



Internal Oversight Division

Reference: IA 2016-08

Audit Report

Audit of Enterprise Risk Management

December 16, 2016

TABLE OF CONTENTS

LIST OF ACRONYMS..... 3

EXECUTIVE SUMMARY..... 4

1. INTRODUCTION..... 5

 (A) BACKGROUND 5

 (B) OBJECTIVES..... 5

 (C) SCOPE AND METHODOLOGY 5

2. OBSERVATIONS AND RECOMMENDATIONS 6

 (A) ACHIEVEMENTS..... 6

 (B) GOVERNANCE AND ORGANIZATIONAL FRAMEWORK..... 7

 (i) Internal Control Framework 7

 (ii) Risk Assessment Process 8

 (iii) Three lines of defense – Gap analysis 9

 (iv) Strategic Risks..... 11

 (C) RISK ASSESSMENT AND MITIGATION 12

 (i) Linkage to work plans/ EPM 12

 (ii) Incident Management 13

 (D) INTERNAL CONTROLS..... 13

 (i) Linkage to controls in authoritative documents 14

 (ii) Design of controls 15

 (iii) Controls attributes..... 15

 (iv) Opportunities for internal controls optimization 16

 (E) SURVEYS..... 17

 (i) External Survey 17

 (ii) Internal Survey 18

TABLE OF RECOMMENDATIONS 19

ANNEXES..... 21

LIST OF ACRONYMS

3LoD	Three Lines of Defense
COSO	Committee of Sponsoring Organizations of the Treadway Commission
EPM	Enterprise Performance Management
ERM	Enterprise Risk Management
FRR	Financial Regulations and Rules
IOD	Internal Oversight Division
IT	Information Technology
OI	Office Instruction
RBM	Results-based Management
RMG	Risk Management Group
SRP	Strategic Realignment Program
SRR	Staff Regulations and Rules
UN	United Nations
WIPO	World Intellectual Property Organization

EXECUTIVE SUMMARY

1. The Internal Oversight Division (IOD) conducted an audit of Enterprise Risk Management (ERM) in WIPO in line with its 2016 work plan. The main objectives of the audit were to take stock of what has been achieved so far in establishing ERM in WIPO and assess adequacy of ERM processes in terms of their design and effectiveness.
2. Since the endorsement of WIPO's accountability framework by the Member States in 2014, considerable progress has been made in establishing a formal and functional ERM process in WIPO. In this regard, the issuance of a risk management policy and risk and internal controls manual, establishment of the Risk Management Group (RMG), adoption of a risk appetite statement and implementation of an ERM Information Technology (IT) platform could be cited among the key steps.
3. WIPO's accountability framework recognizes the "three lines of defense" model in effectively managing its risks through the implementation of internal control with a cohesive and coordinated approach. IOD noted that the monitoring role of second line functions can be further enhanced by formally allocating the task of validating internal control self-assessments conducted by programs in order to determine whether controls are adequate and function as intended.
4. The significant part of internal controls that operate in WIPO are drawn from the Financial Regulations and Rules (FRR), Staff Regulations and Rules (SRR) and related Office Instructions (OI). Hence, as part of management's on-going efforts to document key business processes and internal control activities, it is essential that internal control measures specified by those documents be considered when documenting WIPO's inventory of key internal controls. Furthermore, this exercise also provides an opportunity to assess whether all internal controls, as required by WIPO FRR and SRR, have been put in place and operate as intended.
5. Adequate recording of information relating to the attributes of controls such as control type, its nature, frequency and priority will further help enhance the process of building an inventory of internal controls.
6. IOD conducted a benchmarking survey of ERM practices with United Nations (UN) and other International Organizations. The results of the survey, in which 32 organizations participated, indicate that WIPO's ERM practices are among the more risk-aware organizations. Indicatively, WIPO is among a handful of organizations (~18%) which have implemented a formal ERM IT system.
7. Further improvements to the ERM process can be made by (i) clear categorization and focus on strategic risks facing the Organization; (ii) constantly improving the linkage between annual work plan activities and the identification and assessment of risks; (iii) using incident management records to identify any potential unmitigated risks; and (iv) reviewing inventory of controls within business processes with a view to identifying opportunities for optimization of internal controls.

1. INTRODUCTION

(A) BACKGROUND

8. The foundation for WIPO's formal efforts in Enterprise Risk Management (ERM) was laid down in WIPO's Strategic Realignment Program (SRP) as presented to the Program and Budget Committee in September 2010. Initiative 15 of the SRP concerned strengthening of WIPO's internal control system.

9. Following the SRP initiative, a Risk Management and Internal Controls Board (Office Instruction 37/2012) was established to carry out the internal supervision of the "Strengthen Risk Management and Internal Controls project". This Board was replaced by the establishment of the Risk Management Group in 2014 (OI 18/2014).

10. A Risk Management Policy (the Policy) was established in July 2014 (OI 34/2014) which serves as the formal basis for enterprise-wide risk management at WIPO. The Office of the Controller has been assigned the responsibility for the implementation of the Policy. A risk appetite statement was presented to Member States in September 2014.

11. Since the establishment of the Policy, further progress has been made in WIPO's risk management system through the implementation of an integrated risk management platform. This platform enables all business sectors, within WIPO to utilize a common interface and framework for updating their risk registers.

12. Presently, there is an on-going effort to map business process flows and identify control activities. This will then be linked to risks identified in the risk registers.

(B) OBJECTIVES

13. The objective of the audit was to take stock of what has been achieved so far in establishing ERM at WIPO and assess adequacy of ERM processes in terms of their design and effectiveness. Specifically:

- (a) Governance structure of ERM in terms of organizational positioning and reporting lines;
- (b) Adequacy and implementation of ERM related policy, procedures and guidelines;
- (c) Development of 'key' risks and corresponding key controls;
- (d) Linkage of ERM to other major organizational initiatives/projects/systems such as Business Continuity Management and Enterprise Performance Management (EPM); and
- (e) Management Information Reporting on Risks/Controls.

(C) SCOPE AND METHODOLOGY

14. The audit covered the adequacy and effectiveness of current risk management and internal controls processes and assessed management actions to be taken with a view to establishing an integrated ERM at WIPO. The audit period covered the financial years 2014, 2015 and 2016 (year-to-date).

15. The audit fieldwork included:
- (a) Interviews with key personnel in the Office of the Controller, Finance Division, Security and Information Assurance Division and such other organizational areas as required to obtain an understanding of the risk management processes and systems;
 - (b) Performing walkthroughs with the assistance of relevant personnel to understand the risk identification and internal controls mapping processes;
 - (c) Review of policies and procedures concerning risk management;
 - (d) Review of risk management structure within the Organization; and
 - (e) A survey of Risk Management practices in United Nations (UN) and other international organizations.
16. The audit was performed in accordance with the International Standards for the Professional Practice of Internal Auditing.

2. OBSERVATIONS AND RECOMMENDATIONS

(A) ACHIEVEMENTS

17. Since the re-launch of WIPO's efforts to put in place an effective ERM process in 2014, significant and rapid progress has been made in establishing the formal elements of an ERM system. Specifically:
- (a) The WIPO Accountability Framework (comprising a pillar on Risk Management and Internal Controls) was endorsed by Member States in September 2014;
 - (b) Risk Management Policy and Risk and Internal Control Management Manual were issued in 2014;
 - (c) A Risk Management Group (RMG) was established in 2014 with the objective of promoting 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. The RMG is chaired by the Director General and meets quarterly;
 - (d) A Risk Appetite Statement was prepared by the WIPO Secretariat and taken note of by Member States in 2014;
 - (e) An integrated Risk Management Platform (Acuity STREAM) has been implemented which provides for a common interface for recording and monitoring of identified and assessed risks. This effort includes training end-users in the use of the system and providing support when required; and
 - (f) The reporting of Risk Management information has been incorporated into the Business Intelligence dashboards and provides for a simplified and easy access to risk management information for program managers and their alternates.

