IOD GRC Opinion, Building Blocks: Testing of Key Organization Controls

Internal Oversight Division

IA-2025-06.E

March 2, 2026

Table of Content

1

Executive Summary

As part of forming an annual opinion on WIPO's Governance, Risk Management and **Internal Controls** for the year ending December 31, 2025, the Internal Oversight Division (IOD) tested the design, implementation and operating effectiveness of 39 WIPO key organization-wide controls as defined by Management based on the WIPO Financial and Staff Regulations and Rules. Additionally, 10 controls related to information technology and information security were tested.

The summary of controls tested, and the results thereof are included in Section 4 of this report.

Engagement Conclusion

The 39 key organization-wide internal controls at WIPO were designed, implemented and operated effectively for the year ending December 31, 2025.	Satisfactory
The 10 organization-wide Information Technology Controls, additionally tested by IOD, were designed, implemented and operated effectively for the year ending December 31, 2025.	Satisfactory

2

Background:

System of Internal Controls – Basis for Establishment and Relevant Roles of 1st and 2nd Lines

The WIPO Accountability Framework provides a comprehensive view of the components that provide assurance of the Organization's system of governance and accountability to its Member States, customers, and other stakeholders.

The Framework is informed by the Joint Inspection Unit's (JIU) report Accountability Frameworks in the United Nations System (JIU/REP/2011/5).

The Framework draws on best practices from the public and private sectors, particularly the Committee of Sponsoring Organizations of the Treadway Commission's (COSO) Internal Control - Integrated Framework.

WIPO Internal Control Framework and System: 1st and 2nd Lines

Financial Regulation 5.1 : The **Director General** shall establish frameworks for Results-Based Management, Enterprise Risk Management, and **Internal Controls**. These frameworks shall be components of the Organization's Accountability Framework, providing assurance on performance, results and the effective and economic use of resources to Member States.

Financial Regulation 5.2 : The Director General shall establish an **Internal Control Framework and System** in accordance with relevant and prevailing best practices.

Financial Regulation 5.3 : The Director General establishes and signs an annual **Statement on Internal Control**, providing assurance to stakeholders. The Statement on Internal Control is supported by assurances from designated officials and will draw upon the internal oversight opinion of WIPO's governance, risk management and control environment.

The management of the Internal Control Framework is further delegated to the **Controller**, who must establish a robust and efficient system of delegation of authority, separation of duties, and checks and balances (**Rules 105.1 and 105.2**).

The Office of the Controller is responsible for the implementation of and compliance with WIPO's Financial Regulations and Rules, risk management, **Internal Controls**, policy development and management of cost efficiencies.

The Governance, Risk and Compliance (GRC) Section of the Planning, Budget and Risk Management Division facilitates, coordinates and manages WIPO's risk management and **Internal Control Activities**, including fraud awareness and risk assessments.

The **WIPO Accountability Framework** draws on best practices from both the public and private sectors, particularly the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Control – Integrated Framework. The Framework serves as the foundation for WIPO's Key Controls, which have been developed in alignment with COSO's three objectives and five components. WIPO Key Controls should be understood as entity-level controls, consistent with terminology commonly used within the COSO framework.

In 2025 WIPO had registered 39 Key Controls. More details are provided in Section 4.

2

Background:

System of Internal Controls – Role of Internal Oversight Division (IOD)

WIPO Internal Control Framework and System: 3rd Line

Financial Regulation 6.1: There shall be an Internal Oversight Division (IOD) to conduct independent internal audit, evaluations, inspections and investigations in accordance with the provisions of the WIPO Internal Oversight Charter (IOC) appended to the present Financial Regulations and Rules (Annex I).

IOC Para2: The mission of IOD is to provide independent and objective oversight services that enhance WIPO's operations, governance, risk management, and **internal controls** and support the achievement of the Organization's mission, goals, and objectives.

IOC Para3: … IOD objectives include:

(a) Contributing to the Organization's successful achievement of its objectives, by enhancing its decision-making and oversight, its reputation and credibility with stakeholders, and its ability to serve the public interest;

(b) Assessing the **effectiveness and efficiency** of governance, risk management, and **control processes**;

(c) Identifying means for improving WIPO's relevance, effectiveness, efficiency, and economy of the internal procedures and use of resources;

(d) Assessing whether **cost-effective controls are in place and operate effectively**; and

(e) Assessing compliance with WIPO's Financial Regulations and Rules, Staff Regulations and Rules, relevant General Assembly decisions, the applicable accounting standards, the Standards of Conduct for the International Civil Service, and relevant policies and procedures.

