IOD GRC Opinion: Information Security Section, Security and Information Assurance Division

Internal Oversight Division

IA-2025-06.C1

January 2026



This report has been redacted in line with Internal Oversight Division Report Publication Policy.

Table of Content

1 Executive Summary

2 Background

3 Objectives, Scope, Methodology

4 Observations and Recommendations

5 Annexes

WIPO FOR OFFICIAL USE ONLY

1

Executive Summary

As part of forming an annual opinion on WIPO's Governance, Risk Management and Internal Controls for the year ended December 31, 2025, the Internal Oversight Division (IOD) sought to understand the services provided by the Information Security Section of the Security and Information Assurance Division (SIAD).

Conclusion

The services provided by SIAD to WIPO have been understood by IOD and are summarized in the following pages of this report.	**Understanding Obtained**

2

Background

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) sought to understand the Governance, Risk Management, and Internal Controls around ICTD, CSP, UNICC, and the ISS in SIAD at WIPO.

Information Security ensures the confidentiality, integrity, and availability of organizational systems and information.

ACRONOMYS
CSP – Cloud Service Providers
ICTD – Information and Communication Technology Department
ISS – Information Security Section
SIAD - Security and Information Assurance Division
UNICC – United Nations International Computing Centre

What is covered in this report



- Covered in a separate IOD Report IA 2025-06.C3
- Covered in a separate IOD Report IA 2025-06.C2

- **Covered in this report**
- Reviewed Governance, Risk Management, and Internal Controls relating to ISS, including Information Security Framework, Policies, Standards, Certifications, and Oversight.
- Identified main information security activities performed.
- Reviewed results of the latest Cybersecurity Maturity Assessment.
- Cloud Service Provider Security and associated risk management.
- Data Privacy Office and Roadmap.

The purpose of this report was to obtain an updated understanding of the Governance, Risk Management ,and Internal Controls of the ISS in SIAD at WIPO in 2025. Relevant controls identified during the engagement were tested as part of Key Controls Testing in Q3 – Q4 2025.

WIPO FOR OFFICIAL U

3

Objectives, Scope, Methodology

Objectives

Obtaining understanding of the services provided by the Information Security Section of the Security and Information Assurance Division at WIPO.

Scope

Operations in 2025

(previous periods were reviewed for historical insights)

Metho-dology

- Review and analysis of documents, and

Inquiries

WIPO FOR OFFICIAL USE ONLY

4.1

Information Security Governance, Risk Management and Controls

ACRONOMYS

- ADG – Assistant Director General
- AFMS - Administration Finance and Management Sector
- CSO – Chief Security Officer
- DG – Director General
- IA – Information Assurance
- I&T – Information and Technology
- IAOC – Independent Advisory Oversight Committee
- Infotech – incorporates all aspects of Information and Technology, and IA
- iSOC - Information Security Operations Center
- IS – Information Security
- ISS – Information Security Section
- Security – refers to physical security

DEFINITIONS

- **Governance** - The combination of processes and structures implemented by a Board to inform, direct, manage, and monitor the activities of the organization toward the achievement of its objectives. (Source: Global Internal Audit Standards)
- **Risk Management** – a process to identify, assess, manage, and control potential events or situations to provide reasonable assurance regarding the achievement of the organization's objectives. (Source: Global Internal Audit Standards)
- **Control** - Any action taken by management, the board, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved. (Source: Global Internal Audit Standards)
- **COSO** (Committee of Sponsoring Organisations of the Treadway Commission) - an international internal control framework.

Infotech Board:

- Chaired by DG or designate.
- Senior decision-making body on infotech and security.
- Sets strategy on infotech.
- Oversees security.

Infotech Steering Committee

- Under authority of Infotech Board.
- Chairperson and composition decided by ADG, AFMS.
- Oversees implementation of IA and I&T strategies.

CSO

- Secretariat of Infotech Board and Infotech Steering Committee.
- Coordinates security and IA matters
- Responsible for implementation and compliance with IA elements of the Infotech Framework.

IAOC

- ISS updates the IAOC periodically on IS and data privacy.



- ISS releases information bulletins and offers user training, including mandatory training.
- Business users participate in IS awareness campaigns.
- Users provide feedback through surveys commissioned by ISS on IS and data privacy.
- Users may report incidents to ISS, for example, through email.
- Security & Privacy Champions program was launched in September 2024 - 19 Business security and privacy champions and 25 Technical security and privacy champions as of November 2025).