(B) GOVERNANCE AND ORGANIZATIONAL FRAMEWORK

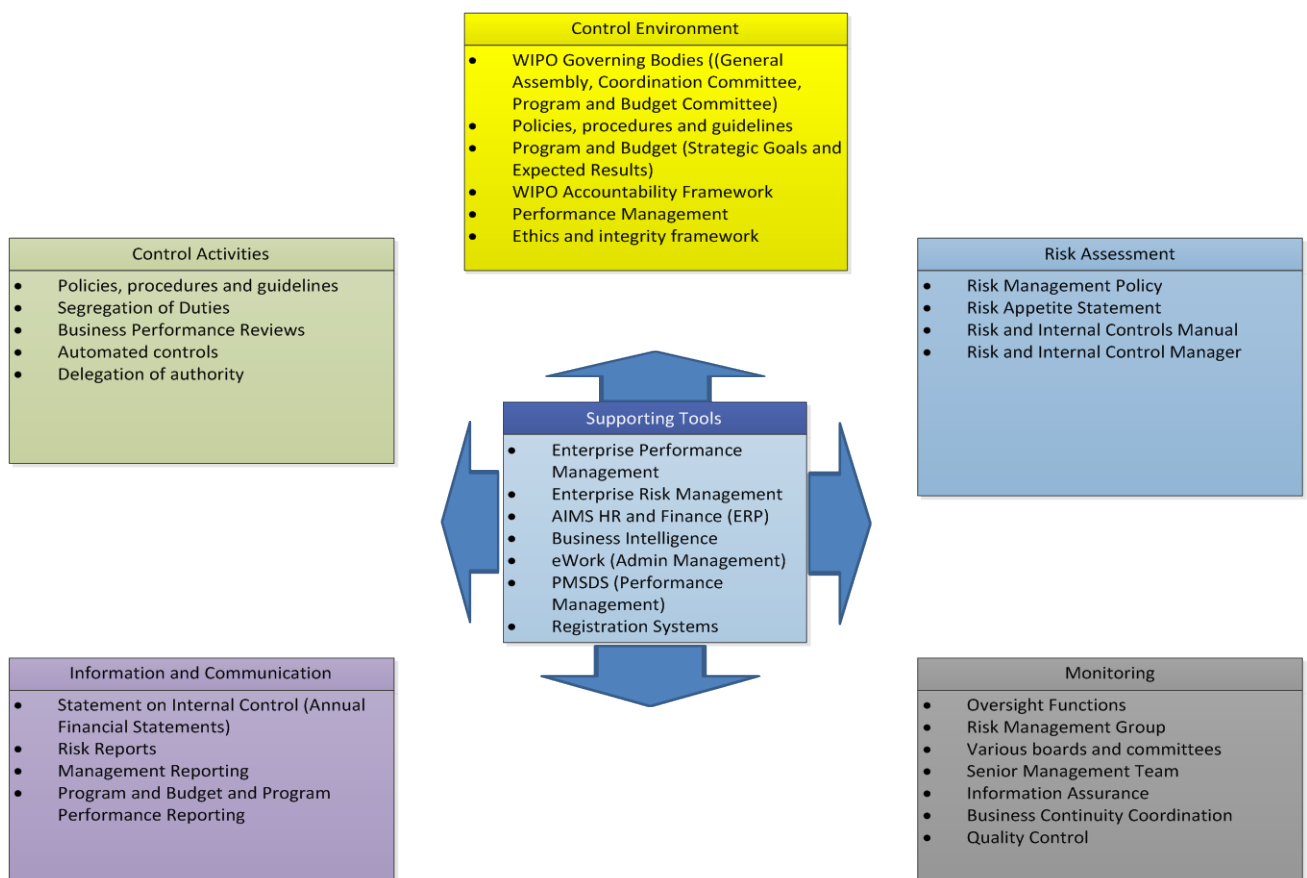
(i) Internal Control Framework

18. The internal control framework of WIPO is based on the Committee of Sponsoring Organizations of the Treadway Commission (COSO) – Internal Control – Integrated Framework. The COSO framework identifies five main components of an effective internal control system:

- (a) Control Environment - The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure.
- (b) Risk Assessment - Risk assessment is the identification and analysis of relevant risks to achievement of the objectives, forming a basis for determining how the risks should be managed.
- (c) Control Activities - Control activities are the policies and procedures that help ensure management directives are carried out. They help ensure that necessary actions are taken to address risks to achievement of the entity's objectives.
- (d) Information and Communication - Information systems produce reports, containing operational, financial and compliance-related information, that make it possible to run and control the business. Effective communication also must occur in a broader sense, flowing down, across and up the organization.
- (e) Monitoring - Internal control systems need to be monitored - a process that assesses the quality of the system's performance over time. This is accomplished through ongoing monitoring activities, separate evaluations or a combination of the two.

19. The COSO internal control components can be linked to the existing elements that comprise the internal control system in WIPO. The diagrammatic representation is available in Figure 1 below.

Figure 1 – COSO Internal Control Components as applied to WIPO



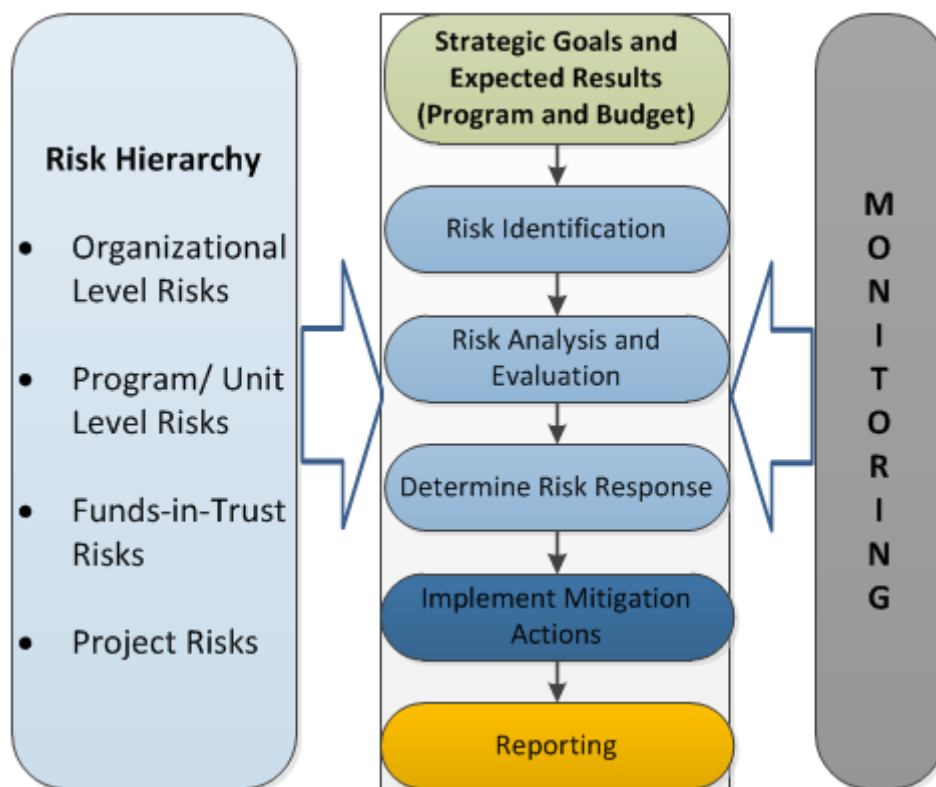
(ii) Risk Assessment Process

20. WIPO's risk assessment process is driven through its Results-based Management (RBM) framework which is codified in the biennial Program and Budget. The Program and Budget sets out the Strategic Goals of the Organization. The Strategic Goals are further broken down to Expected Results within each Strategic Goal. The Program and Budget also allocates the quantum of resources that are available to each WIPO Program.

21. The Strategic Goals and Expected Results in the Program and Budget form the basis for objective setting in a risk management context. Risks are identified and assessed with reference to the Expected Results thereby linking risk management with the RBM framework.

22. WIPO's risk assessment process may be represented as per Figure 2 below.

Figure 2 – WIPO Risk Assessment Process



(iii) Three lines of defense – Gap analysis

23. The Three Lines of Defense (3LoD) model is increasingly being used as a benchmark when assessing the effectiveness of enterprise governance and in particular, risk management. 3LoD provides a simple and effective manner to ensure that risk management and internal control functions are coordinated and complementary across an organization.

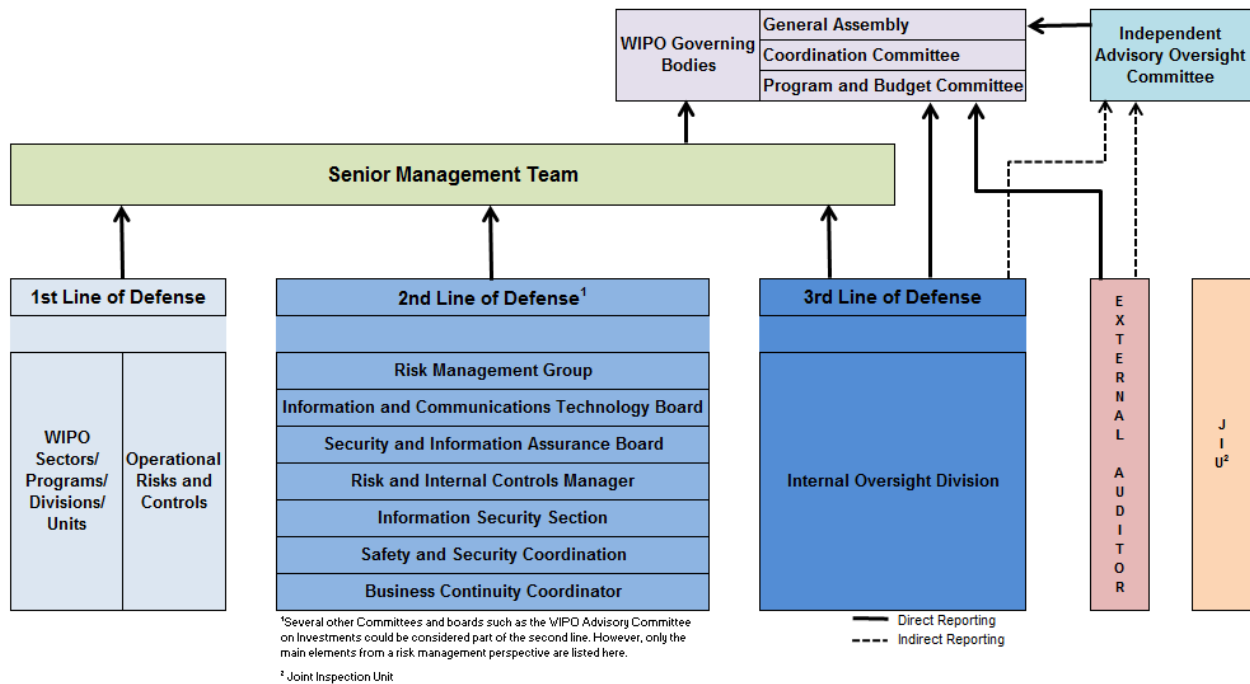
24. Briefly, the 3LoD may be described as follows¹:

- (a) Functions that own and manage risks (First Line) - operational management has ownership, responsibility and accountability for identifying, assessing, controlling and mitigating risks;
- (b) Functions that oversee risks (Second Line) - the risk management, compliance and similar functions facilitate and monitor the implementation of effective risk management practices by operational management and assist the risk owners in reporting adequate risk related information up and down the organization; and
- (c) Functions that provide independent assurance (Third Line) - the internal oversight function, through a risk based approach, provides assurance to the organization's governing body and senior management, on how effectively the organization assesses and manages its risks, including the manner in which the first and second lines of defense operate.

¹ Adapted from the European Confederation of Institutes of Internal Auditing (ECIIA) explanation of the 3LoD (<http://eciia.eu/wp-content/uploads/2013/09/OCV-3.2-3LD-Model.pdf>)

25. A graphical representation of the 3LoD model in WIPO’s context is provided in the diagram below.

Figure 3 – The Three Lines of Defense Model as applied to WIPO



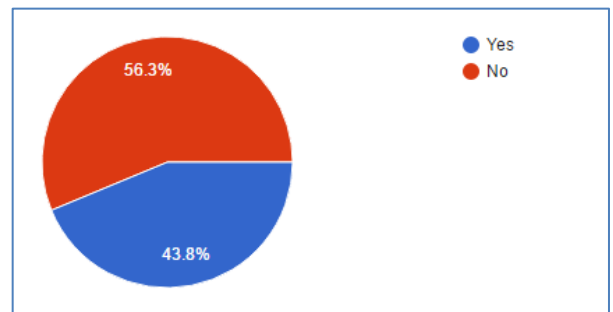
26. Through the risk management efforts in the Organization over the past two years, there has been significant enhancement in the involvement and capabilities of the first line. The core responsibilities of ownership, identification and assessment of risks are now embedded within the first line functions (i.e. line management).

27. While there are several organizational elements which could be considered as forming part of the second line in WIPO (as identified in Figure 3 above), the most significant ones from a risk management and internal control perspective are the Risk Management Group, Risk and Internal Control Manager, Information Security Section and Business Continuity Coordinator. It is evident that the second line functions as envisaged by the 3LoD model do exist in WIPO’s current risk management structure.

28. The two main functions expected of the second line may be specified as:

- (a) Facilitating risk management activities (policies, tools, techniques and support) and providing advice; and
- (b) Monitoring the design and operation of controls in the first line of defense.

Is the role of the risk management function clearly defined in terms of the Three Lines of Defense model?



29. The facilitation of risk management activities by second line functions is clearly recognized in the Risk Management Policy and is an on-going activity within the risk management process. However, the monitoring role of the second line functions is not clearly defined within the existing risk management framework from a controls assessment validation perspective. This is consistent with the results of the survey conducted with other International Organizations which

shows that in 56.3% of respondents, the role of the risk management function was not fully aligned with the 3LoD model.

30. While the first line functions are responsible for identification, assessment and mitigation of operational risks, their reporting on risks and controls is based on self-assessment. The validity of the assurance that management derives from this reporting (i.e. Monitoring the adequacy and effectiveness of internal control and accuracy and completeness of reporting) can only be enhanced if the roles and responsibilities of existing second line functions are clearly defined in terms of monitoring and assurance role they have over the effectiveness of risk management and internal control processes performed by first line functions.

31. To ensure further clarity in the monitoring role of second line functions, the below table contains the actions which need to be taken so as to ensure more cohesive functioning of the risk management process.

Table 1 – Proposed actions for WIPO lines of defense

Function	Actions to be taken
Operational Management (WIPO Programs)	Implementation of Control Procedures/ Mitigation Actions
Risk Management Group	- Ensure properly designed processes and controls are in place within the first line and are operating effectively (monitoring)
ICT Board	
Security and Information Assurance Board	
Risk and Internal Control Manager	
Information Assurance	
Safety and Security	
Legal Counsel	
Business Continuity	

32. In the absence of adequate functions which provide this assurance to management, the Senior Management Team will not have an independent and objective reporting on the status of risk management in WIPO.

(iv) Strategic Risks

33. Broadly, risks may be classified as strategic, operational, financial and compliance related.

34. Strategic risks can be defined as the uncertainties and untapped opportunities embedded in the strategic objectives of the organization and how well they are executed. Presently, there is a risk category for strategic risks in WIPO's categorization of risks, although this category may not include all risks that are "strategic" in nature. Keeping this in mind, the impact measure of the risk scale used by WIPO also defines any risks with a critical or catastrophic impact as having an effect on the achievement of one or more strategic goals of the Organization.

35. It is useful to note that strategic risks may not be restricted only to operational risks that have an organization-wide impact on account of their pervasiveness but also potential events that may occur outside the Organization which have a direct impact on the achievement of the Organization's Strategic Goals.

36. To ensure consistency between the categorization of risks and risks that are considered "strategic" in nature by virtue of their potential impact on the Organization, it would be beneficial if the Risk and Internal Control Manager adopts consistent classification of strategic risks in the risk management system. Consideration should also be given to presenting "strategic" risks facing the organization as a separate item in reports presented to the Risk Management Group. This could be in the form of a strategy map.

Recommendation

1. With the approval of the Risk Management Group, the Office of the Controller should propose a revision to the existing risk management policy to specify the role of the central risk and internal controls manager in the validation of the assessment of internal controls. (Priority: Medium)

