Forum for INTOSAI Professional Pronouncements

Conclusions drawn by FIPP as basis for the approval of

INTOSAI GUID 5101 – Guidance on Audit of Information Security (Endorsement Version)

Background

The transition to computerised information systems and electronic processing of information by public sector entities make it crucial for SAIs to develop appropriate capacity to identify and assess risks related to information systems and respond to these risks. As part of the audit of information systems, there is a need to ensure that controls to maintain confidentiality, integrity, and availability of information (i.e. Information Security) have been implemented by public sector entities and operate effectively.

The Strategic development plan for the INTOSAI Framework of Professional Pronouncements (SDP) 2017-2019 recognised the need for reviewing the pre-existing ISSAI 5310 on Information System Security Review Methodology. This was proposed to be replaced by endorsing a new subject matter specific guidance pronouncement (GUID) on the audit of security of information systems. The development of the new GUID was initiated under Project 2.8, which was approved by the Forum for INTOSAI Professional Pronouncements (FIPP) in November 2017.

The project was initiated with the following objectives:

1. Aligning the guidance with ISSAI 100 and the revised GUID 5300
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

The contents of ISSAI 5310 were reviewed by the project team with due considerations to the latest developments in the field of security of information systems. These were revised and consolidated as GUID 5101.

FIPP conclusions

FIPP received a new Exposure Draft for the GUID 5101 which was discussed in April 2022. The draft aimed at clarifying the overarching role of GUID 5100 for all audits of Information Systems, as well as to narrow the scope of the GUID 5101 indicating areas where the GUID 5101 will not be applicable. FIPP discussed the updated Exposure Draft and concluded that the draft was not ready for an approval.

The reasoning behind this conclusion was that the scope of the GUID in FIPPs opinion was not clear on which audit type the GUID would be relevant for. FIPP adviced the group to cover audits that aim to provide a conclusion that IT Security Management is in compliance with one or more relevant technical standards on the subject. i.e. Coverage of financial or performance audits will make the GUID complicated and render it inadequate for any of the audits.

The project team and FIPP collaborated intensively to develop an updated exposure draft of the GUID which was forwarded to FIPP in February 2024. FIPP concluded that the GUID was ready for exposure. Due to a technical error, the GUID was out on exposure for 90 days and comments received but the INTOSAI was not notified as according to due process. The GUID was therefore exposed one more time, this time through issai.org.

FIPP have concluded that the comments received have been duly addressed in the draft endorsement version. FIPP approved GUID 5101 in September 2024 and forwarded it to INTOSAI Governing Board for endorsement.