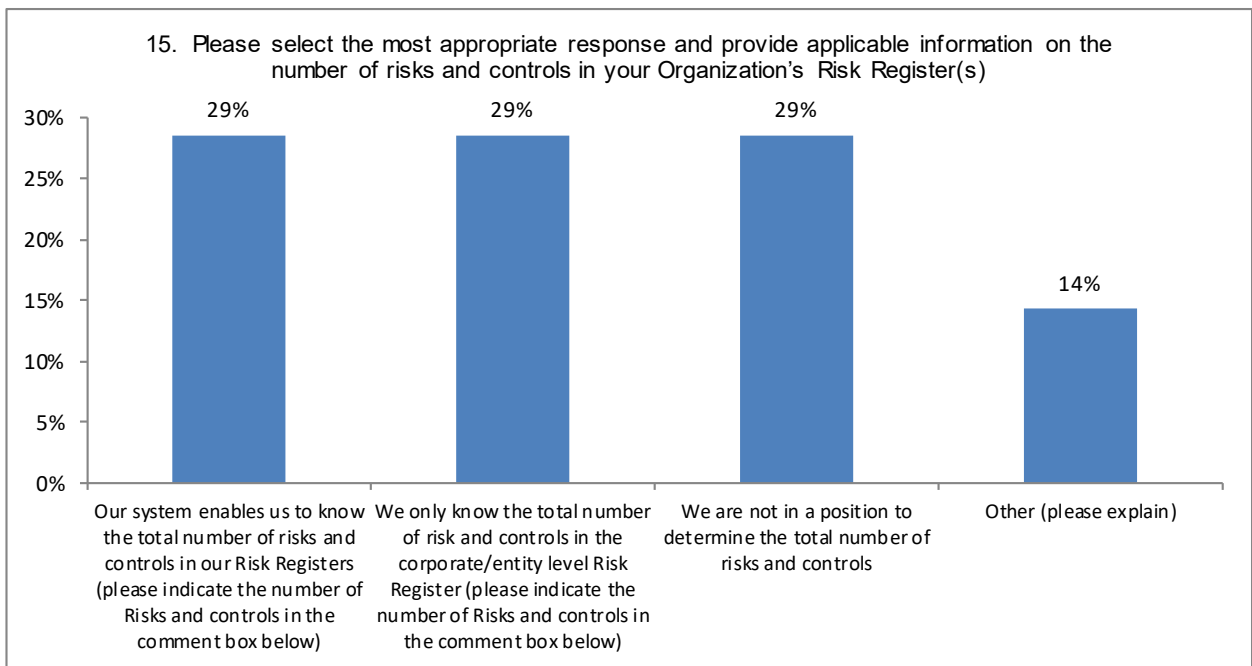
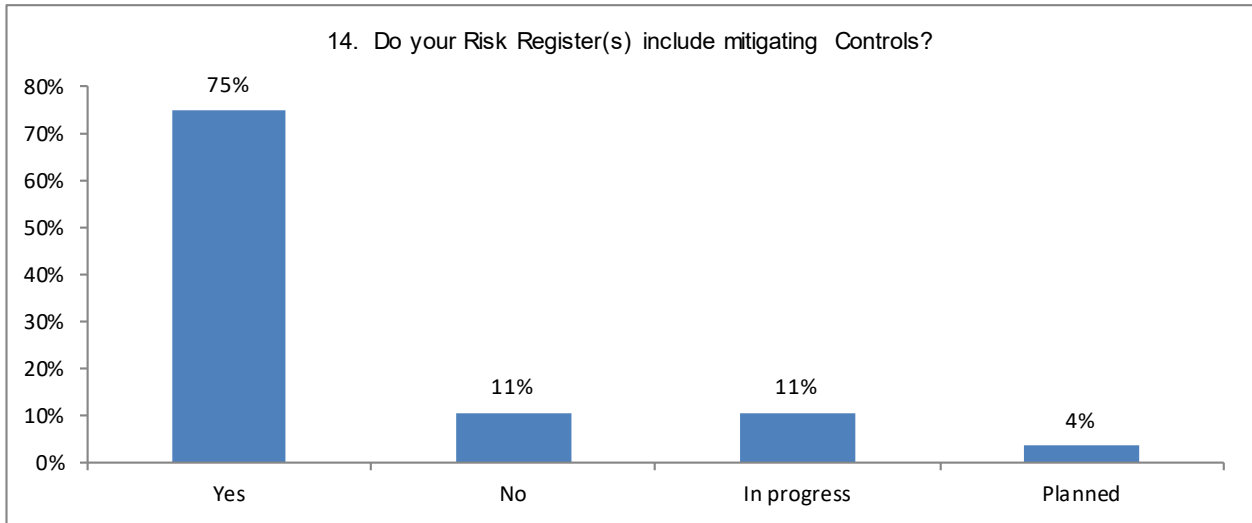


