



# Information Technology Control Environment Self-Evaluation

	Response	Comments
<b>Information Technology Strategic Planning</b>		
(1) Has management prepared strategic plans for Information Technology that aligns business objectives with Information Technology strategies? Does the planning approach include mechanisms to solicit input from relevant internal and external stakeholders affected by the Information Technology strategic plans?		
(2) Does management obtain feedback from business process owners and users regarding the quality and usefulness of its Information Technology plans for use in the ongoing risk assessment process?		
(3) Does an Information Technology planning or steering committee exist to oversee the Information Technology function and its activities? Does committee membership include representatives from senior management, user management and the Information Technology function?		
(4) Are Information Technology strategies and ongoing operations formally communicated to senior management and the board of directors, e.g., through periodic meetings of an Information Technology steering committee?		
(5) Does the Information Technology organization ensure that Information Technology plans are communicated to business process owners and other relevant parties across the organization?		
(6) Does Information Technology management communicate its activities, challenges and risks on a regular basis with the CEO and CFO? Is this information also shared with the board of directors?		
(7) Does the Information Technology organization monitor its progress against the strategic plan and react accordingly to meet established objectives?		
<b>Information Technology Organization and Relationships</b>		
(8) Do Information Technology managers have adequate knowledge and experience to fulfill their responsibilities?		
(9) Have key systems and data been inventoried and their owners identified?		
(10) Are roles and responsibilities of the Information Technology organization defined, documented and understood?		
(11) Do Information Technology personnel have sufficient authority to exercise the role and responsibility assigned to them?		
(12) Does Information Technology staff understand and accept their responsibility regarding internal control?		



## Information Technology Control Environment Self-Evaluation

	Response	Comments
(13) Have data integrity ownership and responsibilities been communicated to appropriate data/business owners and have they accepted these responsibilities?		
(14) Is the Information Technology organizational structure sufficient to provide for necessary information flow to manage its activities?		
(15) Has Information Technology management implemented a division of roles and responsibilities (segregation of duties) that reasonably prevents a single individual from subverting a critical process?		
(16) Are Information Technology staff evaluations performed regularly (e.g., to ensure that the Information Technology function has a sufficient number of competent Information Technology staff necessary to achieve objectives)?		
(17) Are contracted staff and other contract personnel subject to policies and procedures created to control their activities by the Information Technology function, and to assure the protection of the organization's information assets?		
(18) Are significant Information Technology events or failures, e.g., security breaches, major system failures or regulatory failures, reported to senior management or the board?		
(19) Are controls in place to support appropriate and timely responses to job changes and job terminations so that internal controls and security are not impaired by such occurrences?		
(20) Does the Information Technology organization subscribe to a philosophy of continuous learning, providing necessary training and skill development to its members?		
(21) Has the Information Technology organization adopted and promoted the company's culture of integrity management, including ethics, business practices and human resources evaluations?		
(22) Has the entity established procedures for identifying and documenting the training needs of all personnel using information services in support of the long-range plan?		
(23) Does Information Technology management provide education and ongoing training programs that include ethical conduct, system security practices, confidentiality standards, integrity standards and security responsibilities of all staff?		

Points to Consider	Response	Comments
--------------------	----------	----------



## Information Technology Control Environment Self-Evaluation

Points to Consider	Response	Comments
<b>Information Architecture</b>		
(24) Has Information Technology management defined information capture, processing and reporting controls—including completeness, accuracy, validity and authorization—to support the quality and integrity of information used for financial and disclosure purposes?		
(25) Has Information Technology management defined information classification standards in accordance with corporate security and privacy policies?		
(26) Has Information Technology management defined, implemented and maintained security levels for each of the data classifications? Do these security levels represent the appropriate (minimum) set of security and control measures for each of the classifications? Are they reevaluated periodically and modified accordingly?		
<b>Communication of Management Aims and Directions</b>		
(27) Has Information Technology management formulated, developed and documented policies and procedures governing the Information Technology organization’s activities?		
(28) Has Information Technology management communicated policies and procedures governing the Information Technology organization’s activities?		
(29) Does Information Technology management periodically review its policies, procedures and standards to reflect changing business conditions?		
(30) Does Information Technology management have processes in place to investigate compliance deviations and introduce remedial action?		
(31) Does Information Technology management have a process in place to assess compliance with its policies, procedures and standards?		
(32) Does Information Technology management understand its roles and responsibilities related to the Sarbanes-Oxley Act?		

Points to Consider	Response	Comments
<b>Assessment of Risks</b>		
(33) Does the Information Technology organization have an entity- and activity-level risk assessment framework that is used periodically to assess information risk to achieving business objectives? Does it consider the probability and likelihood of threats?		
(34) Does the Information Technology organization’s risk assessment framework measure the impact of risks according to qualitative and quantitative criteria, using inputs from different areas including, but not limited to, management brainstorming, strategic planning, past audits and other assessments?		



