



Internal Oversight Division

Reference: IA 2020-01

IOD Report

Assurance Mapping of WIPO

July 13, 2020

Note: Certain parts of this report have been redacted before publication due to security, safety or privacy reasons and as per Internal Oversight Charter paragraph 36

TABLE OF CONTENTS

LIST OF ACRONYMS..... 3

EXECUTIVE SUMMARY..... 4

1. BACKGROUND..... 5

2. ENGAGEMENT OBJECTIVES 6

3. ENGAGEMENT SCOPE AND METHODOLOGY..... 6

4. ENGAGEMENT RESULT - OUTCOME 7

5. ENGAGEMENT RESULTS – POSITIVE DEVELOPMENTS..... 8

6. ENGAGEMENT RESULTS - OBSERVATIONS AND RECOMMENDATIONS 8

 (A) ASSURANCE GOVERNANCE..... 8

 (B) ASSURANCE PROVIDERS..... 9

 (i) First Line of Defense.....9

 (ii) Second Line of Defense10

 (iii) Third Line of Defense10

 (iv) External Assurance Providers.....10

 (C) ASSURANCE FRAMEWORKS AND PROCESSES.....11

 (D) ASSURANCE SYSTEMS AND TOOLS.....13

 (i) Updating Risk Registers with Validated Controls Linked to Risks15

 (ii) Enhancing Formulation of Risk and Control Information15

 (iii) Gaps in Assurance Map.....16

 (E) LEVEL OF RELIANCE ON ASSURANCE PROVIDERS16

 (F) INTERNAL AUDIT CAPABILITY MODEL AND ROAD MAP.....17

TABLE OF RECOMMENDATIONS20

ANNEXES.....21

LIST OF ACRONYMS

AIMS	Administrative Integrated Management System
BI	Business Intelligence
CMP	Capital Master Plan
DPPF	Department of Program Planning and Finance
EPM	Enterprise Performance Management
ER	Expected Result
ERM	Enterprise Risk Management
ERP	Enterprise Resource Planning
IA	Internal Audit
IAOC	Independent Advisory Oversight Committee
IC	Internal Controls
ICT	Information, Communications and Technology
IEC	International Electro-technical Commission
IIA	Institute of Internal Auditors
IOD	Internal Oversight Division
IP	Intellectual Property
IPPF	International Professional Practice Framework
ISO	International Organization for Standardization
ISOC	Information Security Operations Center
IT	Information Technology
JIU	Joint Inspection Unit
PCT	Patent Cooperation Treaty
PPBD	Program Performance and Budget Division
RM	Risk Management
RMG	Risk Management Group
SIAD	Security and Information Assurance Division
UN	United Nations
WIPO	World Intellectual Property Organization

EXECUTIVE SUMMARY

1. An assurance map is a matrix comprising a visual representation of the organization's risks and all the internal and external providers of assurance services that cover those risks. This visual depiction may help to expose potential coverage gaps and duplications, whilst helping assurance providers to coordinate the timing and scope of their work. A coordinated approach to assurance helps to, among others, ensure appropriate and efficient use of resources and minimizing audit fatigue.
2. The World Intellectual Property Organization's Accountability Framework brings together the various components that provide assurance of the Organization's system of governance and accountability to its Member States. It serves as an overarching framework, setting the basis for the functioning of key elements such as risk management and the system of Internal Controls (ICs). In preparing the WIPO assurance map, the Internal Oversight Division (IOD) used the "three lines of defense" model, which is recognized by the Framework. The first line of defense (operational management), second line (risk management and compliance function) and third line (IOD) coordinate and collaborate their work to manage risks at different levels, through implementing relevant internal controls. In addition, External service providers are engaged to provide additional assurance on different business areas.
3. IOD notes that there are a number of frameworks and processes, which are an important source of assurance. These include, among others, the Risk Management Framework, Risk Management Policy, Results Based Management Framework, Organizational Resilience Strategy, and the Information Security Policies and Standards. The assurance mapping takes into account the contribution and significance of these frameworks and processes in providing a cohesive and coordinated approach to collective assurance.
4. Further, WIPO's information systems and tools have embedded controls that mitigate or reduce risks in different administrative and operational areas. These tools include, but are not limited to; the Enterprise Resource Planning (ERP) system, the Patent Cooperation Treaty (PCT) Platform, Madrid International Registrations Information System Platform, Hague Back Office Platform, Specialized information security tools and the Enterprise Risk Management (ERM) – repository of the entity's risks and associated controls.
5. Whilst these systems and tools provide support for assurance in the areas of their application, and when used in combination with others, there are still opportunities to enhance their contribution to assurance in the Organization. For example, the ERM is a key source of assurance information and therefore it is imperative that business areas/Programs proactively and continually update the tool with properly formulated and validated risks, and relevant controls. Further, a Risk and Control Mapping exercise can help enhance completeness, quality and accuracy of information in the ERM.
6. IOD notes that, based on a review of the ERM and discussions with relevant risk owners, there are no significant assurance gaps in the design of control activities of the Organization. The defense mechanisms, when used in combination with other corporate and entity specific controls, provide relevant coverage and assurance mechanism. However, there are still certain business areas with relatively high residual risks at a strategic level (e.g. Political, Economic and Competitive Environment, and Information security risks). This is mainly explained by the inherent nature of these risks and not weaknesses in the design and/or implementation of relevant controls.
7. Going forward, IOD should finalize its upgrade of continuous auditing project to expand assurance coverage, and continue to enhance collaboration and coordination with other assurance functions of WIPO with a view to (i) better align risk assessment practices; (ii) identify opportunities for synergies and efficiencies where applicable; and (iii) share relevant knowledge and information to enhance providing collective assurance.

1. BACKGROUND

8. Obtaining an assurance that the processes of an Organization operate within the established parameters is an important prerequisite to achieving its objectives and goals. This occurs when processes such as Risk Management (RM) and oversight processes are working effectively, supporting the mitigation of significant risks to acceptable levels. This assurance places reliance on information from multiple providers of assurance services, including internal providers (e.g., RM, internal control, compliance and other control functions as well as the internal audit activity) and external providers (e.g. External Auditors, Consultants and the Joint Inspection Unit (JIU) of the United Nations (UN)).

9. An assurance map is a matrix comprising a visual representation of the organization's risks and all the internal and external providers of assurance services that cover those risks. This visual depiction helps to expose the potential coverage gaps and duplications. Assurance providers may use the map to coordinate the timing and scope of their services preventing audit fatigue within areas and processes under review, except in cases where senior management or the board may need a second opinion or a double check from another assurance provider on a high-risk area.