(C) RISK ASSESSMENT AND MITIGATION

(i) Linkage to work plans/ EPM

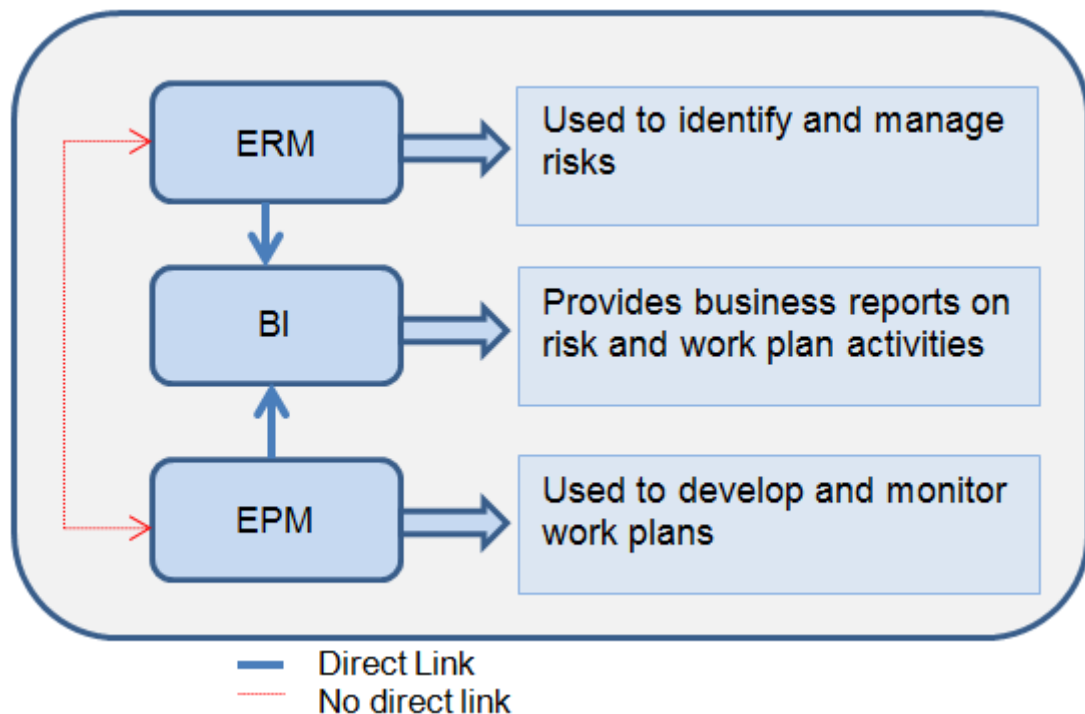
37. The current system of annual work planning for programs/divisions in WIPO uses the EPM system as its basis.

38. Every year, program managers or their alternates prepare annual work plans for each WIPO unit. These work plans are recorded in the EPM system and are linked to the results framework as defined in the relevant Program and Budget.

39. IOD reviewed a sample of 15 units for their work plans in the EPM system and also referred back to the risk management system. It was noted that linkages to Expected Results between the work plan and the risk register was found to be consistent in 12 units while in 3 units the linkage could not be established.

40. Currently, there is no direct link between the EPM work planning system and the risk management system although both systems are configured to link up to the Expected Results as per the relevant Program and Budget.

Figure 5 – Tools used in work plan activities and risk management



41. As a result it is not always apparent whether all risks have been considered for the planned activities. i.e. It is not possible to establish the identified risk(s) that relate to a particular work plan activity.

42. In the absence of a direct link between the systems, Program Managers are reminded to update their program level risks when they update their work plans in the EPM system.

43. Regular reminders by the Department of Program Planning and Finance will benefit WIPO Managers to ensure consistency between the linkages of Expected Results between the EPM work plans and their risk registers.

(ii) Incident Management

44. Incidents which have occurred and have had an impact on the Organizations staff, resources or assets are an important source for identification and assessment of risks.

45. Presently detailed incident management records are maintained by the Premises Management Division and the Security and Information Assurance Division.

46. Although these detailed records exist, no analysis of these records is performed for risk management purposes. Analysis of records of past incidents could be a vital source of information for identification of triggering events or factors that give rise to risks.

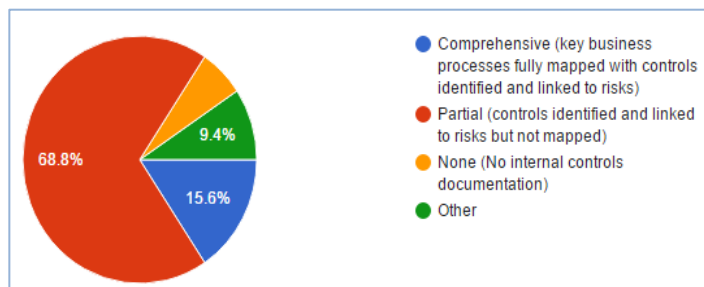
47. Lack of reporting of or analysis of incident records may result in failure to detect common issues that may be occurring over a period of time and therefore provide an indication of potential risks that may exist and remain unmitigated.

48. IOD understands that the Risk Management Group in its meeting held during November 2016 has agreed for inclusion of selected past incidents (based on their criticality) in the reports presented to the Risk Management Group. Work is presently on-going in this area.

(D) INTERNAL CONTROLS


49. Currently, efforts are on-going to document key business processes and identify internal controls within those processes. This is consistent with the results of the survey conducted with other International Organizations which shows that 68.8% of respondents have partially documented their controls and business processes.

What is the extent of documentation of internal controls in your organization?



50. As part of this effort, internal controls that are identified within business processes are also recorded in the risk management system. The objective is to eventually be able to link identified and assessed risks to the identified internal controls. This may also provide an opportunity to identify potential risks where internal controls exist but no relevant risk has been recorded in the risk management system.

Table 3 – Comparison of Current WIPO Controls Documentation Practices with Good Practice



Good practice	WIPO practice	Comment/ Risk/ Consequence
Control attributes relating to the properties of the controls such as their nature, type, frequency etc. are recorded for each control which enables efficient future assessment of the controls.	Controls attributes are not fully recorded as part of the controls inventory. Some information such as control owner and nature (i.e. preventive, detective) are recorded as part of controls properties.	The absence of controls attributes information may lead to inefficiencies and/or gaps in assessment of the effectiveness of controls.
Most controls originate from policy and procedure documents. The source of controls (i.e. origin) should be documented as part of controls information so that any changes in the source documents would trigger a review of linked controls within the controls inventory.	Origin of controls is not clearly indicated in business process/ controls inventory information.	Changes in source documents (such as policies and procedures) may not trigger a review process for controls linked to those documents leading to lack of changes.
The assessment of the effectiveness of the design of controls should be performed separately from the assessment of their operating effectiveness.	There is no provision within the existing workflow for documenting the assessment of the effectiveness of design of controls.	In the absence of proper design assessment of controls, their effectiveness in mitigating the related risks cannot be gauged.

(i) Linkage to controls in authoritative documents

51. The WIPO Financial Regulations and Rules (FRR), Staff Regulations and Rules (SRR) and Office Instructions (OI) contain defined internal control measures. These documents should be considered authoritative as the controls defined in them are required to be put in place by the Organization. The implementation of these controls by the Organization is not optional as they are binding in nature having been approved by the Member States or having been issued by executive order. These controls may be termed as “hard-controls”.

52. Prior to the initiation of the risk management efforts in WIPO, there did not exist any repository or register which identified all these hard controls. The current approach followed to map business key processes and thereby identify controls which should include many of the hard controls.

53. However, based on a review of the business process documentation completed so far as well as the listing of controls in the risk management system, there is no linkage between the identification of these controls and the source document. In essence, the controls put in place within a business process could be as a result of requirement of the authoritative documents or placed by the process owner through standard operating procedures to mitigate identified risks.

54. In order to ensure that all hard-controls that are requirement to be put in place, there should be a listing of these controls as identified from applicable documents. Furthermore, it is

necessary to make a link between the controls identified in business process documentation and the hard controls.

55. In the absence of such linkage, firstly, it will not be known whether all controls as required to be in place as per the authoritative documents actually exist, and secondly, any changes to controls as a result of revisions to these documents would not trigger a process for change in the risk management system.

(ii) Design of controls

56. When the effectiveness of internal controls are assessed there are two aspects which need to be considered:

(a) Whether the controls are designed appropriately to mitigate the relevant risk(s) (i.e. design effectiveness); and

(b) Whether they operate effectively over a period of time so as to actually result in the mitigation of the relevant risk(s) (i.e. operating effectiveness).

57. While operating effectiveness of controls provide significant assurance to management on risk management, without effective design the assurance derived from their operating effectiveness does not hold good.

58. As the process for the assessment of controls in the risk management system is currently in place, it does not take into account the design effectiveness of controls. Design effectiveness of controls usually does not change very frequently over time unless there has been a change in the related risk(s) or a change in the business process.

59. Changes in related risks or business processes should trigger an assessment of the design effectiveness of controls so as to ensure that the control is designed effectively to mitigate the relevant risk(s).

60. If design assessments of controls are not carried out when there are changes in the risks or business process, there is a risk that the control may not continue to mitigate related risks in the manner originally designed.

61. IOD understand that work is ongoing in this area and that the proposed scheme will be presented to IOD for its advice.

(iii) Controls attributes

62. All internal controls can be classified into various categories. Depending on the nature of the control, various attributes can be linked to controls. For example, classification may be by type (automated, manual or IT-dependent manual), nature (preventive, detective, corrective), frequency (daily, weekly, monthly etc.), criticality (key control or not) and level (transaction level, business process level etc.)

63. Control attributes are important in determining the assessment of controls as to whether they function effectively or not. It is therefore important that all relevant information relating to control attributes is accurately captured in the risk management system so as to enable their proper assessment.

64. As the design of the controls information in the Acuity STREAM system currently stands, there is limited information on controls attributes that is being captured in the system. As reviewed by IOD, only information pertaining to nature of the control is being recorded. Furthermore, this information is being captured as part of the assessment framework of the control rather than its implementation data. Controls attributes do not normally change with each assessment of the control and hence should form part of the standing or master data

related to the control rather than their assessment. However, IOD understands that there is a limitation in the functionality of the Acuity STREAM system as a result of which it is only possible to record information on controls attributes as part of each control assessment.

65. Some of the information relating to the control attributes such as control type (i.e. automated or manual) is being recorded in the business process flowcharts but this information does not carry through to the controls data in the risk management system. This is important as certain controls (such as automated controls) inherently do not change in their effectiveness as they are not dependent on manual processes and will continue to operate effectively unless there has been a change in the underlying system configuration or design of the business process. Hence, assessments of the operating effectiveness of these types of controls need not be with the same frequency as those which are purely manual.

66. Lack of adequate information relating to the attributes of controls will result in less effective and efficient assessment of those controls. As at the time of the writing of this report, IOD was informed that a revised set of controls attributes was under development together with a weighting scheme which would be reflected as part of the control assessment information.

(iv) Opportunities for internal controls optimization

67. The process of documenting key business processes and the identification of existing controls is presently on-going. On the completion of this process, an inventory of control activities within each of the business processes will be available.

68. The next step is to link the controls identified with the open risks as per existing risk registers. An outcome of the linking process will be to identify controls that cannot be linked to existing open risks. This could be because (a) the risk which the control is intended to mitigate has not been identified and assessed or (b) the control is redundant because the risk does not exist anymore. Based on the outcome of this activity, management will need to take action to decide on the relevant course of action.

69. On completion of this first step, further analysis may reveal that there are multiple controls which address the same risk. This could indicate redundant controls within the business processes. Redundant controls decrease the efficiency of a business process and add additional overhead to achieving the same result.

70. This would represent an opportunity for internal controls optimization. The focus should be on identifying controls that mitigate more than one risk. These could be termed as "key controls". Having few key controls which mitigate a larger number of risks would be more efficient than having multiple controls addressing the same risks.

71. As part of the on-going efforts to document business processes and control activities, business process owners should be encouraged to review their inventory of controls with a view to identifying opportunities for optimizing controls within their business processes.

Recommendations

The Department of Program Planning and Finance should ensure that:

2. Key controls required as per the authoritative documents such as Financial Regulations and Rules and relevant Office Instructions are identified, linked to business process controls and appropriately documented. (Priority: Medium)
3. Relevant control attributes are accurately and completely recorded as part of the data on controls. (Priority: Medium)

4. The Human Resources Management Department should ensure that key controls required as per the authoritative documents such as the Staff Regulations and Rules and relevant Office Instructions are identified, linked to business process controls and appropriately documented. (Priority: Medium)

(E) SURVEYS

72. IOD conducted a benchmarking survey with United Nations and other International Organizations as well as an internal survey of WIPO managers.

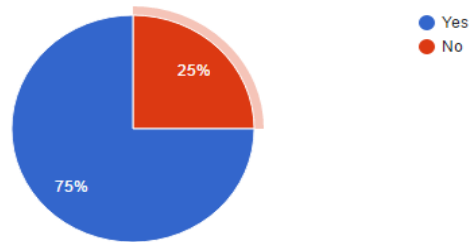
(i) External Survey

73. IOD surveyed ERM status and practices within United Nations and other International Organizations.

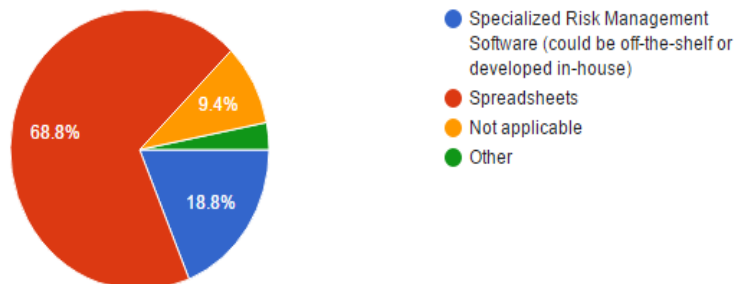
74. A total of 32 organizations responded to the survey. The survey compares WIPO’s ERM status and practices with those of the participating organizations. Overall, WIPO’s risk management processes and practices are placed amongst the more risk aware Organizations, and is evolving in line with its established roadmap.

75. The key results of the survey are summarized below:

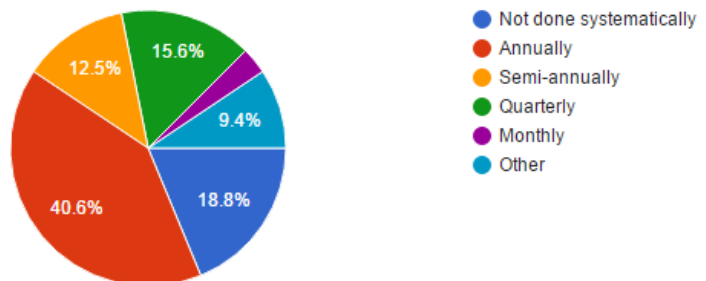
(a) WIPO is among the organizations (75%) which have a formal ERM framework and process in place;



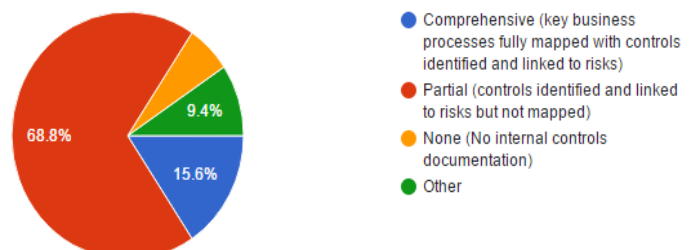
(b) WIPO is among a handful of organizations (~18%) which uses specialized risk management software in maintaining its risk registers;



(c) WIPO is among a handful of organizations which have a quarterly cycle for updating the risk registers; and



(d) WIPO is among a number of organizations (68%) which are in the process of updating their business process and controls documentation.



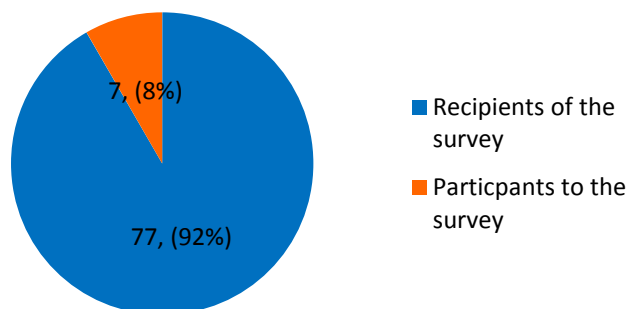
76. The detailed analysis of survey results can be found in Annex II.

(ii) Internal Survey

77. IOD conducted a survey of WIPO managers to obtain feedback on the functioning of the ERM process in WIPO.

78. The survey was sent to 77 WIPO Managers but received only seven completed responses and two partially completed responses.

79. The low level of participation may indicate survey fatigue or lack of managers' engagement in the risk management process.



