Forum for
INTOSAI
Professional
Pronouncements

Project Proposal for revising GUID 5310 on Information Systems' Security Audit SAI India

October 16, 2017

This form is to be used to stand as a record of the proposal from the project team.

PART A: PROJECT IDENTITY

Description	Information
Project number and title as per SDP	**2.8. Consolidating and aligning guidance on IT audit with ISSAI 100**
Working title(s) for the new pronouncement(s)	Guidelines on Information Systems' Security Audit, including Cyber Security (Earlier ISSAI 5310)
Project aim	To revise the pre-existing ISSAI 5310 now GUID: "Guidelines on Information Systems' Security Audit", including a new section on Cyber Security, to be used by auditors of SAIs.
Project objectives	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 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
Project duration	22.06.2017 to 30.06.2019 (~ 24 months).

Name of the lead WG	INTOSAI Working Group on IT Audit						
Key contacts	Name	Surname	Address	Email	Office Phone	Business Mobile Phone	Organization / Sponsoring SAI
Project Group lead	SAURABH	NARAIN	Office of Accountant General (ER&S Audit), Uttar Pradesh, TC-35-VI, Vibhuti Khand, Gomti Nagar, Lucknow - 226010 (INDIA)	narainS@cag.gov.in	+91-522-2722112	+91-9412055623	SAI INDIA
Contact person for the goal chair	K S	SUBRAMANIAN	Director General (International Relations)Office of the Comptroller and Auditor General of	subramanianKS@cag.gov.in	+91-11-23237822	+91-7053030000	SAI INDIA

			India, 9 Deen Dayal Upadhyaya Marg, New Delhi – 110124 (INDIA)				
FIPP Liaison Officer	EINAR	GØRRISSEN	Director General , IDI, Oslo Norway	einar.gorrissen@idi.no			IDI
Other anticipated project team members (list of names and organisations)	SAI India	1. Kartikeya Mathur					
		2. Deepak Raghu					
		3. Sreeraj Ashok					
		4. Narmadha R					
	SAI China	1. Yin Qiang					
	SAI Ecuador	1. Verónica Morejon					
		2. Lisette Villacrés					
		3. Mrs. Daysi Villota					
	SAI Iraq	1. (Yet to be decided)					

	SAI Kiribati	1. Lucas Tatireta
	SAI USA	1. Madhav Panwar
	SAI Poland	1. Pawel Banaś
	ISACA	1. Kris Seeburn
		2. Joe Barkley
	FIPP LO	1. Einar Gørrissen

PART B: PROJECT MILESTONES

Stage	**Due process milestones**				
1.	Project proposal	Start Date	End Date	Expected Time in Total	Comments
		10.10.2017	30.11.2017	50 Days	
		N.B. Allow three months between end date of stage 1 and start date of stage 2 for FIPP approval of the project proposal			
2.	Exposure draft	Start Date	End Date	Expected Time in Total	Comments
		01.03.2018	31.07.2018	5 months	
		N.B. Allow three months between end date above and start date below for FIPP approval of the exposure draft			
	Exposure period	Start Date	End Date	Expected Time in Total	Comments

		01.11.2018	31.01.2019	90 Days	
3	Endorsement version	Start Date	End Date	Expected Time in Total	Comments
		01.02.2019	30.04.2019	3 months	
		N.B. Allow three months between end date of stage 3 and start date of stage 4 for FIPP approval of the project proposal			
4.	Final pronouncement, including translation into all official INTOSAI languages*	Start Date	End Date	Expected Time in Total	Comments
		01.08.2019	15.09.2019	45 Days	
		*"Unless other mechanisms have been established, the working group is responsible for translation of the approved endorsement version into the five official languages." (Due Process, page 9). Time must be allowed to obtain the required translations of the endorsement version(s).			

PART C: INITIAL ASSESSMENT AND PROJECT PROPOSAL

N°	**Initial assessment - Matters to be covered (Due Process, pages 6 and 7)**	
C.1.	Explanation of the need for the project Explanation of the purpose of the project	ISSAI 5310 was issued in 1995, and requires revision by conducting a review of existing standards (such as ISACA), guidelines (such as COBIT) and material related to Information Systems' Security, in view of recent developments in creation, maintenance and provision for security of mobile and wireless data

		networks. The list of assets for which threats and counter measures are enumerated in the existing guidance (former ISSAI 5310) also needs to be appropriately revised. Further, existing guidance in the former ISSAI 5310 (now GUID) of 5300 series on IT Audit, of which the proposed GUID is a part, is intended to form a part of the IFPP, and hence needs to be linked appropriately to the higher level ISSAIs (ISSAIs 100, 200, 300 and 400, as also other relevant IFPP guidance). The proposed GUID would also act as a bridge between the higher level ISSAIs and the detailed practitioner level guidance contained in the WGITA IDI IT Audit Handbook.
C.2.	Description of the categories of auditing or other engagements that will be covered by the new pronouncement(s)	Since the outcome of the project, i.e. Guidelines on Information Systems' Security, is intended to be utilized in order to identify potential risk areas and to recommend appropriate mitigation and/ or avoidance actions, the new pronouncement is intended to cover the Financial, Compliance and Performance Audit engagements. Further, where the statutory framework requires compliance with prescribed standards/statutes for Information Systems' Security, the pronouncement would cover Compliance Audit engagements.