## Information Technology Control Environment Self-Evaluation

Points to Consider	Response	Comments
(35) Is the Information Technology organization's risk assessment framework designed to support cost-effective controls to mitigate exposure to risks on a continuing basis, including risk avoidance, mitigation or acceptance?		
(36) Is a comprehensive security assessment performed for critical systems and locations based on their relative priority and importance to the organization?		
(37) Where risks are considered acceptable, is there formal documentation and acceptance of residual risk with related offsets, including adequate insurance coverage, contractually negotiated liabilities and self-insurance?		
(38) Is the Information Technology organization committed to active and continuous risk assessment processes as an important tool in providing information on the design and implementation of internal controls, in the definition of the Information Technology strategic plan, and in the monitoring and evaluation mechanisms?		
(39) Is access to the data center restricted to authorized personnel, requiring appropriate identification and authentication?		
(40) Has a business impact assessment been performed that considers the impact of systems failure on the financial reporting process?		
<b>Manage Facilities</b>		
(41) Are data center facilities equipped with adequate environmental controls to maintain systems and data, including fire suppression, uninterrupted power service (UPS), air conditioning and elevated floors?		

Points to Consider	Response	Comments
<b>Compliance With External Requirements</b>		
(42) Does the organization monitor changes in external requirements for legal, regulatory or other external requirements related to Information Technology practices and controls?		
(43) Are control activities in place and followed to ensure compliance with external requirements, such as regulatory and legal rules?		
(44) Are internal events considered in a timely manner to support continuous compliance with legal and regulatory requirements?		
<b>Management of Quality</b>		
(45) Is documentation created and maintained for all significant Information Technology processes, controls and activities?		



## Information Technology Control Environment Self-Evaluation

Points to Consider	Response	Comments
(46) Does a plan exist to maintain the overall quality assurance of Information Technology activities based on the organizational and Information Technology plans?		
(47) Are documentation standards in place, have they been communicated to all Information Technology staff, and are they supported with training?		
(48) Does a quality plan exist for significant Information Technology functions (e.g., system development and deployment) and does it provide a consistent approach to address both general and project-specific quality assurance activities?		
(49) Does the quality plan prescribe the type(s) of quality assurance activities (such as reviews, audits, inspections) to be performed to achieve the objectives of the quality plan?		
(50) Does the quality assurance process include a review of adherence to Information Technology policies, procedures and standards?		
(51) Have data integrity ownership and responsibilities been communicated to the appropriate data owners and have they accepted these responsibilities?		
<b>Manage Performance and Capacity</b>		
(52) Does Information Technology management monitor the performance and capacity levels of the systems and network?		
(53) Does Information Technology management have a process in place to respond to suboptimal performance and capacity measures in a timely manner?		
(54) Is performance and capacity planning included in system design and implementation activities?		
<b>Monitoring</b>		
(55) Have performance indicators (e.g., benchmarks) from both internal and external sources been defined, and are data being collected and reported regarding achievement of these benchmarks?		
(56) Has Information Technology management established appropriate metrics to effectively manage the day-to-day activities of the Information Technology department?		
(57) Does Information Technology management monitor IT's delivery of services to identify shortfalls and does Information Technology respond with actionable plans to improve?		
<b>Adequacy of Internal Control</b>		
(58) Does Information Technology management monitor the effectiveness of internal controls in the normal course of operations through management and supervisory activities, comparisons and benchmarks?		



## Information Technology Control Environment Self-Evaluation

Points to Consider	Response	Comments
(59) Are serious deviations in the operation of internal control, including major security, availability and processing integrity events, reported to senior management?		
(60) Are internal control assessments performed periodically, using self-assessments or independent audits, to examine whether or not internal controls are operating satisfactorily?		
<b>Independent Assurance</b>		
(61) Does Information Technology management obtain independent reviews prior to implementing significant Information Technology systems that are directly linked to the organization's financial reporting environment?		
(62) Does Information Technology management obtain independent internal control reviews of third-party service providers (e.g., by obtaining and reviewing copies of SAS 70, SysTrust or other independent audit reports)?		
(63) Is documentation retained in a manner that can be used by the independent auditor or examiner as a basis for reliance?		
<b>Internal Audit</b>		
(64) Does the organization have an Information Technology internal audit department that is responsible for reviewing Information Technology activities and controls?		
(65) Is the audit plan based upon a risk assessment that includes IT? Does it cover the full range of Information Technology audits, e.g., general and application controls, systems development life cycle?		
(66) Are procedures in place to follow up on Information Technology control issues in a timely manner?		