

# Module 6 – