Guidance pronouncements (GUIDs) are issued by INTOSAI, the International Organisation of Supreme Audit Institutions. For more information visit *www.issai.org*

INTOSAI

Explanatory Memorandum on the Exposure Draft of GUID 5101

Guidance on Audit of Security of Information Systems

November 2018

The Forum for INTOSAI Professional Pronouncements (FIPP) adopted a classification of INTOSAI pronouncements under the INTOSAI Framework of Professional Pronouncements (IFPP) and accordingly various documents are classified as Principles, Standards and Guidance. Under the IFPP, Guidance pronouncements (GUIDs) are intended to provide guidance to SAIs on a specific subject matter and for conducting Financial, Compliance and Performance Audits encompassing the related subject matter. Series 5100-5109 of pronouncements has been allocated to the GUIDs on Information Systems Audit under the IFPP. GUID 5101 is intended to be the foundational guidance pronouncement for Audit of Security of Information Systems (IS). It focusses on Information Systems' Security (including Cyber Security) as one of the domains of an audited entity in which Information Technology (IT) plays a crucial role.

The first Strategic Development Plan (SDP) for the IFPP recognized the need to review the existing ISSAI 5310 - Information System Security Review Methodology - which was due for review since 2016 and for endorsing a new draft under the IFPP as subject matter specific guidance pronouncement, i.e. as a GUID. (Project 2.8 of the SDP)

Accordingly, the content of ISSAI 5310 were reviewed in the light of latest developments in the field of Security of Information Systems and has been revised and consolidated as GUID 5101. Thus, GUID 5101 draws upon GUID 5100, and is intended to provide guidance to SAIs for conducting an examination of IT controls related to Security of Information Systems.

Primary objectives of the revision and updating exercise were to create a relevant GUID for use by field Audit practitioners, with the objectives of executing the following processes:

1. Aligning the guidance with ISSAI 100 and the revised GUID 5100
2. Identification of universe of information systems assets in use by audited entity
3. Identification of potential threats and counter measures for mitigation and avoidance of risk exposure to assets
4. Evaluation of internal controls already adopted by audited entity
5. Risk Analysis, quantified in terms of risk exposure determined by combination of criticality of information asset(s) and business impact of failure
6. Issue of recommendations, based on computed risk exposure

GUID 5101 has accordingly been developed within the IFPP by following the Due Process governing the development and revision of Professional Pronouncements.

Accordingly, as part of the Stage 1 of the Due Process, the Project proposal for developing GUID 5101 was referred to the Working Group on IT Audit (WGITA) under the Knowledge Sharing Committee (KSC), and then FIPP for approval. FIPP had accorded approval to the Project proposal in November 2017.

The following measures have been taken by the Project Team as part of the Due Process-

- Comparison with ISSAIs 100, 200, 300 and 400 as well as the proposed GUID 5100, to ensure alignment with the basic concepts and principles.
- Reference to the latest existing literature on the subject matter of Information Systems.
- Involvement of experts and practitioners from various SAIs, who formed part of Project Team members. Inputs received from all the member SAIs have been duly incorporated in the Exposure Draft.

- Involvement of expertise from external organizations such as ISACA, as part of the Project Team membership. Inputs received from ISACA have been factored into the Exposure Draft.
- Involvement of experts from the Sub Committees on Financial Audit, Performance Audit and Compliance Audit. Inputs received from the Sub Committees have been factored into the Exposure Draft.

The proposed GUID 5101 is intended to take effect from 23rd September 2019, after it is referred by the Governing Board to the XXIII INCOSAI for endorsement and is intended to replace the existing pronouncement ISSAI 5310. The endorsement of the GUID would ensure conformity of the subject matter guidance on security of Information Systems with higher level ISSAIs.

The inputs of SAIs, INTOSAI bodies, and external stakeholders on the Exposure Draft of GUID 5101 are welcome at this stage.