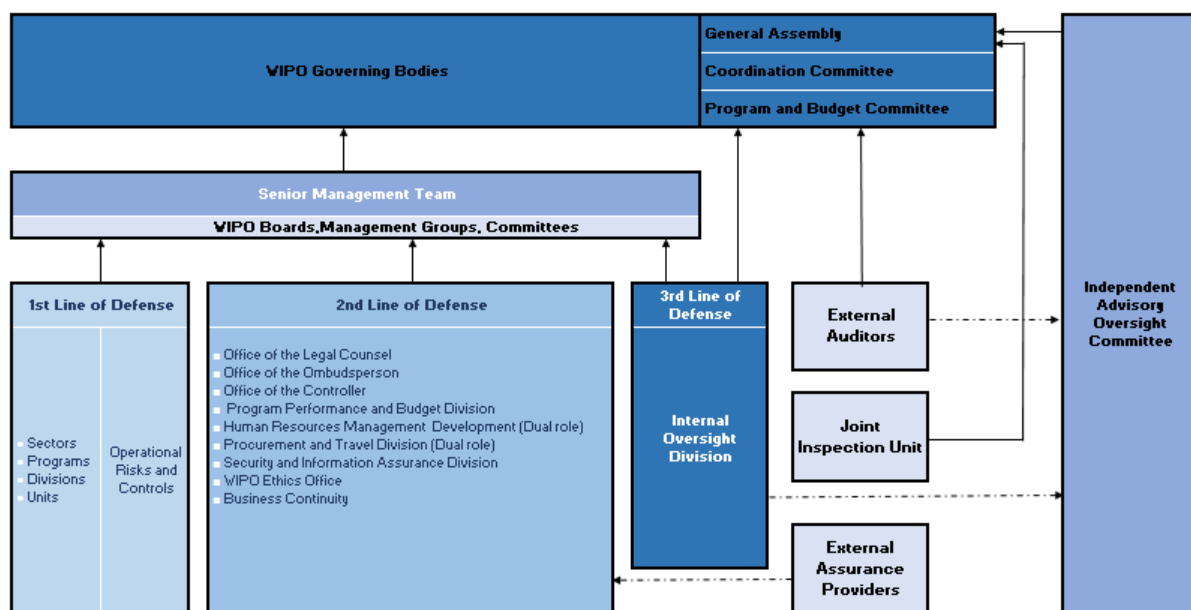
10. An assurance map can be used by various departments throughout the organization to, among others, enhance a comprehensive organization wide risk management process, advance the maturity of assurance functions and strengthen the control environment. Furthermore, the assurance mapping helps to support the Statement on Internal Control that describes the effectiveness of ICs and is signed by the Director General.

11. IOD may use an assurance map as a basis for discussion to determine whether reliance on the work of other assurance providers would be appropriate. Senior management may use the map to ensure that risk management and IC functions are properly aligned and effectively monitored.

12. In preparing the WIPO assurance map, IOD used the "three lines of defense" model. WIPO's accountability framework recognizes this model in effectively managing its risks through the implementation of internal control with a cohesive and coordinated approach.

13. In this model, operational managers are defined as the "first line" of defense – those who own and manage risks and controls during the implementation. The "second line" of defense comprises the Control Activities established by the management of the Organization to strengthen and monitor the first line of defense controls.

14. As a part of the Monitoring, Oversight, Complaints and Response Mechanisms, IOD is the "third line" of defense, while External Auditors, the Independent Advisory Oversight Committee (IAOC) and the governing bodies of Member States provide further oversight. Figure 1 below depicts the three lines of defense model with interrelations amongst assurance providers.

Figure 1: Three lines of Defense Model at WIPO

Source: Compiled by IOD based on the model developed by the Institute of Internal Auditors (IIA)

2. ENGAGEMENT OBJECTIVES

15. The objective of Assurance mapping was to:

- (a) Identify and map the assurance providers and areas covered;
- (b) Identify gaps;
- (c) Provide an overview of reliance levels; and
- (d) Propose relevant recommendations.

3. ENGAGEMENT SCOPE AND METHODOLOGY

16. The scope considered the WIPO Risk and Control universe including previous audits conducted on the related topics. The scope did not include detailed testing of operational effectiveness of all existing controls at WIPO.

17. However, IOD reviewed the design, the underlying principles, and understanding and practices of the various stakeholders in order to assess a certain level of reliance, which it could potentially place on information, data and controls from other internal assurance providers.

18. The methodology included interviews with stakeholders, analyses and review of relevant supporting documentation, and walkthroughs tests, in order to:

- (a) Identify the sources of risk information;
- (b) Organize risks into risk categories;
- (c) Identify assurance providers;

- (d) Gather information and documenting assurance activities by risk category;
- (e) Identify “assurance gaps”, duplications and/or overlaps of RM and IC efforts; and
- (f) Perform a preliminary assessment of reliance on different assurance providers through a maturity assessment.

19. The engagement examined policies and procedures that were operational during the performance of audit procedures.

20. The engagement was not intended to be a full audit of the effectiveness of the operation in the practice of assurance activities at WIPO. The engagement was to offer a map that provides an overview of the key assurance mechanisms in place, with a view to providing a preliminary impression on reliance.

21. The assurance map is an evolving document as the assurance activities evolve and mature. This engagement is thus a starting point and snapshot that will evolve over time as the Organization’s assurance activities mature¹.

4. ENGAGEMENT RESULT - OUTCOME

22. The initial objectives and outcomes of the assurance mapping exercise are summarized below.

Engagement Objectives	Outcome(s)
(a) Identify and map the assurance providers and areas covered;	Description of assurance providers through three lines of defense model, description of assurance process, tools, and systems. The summarized assurance map can be found under Annex II.
(b) Identify gaps;	IOD notes that there are no significant assurance gaps in the design of control activities of the Organization. The defense mechanisms, when used in combination with other corporate and entity specific controls, provide a relevant coverage and assurance mechanism.
(c) Provide an overview of reliance levels;	WIPO functions are at different levels of maturity on the reliance that can be placed on their assurance activities. The level varies due to a number of factors, such as the maturity of controls owned by functions, the formality of risk-assessment processes and other criteria as indicated in Annex V. IOD self-assessment can be found under section 6.F - Internal audit capability model.
(d) Propose relevant corrective actions.	IOD found that enhancing the “pro-activeness” of business areas in updating of risk and controls, can help improve the completeness, quality and accuracy of information in the ERM. A recommendation has been made at the end of this report concerning enhancing coordination among assurance providers. IOD should also finalize the upgrade of its data analytics and continuous auditing activities

¹ According to the Annual Risk Management Report 2019, WIPO has carried out a risk management maturity self-assessment in the context of the UN High Level Committee on Management Reference Maturity Model for risk management. Assessed levels of maturity: Enterprise risk management framework and policy – level 4 (advanced); Governance and organizational structure – level 4 (advanced); Process and integration – level 4 (advanced); Systems and tools – level 4 (advanced); Risk capabilities - level 2 (developing); Risk culture - level 2 (developing).