IOC Para 29: To carry out her/his mandate, the Director, IOD, shall conduct audits, evaluations, and investigations. The types of audits should include, but not be limited to, performance audits, financial audits, **reviews of key controls** and compliance audits.

IOC Para 31(a): In particular, the Director, IOD, shall assess the reliability, effectiveness, and integrity of **WIPO's key controls and other internal control mechanisms**.

IOC Para 34: Based on the scope of work undertaken, the Director, IOD shall issue an **annual overall opinion** on the adequacy and effectiveness of the governance, risk management, and **control processes** that impact the achievement of WIPO's objectives and Expected Results.

2

Background:

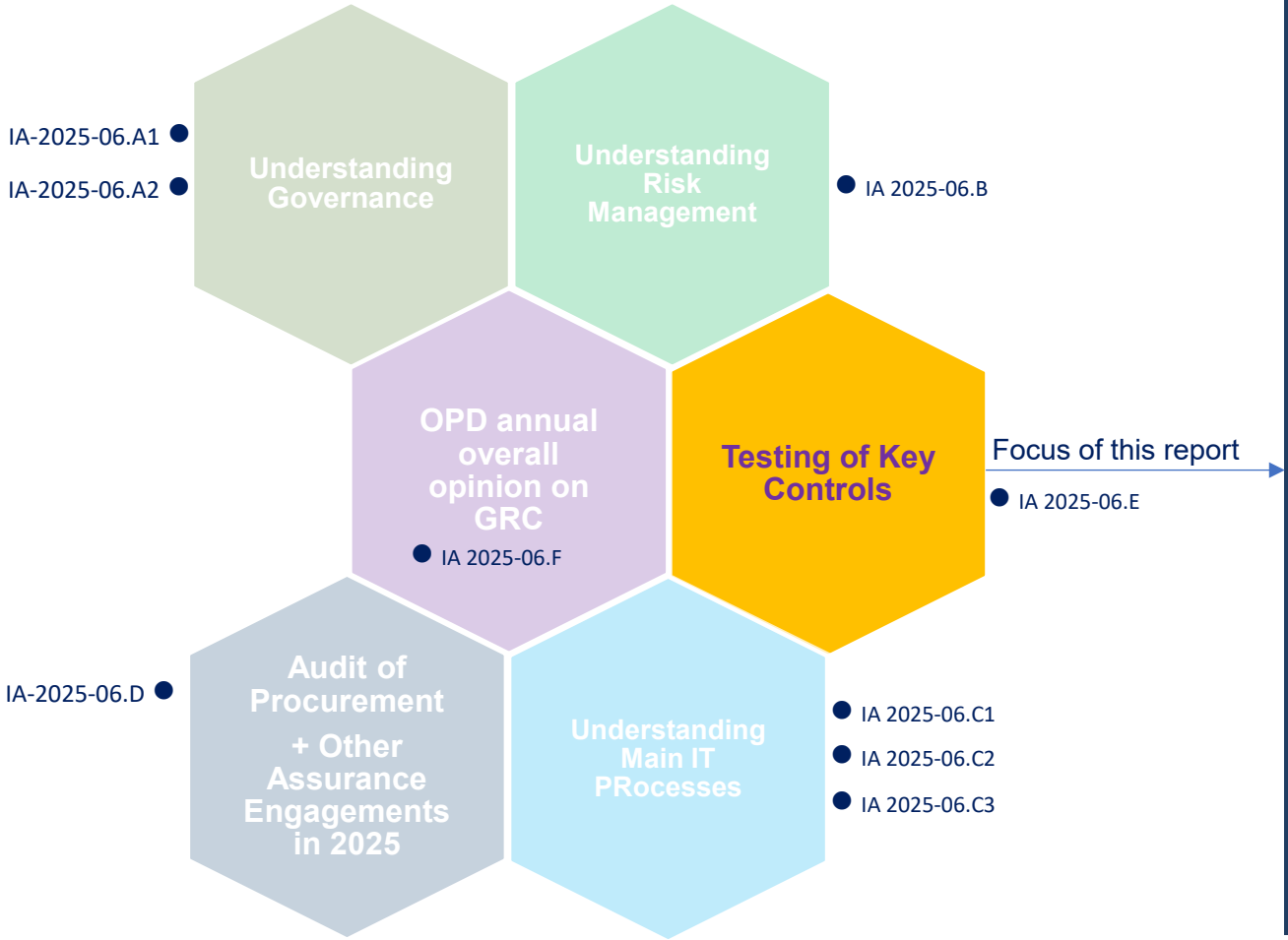
System of Internal Controls – FRR Provisions and the Focus of This Report