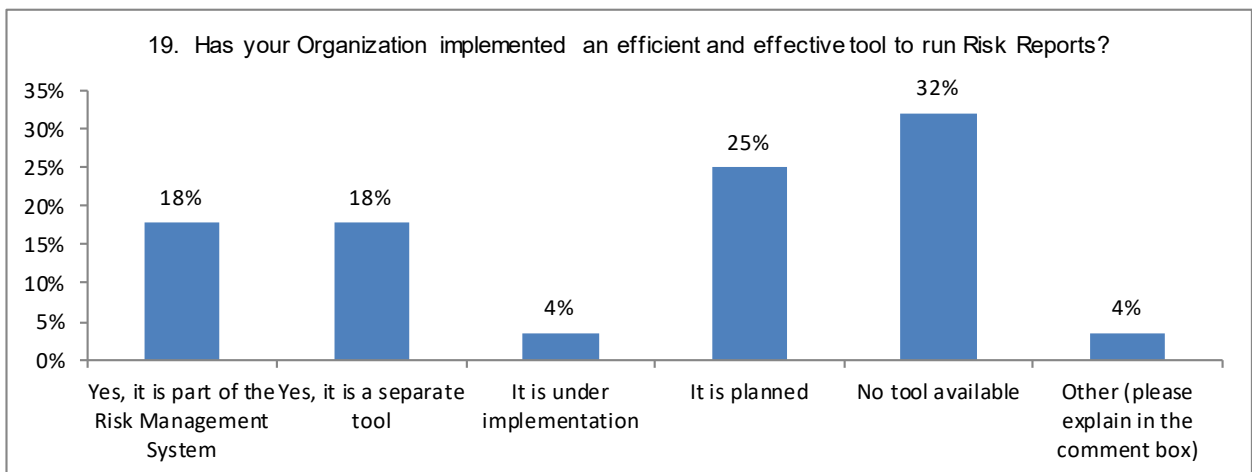
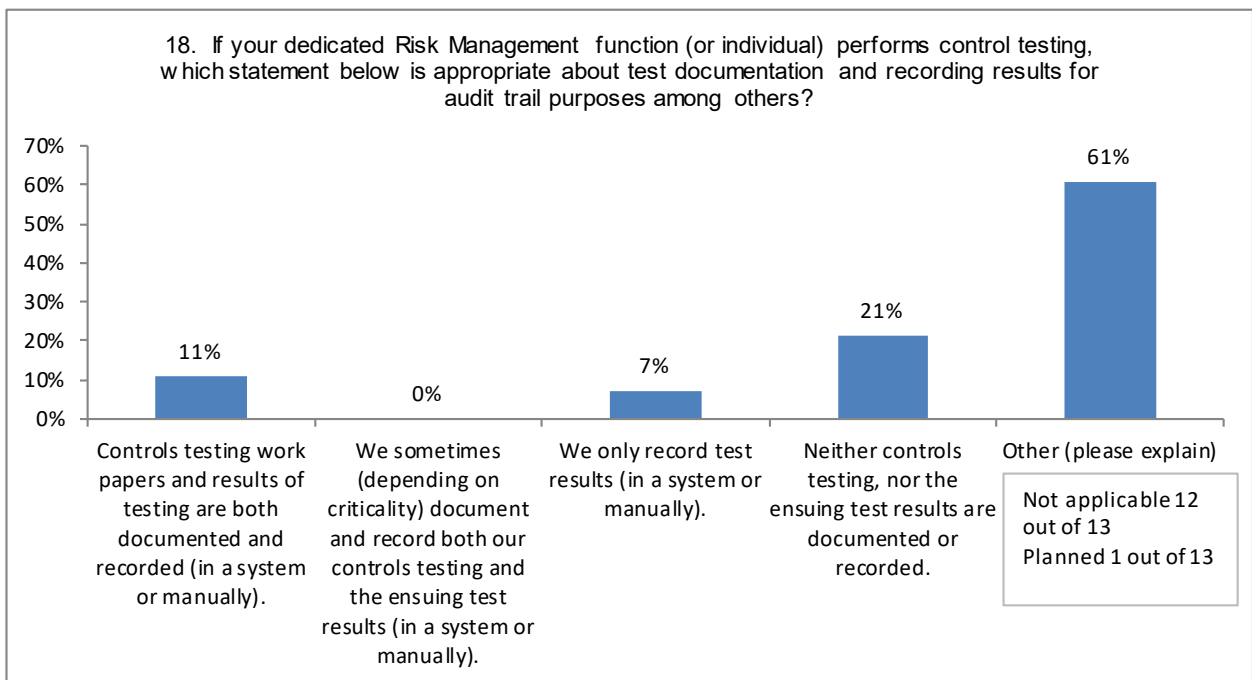
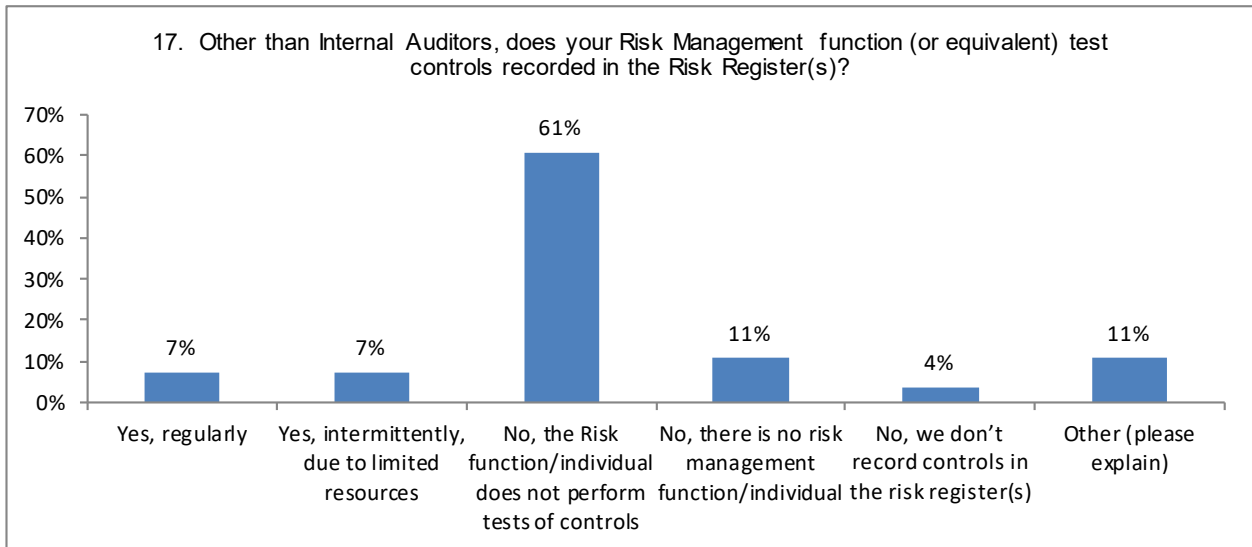
Question 5 *cont...*: If your Organization has established a Risk Management Function/Division/Section/Unit, what is the structure (risk specialists, risk officers, head, etc.) and reporting line, and how many staff members make up the Team?