ACKNOWLEDGMENT

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

Prepared by: Sashidhar Boriah

Reviewed and Approved by: Tuncay Efendioglu

TABLE OF RECOMMENDATIONS

No	Recommendations	Priority	Person(s) Responsible	Management Comments and Action Plan	Deadline
1.	With the approval of the Risk Management Group, the Office of the Controller should propose a revision to the existing risk management policy to specify the role of the central risk and internal controls manager in the validation of the assessment of internal controls.	Medium	C. Narayanaswamy and M. Bona	Management accepts this recommendation. Closure event: issuance of revised Risk Management Policy (OI), specifying the role of the central risk and internal controls manager in the validation of the assessment of internal controls.	31/12/2017
2.	The Department of Program Planning and Finance should ensure that key controls required as per the authoritative documents such as Financial Regulations and Rules and relevant Office Instructions are identified, linked to business process controls and appropriately documented.	Medium	C. Narayanaswamy and M. Bona	Management accepts this recommendation. Closure events: 1. Identification of key controls required by FRRs – list; 2. Key controls reflected in relevant business processes (i.e. shown on the business process maps) and recorded in ERM.	1. 31/03/2017 2. 31/12/2017
3.	The Department of Program Planning and Finance should ensure that relevant control attributes are accurately and completely recorded as part of the data on controls.	Medium	C. Narayanaswamy and M. Bona	Management accepts this recommendation. Closure event: Revised control assessment scheme incorporating the relevant control attributes reflected in the configuration of ERM control assessment.	31/03/2017

No	Recommendations	Priority	Person(s) Responsible	Management Comments and Action Plan	Deadline
4.	The Human Resources Management Department should ensure that key controls required as per the authoritative documents such as the Staff Regulations and Rules and relevant Office Instructions are identified, linked to business process controls and appropriately documented.	Medium	C. Moussa	A management action plan for this recommendation will be elaborated in consultation with all the stakeholders.	TBD

ANNEXES

Annex I.	Priority of Recommendations
Annex II.	Results of Benchmarking Survey conducted with United Nations and other International Organizations

[Annexes follow]

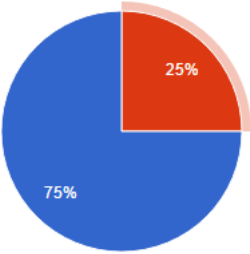
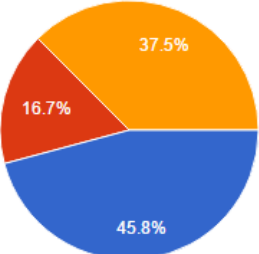
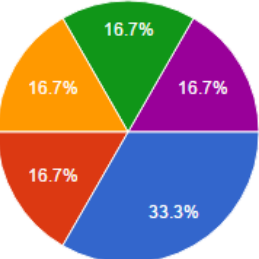
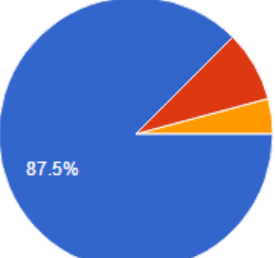
ANNEX I – PRIORITY OF RECOMMENDATIONS

The recommendations are categorized according to priority, as a further guide to WIPO management in addressing the issues. The following categories are used:

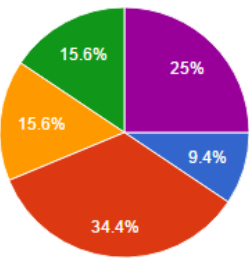
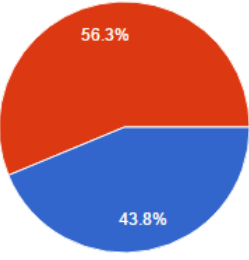
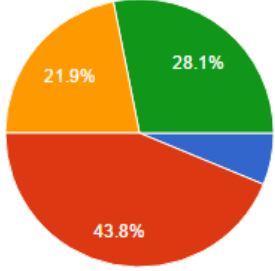
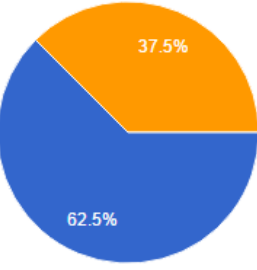
Priority of Audit Recommendations	Nature
Very High	<p>Requires Immediate Management Attention. This is a serious internal control or risk management issue that if not mitigated, may, with a high degree of certainty, lead to:</p> <ul style="list-style-type: none"> • Substantial losses. • Serious violation of corporate strategies, policies, or values. • Serious reputation damage, such as negative publicity in national or international media. • Significant adverse regulatory impact, such as loss of operating licenses or material fines.
High	<p>Requires Urgent Management Attention. This is an internal control or risk management issue that could lead to:</p> <ul style="list-style-type: none"> • Financial losses. • Loss of controls within the organizational entity or process being reviewed. • Reputation damage, such as negative publicity in local or regional media. • Adverse regulatory impact, such as public sanctions or immaterial fines.
Medium	<p>Requires Management Attention. This is an internal control or risk management issue, the solution to which may lead to improvement in the quality and/or efficiency of the organizational entity or process being audited. Risks are limited. Improvements that will enhance the existing control framework and/or represent best practice</p>

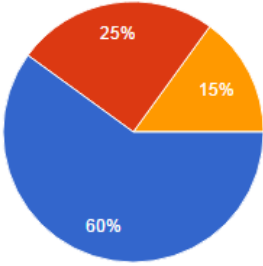
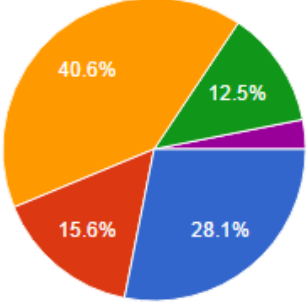
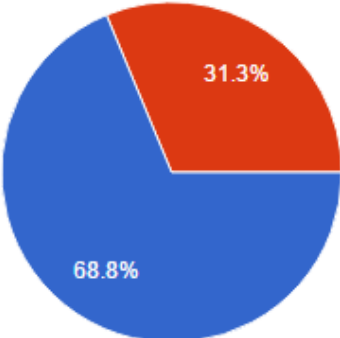
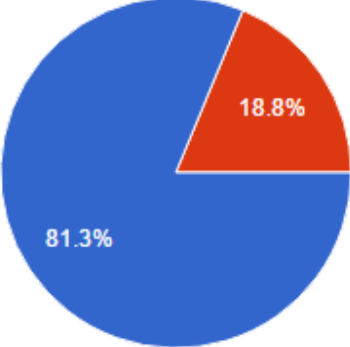
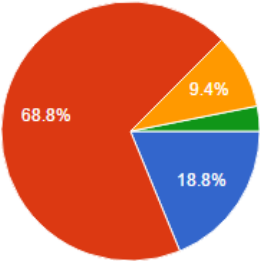
[Annex II follows]

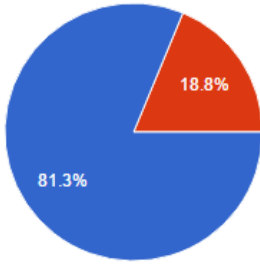
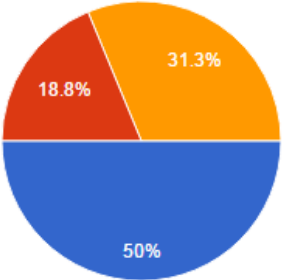
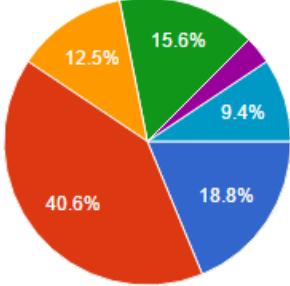
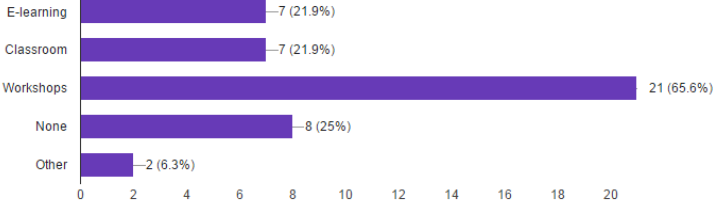
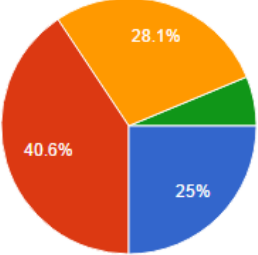
ANNEX II – RESULTS OF BENCHMARKING SURVEY CONDUCTED WITH UNITED NATIONS AND OTHER INTERNATIONAL ORGANIZATIONS (32 RESPONSES)

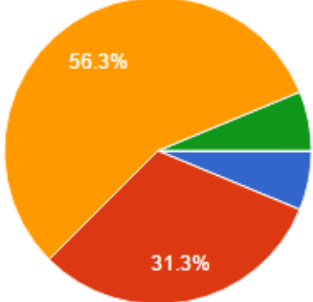
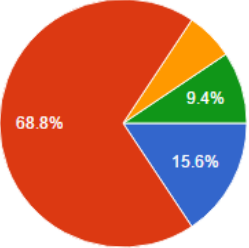
<p>Seventy-five percent of the respondents had a formal ERM framework and process in place.</p> <p>WIPO is among the respondents with a formal ERM framework and process.</p>	 <p>Legend: Yes (Blue), No (Red)</p> <table border="1"> <tr><th>Response</th><th>Percentage</th></tr> <tr><td>Yes</td><td>75%</td></tr> <tr><td>No</td><td>25%</td></tr> </table>	Response	Percentage	Yes	75%	No	25%						
Response	Percentage												
Yes	75%												
No	25%												
<p>Of those respondents which have a formal ERM framework, a significant proportion has implemented this within the last three years.</p> <p>WIPO is among the respondents which have implemented a formal ERM process in the past three years.</p>	 <p>Legend: 0 to 3 years (Blue), 3 to 5 years (Red), More than 5 years (Yellow)</p> <table border="1"> <tr><th>Timeline</th><th>Percentage</th></tr> <tr><td>0 to 3 years</td><td>45.8%</td></tr> <tr><td>3 to 5 years</td><td>16.7%</td></tr> <tr><td>More than 5 years</td><td>37.5%</td></tr> </table>	Timeline	Percentage	0 to 3 years	45.8%	3 to 5 years	16.7%	More than 5 years	37.5%				
Timeline	Percentage												
0 to 3 years	45.8%												
3 to 5 years	16.7%												
More than 5 years	37.5%												
<p>Thirty-three percent of respondents with a formal ERM framework used the COSO ERM framework as the basis. Another 16.7% used the ISO 31000 framework as the basis for their ERM. Yet another 16.7% used a combination of COSO ERM and ISO 31000. In total, 66.7% of respondents used either COSO ERM, ISO 31000 or a combination of the two.</p> <p>WIPO's risk management policy is based on the COSO Internal Control – Integrated Framework as it is applied by the INTOSAI guidelines for internal control standards in the public sector.</p>	 <p>Legend: Yes, COSO ERM (Blue), Yes, ISO 31000 (Red), Yes, COSO ERM and ISO 31000 (Yellow), No (Green), Other (Purple)</p> <table border="1"> <tr><th>Framework</th><th>Percentage</th></tr> <tr><td>Yes, COSO ERM</td><td>33.3%</td></tr> <tr><td>Yes, ISO 31000</td><td>16.7%</td></tr> <tr><td>Yes, COSO ERM and ISO 31000</td><td>16.7%</td></tr> <tr><td>No</td><td>16.7%</td></tr> <tr><td>Other</td><td>16.7%</td></tr> </table>	Framework	Percentage	Yes, COSO ERM	33.3%	Yes, ISO 31000	16.7%	Yes, COSO ERM and ISO 31000	16.7%	No	16.7%	Other	16.7%
Framework	Percentage												
Yes, COSO ERM	33.3%												
Yes, ISO 31000	16.7%												
Yes, COSO ERM and ISO 31000	16.7%												
No	16.7%												
Other	16.7%												
<p>Eighty-seven percent of respondents with a formal ERM process have developed explicit guidelines on ERM.</p> <p>WIPO has developed guidelines on ERM.</p>	 <p>Legend: Yes (Blue), No (Red), In progress (Yellow)</p> <table border="1"> <tr><th>Response</th><th>Percentage</th></tr> <tr><td>Yes</td><td>87.5%</td></tr> <tr><td>In progress</td><td>12.5%</td></tr> <tr><td>No</td><td>0%</td></tr> </table>	Response	Percentage	Yes	87.5%	In progress	12.5%	No	0%				
Response	Percentage												
Yes	87.5%												
In progress	12.5%												
No	0%												

<p>A majority of the respondents with a formal ERM framework have defined risk management policies (91.7 %). While 62.7% had a risk manual and guidelines, only 25% of respondents had defined a risk appetite statement.</p> <p>WIPO has a formal risk management policy, risk management manual and guidelines and defined risk appetite statement.</p>	<table border="1"> <thead> <tr> <th>Category</th> <th>Count</th> <th>Percentage</th> </tr> </thead> <tbody> <tr> <td>Risk manag...</td> <td>22</td> <td>91.7%</td> </tr> <tr> <td>Risk appetit...</td> <td>6</td> <td>25%</td> </tr> <tr> <td>Risk manual...</td> <td>15</td> <td>62.5%</td> </tr> <tr> <td>Other</td> <td>3</td> <td>12.5%</td> </tr> </tbody> </table>	Category	Count	Percentage	Risk manag...	22	91.7%	Risk appetit...	6	25%	Risk manual...	15	62.5%	Other	3	12.5%
Category	Count	Percentage														
Risk manag...	22	91.7%														
Risk appetit...	6	25%														
Risk manual...	15	62.5%														
Other	3	12.5%														
<p>Of those respondents without a formal ERM process in place, a majority (62.5%) have a partial process in place where some risk areas of the organization have been addressed.</p>	<table border="1"> <thead> <tr> <th>Category</th> <th>Percentage</th> </tr> </thead> <tbody> <tr> <td>Partial enterprise-wide risk management process in place (i.e.,...)</td> <td>62.5%</td> </tr> <tr> <td>Other</td> <td>12.5%</td> </tr> <tr> <td>Currently investigating concept of enterprise-wide risk management, but have made no decisions yet</td> <td>25%</td> </tr> <tr> <td>No formal enterprise-wide risk management process in place, but...</td> <td>0%</td> </tr> <tr> <td>No enterprise-wide management process in place</td> <td>0%</td> </tr> </tbody> </table>	Category	Percentage	Partial enterprise-wide risk management process in place (i.e.,...)	62.5%	Other	12.5%	Currently investigating concept of enterprise-wide risk management, but have made no decisions yet	25%	No formal enterprise-wide risk management process in place, but...	0%	No enterprise-wide management process in place	0%			
Category	Percentage															
Partial enterprise-wide risk management process in place (i.e.,...)	62.5%															
Other	12.5%															
Currently investigating concept of enterprise-wide risk management, but have made no decisions yet	25%															
No formal enterprise-wide risk management process in place, but...	0%															
No enterprise-wide management process in place	0%															
<p>Forty-six percent of respondents considered that the current maturity of risk management in their organizations was “Risk-aware” (i.e. Scattered silo-based approach to risk management), while 31% classified themselves as “Risk-managed” (i.e. Enterprise wide approach to risk management; developed and communicated)</p> <p>Within this scale WIPO’s risk management maturity is considered to be “ risk-defined”</p>	<table border="1"> <thead> <tr> <th>Category</th> <th>Percentage</th> </tr> </thead> <tbody> <tr> <td>Risk-enabled (Risk management and internal control fully embedded into...)</td> <td>9.4%</td> </tr> <tr> <td>Risk-managed (Enterprise wide approach to risk management; dev...)</td> <td>31.3%</td> </tr> <tr> <td>Risk-defined (Strategies and policies in place and communicated; risk a...)</td> <td>18.8%</td> </tr> <tr> <td>Risk-aware (Scattered silo-based approach to risk management)</td> <td>40.6%</td> </tr> <tr> <td>Risk-naïve (No formal approach developed for risk management)</td> <td>0%</td> </tr> </tbody> </table>	Category	Percentage	Risk-enabled (Risk management and internal control fully embedded into...)	9.4%	Risk-managed (Enterprise wide approach to risk management; dev...)	31.3%	Risk-defined (Strategies and policies in place and communicated; risk a...)	18.8%	Risk-aware (Scattered silo-based approach to risk management)	40.6%	Risk-naïve (No formal approach developed for risk management)	0%			
Category	Percentage															
Risk-enabled (Risk management and internal control fully embedded into...)	9.4%															
Risk-managed (Enterprise wide approach to risk management; dev...)	31.3%															
Risk-defined (Strategies and policies in place and communicated; risk a...)	18.8%															
Risk-aware (Scattered silo-based approach to risk management)	40.6%															
Risk-naïve (No formal approach developed for risk management)	0%															
<p>Seventy-five percent of respondents had a central co-ordination/ oversight function for risk management and/ or internal controls.</p> <p>WIPO has a central risk management and internal controls coordination function.</p>	<table border="1"> <thead> <tr> <th>Response</th> <th>Percentage</th> </tr> </thead> <tbody> <tr> <td>Yes</td> <td>75%</td> </tr> <tr> <td>No</td> <td>25%</td> </tr> </tbody> </table>	Response	Percentage	Yes	75%	No	25%									
Response	Percentage															
Yes	75%															
No	25%															