FRR – Financial Rules and Regulations

IOD Reports:

IA-2025-06.A1 – GRC Opinion Understanding: Governance (strategic).
IA-2025-06.A2 – GRC Opinion Understanding: Governance (operational).
IA-2025-06.B – GRC Opinion Understanding: Risk Management.
IA-2025-06.C1 – GRC Opinion Understanding: SIAD.
IA-2025-06.C2 – GRC Opinion: United Nations International Computing Centre (UNICC)
IA-2025-06.C3 – GRC Opinion: Information and Communications Technology Department (ICTD) and Cloud Service Providers
IA-2025-06.D – Not used
IA-2025-06.E – GRC Opinion: Testing of Key Controls.
IA-2025-06.F – GRC Opinion : Overall Opinion.

Work informing the Overall Opinion and Focus of this IOD Engagement



Guiding Principles of FRR:

Rule 101.6:

In administering the activities of the Organization in compliance with the Financial Regulations and Rules, the following principles shall be observed:

1. Results based and risk informed decision making based on the framework established by the Director General;

2. Compliance with decisions of the WIPO Assemblies;

3. **Effective and efficient internal controls including separation of duties and checks and balances in accordance with the established internal control system**;

4. Prevention of financial malpractice, in accordance with administrative issuances; and

5. Avoidance of conflicts of interest as well as financial disclosure and declaration of interest in accordance with administrative issuances.

3

Objectives, Scope, Methodology

Objectives

Test the adequacy and operating effectiveness of WIPO's Key organization controls based on the Financial and Staff Regulations and Rules.

Scope

Operations in 2025

(Previous periods reviewed for historical insights)

Metho-dology

- Review and analyses of documents
- Inquiries
- Walkthroughs
- Application of the **Comprehensive Assessment Model (CAM)** for Enterprise Risk Management issued by the Institute of Internal Auditors Research Foundation (IARF) .

International Professional Practices Framework® (IPPF)

4.1 WIPO Key Controls 2025: Alignment with COSO - Overview

WIPO Key Control	COSO Internal Control Principles	COSO Internal Control Components
1. Ethics management and monitoring	1. Demonstrates commitment to integrity and values	Control environment
2. Senior management tone at the top		
3. Standards of conduct		
4. Quality Assurance Reviews	2. Demonstrates independence and exercises oversight responsibility	
5. Delegated authority and designations	3. Establishes structure, authority and responsibility	
6. Workforce Planning	4. Demonstrates commitment to attracting, developing and retaining competent staff	
7. Performance of Sector Leads	5. Enforces accountability	
8. Organizational priorities and performance	6. Specifies suitable, specific objectives	Risk assessment
9. Risk Management Landscape	7. Identifies and analyzes risks	
10. Risk Management Maturity assessm		
11. Fraud Risk Assessment	8. Assesses fraud risk	
12. Reserves planning	9. Identifies and analyzes significant changes	Control activities
13. Organizational resilience	10. Selects and develops control activities that help mitigate risks	
14. Safety and Security		
16. Annual Financial Statements		
17. Utilization of Funds		
18. Automated budgetary and expenditure controls		
19. Payroll processing control		
20. Contracts Review Committee		
21. Contract clauses		
22. Advance payments		
23. Asset management framework		
24. Investment Reports		
25. Treasury Operations Control		
26. PCT fee-netting		
27. Information security management	11. Selects and develops general controls over technology	
28. IT management control		
29. Review of SRR and CoCo Approval	12. Bases controls on thorough policies and procedures	
30. Reviewing Financial Regulations & Rules		
31. Administrative issuance review		
32. Accurate data supports RBM and WPR	13. Uses relevant, high-quality information	Information and communication
33. Internal Communications	14. Communicates internally	
34. Member State Communications		
35. Publications and reports quality control	15. Communicates externally	
36. External Communications		
37. GRC Assessed by IOD	16. Conducts ongoing and/or separate evaluations	Monitoring
38. WPR Validation by IOD		
39. Monitoring organizational governance		
40. Timely communication of internal control deficiencies through SIC	17. Evaluates and communicates deficiencies	