5. ENGAGEMENT RESULTS – POSITIVE DEVELOPMENTS

23. The IOD notes the following positive developments in supporting assurance activities in WIPO:

(a) Results-Based Management (RBM) System: The system is one of the important crosscutting controls of the Program Performance and Budget Division (PPBD). RBM is a critical management tool designed to enhance responsibility, organizational learning and accountability in the implementation of WIPO programs and budgets. While RBM does not provide any direct assurance itself, it is a powerful tool for enforcing and monitoring the effective management of organizational activities.

(b) Business Intelligence (BI) Dashboards: WIPO has developed a number of BI dashboards, which display the status of business analytics, metrics, key performance indicators and important data points for WIPO departments, teams or processes. These dashboards are useful tools providing indications on certain levels of assurance for processes in the area of Human Resources, Finance, Procurement and Travel, Program Performance and Budget and Risk Management. Furthermore, the Organization has implemented data analytics to further support ICs and risk management.

(c) Systems and tools: The Organization has developed and implemented a number of systems and tools that contribute to enhancing and facilitating assurance. For example, the ERP system provides automated workflows and controls that facilitate adherence to regulations, rules and procedures, and an audit trail. Further, the ERM, a risk management solution, gives visibility into various risk levels of WIPO Programs.

(d) In addition, the Security and Information Assurance Division (SIAD) has implemented specialized information assurance and security processes, controls and tools that contribute to the overall assurance position of the Organization. Further, the systems and tools help facilitate segregation of duties and application of internal control mechanisms that operationalize the controls. The standard and customized reports from these systems facilitate control and monitoring by the first and second lines of defense.

(e) Other positive developments include: the establishment and maturing of the ERM function, the mapping of processes, the identification of controls for key administrative processes and anti-fraud program.

6. ENGAGEMENT RESULTS - OBSERVATIONS AND RECOMMENDATIONS

24. Below are the main observations made on assurance mapping in WIPO.

(A) ASSURANCE GOVERNANCE

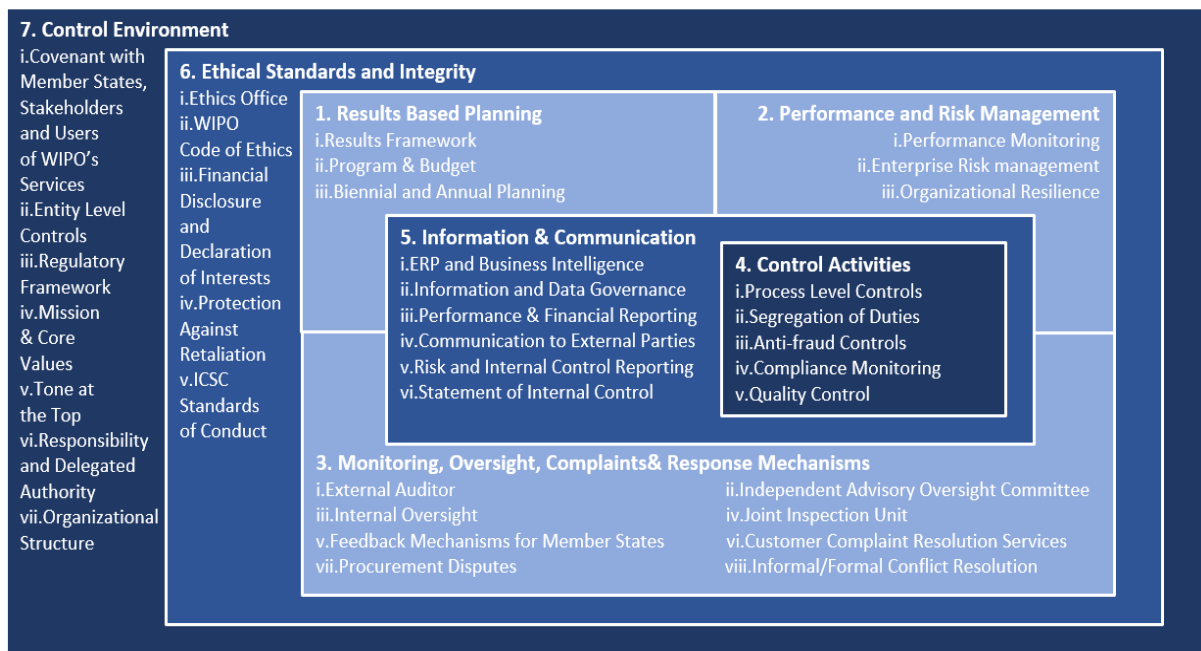
25. **The WIPO Accountability Framework²** brings together the various components that provide assurance of the Organization's system of governance and accountability to its Member States. It serves as an overarching framework document setting the basis for the functioning of key elements such as Risk Management and the System of ICs.

26. Figure 2 below depicts the WIPO Accountability framework. This model reflects a collaboration between Assurance Providers ("People"), Assurance Processes ("Processes"),

² WO/PBC/29/4

and Assurance Technology (“Technology”)³, leading to the achievement of WIPO Strategic Objectives. Further, in the report the IOD analyzes and maps the extent of assurance that these three elements provide.

Figure 2: WIPO Accountability Framework



Source: Compiled by IOD based on the model provided by WIPO Accountability Framework¹

27. Further, a number of information risk management processes exist (nine in total), which include, among others, annual ISO 27001 risk assessments performed by independent external auditors, external penetration testing, certification and accreditation, third party risk assessments and vulnerability assessments.

28. In addition, there are other mechanisms under Performance and Risk Management such as Monitoring, Oversight, and Complaints and Response mechanisms.

(B) ASSURANCE PROVIDERS

(i) First Line of Defense

29. WIPO's Operational management, or line management, is responsible for maintaining effective ICs within the systems and processes. As the “risk owners”, this group aims at ensuring that business risks are addressed, and contribute to achieving ERs.

30. From the reliability of assurance perspective, this line is operational and hence does not have the sufficient objectivity and independence regarding their own risk management and control practices. However, this line provides valuable inputs and insights on business and operational experiences and daily challenges.

31. With regards to WIPO, the mandate, organizational structure, procedures, and integrated nature of systems require some Programs/business areas that are primarily operational management, to also have some embedded second line of defense activities.

³ People Process Technology is a holistic model, which considers that to improve the overall organization, the efforts need to be focused on these three areas. The model is widely used across industries.

32. For instance, the Procurement and Travel Division, Department of Program Planning and Finance (DPPF), and Human Resources Management Development have certain dual roles, with some of their services/functions/duties falling under either first line, or second line (i.e. compliance/control functions).

(ii) Second Line of Defense

33. The WIPO risk and compliance functions provide oversight of management activities performed by the first line of defense. Risk and compliance functions also help provide assurance that regulatory, environmental, ethical, quality, and other essential requirements are met. Compliance functions monitor regulatory requirements related to health and safety, information assurance, etc. Second line activities also include assessing the accuracy and completeness of reports provided by the first line of defense and reviewing automated monitoring processes and organizational databases. Functions that provide second line assurance are not systematically independent from the first line of defense, however, reliance can be placed on their assurance when they demonstrate a certain degree of competence and objectivity.