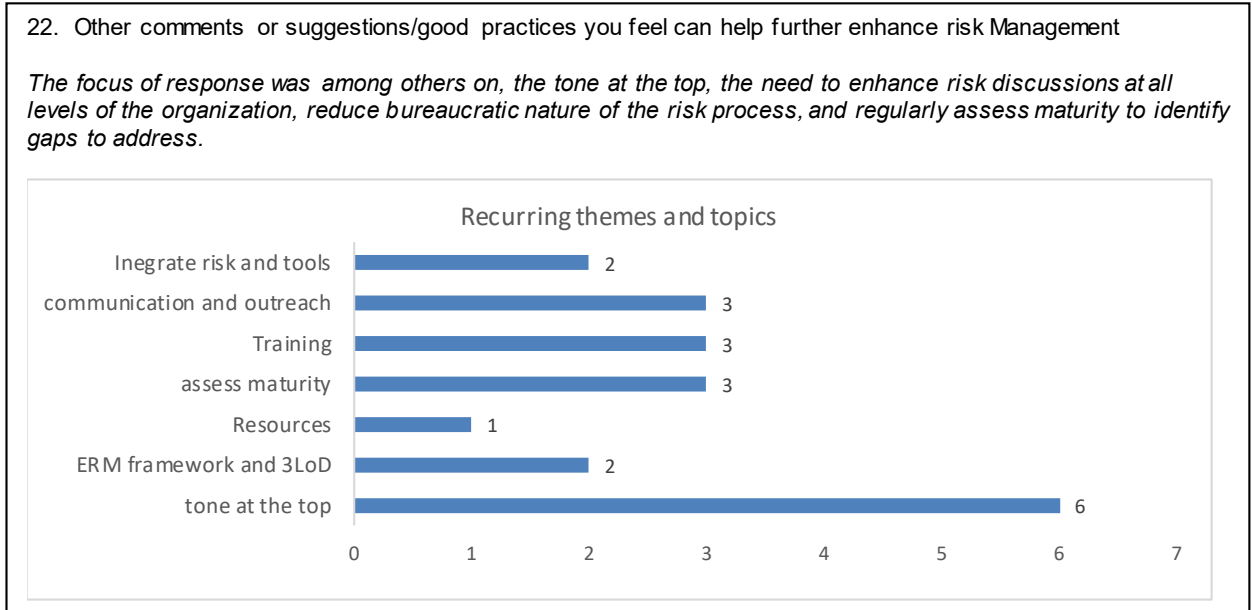
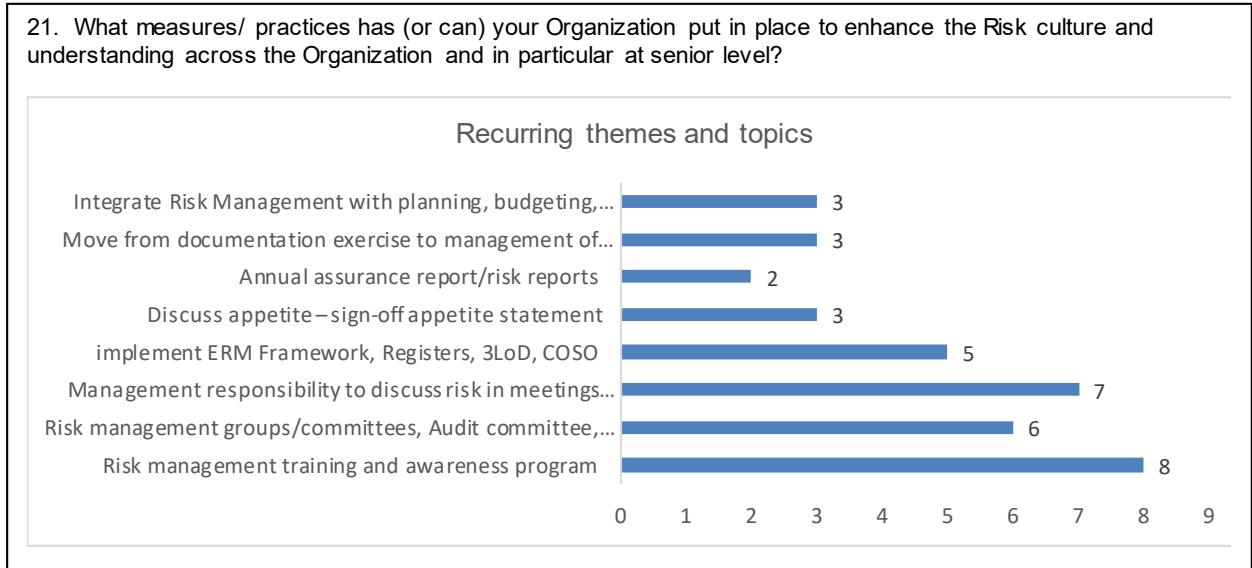
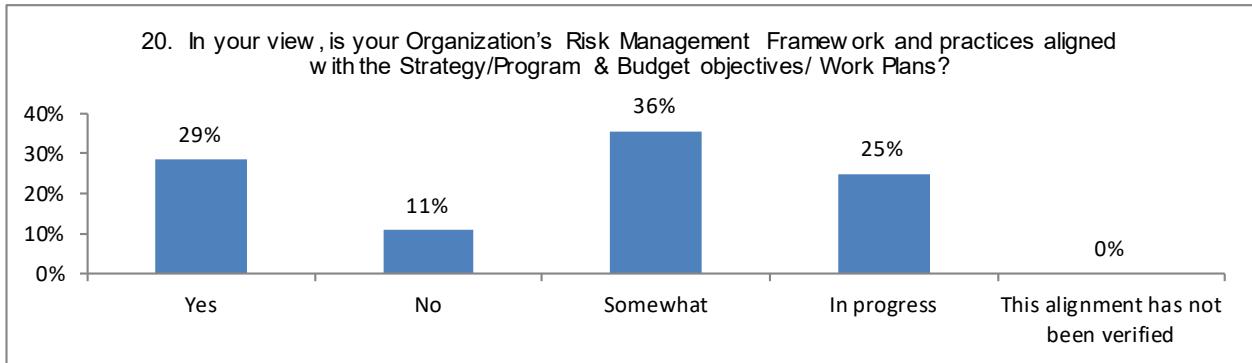












[Annex IV follows]

ANNEX IV: ANALYSIS OF WIPO RISK APPETITE STATEMENT BASED ON GUIDANCE FROM RECOGNIZED ORGANIZATIONS

Topic - Benchmark	Source	Benchmarks sourced from best practices	IOD Comments on current WIPO RAS
Articulation and Wording of the Risk Appetite Statement	IRM - Risk appetite and tolerance guidance paper	There is a good balance between complexity and excessive simplicity of the Risk Appetite Statement (RAS). The RAS is practical, guiding management to make risk-intelligent decisions.	*Good balance between complexity and excessive simplicity;
	COSO - Risk Appetite - Critical to Success	COSO suggests organizations adopt language that resonates with both the stakeholder group and at varying levels within the organization.	*The language mimics that used for WIPO Strategy and Expected Results.
		Stakeholders prefer risk statements that are not generic, but rather refer to how management and the board run the organization. Often, as organizations become more experienced and their risk management capabilities mature, their appetite statements become more precise. COSO suggests that organizations view the current level of precision in their appetite statement and ask if it has evolved as overall risk management capabilities have matured.	*While the RAS does not explain the difference between the RA and Risk Tolerance, it is explicitly explained in the WIPO Risk and Control Manual.
		COSO suggests organizations use language that mimics that used for strategy and objectives.	
	GFF - Risk Appetite Guidance Note	Risk Appetite and Risk Tolerance differ	
	IRM - Risk appetite and tolerance guidance paper	RAS should specify whether their appetite statements apply to a risk's inherent or residual assessment	
	HLCM Guidelines on Risk Appetite Statements	The risk appetite statement clearly describes the linkage between the Risk Appetite, Risk Tolerance and Performance over time. The RAS clearly explains While Risk Appetite is about the pursuit of risk, Risk Tolerance is about what you can allow the organization to deal with.	
Alignment with the Strategy	COSO - Risk Appetite - Critical to Success	Effective Risk Appetite Statements should not be fully stand-alone but rather have a clear anchor to the wider organizational design. The Risk Appetite Statement should be aligned with the organization's purpose, vision and values, take into consideration the organization's operating environment, and be informed and shaped by the risk maturity.	*Current Risk Appetite structure is based on the components of the WIPO Accountability Framework. This setup makes it difficult to demonstrate the linkage between the Risk Appetite and WIPO Strategic Goals. It is suggested to consider the restructuring of the Risk Appetite Statement in order to demonstrate a clear alignment with WIPO Strategic Pillars, Expected Results and associated Risks.
		The development of risk appetite should align with the development of strategy and business plans, otherwise it may appear that views on strategy and risk appetite are conflicting. Approaches: Objective-focused approach; Risk-focused approach. COSO suggests organizations adopt an objective-focused approach, which cascades into risk considerations, unless there are specific regulatory or other business reasons limiting this choice.	
	COSO suggests that organizations capture key inputs and consider how to incorporate them into risk appetite (e.g., mission and vision, current strategic direction, risk profile, and culture).		

