Project 2.8 of the SDP 2017-2019

EXPLANATORY MEMORANDUM ON THE 2ND EXPOSURE DRAFT

INTOSAI

REQUEST FOR COMMENTS

This Second Exposure Draft of GUID 5101 *Guidance on Audit of Security of Information Systems* was elaborated by the INTOSAI Working Group on IT Audit (WGITA) of the Knowledge Sharing Committee (KSC) under Project 2.8 of the Strategic Development Plan (SDP) 2017-2019 for the IFPP.

Respondents are asked to submit their comments electronically by [INSERT MONTH AND DATE], 2024 to the e-mail addresses: [INSERT E-MAIL ADDRESSES]. Please submit comments to specific paragraphs using the file circulated at the same time as the exposure draft. General comments may be submitted using PDF or Word documents. All comments will be considered a matter of public record and may be posted on the issai.org website.

Kommentert [MRI1]: The usual comment period is 90 days. The deadline will depend on the date of exposure.

The WGITA will consider all comments received when preparing the final version of the textfor submission to the Forum for INTOSAI Professional Pronouncements (FIPP) for approval.

The FIPP has approved this exposure draft on February 27, 2024 (cf. section 2.1 of the due process for the IFPP). The final pronouncement is expected to take effect from [INSERT MONTH DATE, YEAR].

Kommentert [MRI2]: Check whether the date is correct.

Introduction

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.

In the light of the escalating relevance of information security, GUID 5101 is developed to provide SAIs with non-mandatory specific guidance on the audit of security of information systems. The GUID is closely related to GUID 5100 *Guidance on Audit of Information Systems* and offers additional direction without replicating the content of GUID 5100.

The exposure draft for GUID 5101 focuses on compliance audit. The GUID is intended to support auditors in understanding how to apply the relevant ISSAIs for the subject matter of security of information systems. The GUID covers the planning, conducting, reporting and follow-up stages of the audit process.

Background

The SDP 2017-2019 recognised the need for reviewing the pre-existing ISSAI 5310 *Information System Security Review Methodology* and 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 FIPP in November 2017. The project team was led by the SAI of India.

Accordingly, the content of ISSAI 5310 was reviewed in the light of the latest developments in the field of security of information systems and was revised and consolidated as GUID 5101. The proposed draft was drawn on GUID 5100 *Guidance on Audit of Information Systems.*

The first exposure draft of GUID 5101 was approved by FIPP in November 2018. However, the comments received from the respondents during the exposure period indicated that the GUID should be further elaborated to add value to auditors. FIPP therefore concluded that the document was not yet ready to be endorsed.

FIPP guided and supported the project team in developing the GUID by providing feedback and advice on how key issues related to the content, scope and structure of the pronouncement should be resolved. Emphasis was placed on focusing the GUID on compliance audit and making its content distinct from GUID 5100.

FIPP approved this second exposure draft of GUID 5101 in February 2024, concluding that the proposed pronouncement is of high quality and adds value to the IFPP.

Questions to consider

The inputs of SAIs, INTOSAI bodies and external stakeholders on this Second Exposure Draft are welcome at this stage. Respondents are especially encouraged to consider the following questions:

1) Does this GUID provide useful guidance for your SAI in carrying out a compliance audit of security of information systems?
2) Does the GUID include the necessary definitions related to the audit of security of information systems?

INTOSAI

IFPP