**Detailed Outline of the proposed GUID on Information System Security Audit (Project 2.8 of SDP)**

|  |  |  |
| --- | --- | --- |
|  | **List of contents of the proposed GUID** | **Explanation of the intended inclusion of material** |
| 1 | Definitions- Information Systems, Information Security Framework, including Cyber Security | This section shall introduce Information System Security and Information System Security Audit. Another key explanation to be included in this section would be the relationship between a wider Information Technology Audit, and more specific Information System Security Audit.  It shall also define the key terms and concepts which shall be used in the guidance material.  This section shall also highlight the linkages between ISSAI 100, GUID on IT Audit (former ISSAI 5300) and the Handbook on IT Audit; and how the various guidance material may be used by SAIs. |
| 2 | ·Key elements of Information Systems’ Security | This section shall introduce the key elements of Information Systems Security for an audited entity such as information assets inventory, classification and prioritization of assets, risk factors which may impact assets, controls to be adopted for IS Security, Disaster Management and Business Continuity and various Management roles involved in IS Security.  The section shall facilitate the process of understanding the IS Security environment within the audited entity. |
| 3 | ·Necessity for Information Systems’ Security | This section shall introduce the key elements of Information Systems’ Security, such as ensuring confidentiality, integrity, availability of information. It shall also introduce related concepts of non-repudiation, authorization, authentication, etc. |
| 4 | Roles and Responsibilities of the Management in security of information systems | This section shall include generic classification of Management Roles and their Responsibilities, such as Information Owner, Data Custodian, System Owner,  Security Administrator,  Security Analyst, etc. |
| 5 | ·IS Security threats and counter-measures | This section shall include major categorization of security threats and counter- measures, which would be introduced in the guidance. The project team shall prepare a more detailed section on this topic, which may then be considered for incorporation into future versions of the Handbook on IT Audit. |
| 6 | ·IS Security Audit Planning | This section shall introduce the risk factors that may be considered before taking up IS Security Audit, either as a standalone assignment or as part of a larger IT Audit assignment. This section will also enlarge upon how, depending on the Audit criteria adopted, these assignments may be of Compliance Audit, Financial Audit or Performance Audit types. The guidance will also focus upon how the information security threats faced by the audit entities would also form part of a SAI’s overall risk management while firming up the Audit Plan prepared in accordance with ISSAI 100. |
| 7 | Risk based approach | This section shall provide linkage to the principles of adopting a risk based approach for all audit assignments, as laid down in ISSAI 100 which would be applicable for all IS Security Audit assignments too. |
| 8 | Identification of domain wise Audit Objectives | This section shall explain the process of identification of Audit Objectives across domains such as Asset Management, Physical and Environmental Security Management, Human Resources Security Management, Communications and Operations Management, IT Systems Acquisition, Development and Maintenance Management and Business Continuity and Disaster Recovery Management. |
| 9 | Audit Execution | This section will explain how the audit should be executed, in accordance with ISSAI 100 and GUID on IT Audit. Sections 10, 11 and 12 detail the audit process. |
| 10 | Assessment of IS Security Controls | This section would include a brief explanation on assessment of controls adopted by the audited entity across each of the audit domains identified above. |
| 11 | Information Gathering | This section will explain the 1) sources of information 2) methods of gathering information 3) and systems for preserving information |
| 12 | Substantive Testing | This section will define what substantive testing shall entail, in an IS Security Audit. |
| 13 | Reporting, Documentation and Follow up of IS Security Audit findings | This section will link the general reporting format and documentation of Information Security Audit, in line with ISSAI 100 and GUID on IT audit, and any specific requirements that reporting of an IS Audit might entail. |