Topic - Benchmark	Source	Benchmarks sourced from best practices	IOD Comments on current WIPO RAS
	HLCM Guidelines on Risk Appetite Statements	<p>COSO suggests organizations keep the organization's strategic plan, including mission and vision, at the forefront of facilitated discussions on appetite. Avoid biasing discussions toward only one or two lines of the business.</p> <p>COSO suggests to develop and communicate a common approach for grouping appetite into categories that align with strategy, objectives, or risks.</p> <p>It is important to determine how the organization will ensure that risk appetite will be forward-looking and aligned with the organization's strategic goals.</p>	
Risk Appetite Scaling: strategic, tactical, operational levels	IRM - Risk appetite and tolerance guidance paper	<p>Risk appetite is not a single, fixed concept. There is a range of appetites for different risks which are aligned.</p> <p>The Risk Appetite is addressed throughout the organization; there are different Risk Appetites at a strategic, tactical and operational levels.</p>	* Current WIPO RA Statements is focused on Strategic Level risk management. The document could render more value by providing guidance on the application of the Risk Appetite at all levels (Strategic, Tactical, and Operational).
COSO - Risk Appetite - Critical to Success	<p>The RA is intentionally broad to apply across an organization, recognizing that it may differ within various parts of the organization while remaining relevant in changing business conditions</p> <p>COSO suggests that organizations develops a view on how risk appetite will cascade into the organization through the use of tolerance, indicators and triggers (e.g., at the board and senior management level, day-to-day-operations, compliance, and monitoring).</p>		
HLCM Guidelines on Risk Appetite Statements	It is important to determine how risk appetite will be cascaded down to business units; how will risk appetite take into account differing views at a strategic, tactical and operational level.		
Risk Taking, Opportunities and Performance	IRM - Risk appetite and tolerance guidance paper	<p>The RAS explicitly states, what are the risks the organization IS willing to take; NOT willing to take (Propensity to take risks).</p> <p>The management at Strategic level has a proportionally higher propensity to take risk than to exercise control. At the same time, the management at Operational level is more about exercising control.</p>	*The RAS could include the statement on importance of Risk Taking and Exploiting the Opportunities. The whole RAS content should support that statement where relevant.
COSO - Risk Appetite - Critical to Success	RA is not about making all decision-makers risk-averse, but about encouraging decisions that recognize that every successful organization takes risks. This may be done by linking risk considerations with strategy setting or by incorporating both lower and upper boundaries of risk into appetite statements.	* The RAS could include areas, where management would accept higher risk for greater performance or whether it would be satisfied to accept lower performance to limit risk.	

Topic - Benchmark	Source	Benchmarks sourced from best practices	IOD Comments on current WIPO RAS
		COSO suggests organizations develop a philosophy on risk-taking and performance; for example, whether it would accept higher risk for greater performance or whether it would be satisfied to accept lower performance to limit risk.	
	GFF - Risk Appetite Guidance Note	Public sector organizations cannot be culturally risk averse and be successful. Effective and meaningful risk management in government remains more important than ever in taking a balanced of risk and opportunity in delivering public services	
	HLCM Guidelines on Risk Appetite Statements	RAS sets out to propose that risk taking is a business necessity, since seeking zero risk is prohibitively costly, and moreover that some objectives deserve to attract relatively more or less risk than other objectives.	
Risk Appetite Metrics	IRM - Risk appetite and tolerance guidance paper	The risk appetite metrics / indicators are sufficiently measurable; they are supported by good data governance.	*While WIPO Risk and Internal Controls Manual explains different dimensions for impact assessment (financial, reputational, personal damage, etc.), the Risk Appetite Statement does not contain this information. It makes the RAS rather "academic" and less practicable in everyday decision making. Moreover, the existing dimensions are not always relevant for operational / project level risks. *RAS may include the approach to dealing with "fast" and "slow" clock speed risks and describe the appetite towards these two different types of risks. *Some organizations also state what main controls are applied to different types of Risks in the RA Statement.
		The RAS explicitly states, what are the levels of controls applied to significant risks (Propensity to exercise controls).	
		The RAS distinguishes between "fast" and "slow" clock speed risks and describes the organizational appetite towards these two different types of risks. [Best Practice].	
	COSO - Risk Appetite - Critical to Success	Risk appetite is much more than a metric. With the increasing availability of data and data analytic tools, organizations may develop data rich contexts that provide insight into the impact of various strategic and operational decisions on entity performance.	
	HLCM Guidelines on Risk Appetite Statements	A default level of risk appetite may be particularly useful for organizations that may frequently have to enter into new forms of activities that otherwise would lack a risk appetite level initially.	
HLCM Guidelines on Risk Appetite Statements	It is important to determine how will risk appetite guide decision making, facilitate measurable actions and support monitoring.		
RM Capacity and Maturity and RM Culture	IRM - Risk appetite and tolerance guidance paper	Risk function Capacity and the overall RM Maturity are at sufficient level and there is a RM Maturity Improvement process in place. These are pre-requisites for high-quality Risk Appetite statement.	*RM Maturity at WIPO is sufficient to produce high-quality RAS.

Topic - Benchmark	Source	Benchmarks sourced from best practices	IOD Comments on current WIPO RAS
	HLCM Guidelines on Risk Appetite Statements	While it is possible to introduce a formal Risk Appetite Statement at any level of risk maturity, it may be more useful for United Nations organizations to implement risk appetite when they are otherwise at the Developing or Established maturity level in most or all of the dimensions of the Reference Maturity Model.	*While the RM Culture at WIPO needs an enhancement, it impacts mainly the application of the RAS in everyday operations, not RAS content.
	COSO - Risk Appetite - Critical to Success	Applying appetite requires a culture that is aware of strategy, objectives, and risk.	
Consultations with Stakeholders	IRM - Risk appetite and tolerance guidance paper	The development of the Risk Appetite Statement included appropriate consultation with relevant external and internal stakeholders (At least DG, ADG, DDG, RMG, Nations).	*While there is always a room for wider inclusion of relevant stakeholders, WIPO RAS seem to be prepared in consultation with a sufficient number of relevant stakeholders.
	COSO - Risk Appetite - Critical to Success	Boards and management often consider appetite in relation to only a few stakeholders—typically shareholders and regulators. That view is limited. Stakeholder activism can become more vocal when stakeholders view actions as outside their boundaries of acceptable risk, at times going so far as impacting the reputation, brand, and trust in the organization. COSO suggests organizations include in the development of appetite both senior levels of management and those engaged in day-to-day activities.	
	GFF - Risk Appetite Guidance Note	Facilitated sessions engaging stakeholders, including Function leads as appropriate, are required to support the development of optimal and tolerance levels. This approach may range from in-depth processes involving wide ranging stakeholder engagement, to focused engagement with senior management.	
	HLCM Guidelines on Risk Appetite Statements	While an organization's senior leadership is responsible to articulate its risk appetite (for governing body approval), it is also important to understand and engage other stakeholders throughout the process of developing and implementing risk appetite.	
Communication and reporting	COSO - Risk Appetite - Critical to Success	Once an overall risk appetite is developed, management must then choose a mechanism for communicating it. The clarity of communicating appetite improves when there is a commonly applied structure, one that considers the choice of language, the intended level of precision, and preferably a focus on strategy and objectives rather than risks. Regardless of approach, appetite does need to flow from the board down through senior management, middle management, operational leaders, and staff. Each organization should determine the best way to communicate appetite to operational leaders in a manner specific enough to provide clarity to those tasked with monitoring whether risks are being managed within appetite.	*Results of IOD Internal survey and interviews with WIPO staff indicate rather low awareness about WIPO Risk Appetite Statement and its practical application in day-to-day decision-making. Better communication is needed.
	IRM - Risk appetite and tolerance guidance paper	"The organization's risk appetite should be established and/or approved by the board (or equivalent) and effectively communicated throughout the organization.	