<p>In 34% of respondents with central risk management coordination functions, the positioning of this functioning was within the office of the Chief Executive or equivalent.</p> <p>WIPO’s risk management and internal control coordination function is located within the Office of the Controller.</p>	 <ul style="list-style-type: none"> ● Office of CFO/ Controller/ Head of Finance ● Office of the Chief Executive/ Director General/ Secretary General ● Independent (with administrative reporting to the CEO) ● Not applicable ● Other
<p>Forty-three percent of respondents had clearly defined the role of their central risk coordination function in line with the Three Lines of Defense position paper of the Institute of Internal Auditors.</p> <p>WIPO is yet to align its risk management and internal control framework with the three lines model.</p>	 <ul style="list-style-type: none"> ● Yes ● No
<p>Forty- three percent of respondents had a results-based management (RBM) system to which their ERM process had been partially integrated while 28% had fully integrated their ERM process with their RBM framework.</p> <p>The ERM system in WIPO is fully linked with the expected results as per the biennial program and budget. However annual work planning activities are not directly linked to the ERM process.</p>	 <ul style="list-style-type: none"> ● Yes ● Partially ● No ● Not applicable
<p>A majority of respondents (62.5%) had processes for reporting key risks to their governing bodies and senior management, while 37.5% reported on key risks only to senior management.</p> <p>WIPO reports key risk information to Senior Management but not directly to Member States although reporting on risks is contained within the Program Performance Reports.</p>	 <ul style="list-style-type: none"> ● Yes, both Governing Body and Senior Management ● Yes, only Governing Body ● Yes, only Senior Management ● No

<p>Those respondents which reported on key risks to their governing bodies typically performed this reporting once a year (60%).</p>	 <ul style="list-style-type: none"> ● Minimal (Once a year) ● Moderate (at least twice a year) ● Frequent (at least every quarter)
<p>Those respondents reporting to senior management on key risks typically reported on a quarterly basis (40.6%).</p> <p>WIPO produces quarterly reports on risk management for its senior management.</p>	 <ul style="list-style-type: none"> ● Yearly ● Half-yearly ● Quarterly ● Monthly ● Not applicable
<p>A majority of respondents (68.8%) had a formal management committee to review risk reports and monitor risk management progress.</p> <p>WIPO's Risk Management Group (RMG) is tasked with oversight of the risk management process.</p>	 <ul style="list-style-type: none"> ● Yes ● No
<p>A majority of respondents (81.3%) maintained corporate risk registers.</p> <p>WIPO maintains its corporate risk registers within the Acuity STREAM system.</p>	 <ul style="list-style-type: none"> ● Yes ● No
<p>Spreadsheets are used by majority of respondents (68.8) to maintain risk registers. A smaller proportion of respondents have invested in specialized risk management software for the purpose (18.8%)</p> <p>WIPO uses Acuity STREAM system, which is a specialized off-the-shelf risk management platform.</p>	 <ul style="list-style-type: none"> ● Specialized Risk Management Software (could be off-the-shelf or developed in-house) ● Spreadsheets ● Not applicable ● Other

<p>A large number of respondents (81.3%) have conducted risk identification and assessment sessions within their organizations.</p> <p>WIPO does not conduct risk identification and assessment sessions although support is provided to programs as required.</p>	 <p>Legend: Yes (Blue), No (Red)</p> <table border="1"> <thead> <tr> <th>Response</th> <th>Percentage</th> </tr> </thead> <tbody> <tr> <td>Yes</td> <td>81.3%</td> </tr> <tr> <td>No</td> <td>18.8%</td> </tr> </tbody> </table>	Response	Percentage	Yes	81.3%	No	18.8%												
Response	Percentage																		
Yes	81.3%																		
No	18.8%																		
<p>Self-assessments were the most common method (50%) used for conducting risk-assessment sessions. Some respondents (18.8%) also conducted</p> <p>In WIPO risks are self-assessed although no sessions are held for the purpose as it is the responsibility of WIPO program managers or their alternates to keep their risk registers up-to-date.</p>	 <p>Legend: Self-assessed (Blue), Facilitated Risk sessions (Red), Other (Yellow)</p> <table border="1"> <thead> <tr> <th>Method</th> <th>Percentage</th> </tr> </thead> <tbody> <tr> <td>Self-assessed</td> <td>50%</td> </tr> <tr> <td>Facilitated Risk sessions</td> <td>18.8%</td> </tr> <tr> <td>Other</td> <td>31.3%</td> </tr> </tbody> </table>	Method	Percentage	Self-assessed	50%	Facilitated Risk sessions	18.8%	Other	31.3%										
Method	Percentage																		
Self-assessed	50%																		
Facilitated Risk sessions	18.8%																		
Other	31.3%																		
<p>The frequency of updating key risk registers was mostly annual (40.6%).</p> <p>In WIPO, program managers are reminded on a quarterly basis to update their risk registers.</p>	 <p>Legend: Not done systematically (Blue), Annually (Red), Semi-annually (Yellow), Quarterly (Green), Monthly (Purple), Other (Cyan)</p> <table border="1"> <thead> <tr> <th>Frequency</th> <th>Percentage</th> </tr> </thead> <tbody> <tr> <td>Not done systematically</td> <td>18.8%</td> </tr> <tr> <td>Annually</td> <td>40.6%</td> </tr> <tr> <td>Semi-annually</td> <td>12.5%</td> </tr> <tr> <td>Quarterly</td> <td>15.6%</td> </tr> <tr> <td>Monthly</td> <td>6.3%</td> </tr> <tr> <td>Other</td> <td>9.4%</td> </tr> </tbody> </table>	Frequency	Percentage	Not done systematically	18.8%	Annually	40.6%	Semi-annually	12.5%	Quarterly	15.6%	Monthly	6.3%	Other	9.4%				
Frequency	Percentage																		
Not done systematically	18.8%																		
Annually	40.6%																		
Semi-annually	12.5%																		
Quarterly	15.6%																		
Monthly	6.3%																		
Other	9.4%																		
<p>A large proportion of respondents had formal ERM training in place in the form of workshops (65.5%).</p> <p>In WIPO, ERM training has been provided through a combination of workshops, classroom and online training.</p>	 <table border="1"> <thead> <tr> <th>Method</th> <th>Count</th> <th>Percentage</th> </tr> </thead> <tbody> <tr> <td>E-learning</td> <td>7</td> <td>21.9%</td> </tr> <tr> <td>Classroom</td> <td>7</td> <td>21.9%</td> </tr> <tr> <td>Workshops</td> <td>21</td> <td>65.6%</td> </tr> <tr> <td>None</td> <td>8</td> <td>25%</td> </tr> <tr> <td>Other</td> <td>2</td> <td>6.3%</td> </tr> </tbody> </table>	Method	Count	Percentage	E-learning	7	21.9%	Classroom	7	21.9%	Workshops	21	65.6%	None	8	25%	Other	2	6.3%
Method	Count	Percentage																	
E-learning	7	21.9%																	
Classroom	7	21.9%																	
Workshops	21	65.6%																	
None	8	25%																	
Other	2	6.3%																	
<p>The communication of risk information within respondent organizations was mostly through scheduled discussions at management meetings (40.6%)</p> <p>The RMG in WIPO meets on a quarterly basis to review the risk management reports.</p>	 <p>Legend: Ad-hoc discussions at management meetings (Blue), Scheduled agenda discussion at management meetings (Red), Written reports prepared either: monthly, quarterly, or annually (Yellow), Other (Green)</p> <table border="1"> <thead> <tr> <th>Method</th> <th>Percentage</th> </tr> </thead> <tbody> <tr> <td>Ad-hoc discussions at management meetings</td> <td>25%</td> </tr> <tr> <td>Scheduled agenda discussion at management meetings</td> <td>40.6%</td> </tr> <tr> <td>Written reports prepared either: monthly, quarterly, or annually</td> <td>28.1%</td> </tr> <tr> <td>Other</td> <td>6.3%</td> </tr> </tbody> </table>	Method	Percentage	Ad-hoc discussions at management meetings	25%	Scheduled agenda discussion at management meetings	40.6%	Written reports prepared either: monthly, quarterly, or annually	28.1%	Other	6.3%								
Method	Percentage																		
Ad-hoc discussions at management meetings	25%																		
Scheduled agenda discussion at management meetings	40.6%																		
Written reports prepared either: monthly, quarterly, or annually	28.1%																		
Other	6.3%																		

<p>The discussion of top risk exposures when the strategic plans of the organization are discussed is not fully consistent.</p>	 <ul style="list-style-type: none"> ● Extensively ● Mostly ● Somewhat ● Rarely ● None
<p>A majority (68.8%) of respondents have only partial documentation of their internal controls within their organizations.</p> <p>WIPO is in the process of documenting its internal controls and linking them to identified and assessed risks.</p>	 <ul style="list-style-type: none"> ● Comprehensive (key business processes fully mapped with controls identified and linked to risks) ● Partial (controls identified and linked to risks but not mapped) ● None (No internal controls documentation) ● Other

[End of Annex II and of document]