Key Control 15 eliminated. Refer to Slide 4.3 for details

WIPO established 39 Key Controls, designed in alignment with the 17 COSO Internal Control Principles across the five COSO components.

These Key Controls should be understood as entity-level controls within the COSO Cube (see below).Collectively, the 39 Key Controls address WIPO's Operational, Reporting, and Compliance objectives.

Next slide illustrates the WIPO functions (departments, divisions, and sections) responsible for the effective operation of these Key Controls.

4.2 WIPO Key Controls 2025: Functions responsible for Key Controls

The matrix on the right shows which WIPO Departments, Divisions, and Sections are responsible for specific Key Controls and highlights the corresponding functional areas of WIPO to which these controls apply.

ODG – Office of Director General
GRC – Governance, Risk and Compliance
CSD – Central Services Division
IOD – Internal Oversight Division
HRMD – Human Resources Management Department
DG – Director General
PPBS – Program Performance and Budget Service
AFMS – Administration, Finance and Management Sector
SIAD – Security and Information Assurance Division
ICTD – Information and Communication Technology Department
OLC – Office of the Legal Counsel
DEAA – Diplomatic Engagement and Assemblies Affairs Division
NMD – News and Media Division
IDOD - Information and Digital Outreach Division

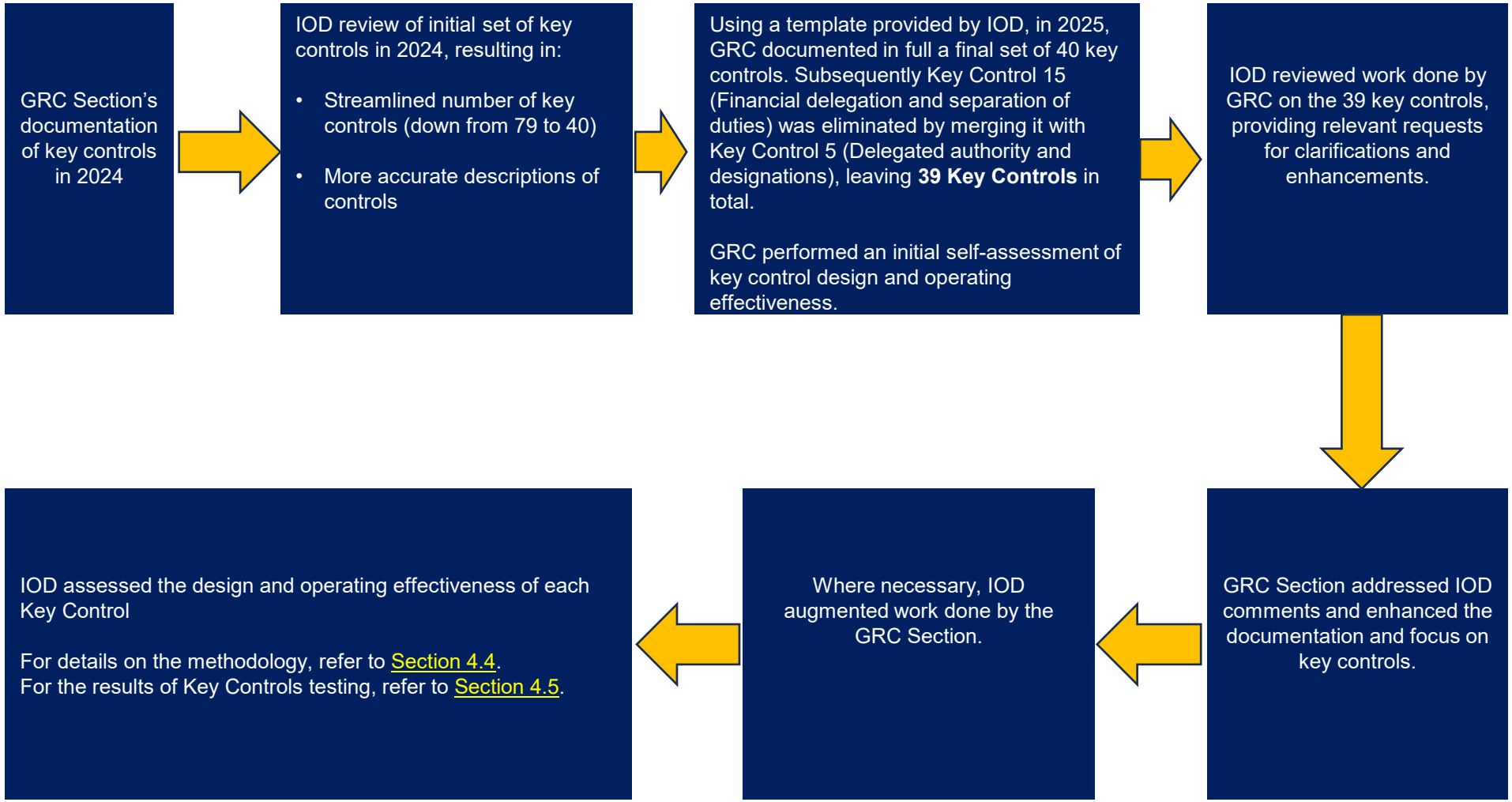
COSO Internal Control Components	COSO Internal Control Principles	Control	Ethics	ODG	GRC	CSD	IOD	HRMD	DG	PPBS	AFMS	SIAD	Finance	ICTD	OLC	DEAA	NMD	IDOD	Ombuds
Control environment	1. Demonstrates commitment to integrity and values	1. Ethics management and monitoring	■																
		2. Senior management tone at the top	■	■	■														
		3. Standards of conduct	■	■	■			■											
	2. Demonstrates independence and exercises oversight responsibility	4. Quality Assurance Reviews	■		■		■												■
	3. Establishes structure, authority and responsibility	5. Delegated authority and designations			■														
	4. Demonstrates commitment to attracting, developing and retaining competent staff	6. Workforce Planning						■											
	5. Enforces accountability	7. Performance of Sector Leads						■	■										
Risk assessment	6. Specifies suitable, specific objectives	8. Organizational priorities and performance								■									