Topic - Benchmark	Source	Benchmarks sourced from best practices	IOD Comments on current WIPO RAS
	HLCM Guidelines on Risk Appetite Statements	Operationalizing risk appetite requires clear communication both internally and externally. Internal communication is likely to be more detailed and more regular than external communication. Internal communication is also likely to need to be drive action.	
Risk Escalation Mechanisms	IRM - Risk appetite and tolerance guidance paper	Management is also responsible for ensuring that the company operates a system of risk escalation when any risk exposure approaches the maximum level that the company is willing to tolerate.	*While WIPO Risk and Internal Controls Manual explains the procedure of risk escalation, current WIPO Risk Appetite Statement does not cover this process. Updated RAS potentially could explain the modalities of risk escalation.
	COSO - Risk Appetite - Critical to Success	Business operations may also develop specific indicators to alert management when the level of acceptable risks is exceeded. When this happens, it should trigger discussion within the organization.	
	HLCM Guidelines on Risk Appetite Statements	An organization will need to establish clear procedures for what happens when a threshold or a limit of risk appetite is breached. This includes the designation of escalation authorities, timelines and potential remedial actions.	
Revision of the Risk Appetite	IRM - Risk appetite and tolerance guidance paper	There is a Risk Committee (or similar). Its agenda among others includes creation and monitoring of approaches to risk appetite and risk tolerance.	*RA Statement last time reviewed in 2019. Now (November 2021) another review of the RA is initiated.
		The Risk Appetite Statement includes a review process at the end of the cycle (bi-annual) so that appropriate lessons can be learned. The process ensures that the risk appetite can and will change over time (as, for example, the economy shifts from boom to bust, or as cash reserves fall etc.).	
	COSO - Risk Appetite - Critical to Success	Risk appetite must also be flexible enough to adapt to changing conditions, helping an organization to remain relevant in the evolving landscape	
		COSO suggests organization to set a specific time period for revisiting the RA to ensure that risk appetite remains current.	
	GFF - Risk Appetite Guidance Note	As organizations consider and maintain their risk appetite to reflect context and changing environmental factors, there may be circumstances, such as those experienced dealing with government's response to the Covid-19 crisis, when it becomes necessary to significantly alter the level, nature and balance of risks with which an organization is willing to, or is required to, operate to deliver public services for a period of time.	
HLCM Guidelines on Risk Appetite Statements	The Risk Appetite Statement should be periodically monitored, reported on, and discussed, as required, with the governing body, donors, external auditors and regulators, and other stakeholders. This will help to ensure that the Risk Appetite Statement remains relevant, current and value-adding. It will allow for incremental improvements, and for new risks or risk areas requiring articulated risk appetites to be identified, including those that may be difficult to quantify. Additionally, revision should be backward looking to assess whether the risk appetite framework in its current form has been effective in terms of supporting strategic and risk objectives.		

Topic - Benchmark	Source	Benchmarks sourced from best practices	IOD Comments on current WIPO RAS
		<p>As a minimum it is recommended to review a Risk Appetite Statement at least once every five years. Where an organization has a specified time period for reviewing its strategic plans (such as every three or four years in some cases), the Risk Appetite Statement could also be reviewed and updated as part of this process.</p>	

[Annex V follows]

ANNEX V: RISKS AND RISK RESPONSE STATUS UPDATE IN ERM

Program	Status as of 20 November 2021			Status as of 26 November 2021		
	Updated	Partially Updated	Not Updated	Updated	Partially Updated	Not Updated
1			X		X	
2			X	X		
3			X			X
4			X			X
5		X			X	
6	X			X		
7		X			X	
8			X	X		
9			X	X		
10			X		X	
11	X			X		
12	X			X		
13	X			X		
14			X	X		
15	X			X		
16			X			X
17		X			X	
18		X			X	
19	X			X		
20			X		X	
21		X			X	
22	X			X		
23		X			X	
24		X			X	
25		X			X	
26	X			X		
27	X			X		
28	X			X		
30			X			X
31		X			X	
32			X	X		

Source: ERM Risk Register data

[Annex VI follows]

ANNEX VI: Annex withheld

[Annex VII follows]

ANNEX VII: WIPO CORPORATE AND PROJECT RISK SCALE

WIPO Corporate risk scale

Likelihood		Impact			
HIGH Probability: 80-99% Frequency: 1 event per year	4				
MODERATE Probability: 50-80% Frequency: 1 event every 1-2 yrs	3				
LOW Probability: 20-50% Frequency: 1 event every 2-5 years	2				
MINIMAL Probability: below 20% Frequency: 1 event every 5 years or more	1				
		1	2	3	4
		SMALL	NOTICEABLE	CRITICAL	CATASTROPHIC
DIMENSIONS		<i>Select and apply the dimension and impact which represents the worst case.</i>			
Financial		0 - 200,000 Sfr.	200,000 - 1,000,000 Sfr.	1,000,000 - 5,000,000 Sfr.	> 5,000,000 Sfr.
Operations		Small interruption of operation: there is little or no impact on internal operations.	Noticeable interruption of operations: there is a some, but not grave impact on internal operations.	Critical interruption of operations: there is a grave impact on the Organization, probably over an extended period.	Catastrophic interruption of operations: a significant part or all of the Organization's continuation is jeopardized.
Strategic Goals		One expected result is in jeopardy of not being reached, if the event occurred, however the strategic goal as a whole is not affected considerably.	Some expected results are in jeopardy of not being reached, if the event occurred. The strategic goal as a whole may also be affected.	There is reasonable likelihood that a strategic goal will not be achieved, if this event occurs.	There is high likelihood that one or more strategic goals will not be achieved, if this event occurs.
Clients		Clients and/or external stakeholders are not affected.	Services to a small number of clients and/or external stakeholders are affected.	Services to a larger number of clients and/or external stakeholders are affected over a short period of time.	Service to a large number of clients and/or external stakeholders are affected over a long time of period.
Reputation		No negative impact on WIPO's reputation.	Limited negative impact on WIPO's reputation.	Significant but geographically limited negative impact on WIPO's reputation.	Sustained and geographically unlimited negative impact on WIPO's reputation.
Personal Damage		Several minor injuries.	Several medium-heavy injuries.	Several major injuries.	Fatal injuries.

