

The following correction applies to pages 74-75 of the *CISA Review Manual 26th Edition*. The explanations, key concepts and references have been corrected for K2.4 and K2.6.

K2.4 Knowledge of relevant laws, regulations and industry standards affecting the organization

Explanation	Key Concepts	Reference in Manual
<p>The complex nature of IT and global connectivity has introduced various types of risk within the organization's information life cycle—from receipt, processing, storage, transmission/distribution through destruction. In order to protect stakeholder interests, various legal and regulatory requirements have been enacted. The major compliance requirements that are considered globally recognized include protection of privacy and confidentiality of personal data, intellectual property rights and reliability of financial information. In addition, there are some compliance requirements that are industry specific. All of these drivers demand the development and implementation of well maintained, timely, relevant and actionable, organizational business policies, procedures and processes.</p> <p>Legislative and regulatory requirements pertaining to the access and use of IT resources, systems and data should be reviewed to assess whether the IT organization is protecting IT assets and effectively managing associated risk. For the CISA exam, the IS auditor must be aware of these globally recognized concepts; however, knowledge of specific legislation and regulations will not be tested.</p>	<p>Impact of legislative requirements on organizations standards, policies, procedures and processes</p>	<p>2.7.1 Policies 2.8.2 Risk Management Process 2.9.2 Sourcing Practices 2.9.6 Information Security Management 2.10.2 Segregation of Duties Within IT 2.10.3 Segregation of Duties Controls 2.11 Auditing IT Governance Structure and Implementation 2.11.1 Reviewing Documentation 2.11.2 Reviewing Contractual Commitments</p>

K2.5 Knowledge of the organization's technology direction and IT architecture and their implications for setting long-term strategic directions

Explanation	Key Concepts	Reference in Manual
<p>Effective IT strategic planning involves a consideration of the enterprise's requirements for new and revised IT systems and the IT organization's capacity to deliver new functionality through well-governed projects. Determining requirements for new and revised IT systems will involve a systematic consideration of the enterprise's strategic intentions, how these translate into specific objectives and business initiatives and what IT capabilities will be needed to support these objectives and initiatives. In assessing IT capabilities, the existing system's portfolio should be reviewed in terms of functional fit, cost and risk. The strategic IT plan should balance the cost of maintenance of existing systems against the cost of new initiatives or systems to support the business strategies.</p> <p>The IS auditor should be aware that a key input to determining the long-term strategic direction of an IT organization is the review, analysis and assessment of its IT architecture. The review, analysis and assessment may take the form of a road map and may illustrate current and future states. Review of the enterprise's IT architecture and its usage can help to determine whether management is following its IT strategy and whether that strategy needs to be adapted to changing business needs.</p>	<p>Relevance of different elements of enterprise architecture and their impact on IT governance</p> <p>Alignment of policies with enterprise architecture and their relation to IT governance</p>	<p>2.3.5 Enterprise Architecture 2.4.1 Strategic Planning 2.7.1 Policies</p>

K2.6 Knowledge of the processes for the development, implementation and maintenance of IT strategy, policies, standards and procedures

Explanation	Key Concepts	Reference in Manual
Senior management should define a process for developing IT strategies that achieve business objectives. These IT strategies must be based wholly on defined business objectives with a clear understanding of the relevant laws, regulations and industry standards that the organization must comply with across all locations within the enterprise.	Factors that contribute to the development and implementation of an IT strategy	2.4.1 Strategic Planning 2.8.2 Risk Management Process
The successful integration of both sound IT strategy and compliance processes enable organization to achieve business objectives. Key to this success is the quality of governance processes related to the development and implementation of IT strategic and tactical policies, standards and procedures. The IT strategy must be subjected to periodic review to ensure that the strategy continues to address both emerging and developing business needs and regulatory and industry risk. Specifically, good IT governance requires that all the dynamic industry and regulatory influences to be identified, considered as their impacts, approved by business executive management and subsequently monitored. These practices form part of the IT governance program and should be understood by the IS auditor.	Factors that contribute to effective information security governance and management	2.3.4 Information Security Governance 2.9.6 Information Security Management

K2.7 Knowledge of the use of capability and maturity models

Explanation	Key Concepts	Reference in Manual
The effectiveness and efficiency of IT governance efforts in the organization are dependent on the quality management strategies and policies that are embedded in the IT governance framework.	Understanding management techniques to continuously improve IT performance	2.5 Maturity and Process Improvement Models
The integration of defined processes and corresponding process management techniques across the organization's enterprise is related to the effectiveness and efficiency of the IS organization. Quality management strategies and policies outline how the IT strategies, policies, procedures and standards are maintained, used and improved over time as the organization changes.	Knowledge of quality standards	2.9.5 Quality Management 2.9.7 Performance Optimization
The IS auditor needs to understand how the development, implementation and integration of capability and maturity modeling quality tools, techniques and processes (TTPs) will facilitate and foster the quality of enterprise IT policies and procedures. These TTPs can be based on a variety of standard frameworks. The use of quality standards within an IS organization enhances the ability of the IT organization to realize greater value and mission success.		

K2.8 Knowledge of process optimization techniques

Explanation	Key Concepts	Reference in Manual
Maturity and process improvement models help enterprises evaluate the current state of their internal controls environment in comparison to the desired state and help identify activities for moving toward the desired state.	Current practices in measuring the maturity state of the organization	2.3.5 Enterprise Architecture 2.5 Maturity and Process Improvement Models
A variety of improvement and optimization methodologies are available that complement simple, internally developed approaches. These include: <ul style="list-style-type: none"> • Continuous improvement methodologies, such as the Plan-Do-Check-Act cycle and specifically as implemented during agile development/project management • Comprehensive best practices, such as ITIL® • Frameworks, such as COBIT and Val IT™ • The Zachman Framework™ 	Impact of sourcing practices on the current maturity state and desired maturity state	2.9.2 Sourcing Practices
This evaluation is important to the IS auditor because the results illustrate to executive management the effectiveness, compliance and relevance of its IT procedures, tools and processes in support of alignment with business needs. This evaluation can be further used to review management practices within IT to determine compliance with organizational IT strategies and policies.	Role of quality management in bridging the gap between current state and desired state	2.9.5 Quality Management 2.9.7 Performance Optimization