	7. Identifies and analyzes risks	9. Risk Management Landscape			■														
		10. Risk Management Maturity assessm			■														
	8. Assesses fraud risk	11. Fraud Risk Assessment			■														
Control activities	9. Identifies and analyzes significant changes	12. Reserves planning								■									
	10. Selects and develops control activities that help mitigate risks	13. Organizational resili									■								
		14. Safety and Security										■							
		16. Annual Financial Statements											■						
		17. Utilization of Funds								■									
		18. Automated budgetary and expenditure controls								■									
		19. Payroll processing control						■					■						
		20. Contracts Review Committee				■													
		21. Contract clauses				■													
		22. Advance payments				■													
		23. Asset management framework				■													
		24. Investment Reports											■						
		25. Treasury Operations Control											■						
		26. PCT fee-netting											■						
	11. Selects and develops general controls over technology	27. Information security management										■							
		28. IT management control												■					
	12. Bases controls on thorough policies and procedures	29. Review of SRR and CoCo Approval						■											
		30. Reviewing Financial Regulations & Rules			■														
		31. Administrative issuance review													■				
Information and communication	13. Uses relevant, high-quality information	32. Accurate data supports RBM and WPR								■									
	14. Communicates internally	33. Internal Communications															■		
		34. Member State Communications														■			
	15. Communicates externally	35. Publications and reports quality control																■	
		36. External Communications															■		
Monitoring	16. Conducts ongoing and/or separate evaluations	37. GRC Assessed by IOD					■												
		38. WPR Validation by IOD					■												
		39. Monitoring organizational governance					■												
	17. Evaluates and communicates deficiencies	40. Timely communication of internal control deficiencies through SIC			■														

4.3

IOD Work with respect to Key Controls

The workflow on the right illustrates, at a high level, the work performed by IOD since 2024 to review, and test Key Organizational Controls.

