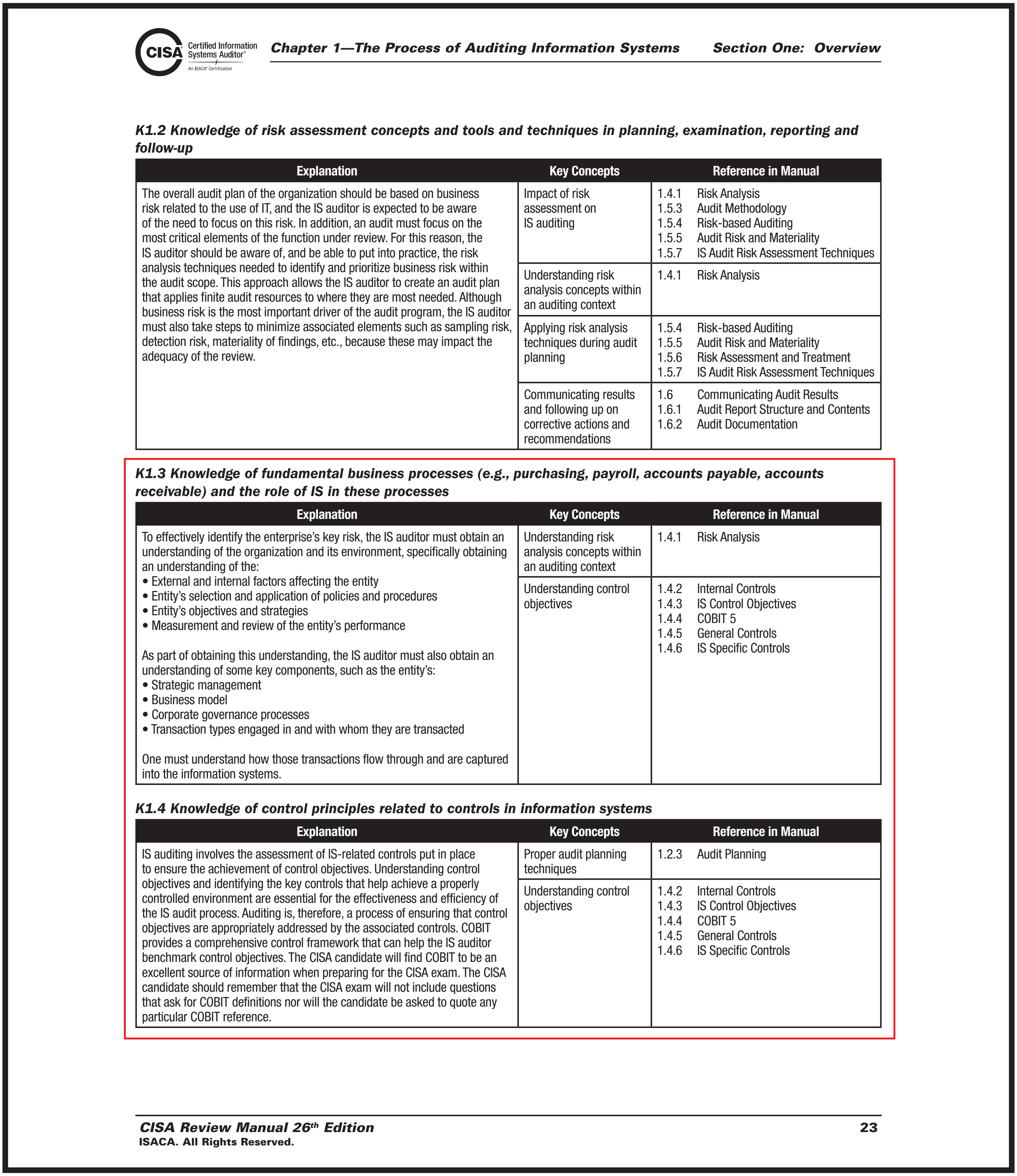
The following correction applies to pages 23-24 of the *CISA Review Manual 26th Edition*. The explanations, key concepts and references have been corrected for K1.3, K1.4 and K1.5.