C.3.	Description of different types of SAIs / audit engagements that must be accommodated in the new pronouncement	INTOSAI WGITA recognizes the different levels of maturity of Information Systems' Security in the government sector and Audit of such Systems as practiced by different SAIs. The GUID will therefore attempt to address concerns of SAIs at both the ends of spectrum of technological differential in terms of Information Systems Audits being undertaken by various SAIs subject to their respective mandates as warranted by their individual statutes. Therefore, the application of the proposed GUID (former ISSAI 5310) will have to be carefully evaluated by each SAI in terms of its own Statute and mandate, as derived from both law and practice(s). The GUID would cover basic principles involved in auditing Information Systems' Security including cyber security in the respective Public Sectors of member countries. Developmental Process will ensure that the basic issues inherent in Audit of Information Systems Security are appropriately linked to the different forms of audit conducted by SAIs – viz~ Financial Auditing, Performance Auditing and Compliance Auditing. Above is either derived from the fact that any review of Information Systems' Security is likely to involve a comparison with specific guidelines (verification of Compliance with such guidelines or frameworks, if adopted by the audited entity) or with best practices included in this GUID or any other International/national

		standards and frameworks adopted by the audited entity. Typically, Security audit engagements undertaken by any SAI could be a part of Financial, Compliance Audit and/or Performance Audit, depending on the maturity stage of Information Systems' Security adopted by audited entities.
C.4.	Challenges, if any foreseen, that would have to be managed by SAIs in implementing the new pronouncements	Capacity Building in terms of equipping the audit teams in terms of Human Resources of required technical exposure and expertise, technology awareness and the ability of the personnel to evaluate information systems in terms of security controls adopted by the audited entities. The revised GUID will also address the challenges that SAIs face in adopting and developing enduring capacities and capabilities in the use of appropriate audit tools and technologies in conducting efficient and effective IS Audits.
C.5.	Explanation of how consistency with ISSAI 100, other existing ISSAIs and other professional pronouncement(s)will be ensured	Revised GUID 5310 will be consistent with ISSAI 100.
Nº	**Project proposal - Matters to be covered (Due Process, page 7)[2]**	
C.7.	Explanation of organisation of the project describing how project group members will	Project Team members are drawn from the INTOSAI WGITA membership. Professional guidance will be sought from ISACA, which is associated with the

	be drawn from relevant sub committees/ working groups/ other interested parties	Project Team. We will engage with various sub-committees of the PSC appropriately.
C.8.	Explanation of the outcome of the project specifying how existing professional pronouncements may be affected.	Revised GUID will be aligned with ISSAI 100 and GUID 5300. No other pronouncement is expected to be impacted by this GUID. The following is the proposed list of contents for the new pronouncement- • Definitions- Information Systems, Information Security Framework, including Cyber Security • Key elements of Information Systems' Security • Necessity for Information Systems' Security • Roles and Responsibilities of the Management in security of information systems • IS Security threats and counter measures • IS Security Audit Planning • Risk based approach to prioritize and select auditable Information Systems, by creating an inventory of such Systems, along with key criteria for carrying out risk assessment • Identification of domain wise Audit Objectives, such as IS Security Policy and Organization, Communications and Operations Management, Asset Management, Human Resources Management, Physical and Environmental security, Access Control, Cyber Security, Incident Reporting and so on • Audit Execution- Procedure and techniques • Assessment of IS Security & Cyber Security Controls for maintenance of

		• § Data Confidentiality • § Data Integrity • § Data Availability • Information Gathering • § Sources of information • § Methods of gathering information • § Systems for preserving information • Substantive Testing • § Data queries • § Sampling and data extraction • § Data Analysis • § Checklists for examination • Reporting, Documentation and Follow up of IS Security Audit findings
C.9.	Explain the quality processes that will be applied in the drafting process (see Due Process, page 7 and 8) along with the parties that the project group will consult and engage with.	The work will be carried out according to the Due Process. The quality process will cover the following: 1. The Project Team will function on the principle of continuous internal peer review of its products and mutual consultations. For this purpose, specific areas would be assigned to each Project Team member for specific inputs before initial drafting is taken up. These inputs will form the basis for drafting of Exposure Draft of the GUID. The Project Team will also review the existing material in the former ISSAI 5310, and existing international and national standards and guidance to identify all possible areas that need to be incorporated in the initial draft that would be taken up for discussions.

		2. The Project Team would have a two-stage internal peer review system. In stage I, the SAI India sub Team would deliberate upon the deliverables, and the inputs received from Subject Matter Experts from amongst the Project Team members (refer para 1), and draft a preliminary document for discussions. This discussion draft would be deliberated upon by the Project Team through exchange of emails to arrive at a mutually agreed upon draft. In stage II, the entire Project Team will engage through exchange of emails, tele-conferences, videoconferences and physical face-to-face meetings (if deemed required) for detailed deliberations and review of deliverables. These discussions would aim to flesh out the GUID. These interactions will follow a mutually agreed upon agenda circulated amongst the Project Team well in advance. The designated Subject Matter experts would lead these interactions for their respective areas. 3. While drafting, Drafting Guidelines issued by FIPP would be followed. Further, Project Team will ensure consistency with ISSAI 100 and other relevant ISSAIs viz. ISSAI 200, 300 and 400. 4. ISACA has been associated with the Project to ensure that the pronouncement is in line with the best international practices in the field. 5. Once the Project Team finalizes its deliverables, the same would be reviewed by FIPP, before they are circulated amongst the INTOSAI WGITA and the larger INTOSAI Community for comments and suggestions. This would enable auditors from different national settings to apply the pronouncement in their environment and determine universal applicability of the GUID. 6. Exposure draft will be posted on the www.issai.org for 90 days for comments and suggestions from INTOSAI community and other interested stakeholders.

		7. Final output i.e. the Endorsement Version of GUID, after approval by the FIPP, would be hosted on INTOSAI web site. 8. The GUID will be put through a language review by an expert before final adoption by the INCOSAI.

PART D: AUTHORITIES

PERSON	NAME	SURNAME	DATE	SIGNATURE
Project leader	SAURABH	NARAIN		
Responsible Goal Chair	RAJIV	MEHRISHI		