GRC – Governance, Risk and Compliance
IIA – Institute of Internal Auditors



4.4

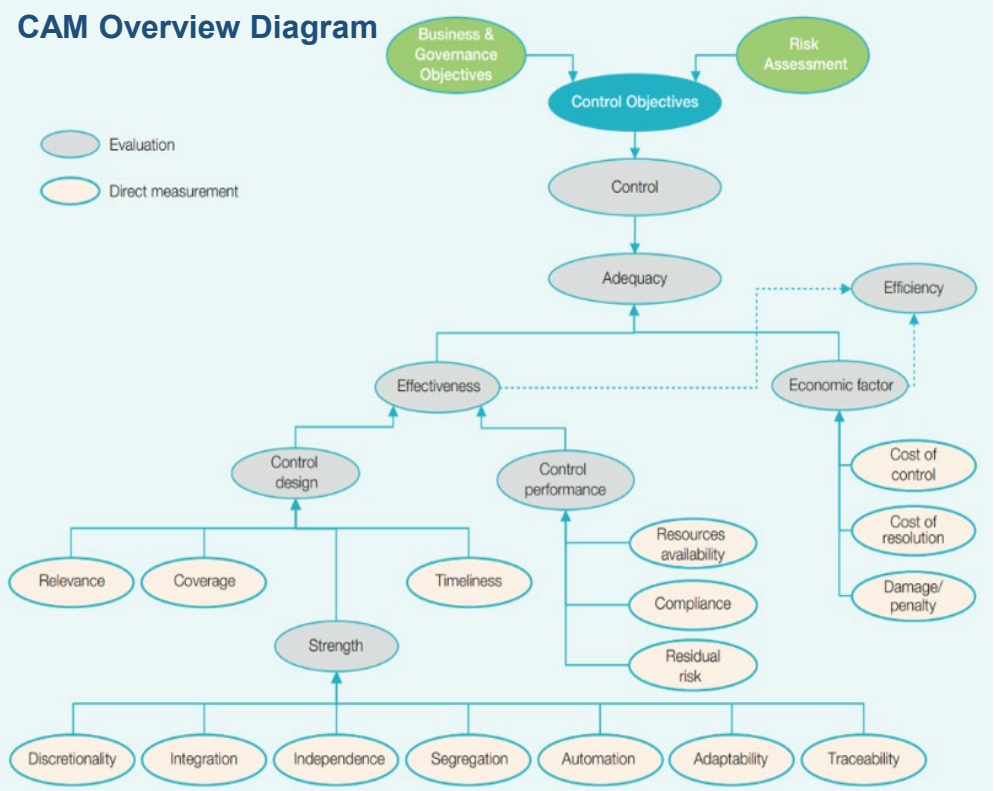
IOD Methodology for assessing Key Controls

IOD assessed the design and operating effectiveness of each Key Control using the Institute of Internal Auditors' (IIA) Comprehensive Assessment Model (CAM) for Enterprise Risk Management.

Each control was assessed against Direct Measurements: Relevance; Coverage; Timeliness; Discretionality; Integration; Independence; Segregation; Automation; Adaptability; Traceability; Resources; Compliance; Residual risk; and an aggregate direct measurement 'benefit versus cost of control'.