34. For instance, the Office of the Controller, which falls under the DPPF, amongst other duties, is responsible for comprehensive risk reporting and development of the Organization's risk and ICs management strategy. The Risk and Internal Control Manager, working in the Office of the Controller, is responsible for, among others, coordinating the risk and control management processes of the Organization, escalating risk management and internal control issues to the Risk Management Group (RMG), and ensuring that organization-level risks are adequately identified and recorded in the risk management system of the Organization.

35. Further, the SIAD plays a key role in, among others, helping to safeguard information assets, staff, delegates and physical assets, through the implementation of security and information assurance strategies, continual assessment and monitoring of security and information security threats and risks, performing procedural and technical security checks, and ensuring the compliance with the regulatory framework.

36. Information from risk areas covered by second line functions, including the results of their evaluations and the extent and quality of their work, provide valuable input for the assurance map.

(iii) Third Line of Defense

37. WIPO's third line of defense, IOD, as per Internal Oversight Charter⁴, is an independent internal oversight body. It supports the Director General in his management responsibilities and assists Program Managers in attaining WIPO's objectives. The Internal Oversight Charter, approved by the WIPO General Assembly, governs the work of IOD. IOD engages with the various stakeholders, internal and external in determining, planning and providing assurance coverage.

(iv) External Assurance Providers

38. WIPO regularly engages External assurance providers to provide assurance on different business areas. WIPO pays significant attention to the scope of work of External assurance providers, the objectivity and competence of the parties involved, the rigor of the assessment and testing processes, and the timeliness of the conclusions.

39. For example, the External Auditors provide independent assurance to Member States on WIPO financial statements and add value to the financial management and

⁴ Annex I to the WIPO Financial Regulations and Rules.

governance whilst other specialized firms provide assurance in the areas of information security and cybersecurity.

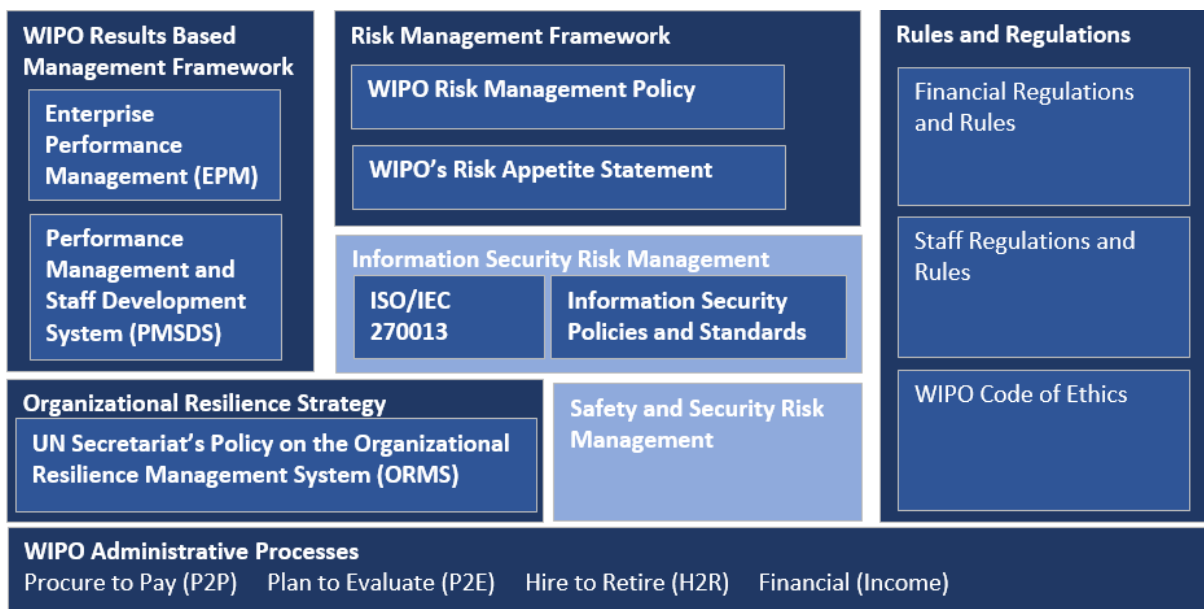
40. In addition, the JIU, an independent external oversight body of the UN system, is mandated to conduct evaluations, inspections and investigations system-wide. The work of the JIU contributes to providing assurance to WIPO on a number of cross cutting issues.

41. Annex II of the report represents the Assurance Map, where IOD has summarized the WIPO assurance providers and the estimated level of assurance they provide. The Assurance Map is based on the data “snapshot” from WIPO information systems (ERM and BI) and the IOD analysis, performed in February 2020. To be relevant, the Assurance Map must be regularly updated.

(C) ASSURANCE FRAMEWORKS AND PROCESSES

42. The Figure 3 below displays the WIPO Main Frameworks and Processes, which are considered important sources of assurance.

Figure 3: Frameworks and Processes



Source: Compiled by IOD

43. **WIPO Risk Management Framework** is guided by the risk appetite noted by Member States in **WIPO Risk Appetite Statement**⁵, updated in 2019. This Risk Appetite Statement forms one element of a comprehensive risk management framework, which has been developed over the past four biennia, and is, in turn, one element of WIPO's Accountability Framework⁶

44. The **RMG**⁷ was established in 2016 to promote a culture of responsible and effective financial and risk management in the Organization. The RMG reviews and monitors WIPO's financial situation and the key risks to the achievement of the Organization's ERs. It approves the risk strategy and proposes a suitable Organizational risk appetite for approval by Member States.

⁵ WO/PBC/29/5

⁶ WO/PBC/29/4

⁷ OI 33/2016

45. The **WIPO Risk Management Policy**⁸ sets out WIPO's approach to managing risks and ICs in a consistent and business-oriented manner in order to support the achievement of its strategic goals and ERs. As a complementary document to the Risk Management Policy, there is a Risk and Internal Control Management Manual⁹ in place, which further covers the day-to-day operational details of managing risks and controls at WIPO. Further, the **Risk and Internal Control Management Manual**, which covers the day-to-day operational details of risk and control management at WIPO, complements this policy document.

46. **WIPO Results Based Management Framework** presented in the Organization's Program and Budget consists of Strategic Goals cascaded into ERs. The contribution of WIPO Programs to ERs is defined through Performance Indicators, which have baselines and targets established for the biennium.

47. The Results Based Management Framework, approved by Member States, comprises a set of organizational expected results implemented through the Program and Budget and annual work plans. It is supported both by a suite of ERP tools such as the Organizations financial and human resource systems as well as Enterprise Performance Management (EPM) and BI tools, comprising biennial planning, annual work-planning, implementation and monitoring and performance assessment, reporting and analytics. The ERs are guided by the Strategic Goals in WIPO's Medium-Term Strategic Plan 2016-2021.

