The Institute of Internal Auditors

Richard F. Chambers
Certified Internal Auditor
Qualification in Internal Audit Leadership
Certified Government Auditing Professional
Certification in Control Self-Assessment
Certification in Risk Management Assurance
President and Chief Executive Officer

T: +1-407-937-1200
E-mail: richard.f.chambers@theiia.org

April 24, 2019

International Organisation of Supreme Audit Institutions
Project Team for Exposure Draft of GUID 5100
Emailed to: goelrk@cag.gov.in and ir@cag.gov.in

Dear Sir/Madam:

The Institute of Internal Auditors (IIA) thanks INTOSAI for the opportunity to share comments on exposure drafts of Guidance on Audit of Information Systems and Guidance on Audit of Security of Information Systems.

For 78 years, The IIA and its more than 200,000 internal audit members have aided sound governance and risk-management efforts in public- and private-sector organizations, encouraging strong internal controls and an enterprisewide approach. Auditing information systems and security is top of mind in this age of digital transformation.

The IIA appreciates the working group's diligence in aligning the Exposure Draft for GUID 5100 with ISSAIs 100, 200, 300, and 400, and incorporating the expertise of practitioners.

In general, The IIA suggests in reference to Guidance on Audit of Security of Information Systems that the revision maintains clear definitions of, and references consistently, Information Systems Security and Cyber Security. Given the inconsistencies in the exposure draft definitions, for example of information systems, The IIA also suggests item 1.2 be removed to avoid any future misalignment between guidance and the WGITA-IDI Handbook on IT Audit.

Equipping the team with generalized knowledge for technical exposure, SAIs may also want to consider how this knowledge will be sustained and react to changes in technology and information systems. This may be pertinent to increasing awareness of cloud-based information systems provided as software as a service (SaaS). The IIA is aware that information systems providing end-to-end finance and ERP applications for small to medium enterprises are migrating at an increasing pace to cloud-based SaaS solutions.

With many information systems no longer being hosted locally and provided in the cloud as SaaS, the auditee may wish to take an alternative view of risk for items that they lose control of as a SaaS user, such as management of users and passwords and where data is stored and backed up. There may also be international regulatory considerations regarding data protection and information governance within constituent countries. For EU member states, this is prescribed by the General Data Protection Regulation (GDPR). This may provide SAIs with an opportunity to address the strategic importance to attach to information system security relative to cyber security, noting that the former may prove more of an imperative from the auditees' risk profile.

Specifically in reference to the Guidance on Audit of Information Systems Exposure Draft, The IIA offers the following suggestions:

- Para 5.3. Identify from the outset which financial applications are managed locally and which are managed as SaaS. It may be likely for those managed as SaaS that no support will be provided by the client's ICT Service because of the nature of its external hosting. Therefore, it might be wise to separate asset management to specifically examine application management — in effect, a robust populated application register. The applications control element referred to later in the document could then be used as a key control for this wider area.

- Para 5.3. For point 12, you should consider consolidating this within the context of the wider ICT Business Continuity. Cyber Incident Management now forms a major part of the identification and recovery routines, with the Disaster Recovery Plan being a key control to mitigate a total loss of systems and data. These remain important controls to consider, but it may be important to take into account the distinction between them as highlighted above when also involving incident management.

- Para 5.9. From a developmental point of view, SAIs may want to consider a level of upskilling with the general auditor population with IS auditors able to provide specific advice on risks, formulating audit plans and programs, and providing work paper reviews. As technology becomes embedded further in financial systems, this may become a must-have skill rather than a should-have skill for general auditors.

- Para 6.3. This is key to any IS audit initiation.

- Para 6.5. For points 6-7, an outlying risk would be that the defined process was not sufficiently robust prior to roll out. A key question to ask is, "what business analysis had been undertaken to define these processes?" Also, "what are the controls if the processes require change or revision?" For points 11-13, the auditor should also form an opinion as to the adequacy of these management areas. Processes may have been adopted, but these may not match the specific requirements of the organization for them to achieve service objectives.

- Para 6.7. This might be usefully embedded into para 6.5, as this advises on the additional assurance that the auditor may seek. This could help in the assurance required for the areas in 6.5.

- Para 6.9. Given the proposed audience, the guidance could provide an additional cross reference regarding definition and examples of a CAAT.

- Para 7.2. The guidance should reflect that auditors should be encouraged to use a glossary of terms in their report, as sometimes the substance of a finding may require reference to a very specific technical element. A glossary could cross reference the definition of an acronym or a term with a scenario-based explanation of how this operates in a controlled environment.

The IIA appreciates the opportunity to offer its comments, observations, and insights on this important guidance. Please don't hesitate to contact The IIA's Managing Director of Global Advocacy, Francis Nicholson, at francis.nicholson@theiia.org for questions or comments.

Best regards,

Richard F. Chambers

Richard F. Chambers, CIA, QIAL, CGAP, CCSA, CRMA
President and Chief Executive Officer
The Institute of Internal Auditors