K1.2 Knowledge of risk assessment concepts and tools and techniques in planning, examination, reporting and follow-up

Explanation	Key Concepts	Reference in Manual
The overall audit plan of the organization should be based on business risk related to the use of IT, and the IS auditor is expected to be aware of the need to focus on this risk. In addition, an audit must focus on the most critical elements of the function under review. For this reason, the IS auditor should be aware of, and be able to put into practice, the risk analysis techniques needed to identify and prioritize business risk within the audit scope. This approach allows the IS auditor to create an audit plan that applies finite audit resources to where they are most needed. Although business risk is the most important driver of the audit program, the IS auditor must also take steps to minimize associated elements such as sampling risk, detection risk, materiality of findings, etc., because these may impact the adequacy of the review.	Impact of risk assessment on IS auditing	1.4.1 Risk Analysis 1.5.3 Audit Methodology 1.5.4 Risk-based Auditing 1.5.5 Audit Risk and Materiality 1.5.7 IS Audit Risk Assessment Techniques
	Understanding risk analysis concepts within an auditing context	1.4.1 Risk Analysis
	Applying risk analysis techniques during audit planning	1.5.4 Risk-based Auditing 1.5.5 Audit Risk and Materiality 1.5.6 Risk Assessment and Treatment 1.5.7 IS Audit Risk Assessment Techniques
	Communicating results and following up on corrective actions and recommendations	1.6 Communicating Audit Results 1.6.1 Audit Report Structure and Contents 1.6.2 Audit Documentation

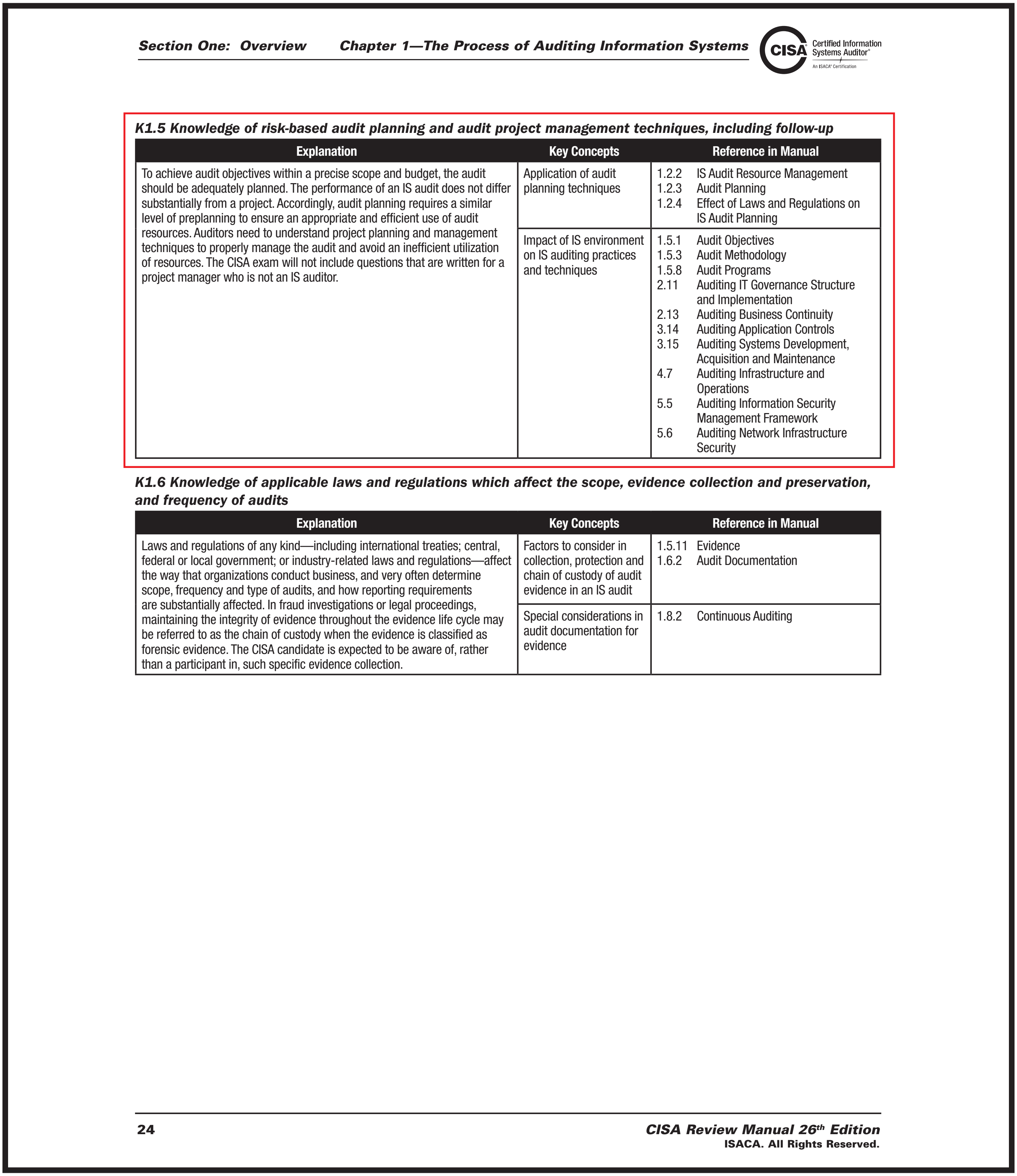
K1.3 Knowledge of fundamental business processes (e.g., purchasing, payroll, accounts payable, accounts receivable) and the role of IS in these processes