48. Biennial planning is operationalized through the Annual Planning process, which is supported by the **EPM system**. The EPM is one of the most important controls over the achievement of WIPO objectives.

49. A **Performance Management and Staff Development System** has been in place since 2009, setting work objectives that contribute to the Organizational ERs for every staff member.

50. WIPO undertakes proactive and continuous Information Security Risk Management through the successful maintenance of the **ISO/IEC 27001** Information Security certification covering all of WIPO's Global Intellectual Property (IP) Systems and some administrative processes in Finance. The certification is verified annually by independent certification bodies.

51. **Information Security Policies and Standards** provide the necessary directives for secure management of WIPO's information assets. Staff members are also made aware of security threats and acceptable security behaviors through an ongoing and annual information security awareness and education program.

52. **Security Risk Management System** at WIPO provides continuous professional safety and security risk management services in the implementation of its broad Duty of Care responsibilities to staff and personnel working across all WIPO's operations, including in high-risk environments if operational needs so dictate. The WIPO Security Risk Management System has been developed using as guidance the framework for accountability for the UN Security Management System.

53. The **WIPO Organizational Resilience Strategy** identifies and focuses priority on the Organization's critical business processes and operations. WIPO has adopted the UN Secretariat's Policy on the Organizational Resilience Management System¹⁰, which is a common emergency management framework applied across all organizations in the UN system.

⁸ OI 41/2017

⁹ http://intranet.wipo.int/homepages/controller/en/documents/risk_and_internal_controls_manual.pdf

¹⁰ CEB/2014/HLCM/17

54. **Risk Management at Project and Program Level:** the Organization requires continued capital investments in the areas of premises, safety and security, and Information, Communications and Technology (ICT) initiatives in order to remain fit-for-purpose. For this purpose, there is an approved Capital Master Plan (CMP)¹¹ which has a number of high-priority ICT projects, such as, IP Portal, Enterprise Content Management, and Web Content Management System.

55. The Assurance mapping takes into account the Project and Program risk management and related controls that can affect the effective and efficient implementation of the CMP, particularly ICT projects. There are a number of mechanisms that have been put in place to manage these risks such as Project governance structures and a Project management methodology. These mechanisms are aimed at ensuring that risk management is performed at Project and Program levels.

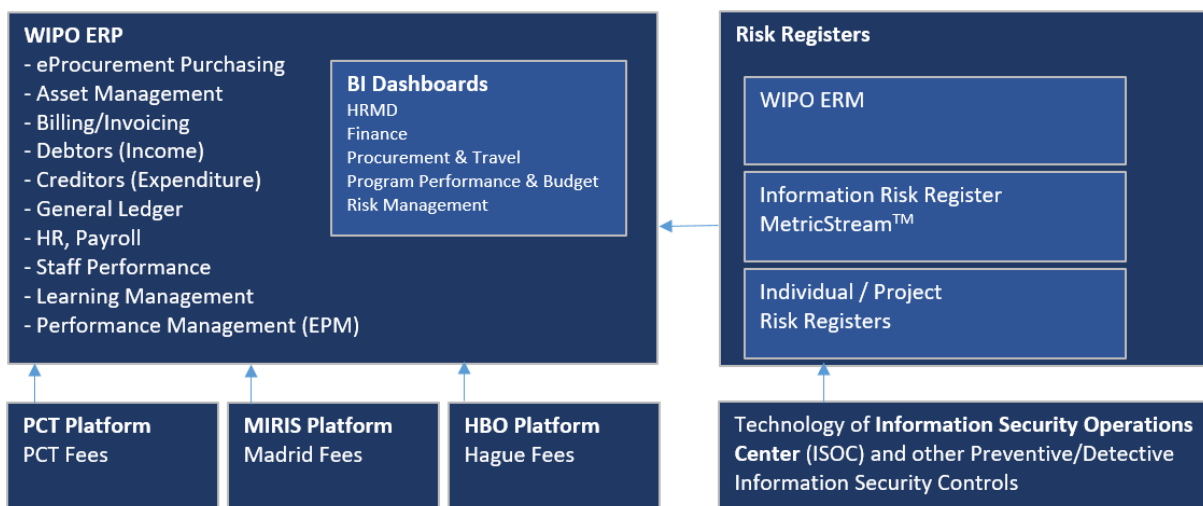
56. In addition, there are procedures in place that facilitate the identification of systematic risks or cumulative risks that exceed the risk tolerance of specific projects. These risks are then aggregated and consolidated at a corporate or strategic level, and escalated to the ERM when required. A more in-depth review of risk management including the treatment of project/program and portfolio risks will take place in the planned 2021 audit of ERM.

(D) ASSURANCE SYSTEMS AND TOOLS

57. Technology plays significant role at WIPO. Controls imbedded in WIPO's information systems and tools mitigate or reduce risks in different administrative and operational areas. The tools developed based on existing information systems provide additional assurance in the areas of their application.

58. Figure 4 below illustrates main WIPO information systems and tools from the Assurance and Risk Management perspective.

Figure 4: WIPO Main Information Systems and Tools



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

59. **WIPO ERP** modules contain extensive number of controls including anti-fraud related controls to mitigate risks. Some of the main controls imbedded in the Administrative Integrated Management System (AIMS) are as follows:

¹¹ https://www.wipo.int/edocs/mdocs/govbody/en/wo_pbc_30/wo_pbc_30_11.pdf

- (a) Segregation of Duties is systematically enforced by the ERP to reduce opportunities for fraudulent, malicious, or unintentional erroneous actions. A module of the ERP system is used to ensure that such roles are defined and assigned in line with delegated authority;
- (b) Transaction data validation - all transaction data are validated at the time of entry;
- (c) End-to-end commitment control through the procurement and travel processes;
- (d) Automated workflow processes, ensuring four-eyes principle;
- (e) Single integrated system used by all sections of the Organization for finance, commitment control, procurement, and travel related transactions; and
- (f) Controls over duplication of data entry across end-to-end processes with business users creating Requisitions, buyers converting this data into Purchase Orders, and financial transactions (reservations and obligations) being automatically created by the system.

60. **BI** is a module of the ERP system providing data to management to enable timely and transparent decision-making as well as identification of potential risks. WIPO has developed a number of BI Dashboards in the area of Finance, Human Resources, Procurement, Budgeting and Performance of Programs, and Risk Management.

61. Furthermore, the Organization is using data analytics to support ICs and cover key risk areas such as procurement and payroll. This is an ongoing exercise that is aimed at increasing the use of data analytics to support the work of the second line of defense. This is also part of the WIPO Anti-Fraud initiatives that have resulted in the updating and formalization of fraud controls across the business areas.