Risk appetite

WIPO Project Risk Scale Template

Likelihood		Impact		
HIGH Probability 75-99%	3			
MODERATE Probability 25-75%	2			
LOW Probability below 25%	1			
		1	2	3
		SMALL	MEDIUM	LARGE
DIMENSIONS		<i>Select the dimensions for the project and delete the dimensions not required.. Where possible, enter absolute numbers in place of the indicative percentages below relevant to the project, which the project board should review and confirm.</i>		
Financial		< 10% project budget	10 -30% project budget	> 30% project budget
Objective		The project objective would be compromised to a minor degree	The project objective would be compromised significantly	The entire project objective is at risk
Schedule slippage		< 10% of overall schedule	10-30% of overall schedule	> 30% of overall schedule
Existing operations		Minor unplanned impact on operations, clients or reputation.	Significant unplanned impact on operations, clients or reputation.	Major unplanned impact on operations, clients or reputation.

Source: WIPO Risk and Internal Control Manual

[Annex VIII follows]

ANNEX VIII: WIPO CONTROLS BY PROCESS

Related Process	COUNT OF CONTROLS					Grand Total	
	0	1	2	3	4		5
CONTROL MATURITY LEVEL:							
Accountability (COSO Principle 5)				3			3
Alternative Procurement Procedures [APP]				1			1
Application Management				4			4
Approvals [APR]				2			2
Asset Management Processes [AMP]				13			13
Asset Register Maintenance [ARM]				1			1
Biennial Planning [PLN]		2		1	2		5
Budget [BUD]				3	1		4
Classification [CLS]				12			12
Commitment to Competence				3			3
Commitment to Integrity & Ethical Values (COSO Principle 1)				7			7
Conflict Resolution			1	9			10
Conflicts Of Interest [COI]			1	7			8
Contract Award and Approval [CAP]				9			9
Contract Management [CMT]			1	4	2		7
Contract Review Committee [CRC]				6			6
Control Activities				3			3
Cooperate with Organizations for Procurement [COP]				1			1
Delegation Of Authority [DOA]				7	2		9
Disciplinary Measures		1		2			3
Enterprise Solutions Division		1		2			3
Expenditure [EXP]		1	1	12	6		20
Financial Confirmation Approval				1			1
Financial Management Approval				5	2		7
Governing Body Oversight Responsibilities (COSO Principle 2)				2			2
Health Measures				1			1
Income [INC]		1	2	4	1		8
Information & Communication				6	2	1	9
Information Technology Management [ITM]				7			7
Internal Audit Section [IAS]				1			1
Investigation Section [IVS]				1			1
Leave Entitlement [LET]			1	13	2		16
Monitoring Activities				6		1	7
Not assigned	3		8	16		4	31
Office of the Legal Counsel				1			1
Organization Structure, Responsibility & Authority				2	2		4
Payments [PAY]				3			3

Performance Management and Staff Development System [SDS]				2			2
Planning [PLN]	1		3				4
Premises controls			2				2
Program and Financial Performance Assessment [PPA]				1			1
Project Management Office [PMO]			6				6
Property Survey Board [PSB]			3				3
Purchase Requisitions (PRC)			1				1
Records Information Management	1		1				2
Recruitment Appointment and Promotion [RAP]	1		25				26
Reporting [REP]	1	3	5	8			17
Reserves planning			2				2
Risk Assessment			1	1			2
Safety and Security Coordination Service			2				2
Salaries and Allowances [SAL]	1		26	4			31
Security and Information Assurance Division		1					1
Separation from Service [SFS]			15				15
Skills and Learning	1		1				2
Standards Of Conduct [SOC]		1	3				4
Tender Submission and Evaluation [TSE]			7				7
Tendering and Offers Processes [TOP]			13				13
Training and Awareness Raising			1	1			2
Travel and Mission Support [TMS]		3	22				25
Travel Related Entitlements [TRE]	3	2	7				12
Travel Related Expenses (TRE)	2		3				5
Treasury [TRS]	2	1	19	2			24
Unforeseen	1						1
Vendor Identification [VID]			3	1			4
Vendor Sanctions Processes [VSP]			6				6
WIPO Ethics Office			3				3
WIPO Insurance Board			1				1
Working Time Arrangements [WTA]			6	2			8
Grand Total	3	17	29	370	42	6	467

Source: WIPO ERM Risk Register, status as of December 8, 2021

[Annex IX follows]

ANNEX IX: MITIGATION ACTIONS DETAILS

When last assessed	ACTION STATUS					Grand Total
	Proposed	Approved to implement – reflected in work plan	Under implementation – reflected in work plan	In Place	No status	
Nov_2020			3			3
Dec_2020		1	25			26
April_2021			6	1		7
Jun_2021			2			2
Sep_2021	1	1	2	1		5
Oct_2021			2			2
Nov_2021	8	7	125	51	3	194
Dec_2021	8	4	52	19		83
Grand Total	17	13	217	72	3	322

Source: WIPO ERM Risk Register, status as of December 8, 2021

[Annex X follows]

ANNEX X: Annex withheld

[Annex XI follows]

ANNEX XI: Annex withheld

[Annex XII follows]

ANNEX XII: Annex withheld

[Annex XIII follows]

ANNEX XIII: ANALYSIS OF RISKS, CONTROLS AND MITIGATING ACTIONS

Table 1: Analysis of Formulation of Risks in WIPO Risk Registers

Risk Element	ERM Risk Register	Project Risk Registers (IT projects)	Project Risk Registers (Non-IT projects)
Risk Event / Condition	*Well described risk events / conditions. Sometimes the description is too wordy.	*Well described risk events / conditions	*Well described risk events / conditions
Cause	*While for Risk Owners causes could be rather obvious, their descriptions were frequently missing. Sometimes causes could not be known.	*While causes are not always clearly articulated, generally it is possible to understand what could be the potential reason for risk materialization	*While for Risk Owners causes could be rather obvious, their descriptions were frequently missing. Sometimes causes could not be known.
Consequence	*Consequences are rarely described.	*Clearly described consequences and impact on the project	*Consequences are rarely described.

Source: IOD test results

Table 2: Analysis of Formulation of Controls in WIPO ERM Risk Register

Control Element	Entity Level Controls (13 analyzed)	Process / Implementation level controls (57 analyzed)
Clear Wording	12/13=92% of ELC wordings were relatively easy to read and understand.	51/57=89% of controls wordings were relatively easy to read and understand.
Conciseness	3/13=23% of ELC were assessed as concise. While Entity Level Controls tend to have longer description due to their broader coverage, many analyzed controls seemed to be copy-pasted from Rules and Regulations, descriptions of different WIPO Functions and other normative documents. This made control descriptions less focused and difficult to understand how they reduce specific risks linked to them.	51/57=89% of controls were assessed as concise. Note: the majority of control descriptions that have been assessed as unconcise were found in the Tendering and Offers Process controls (TOP). Control descriptions seemed to be directly copy-pasted from WIPO procurement regulations.
Frequency	13/13 = 100% of analyzed controls had a description of frequency of execution.	57/57 = 100% of analyzed controls had a description of frequency of execution.
Type and Function	13/13 = 100% of analyzed controls had a description of control Type and Function.	57/57 = 100% of analyzed controls had a description of control Type and Function.
Control Owner assigned	13/13 = 100% of analyzed controls had a control owner assigned.	57/57 = 100% of analyzed controls had a control owner assigned.
Addressing the risk	10/13=77% of ELC were assessed clearly addressing the risks allocated to them. While ELC have more pervasive nature, three ELC have been found too indirect to make any notable risk reduction effect on linked risks.	47/57=82% of controls were assessed as clearly addressing the risks allocated to them. Note: the majority of controls that have been assessed as not addressing the associated risks were found in the Tendering and Offers Process controls (TOP). Control descriptions seemed to be directly copy-pasted from WIPO procurement regulations.

Source: IOD test results

Table 3: Analysis of Formulation of Mitigating Actions in WIPO ERM Risk Register

Action Element	Comments on Mitigating Actions (100 actions analyzed)
Clear Wording	96/100=96% of Mitigation Action wordings were relatively easy to read and understand.
Specific, Measurable	60/100=60% of Mitigation Actions were assessed as specific and measurable. In many cases actions were weakly formulated, not allowing to assess their achievement by the end of the deadline. Lack of quantifiable expected results.
Action Owner assigned	92/100 = 92% of analyzed Mitigation Actions were assigned to an owner. Some actions were either in the process of owner change or recently developed with owner not assigned yet.
Action Deadline set	100/100 = 100% of analyzed Mitigation Actions had a deadline.
Addressing the risk	100/100 = 100% of analyzed Mitigation Actions were related to the associated risk either directly or indirectly.
It is a one-off measure; not a Control by its nature	61/100=61% of Mitigation Actions were assessed as being “actions” by nature; remaining ones did not seem to be a “one-off” measures, but rather systematic, continuous activities, having properties of controls.

Source: IOD test results

Table 4: Analysis of last control (self) assessment validation dates in ERM

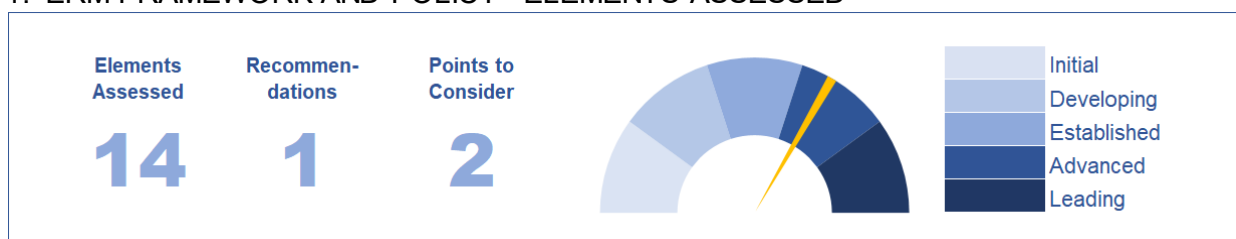
Last assessment period	Number and percentage of assessed and validated controls		Number and percentage of controls with evidence attachments	
	Number	Percentage	Number	Percentage
NOV_2021	446	96%	157	34%
MAR_2021	5	1%	5	1%
FEB_2021	8	2%	4	1%
MAR_2019*	1*	0%	-	-
JAN_2019*	2*	0%	-	-
FEB_2018*	1*	0%	-	-
OCT_2017*	4*	1%	-	-
Grand Total	467	100%	166	36%

Source: ERM Risk Register as of 8 December 2021. *These controls have already been transferred to the dedicated information risk management tool used by the Security and Information Assurance Division. These controls are no longer active in ERM and will be removed.

[Annex XIV follows]

ANNEX XIV: GAP ANALYSIS DETAILS

1. ERM FRAMEWORK AND POLICY– ELEMENTS ASSESSED



ELEMENTS ASSESSED		POINTS FOR CONSIDERATION / RECOMMENDATIONS
ERM framework is in place		<p>R1 The Office of the Controller in collaboration with the Risk Management Group and Sector Risk Coordinators should raise staff awareness about the WIPO Risk Appetite Statement.</p> <p>P1 There are opportunities to increase the visibility of Accountability and Risk Management frameworks. While more respondents tend to agree with the usefulness of the RM and IC documentation, there is a room for improvement and better alignment with operational daily decision-making.</p> <p>P2 WIPO would benefit from: (a) Highlighting the importance of Risk taking and exploiting Opportunities in the RAS; (b) Explaining in the Risk and Internal Controls Manual, the application of the Risk Appetite at operational levels and describing the modalities of risk escalation process, including how to measure impact at the level of Sector/Department/Division/Section and Unit, will help operationalizing the RAS.</p>
Sufficiency of organization's risk guidelines, policies, procedures and processes.		
Visibility of the Accountability and RM Framework	P1	
ERM integration in Planning, Internal Controls, Strategy Setting and Decision-Making.		
Methodology for Risk Measurement; developed Risk Scales		
Design of 2nd line functions' roles in RM		
Setting the Risk Appetite		
Communicating the Risk Appetite	R1, P2	
Design of Risk Escalation		
RA Linkage to the strategy		
RA update Frequency		
Emphasis on the importance of Risk Taking and seeking for Opportunities	P2	
ERM framework updates		
RM Self-assessment mechanism		

R – Recommendation
P – Point for Consideration

2. GOVERNANCE AND ORGANIZATIONAL STRUCTURE– ELEMENTS ASSESSED



ELEMENTS ASSESSED		POINTS FOR CONSIDERATION / RECOMMENDATIONS
Design of Risk Governance Structure	P3	R2 Sector Leads and Relevant Managers should ensure that the PMSDS of designated staff members include objectives related their role as Sector Risk Coordinators.
Effective Setting Risk roles & responsibilities	R2, P3	P3 Enhance Risk Management Framework by: (a) Broadening the focus of RMG discussions and including other elements on the WIPO risk map; including an additional agenda item on “Identifying Opportunities”;
Risk-based delegation of authority		(b) Enhancing the Sector Leads knowledge of the discussions of the RMG through for instance, inviting a Sector Leads to a RMG, or presenting the results of the RMG meetings to Sector Leads on a regular basis;
WIPO Risk Management function has a Charter or equivalent		(c) Developing a coherent and consistent approach for determining membership of Sector Risk Coordinators (SRCs); and
There is an independent RM function, implemented with clear role and responsibility for RM		(d) Establishing a fixed term (e.g. maximum five years) for SRCs, to enable different staff members to take on the role, and contribute to a community of practice and the growth of the risk management culture at WIPO.
RM function's role is integrated with strategy setting and clearly anchored with management across the organization		
RM function accountability against IAOC		