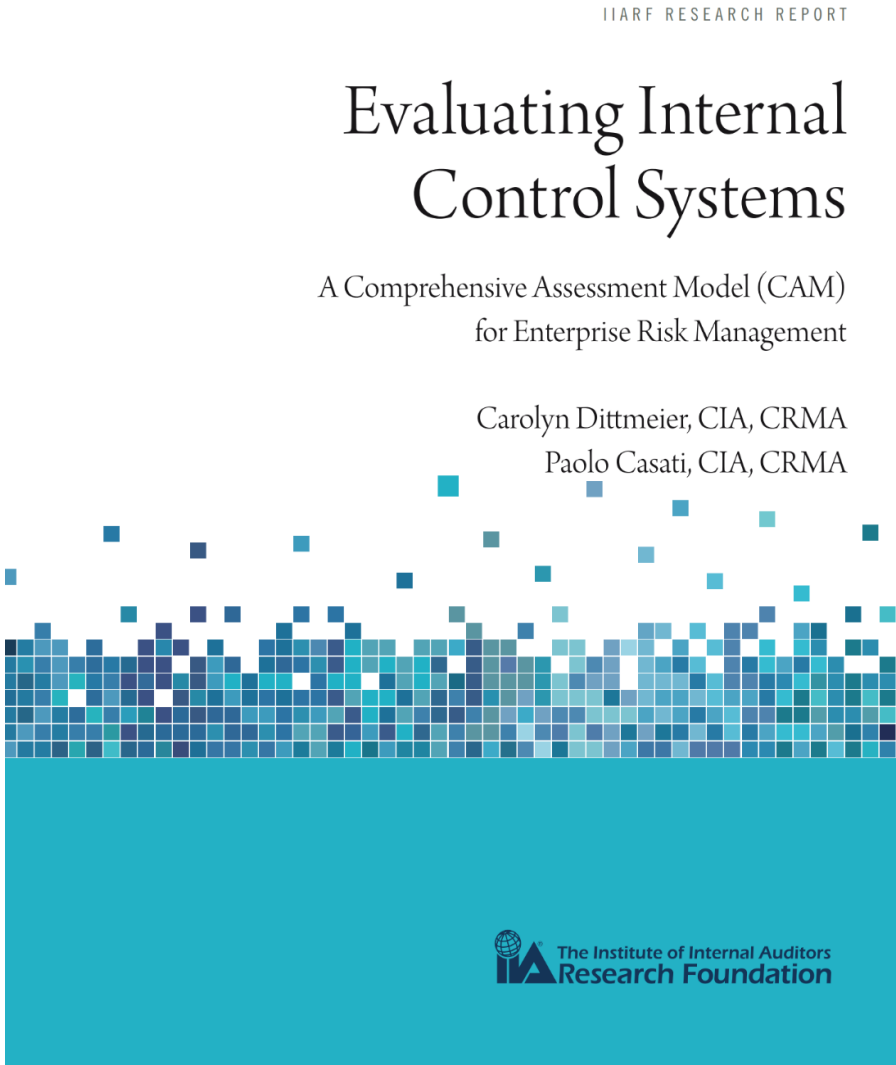
The conclusion on control effectiveness was derived from an overall assessment of direct measurement results. While the original CAM methodology applies a five-point rating scale (1 to 5) to assess controls, IOD applies a binary assessment, classifying controls as either "Effective" or "Not Effective" based on its analysis of direct measurements. Under the CAM methodology, an Effective control corresponds to a Rating of 1 or 2 (see table on the right).

CAM Overview Diagram



Overall Assessment of the Internal Control System of a Process	
Rating 1	**Adequate or sound control system:** a system that achieves the control objectives intended to mitigate the risks correlated to the business and governance objectives relevant to the process (based on risk acceptance strategy).
Rating 2	**Adequate internal control system with some areas of improvement:** a system that achieves the control objectives intended to mitigate the risks correlated to the business and governance objectives relevant to the process (based on risk acceptance strategy) with evidence of some areas, though not critical, subject to improvement to meet the requisites of sound controls.
Rating 3	**Generally adequate internal control system, with some critical areas:** the system achieves, in general terms, the control objectives intended to mitigate the risks correlated to the business and governance objectives relevant to the process (based on risk acceptance strategy). The characteristics of some of the controls, however, are not fully consistent with requisites of sound controls (for example, lack of automation, of traceability, of segregation, etc.).
Rating 4	**Inadequate internal control system, subject to significant improvements:** the controls only partially achieve the control objectives intended to mitigate the risks correlated to the business and governance objectives relevant to the process (based on risk acceptance strategy).
Rating 5	**Insufficient internal control system:** the combination of controls is not sufficient to achieve the control objectives intended to mitigate the risks correlated to the business and governance objectives relevant to the process (based on risk acceptance strategy).