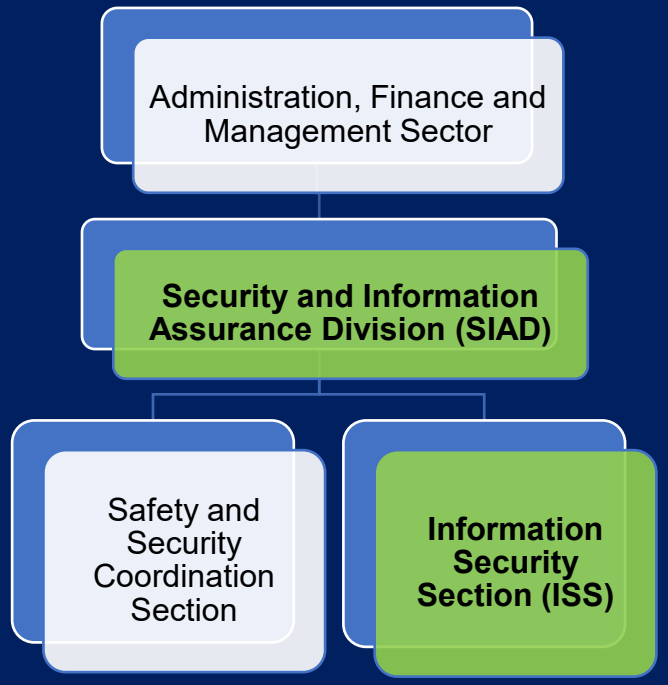
- Documented IS policies, procedures and Standards.
- Physical, and logical access controls, including multi-factor authentication.
- Data loss prevention.
- Information classification and handling.
- Continuous monitoring, detection, analysis and response to security threats and incidents by iSOC.
- Cybersecurity technical defense and detection.
- User awareness campaigns
- ISO 27001 certification.

- WIPO Risk Management Policy applies to ISS.
- IS risks are documented, reviewed and monitored through the Risk Management Working Group.
- A Service Provider Security Risk Management process has been defined and documented.
- Regular vulnerability assessments and penetration tests are conducted.
- Critical IS risks are reported.

WIPO FOR OFFICIAL USE ONLY

4.2

Information Security Section Placement and Roles



ISS offers the following services:

- **Information Risk Management:** ensures that threats and risks to WIPO's information assets and service providers are identified, assessed, remediated and reported, in line with WIPO's risk management policy.
- **Incident Management:** monitoring, identifying and responding to information security incidents.
- **Application Security:** ensures that all applications deployed in WIPO's environment are secure and comply with WIPO's security requirements.
- **Compliance Management:** develops WIPO's Information Security Policy Framework and ensures the implementation of associated policies and standards.
- **Security Architecture:** seeks to ensure that business processes and information systems satisfy business requirements for security, in line with the risk management strategy and defined security principles.
- **Awareness and Training:** ensures that relevant and timely information is available to users to increase their information security and data privacy awareness.

WIPO FOR OFFICIAL USE ONLY

4.4

Information Security Framework Hierarchy and Review Process

ACRONOMYS

IS – Information Security
SIAD – Security and Information Assurance Division

Multiple levels of InfoSec Framework:

1. WIPO's information security framework has multiple levels with each level representing a function in defining, communicating and enforcing information security.

