

Section Two: Content

1.1 QUICK REFERENCE

Quick Reference Review

Chapter 1 outlines the framework for performing IS auditing, specifically including those mandatory requirements regarding IS auditor mission and activity, as well as best practices to achieve an appropriate IS auditing outcome. CISA candidates should have a sound understanding of the following items, not only within the context of the present chapter, but also to correctly address questions in related subject areas. It is important to keep in mind that it is not enough to know these concepts from a definitional perspective. The CISA candidate must also be able to identify which elements may represent the greatest risk and which controls are most effective at mitigating this risk. Examples of key topics in this chapter include:

- IS auditor roles and associated responsibilities, including expected audit outcomes: differences between IS auditing tasks within an assurance assignment and those within a consulting assignment.
- The need for audit independence and level of authority within the internal audit environment as opposed to an external context.
- Minimum audit planning requirements for an IS audit assignment, regardless of the specific or particular audit objective and scope.
- Understanding the required level of compliance with ISACA standards for IS auditing, as well as for ISACA guidelines.
- When planning audit work, the importance of clear identification of the audit approach related to controls defined as “general” versus auditing controls that are defined as “application controls.”
- Scope, field work, application and execution of the concepts included in “audit risk” versus “business risk.”
- The key role of requirements-compliant audit evidence when supporting the credibility of audit results and reporting.
- The reliance on electronic audit work papers and evidence.
- Purpose and planning opportunities of compliance testing versus substantive testing.
- Audit responsibility and level of knowledge when considering legal requirements affecting IT within an audit scope.
- The IS risk-oriented audit approach versus the complementary need for IS auditors to be acquainted with diverse IS standards and frameworks.
- Understanding the difference between the objectives of implemented controls and control procedures.
- Understanding evidence collection, sampling and evidence analysis techniques and its importance while conducting an IS audit.
- Understanding reporting and communication methods.

1.2 MANAGEMENT OF THE IS AUDIT FUNCTION

The audit function should be managed and led in a manner that ensures that the diverse tasks performed and achieved by the audit team will fulfill audit function objectives, while preserving audit independence and competence. Furthermore, managing the audit function should ensure value added contributions to senior management regarding the efficient management of IT and achievement of business objectives.

1.2.1 ORGANIZATION OF THE IS AUDIT FUNCTION

IS audit services can be provided externally or internally.

The role of the IS internal audit function should be established by an audit charter approved by senior management. IS audit

can be a part of internal audit, function as an independent group, or ~~integrated~~ within a financial and operational audit (see **exhibit 1.11**) to provide IT-related control assurance to the financial or management auditors. Therefore, the audit charter may include IS audit as an audit support function. The charter should clearly state management’s responsibility and objectives for, and delegation of authority to, the IS audit function. This document should outline the overall authority, scope and responsibilities of the audit function. The highest level of management and the audit committee, if one exists, should approve this charter. Once established, this charter should be changed only if the change can be and is thoroughly justified. ISACA IS auditing standards require that the responsibility, authority and accountability of the IS audit function are appropriately documented in an audit charter or engagement letter (1001 Audit Charter). It should be noted that an audit charter is an overarching document that covers the entire scope of audit activities in an entity while an engagement letter is more focused on a particular audit exercise that is sought to be initiated in an organization with a specific objective in mind.

If IS audit services are provided by an external firm, the scope and objectives of these services should be documented in a formal contract or statement of work between the contracting organization and the service provider.

In either case, the internal audit function should be independent and report to an audit committee, if one exists, or to the highest management level such as the board of directors.

1.2.2 IS AUDIT RESOURCE MANAGEMENT

IS technology is constantly changing. Therefore, it is important that IS auditors maintain their competency through updates of existing skills and obtain training directed toward new audit techniques and technological areas. ISACA IS Auditing Standards require that the IS auditor be technically competent (1006 Proficiency), having the skills and knowledge necessary to perform the auditor’s work. Further, the IS auditor is to maintain technical competence through appropriate continuing professional education. Skills and knowledge should be taken into consideration when planning audits and assigning staff to specific audit assignments.

Preferably, a detailed staff training plan should be drawn for the year based on the organization’s direction in terms of technology and related risk that needs to be addressed. This should be reviewed periodically to ensure that the training efforts and results are aligned to the direction that the audit organization is taking. Additionally, IS audit management should also provide the necessary IT resources to properly perform IS audits of a highly specialized nature (e.g., tools, methodology, work programs).

1.2.3 AUDIT PLANNING

Annual Planning

Audit planning consists of both short- and long-term planning. Short-term planning takes into account audit issues that will be covered during the year, whereas long-term planning relates to audit plans that will take into account risk-related issues regarding changes in the organization’s IT strategic direction that will affect the organization’s IT environment.