Source:



4.5 Key Control Testing Results (assessment for the year 2025)

COSO Internal Control Components	COSO Internal Control Principles	Control	Control Effectiveness	Note
Control environment	1. Demonstrates commitment to integrity and values	1. Ethics management and monitoring	EFFECTIVE	
		2. Senior management tone at the top	EFFECTIVE	
		3. Standards of conduct	EFFECTIVE	
	2. Demonstrates independence and exercises oversight responsibility	4. Quality Assurance Reviews	EFFECTIVE	
	3. Establishes structure, authority and responsibility	5. Delegated authority and designations	EFFECTIVE	
	4. Demonstrates commitment to attracting, developing and retaining competent staff	6. Workforce Planning	EFFECTIVE	
	5. Enforces accountability	7. Performance of Sector Leads	EFFECTIVE	
Risk assessment	6. Specifies suitable, specific objectives	8. Organizational priorities and performance	EFFECTIVE	
	7. Identifies and analyzes risks	9. Risk Management Landscape	EFFECTIVE	
		10. Risk Management Maturity assessm	EFFECTIVE	
	8. Assesses fraud risk	11. Fraud Risk Assessment	EFFECTIVE	
Control activities	9. Identifies and analyzes significant changes	12. Reserves planning	EFFECTIVE	
	10. Selects and develops control activities that help mitigate risks	13. Organizational resili	EFFECTIVE	
		14. Safety and Security	EFFECTIVE	
		16. Annual Financial Statements	EFFECTIVE	
		17. Utilization of Funds	EFFECTIVE	
		18. Automated budgetary and expenditure controls	EFFECTIVE	
		19. Payroll processing control	EFFECTIVE	
		20. Contracts Review Committee	EFFECTIVE	
		21. Contract clauses	EFFECTIVE	
		22. Advance payments	EFFECTIVE	
		23. Asset management framework	EFFECTIVE	
		24. Investment Reports	EFFECTIVE	
		25. Treasury Operations Control	EFFECTIVE	(A)
		26. PCT fee-netting	EFFECTIVE	
	11. Selects and develops general controls over technology	27. Information security management	EFFECTIVE	
		28. IT management control	EFFECTIVE	
	12. Bases controls on thorough policies and procedures	29. Review of SRR and CoCo Approval	EFFECTIVE	
		30. Reviewing Financial Regulations & Rules	EFFECTIVE	
		31. Administrative issuance review	EFFECTIVE	
Information and communication	13. Uses relevant, high-quality information	32. Accurate data supports RBM and WPR	EFFECTIVE	
	14. Communicates internally	33. Internal Communications	EFFECTIVE	
		34. Member State Communications	EFFECTIVE	
	15. Communicates externally	35. Publications and reports quality control	EFFECTIVE	
		36. External Communications	EFFECTIVE	
Monitoring	16. Conducts ongoing and/or separate evaluations	37. GRC Assessed by IOD	EFFECTIVE	
		38. WPR Validation by IOD	EFFECTIVE	
		39. Monitoring organizational governance	EFFECTIVE	
	17. Evaluates and communicates deficiencies	40. Timely communication of internal control deficiencies through SIC	EFFECTIVE	

Comments

(A) The 2025 Audit of Investment Management at WIPO (IA-2025-07) resulted in 11 recommendations. Considering the corrective actions taken and the outcomes of IOD follow-up on outstanding recommendations, the Key Control is considered effective.

The effectiveness of the controls may be subject to further review should subsequent information indicate deficiencies in the performance of Key controls.

4.6 Additional Information Technology (IT) Organization- wide controls tested in 2025

Control Code	Control Name	Control Effectiveness	Note
AC1.AFM.0094.008	Annual software usage reporting (network scan) to ensure compliance	Effective	
ELC 2.3	Organizational resilience control	Effective	
ELC 3.2.1	Information security management	Effective	
ELC 3.2.2	Information security management	Effective	
ISC-001_1	Data loss prevention controls	Effective	
ISC-001_2	Data loss prevention controls	Effective	
SOP-001	Information Security Operations Center monitoring and incident response	Effective	
SOP-003	Data Leakage Prevention (DLP)	Effective	
TAR-001_ORG.013	Infosec training/awareness raising program	Effective	
TAR-002	Anti-fraud training/awareness raising program	Effective	

Comments

The effectiveness of the controls may be subject to further review should subsequent information indicate deficiencies in the performance of IT controls.

Acknowledgement

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

Prepared by: Dainis Reinieks, Acting Head of Internal Audit Section

Reviewed and approved by:

Julie Nyang’aya, Director, IOD.