62. The **PCT Platform** – a customized Information Technology (IT) solution, which administers PCT fees (approximately 75 per cent of WIPO revenues). The platform has a number of controls, ensuring the completeness, existence and accuracy of revenue streams. The system provides assurance that patent applications are processed and published timely without any confidential information being compromised.

63. The **Madrid International Registrations Information System Platform** – another customized IT solution, managing Madrid fees – the second biggest source of WIPO revenues. The platform has a set of implemented controls that help to mitigate the associated risks.

64. The **Hague Back Office Platform** was introduced in 2018 and is used to administer fees for the Hague system. The Platform ensures a practically live synchronization with AIMS. The traceability of Received fee payments is ensured through the integrated payment platform EPAY2, which allows viewing and payment processing through the WIPO IP Portal. The processing of the Hague fees is covered by similar set of controls as for PCT and Madrid systems.

65. The Organization has implemented several preventive and detective controls to ensure, among others, the security of its information systems on premise and in the cloud, including a 24/7 **Information Security Operations Center (ISOC)**, endpoint security controls, network and application security controls, access controls, security architecture patterns. The technology in use by the ISOC provides continuous monitoring, detection, and response to information security incidents in the WIPO ICT environment, increasing the ability to rapidly detect and contain information security incidents.

66. The **WIPO ERM** is a repository of the entity's risks and associated controls that mitigate those risks. 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.

67. WIPO considers risks to exist at three levels: Organizational Risks (risks facing WIPO's Strategic Goals, monitored by Risk Management Group); Program Risks (Risks facing WIPO's Expected Results, monitored by Program Managers), and Project Risks (ones that could affect the achievement of a project's objective(s), monitored by Project Board and Project Managers).

68. Organizational Risks and Program Risks are kept in the WIPO ERM, while risks at the level of Projects are captured in separate **Risk Registers of Projects**. If relevant, these risks may also be recorded into WIPO ERM through the process of escalation.

69. Due to specific operational needs, the Information Security Section at WIPO is using an automated solution, MetricStream™ to manage its Information Security Governance, Risk and Compliance processes¹². The Information risks from the tool are regularly communicated to the ERM at more aggregated level on a manual basis.

70. IOD makes the following observations with regards to the Risk Registers and Assurance mapping:

(i) Updating Risk Registers with Validated Controls Linked to Risks

71. The ERM needs to be continually updated with validated existing controls, linked to risks. During the meetings with different WIPO functions, IOD identified several control activities, which either were not recorded in the register or were recorded, but not linked to risks. For example, while the PPBD had several important and cross-cutting internal controls, they were not linked to specific risks in the Risk Register (refer to Annex II).

72. IOD notes that besides the annual risk assessment, continual collaborative work between the Office of the Controller and Program Managers has resulted in relevant business areas updating their risks and controls. For example, following a series of Fraud Awareness workshops, various business areas have updated the Risk Register with relevant fraud risks and controls. This is depicted in Annex III to the report.

(ii) Enhancing Formulation of Risk and Control Information

73. Through interviews with relevant Risk/Control owners and detailed review of the ERM, IOD notes that certain business areas still need assistance (facilitation) in the proper formulation of risks and controls. For example, IOD observed that some control descriptions in the ERM are vaguely worded or represent plain text extracted from applicable or existing rules and regulations without having a comprehensive description of the control design.

74. Going forward, enhancing the "pro-activeness" of business areas in updating of risk and controls, can help improve the completeness, quality and accuracy of information in the ERM. This would represent a paradigm shift from the current approach where the update of the ERM is mainly driven by the Office of the Controller.

75. It would be beneficial to the Organization to continue reviewing the control descriptions in the ERM and enhancing where relevant. Further, performing a Risk and Control Mapping exercise would help to ensure that business areas update the ERM with significant controls.

¹² 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.

IOD encourages continual dialogue and interactions with a view to ensuring a consistent approach to addressing risks at multiple levels, from risk conception to assessment, and management.

(iii) Gaps in Assurance Map

76. Based on a review of the ERM and interviews with relevant designated risk owners, IOD notes that there are no significant assurance gaps in the design of control activities of the Organization. The defense mechanisms, when used in combination with other corporate and entity specific controls, provide a relevant coverage and assurance mechanism.

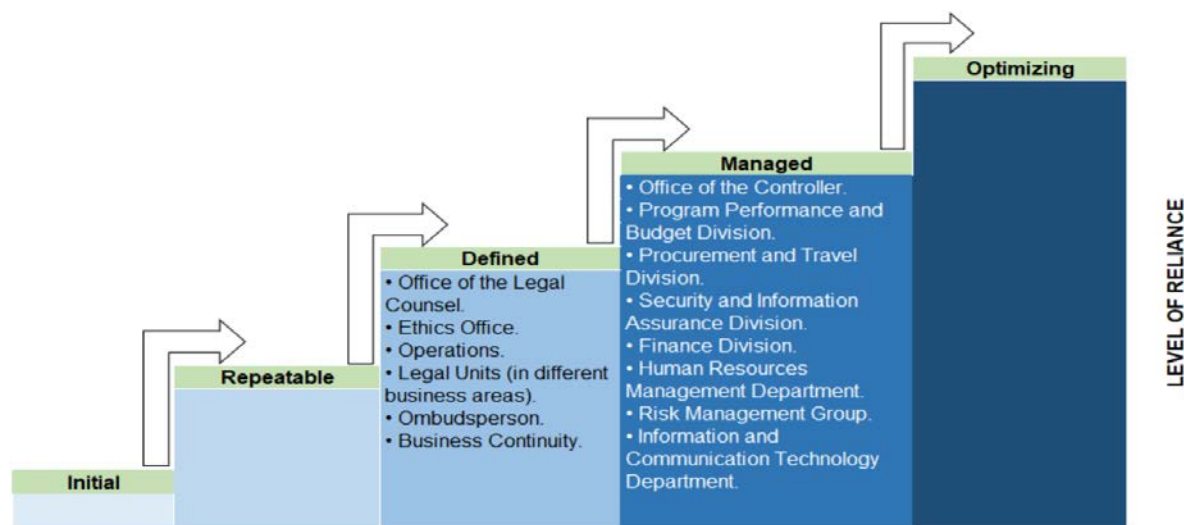
77. Further, IOD's analysis of risk data extracted from the ERM, shows that there are no significant risk categories which have not been covered by WIPO's assurance activities. However, there are still certain business areas with relatively high residual risks at a strategic level (e.g. Political, Economic and Competitive Environment, and Information security risks). This is mainly explained by the inherent nature of these risks, and not by weaknesses in the design and/or implementation of relevant controls.

(E) LEVEL OF RELIANCE ON ASSURANCE PROVIDERS

78. Various providers of assurance contribute to an overall organization-wide risk and control structure at WIPO, together assuring that risks are identified and addressed to an acceptable level. However, the providers differ in their reporting responsibilities, their level of independence from the activities over which they provide assurance and the reliability of the assurance provided.