R – Recommendation
P – Point for Consideration

3. PROCESS AND INTEGRATION – ELEMENTS ASSESSED



ELEMENTS ASSESSED		POINTS FOR CONSIDERATION / RECOMMENDATIONS
Risk identification - following policies		<p>R3 The Office of the Controller should review and update the Risk Manual, including guidance for risk responses, risk escalation (including project risks), and the relationship between risks and controls.</p> <p>P4 Visibility of key project risks can be further enhanced by considering: (a) using Sector Risks Coordinators to engage with project managers in respective Sectors, to identify key project risks that can be escalated at Sector or organizational levels; and (b) adding a line on awareness of key project risks and related responses in the Management Representation Letter of respective Sector Leads.</p> <p>P5 Sectors to take measures to timely update their risks and risks responses before the deadline for submitting the annual work plans, to among others, ensure that risks related to planned activities are timely captured, and applicable mitigations budgeted in compliance with relevant PPBD Guidance.</p>
Risk identification – completeness		
Formulation of risks		
Risk scales for different level risks		
Systematic risk responses		
Institutionalization of risk ownership		
Identification of Internal Controls		
Formulation of Risk Responses	R3	
Integration between RM and IC		
Number of existing controls		
Established control criteria		
Addressing control gaps		
Documentation of key processes		
Follow-up of risks		
Identification of risk response overlaps		
Iterative evaluation of the process		
SIC preparation process	P4	
RM and Work planning integration	P5	
RM and Staff PM integration		
Documentation and Guidance		

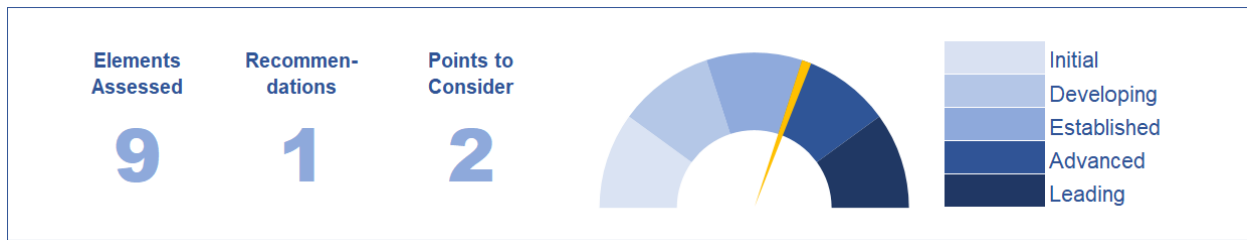
4. ERM SYSTEMS AND TOOLS – ELEMENTS ASSESSED



ELEMENTS ASSESSED		POINTS FOR CONSIDERATION / RECOMMENDATIONS
Modern and Automated RM Tools		<p>P6 The value from the existing ERM software can be maximized by among others:</p> <p>a) Enhancing the responsibility and accountability of managers and risk owners in using the system;</p> <p>b) Identifying the key challenges in the use of the current system and finding cost-effective solutions;</p> <p>c) Raising awareness and educating relevant staff to work with Acuity STREAM™ more efficiently.</p>
Management of Project Risk Registers		
Process of Risk Register updates		
Dynamic risk dashboards		
Risk modelling and forecasting tools		
Staff skills to work with Risk Registers	P6	
ERM linkage with other systems		

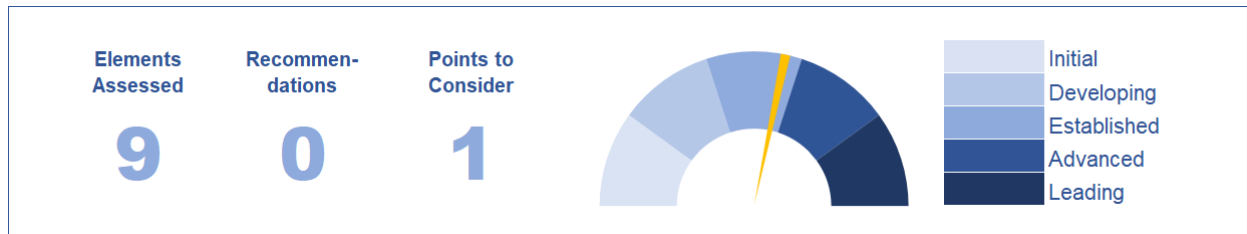
R – Recommendation
P – Point for Consideration

5. RISK CAPABILITIES– ELEMENTS ASSESSED



ELEMENTS ASSESSED		POINTS FOR CONSIDERATION / RECOMMENDATIONS
Staff - Risk Management Skills		<p>R4 The Office of the Controller in coordination with the Internal Training Program of the WIPO Academy, should further raise risk management and internal controls awareness by introducing updated training offerings to address the needs of staff members at different levels and relationships and responsibilities towards Risk Management and Internal Controls.</p> <p>P7 The Enterprise Solutions Division should consider adding a button “My Risks” in the Quick-links of the new AIMS Portal. The button should take the user to the “Risk and Response” BI Risk Dashboard, showing all Risks / Controls / Actions related to that specific user.</p> <p>P8 Formalizing of Data Analytics for Internal Controls as a project and allocate dedicated resources to secure the transparent and efficient implementation of the Roadmap.</p>
Continuous development and Tailored RM Trainings	R4	
RM staff qualifications		
Risk awareness is a recognized competency		
Timely and sufficient risk information for decision making		
Ease of access to Risk Information	P7	
Ability to generate robust risk reports		
Capability to provide a Positive Assurance	P8	
Documentation		

6. RISK CULTURE– ELEMENTS ASSESSED



ELEMENTS ASSESSED		POINTS FOR CONSIDERATION / RECOMMENDATIONS
Senior management communicates risk information	P9	<p>P9 Develop initiatives to enhance the Risk Management Culture, such as:</p> <p>(a) Taking measures to further enhance the tone at the top on risk management, raise risk management commitment, and capacity building; and</p> <p>(b) Put in place processes and practices to encourage and support calculated risk taking.</p>
Senior management creates an active, organization-wide dialogue on risks	P9	
Organizational Culture supports the Risk Culture	P9	
Risk is a standing agenda item on senior management meetings.		
Staff confidence to frankly discuss risks and escalate them	P9	
Collecting and analysis of risk events and incidents	P9	
RM information is shared by senior management	P9	
Documentation of RM successes and Failures and using them as lessons learned and for corrective actions	P9	
Business decisions are supported by calculated risk and reward	P9	

R – Recommendation
P – Point for Consideration

[End of Annexes and of Document]

World Intellectual Property Organization
34, Chemin des Colombettes
P.O. Box 18
CH-1211 Geneva 20
Switzerland

Tel: +41 22 338 91 11
Fax: +41 22 733 54 28

For contact details of WIPO's
External Offices visit:
www.wipo.int/about-wipo/en/offices