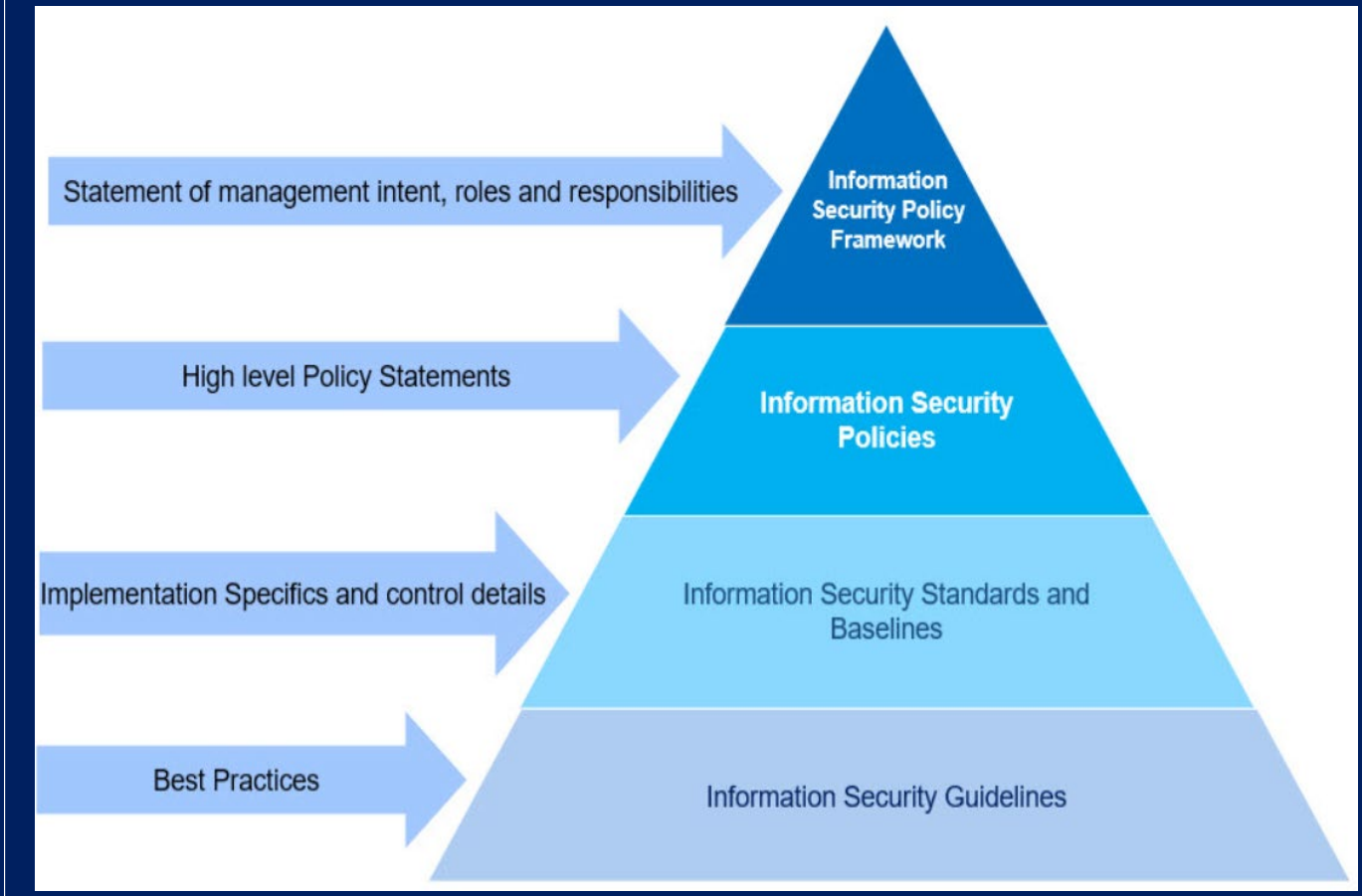
2. High-level policy documents communicate management's expectations "why" for information security at WIPO.

3. Lower levels in the framework contain supporting Standards and baselines, defining the "What" and "How", respectively.

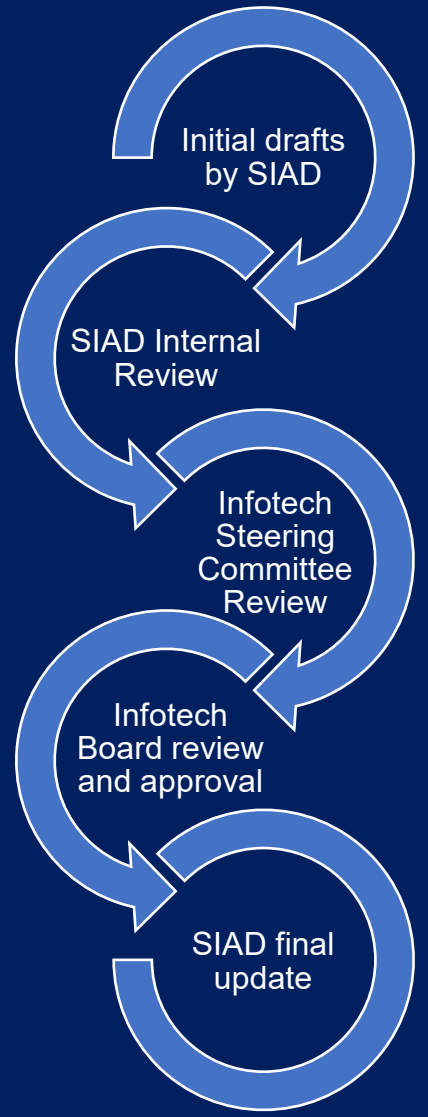
4. A review process is defined and followed for changes to Policies and Standards.

5. IS Policies and Standards are shown in the next slide.

Information Security Framework Hierarchy



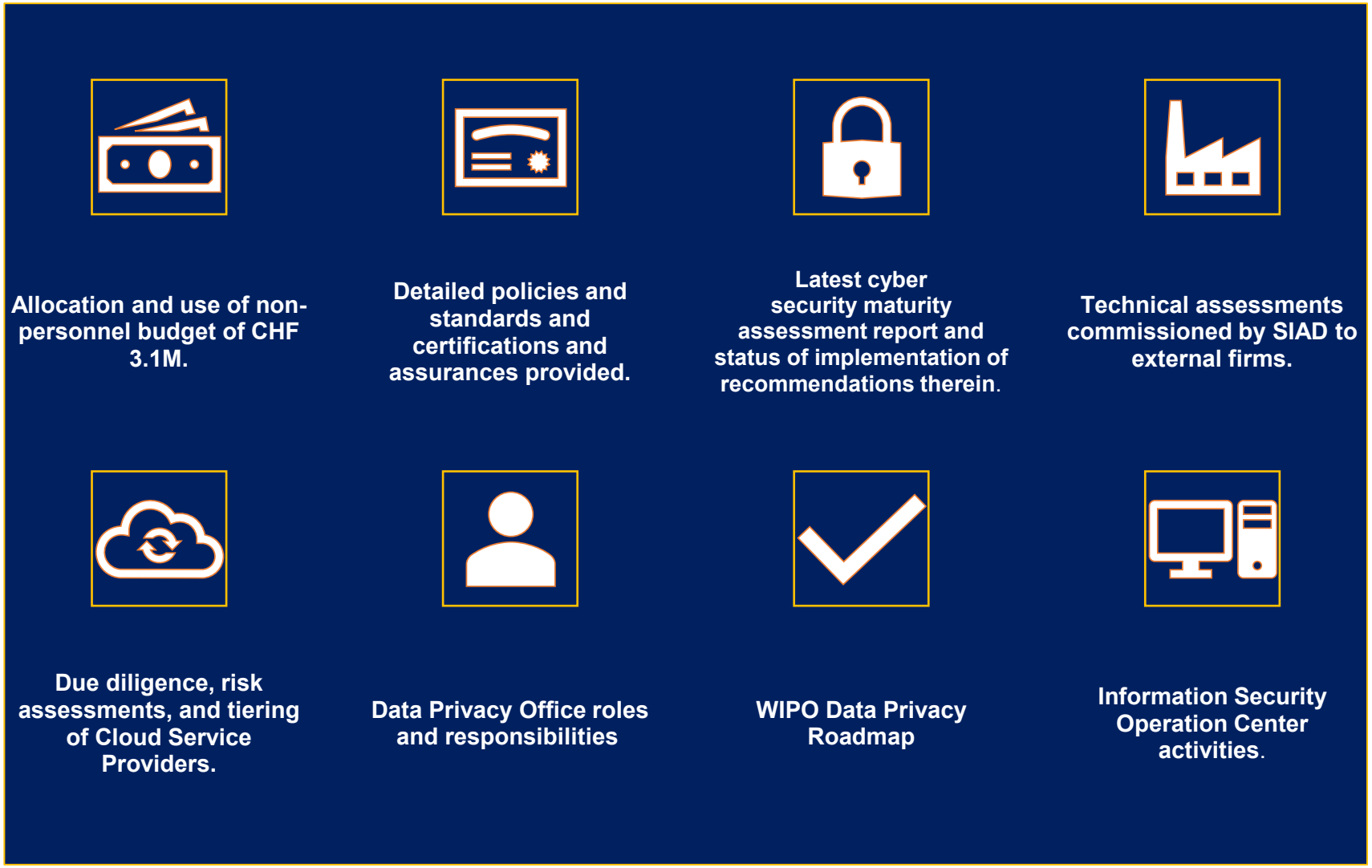
Review Process – IS Policies and Standards



Source: Policies and Standards

WIPO FOR OFFICIAL USE ONLY

4.5 Other SIAD areas that were reviewed for understanding



WIPO FOR OFFICIAL USE ONLY

Acknowledgement

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

Consolidated by: Solomon Simutowe, Senior Internal Auditor, IOD

Reviewed and approved by: Julie Nyang'aya, Director, IOD.