79. When assessing the level of assurance provided it is critical to determine the extent of reliance that can be put on specific assurance provider. IOD has estimated the level of reliance on WIPO assurance providers. The assessment was based on the International Professional Practices Framework (IPPF) Practice Guide "Reliance by Internal Audit on Other Assurance Providers". According to the Practice Guide, the extent of reliance to be placed on the other internal or external assurance providers can be assessed from the perspective of the following five principles: Purpose, Independence, Competence, Elements of Practice, and Communication of Results, and Impactful Remediation. These terms are explained in Annex IV.

Figure 5: Level of Reliance on WIPO Assurance Providers (Maturity Assessment)



Source: Compiled by IOD

80. Figure 5 above illustrates IOD’s assessment of the level of reliance on WIPO internal and external assurance providers. Each assurance provider was assigned a “Reliance maturity level” on the scale of five maturity levels: “Initial” (lowest), “Repeatable”, “Defined”, “Managed”, and “Optimizing” (highest).

81. Based on IOD’s assessment, WIPO functions are at different levels of maturity on the reliance that can be placed on their assurance activities. The level varies due to a number of factors, such as the maturity of controls owned by functions, the formality of risk-assessment processes and other criteria as indicated in Annex V.

(F) INTERNAL AUDIT CAPABILITY MODEL AND ROAD MAP

82. As the third line of defense, IOD provides the WIPO IAOC and Senior management with broad range of assurance based on the audit and advisory carried out in accordance with an approved workplan. IOD provides assurance on the effectiveness of governance, risk management, and internal controls, including the manner in which the first and second lines of defense achieve risk management and control objectives. The scope of this assurance covers a broad range of objectives, including efficiency and effectiveness of operations; safeguarding of assets; reliability and integrity of reporting processes; and compliance with laws, regulations, policies, and procedures.



83. IOD performs its work in accordance with the Internationally accepted Standards and Professional Frameworks that apply to the three functions – Internal audit, Evaluations, and Investigations. However, for the purpose of the capability model, we will focus on the Internal Audit (IA) function that operates in line with the Professional Practices of Internal Auditing (Standards) issued by the IIA, the IOD IA Strategy, and the IA Manual.

84. As part of its continuous improvement efforts and adding value to the Organization, IOD has adapted an IA Capability Model. The model identifies and highlights the fundamentals needed for effective internal auditing. The model illustrates the levels and stages through which IOD IA can evolve as it defines, implements, measures, controls, and improves its processes and practices that will ultimately result in improved efficiency and effectiveness, value addition, and relevance to the Organization.

85. The levels or stages of the IA Capability Model and IOD’s Internal Audit Function’s self-assessment are shown in Figure 6 below:

Figure 6: Internal Audit Capability Model

Maturity Level	Services and Role of IA	People Management	Professional Practices	Performance Management and Accountability	Organizational Relationships and Culture	Governance Structures	Use of Technology
Level 5 - Optimizing	IA Recognized as Key agent of Change.	Leadership involvement with Professional Bodies. Workforce Projection.	Continuous involvement in Professional Practices. Strategic IA Planning.	Public Reporting of IA Effectiveness. 	Effective and Ongoing Relationships. 	Independence, Power, and Authority of the IA Activity.	Continuous Assurance of Enterprise Risk Management
Level 4 - Managed	Overall Assurance on Governance, Risk Management and Control.	IA Contributes to :  Management Development IA Activities support	Audit Strategy Leverages Organization’s Management of Risk. 	Integration of Qualitative and Quantitative Performance Measures.	CAE Advises and Influences Top Level Management.	Independent Oversight of IA Activities.  CAE Reports to Top level Authority.	Integrated Continuous Auditing and Continuous Monitoring.

		Professional Bodies. Workforce Planning.					
Level 3 - Integrated	Advisory Services. Performance/Value-for-Money Audits.	Team Building and Competency. Professionally Staff. Workforce Coordination.	Quality Management Framework. Risk Based Audit Plans.	Performance Measures. Cost Information.	Coordination with Other Review Groups. Integral Component of Management Team.	Management Oversight of the IA Activity. Funding Mechanisms.	Continuous Risk Assessment and Continuous Auditing.
Level 2 - Repeatable	Compliance Auditing.	Individual Professional Development. Skilled people Identified and Recruited.	Professional Practices and Processes Framework. Audit Plan Based on Management / Stakeholder Priorities.	IA Operational Budget. IA Business Plan.	Managing within the IA Activity.	Full Access to the Organization's Information, Assets and People. Reporting Relationships Established.	Ad-Hoc Integrated Analytics. 
Level 1 - Initial	Ad-hoc and unstructured; isolated single audits or reviews of documents and transactions for accuracy and compliance. Outputs dependent upon the skills of specific individuals holding the position. No specific professional practices established other than those provided by professional associations. Funding approved by management, as needed. Absence of infrastructure; auditors are likely part of a larger organizational unit; no established capabilities; therefore, no specific key process areas.						Traditional Auditing; No specific technologies.

Source: Compiled by IOD

86. IOD regularly seeks to advance its approach to auditing and assurance. The Division is using a maturity model that helps benchmarking the IA function using a few basic characteristics (as shown in Figure 6 above). The model provides a clear path towards achieving a data analytics-enabled internal auditing, continuous auditing, and beyond. Rooted in an IA methodology, the maturity model serves as a guide along the journey from traditional IA models towards more mature levels of continuous auditing, and management engagement, through to the continuous assurance of the ERM.

87. A key first step within the maturity model is the continual enhancement of data analytics and successful integration of continuing auditing and robotics. IOD will soon begin the project to upgrade its data analytics capabilities in order to shift to a continuous auditing setting.

88. Whilst recent IOD engagements have covered or touched on a number of significant and cross cutting risks such as those related to Economic and Competitive environment, Fraud and Information Security, more can be done to provide further and more in-depth assurance and coverage. The WIPO ERM shows a number of high residual risks, many of which are not directly dependent on WIPO operations and processes. However, these risks can affect WIPO if they materialize, and if insufficient or ineffective controls have been put in place to address them. The WIPO RMG has the authority to endorse risks above the risk appetite. Annex II and III respectively summarize assurance and control activities.

89. Going forward, more efforts should be made to enhance coordination of all assurance providers including, among others:

- (a) Reconciling the risks in the IOD oversight universe with those identified and ranked as significant in the ERM;
- (b) Actively exchanging risk and controls Information amongst assurance functions; and

(c) Aligning IOD risk rating methods to allow utilizing, to the extent possible, the WIPO ERM as a one-stop-shop for risks and controls.

90. This enhanced collaboration and coordination would facilitate comprehensive assessment and ranking of the level of maturity, and in providing collective assurance.