Explanation	Key Concepts	Reference in Manual
To effectively identify the enterprise's key risk, the IS auditor must obtain an understanding of the organization and its environment, specifically obtaining an understanding of the: • External and internal factors affecting the entity • Entity's selection and application of policies and procedures • Entity's objectives and strategies • Measurement and review of the entity's performance As part of obtaining this understanding, the IS auditor must also obtain an understanding of some key components, such as the entity's: • Strategic management • Business model • Corporate governance processes • Transaction types engaged in and with whom they are transacted One must understand how those transactions flow through and are captured into the information systems.	Understanding risk analysis concepts within an auditing context	1.4.1 Risk Analysis
	Understanding control objectives	1.4.2 Internal Controls 1.4.3 IS Control Objectives 1.4.4 COBIT 5 1.4.5 General Controls 1.4.6 IS Specific Controls

K1.4 Knowledge of control principles related to controls in information systems

Explanation	Key Concepts	Reference in Manual
IS auditing involves the assessment of IS-related controls put in place to ensure the achievement of control objectives. Understanding control objectives and identifying the key controls that help achieve a properly controlled environment are essential for the effectiveness and efficiency of the IS audit process. Auditing is, therefore, a process of ensuring that control objectives are appropriately addressed by the associated controls. COBIT provides a comprehensive control framework that can help the IS auditor benchmark control objectives. The CISA candidate will find COBIT to be an excellent source of information when preparing for the CISA exam. The CISA candidate should remember that the CISA exam will not include questions that ask for COBIT definitions nor will the candidate be asked to quote any particular COBIT reference.	Proper audit planning techniques	1.2.3 Audit Planning
	Understanding control objectives	1.4.2 Internal Controls 1.4.3 IS Control Objectives 1.4.4 COBIT 5 1.4.5 General Controls 1.4.6 IS Specific Controls

The following correction applies to pages 23-24 of the *CISA Review Manual 26th Edition*. The explanations, key concepts and references have been corrected for K1.3, K1.4 and K1.5.



Section One: Overview   Chapter 1—The Process of Auditing Information Systems

K1.5 Knowledge of risk-based audit planning and audit project management techniques, including follow-up

Explanation	Key Concepts	Reference in Manual
To achieve audit objectives within a precise scope and budget, the audit should be adequately planned. The performance of an IS audit does not differ substantially from a project. Accordingly, audit planning requires a similar level of preplanning to ensure an appropriate and efficient use of audit resources. Auditors need to understand project planning and management techniques to properly manage the audit and avoid an inefficient utilization of resources. The CISA exam will not include questions that are written for a project manager who is not an IS auditor.	Application of audit planning techniques	1.2.2 IS Audit Resource Management 1.2.3 Audit Planning 1.2.4 Effect of Laws and Regulations on IS Audit Planning
	Impact of IS environment on IS auditing practices and techniques	1.5.1 Audit Objectives 1.5.3 Audit Methodology 1.5.8 Audit Programs 2.11 Auditing IT Governance Structure and Implementation 2.13 Auditing Business Continuity 3.14 Auditing Application Controls 3.15 Auditing Systems Development, Acquisition and Maintenance 4.7 Auditing Infrastructure and Operations 5.5 Auditing Information Security Management Framework 5.6 Auditing Network Infrastructure Security

K1.6 Knowledge of applicable laws and regulations which affect the scope, evidence collection and preservation, and frequency of audits

Explanation	Key Concepts	Reference in Manual
Laws and regulations of any kind—including international treaties; central, federal or local government; or industry-related laws and regulations—affect the way that organizations conduct business, and very often determine scope, frequency and type of audits, and how reporting requirements are substantially affected. In fraud investigations or legal proceedings, maintaining the integrity of evidence throughout the evidence life cycle may be referred to as the chain of custody when the evidence is classified as forensic evidence. The CISA candidate is expected to be aware of, rather than a participant in, such specific evidence collection.	Factors to consider in collection, protection and chain of custody of audit evidence in an IS audit	1.5.11 Evidence 1.6.2 Audit Documentation
	Special considerations in audit documentation for evidence	1.8.2 Continuous Auditing

24   ***CISA Review Manual 26th Edition***
ISACA. All Rights Reserved.

Trust in, and value from, information systems