Recommendations

1. The Internal Oversight Division should:

(a) Engage with other assurance functions of WIPO with a view to (i) better align risk assessment practices; (ii) identify opportunities for synergies and efficiencies where applicable; and (iii) share relevant knowledge and information to enhance providing collective assurance; and

(b) Reassess the WIPO assurance map at least every two years, or as may be deemed appropriate, to determine if there are new or notable changes to assurance activities, assurance providers, or the risk profile of the Organization.

ACKNOWLEDGMENT

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

Prepared by: Dainis Reinieks, Senior Internal Auditor, IOD
Bevan Chishimba, Internal Auditor, IOD

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

Approved by: Rajesh Singh, Director, IOD.

TABLE OF RECOMMENDATIONS

No.	Recommendations	Priority	Person(s) Responsible	Other Stakeholder	Management Comments and Action Plan	Deadline
1.	<p>The Internal Oversight Division should:</p> <p>(a) Engage with other assurance functions of WIPO with a view to (i) better align risk assessment practices; (ii) identify opportunities for synergies and efficiencies where applicable; and (iii) share relevant knowledge and information to enhance providing collective assurance.</p> <p>(b) Reassess the WIPO assurance map at least every two years, or as may be deemed appropriate, to determine if there are new or notable changes to assurance activities, assurance providers, or the risk profile of the Organization.</p>	Medium	Director, IOD	Administration and Management Sector	<p>Arrange meetings with relevant second line functions to share information on assurance activities, including identifying opportunities for synergies, such as alignment with data analytics activities carried out by the Office of the Controller, or the Procurement and Travel Division.</p> <p>An internal status review of the assurance map will take place in the 2022/23 biennium to assess the evolution of the map, with a view to identifying the impact of changes in activities, processes, and tools on the collective assurance.</p>	<p>30.6.2021</p> <p>31.12.2022</p>

ANNEXES

ANNEX I.	Risk Rating and Priority Of Audit Recommendations
ANNEX II.	Assurance Map (Withheld)
ANNEX III.	Summary Of Control Activities (Withheld)
ANNEX IV.	Reliance Criteria Terminology
ANNEX V.	Elements That Are Demonstrating The Extent The Assurance Provider Meets The Principles For Reliance

[Annexes follow]

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

[Annex IV follows]

ANNEX IV: Reliance Criteria Terminology

IPPF Practice Guide “Reliance by Internal Audit on Other Assurance Providers”: Reliance Criteria Terminology

Purpose: the assurance provider is clear in purpose and committed to providing assurance on a specified risk area. For internal providers, the purpose should be established in a charter or other similar documentation. For external providers this should be provided for in a contract or statement of work.

Independence & Objectivity: the professional judgment of the assurance provider is impartial, without inappropriate interference from others. The assurance provider should demonstrate a sufficient degree of objectivity in the course of its work. Although internal assurance providers often report to management and thus are not truly independent, they can be relied on when they demonstrate appropriate objectivity and competence.

Competence: the assurance provider is knowledgeable of the risks to the organizational processes, how controls are designed to operate in response to the risks, and what constitutes a weakness or deficiency. Characteristics of proficiency for internal or external assurance providers include organizational process expertise, education level, professional experience, relevant professional certifications, continuing education, and the assurance provider’s reputation for sound judgment.

Elements of Practice: The assurance provider has established policies, programs, and procedures and follows them. In execution, assurance work is appropriately planned, supervised, documented, and reviewed. Results are based on persuasive evidence sufficient to support the level of assurance. They also should have the authority to access sufficient information to reach a conclusion

Communication of Results & Impactful Remediation: The assurance provider communicates results and ensures management takes timely action. Weaknesses and deficiencies are reported to the person directly responsible for taking corrective actions and to the members of management that have oversight responsibilities. Ongoing monitoring ensures the resolution is sustained as intended. Rigorous process and persuasive and reliable communication results in prompt corrective action. In turn, management action validates an effective assurance process that assurance information users can place greater reliance on.

[Annex V follows]

ANNEX V: Elements that Demonstrate the Extent to which Assurance Providers meet the Principles for Reliance

	Initial	Repeatable	Defined	Managed	Optimizing
Purpose of the Function	1st LoD, clearly operational functions, providing no or little assurance.	1st LoD; operational functions with some elements of assurance activities.	Specific functions that are operational by nature, but may be used as good sources of assurance. The confidentiality restrictions may limit the assurance information.	2nd LoD functions or first liners, who also perform as a 2nd LoD (dual roles).	Function's charter or objective statement provides authority and scope of assurance activities.
Independence & Objectivity	Due to their reporting lines, functions are lacking objectivity. Function's competence in the area of risks and controls keeps the assurance reliability at low level.		Although functions often report to management and thus are not fully independent, they can be relied on when they demonstrate appropriate objectivity and competence.		The professional judgment of the assurance provider is impartial, without inappropriate interference from others. The assurance provider should demonstrate a sufficient degree of objectivity in the course of its work.
Competence	The function has little knowledge of the risks to the organizational processes, how controls are designed to operate in response to the risks, and what constitutes a weakness or deficiency.		The assurance provider is knowledgeable of the risks to the organizational processes, how controls are designed to operate in response to the risks, and what constitutes a weakness or deficiency.		

<p>Risk and Control Assessment, Planning</p>	<p>Functions do not have formally assigned controls under their ownership and they do not formally assess their risks and controls. Assessment activities are not planned.</p>	<p>Functions have informal internal controls under their ownership and they informally assess their risks and controls. Informal planning of the assessment activities exists.</p>	<p>Functions have limited number of internal controls under their ownership and they formally assess their risks. Formal planning of the assessment activities exists or it is facilitated by the dedicated Risk professional.</p>	<p>Functions have extensive number of internal controls under their ownership and they formally assess their risks. Formal autonomous planning of the assessment activities exists and normally does not need facilitation by Risk Function.</p>	<p>Assurance activities are guided by appropriate policies and procedures and include plans that incorporate an assessment of risks.</p>
<p>Assurance Execution (Testing)</p>	<p>The function has no control activities.</p>	<p>The function has informal, not documented control activities with no audit trail. Tested samples are not representative for making conclusion.</p>	<p>The evidence of control activities exists, but no documented audit trails. Tested samples are sufficient for making conclusion.</p>	<p>Control activities are sufficiently documented and have an audit trail. Tested samples are sufficient for making conclusion.</p>	<p>The assurance provider has a demonstrated performance history of delivering to the established objectives and producing competent and reliable results. Documentation is maintained as an evidence of performance.</p>
<p>Reporting and Follow-up</p>	<p>No reporting and follow-up mechanisms in place.</p>	<p>Informal reporting on results of control activities and informal follow-up.</p>	<p>Formal reporting on results of control activities to direct management and formal follow-up.</p>	<p>Formal reporting on results of control activities to direct management and other involved parties (if needed) and formal follow-up.</p>	<p>The results of assurance activities are reported to an appropriate level of management and issues are tracked until they are mitigated.</p>

[End of Annexes and of Document]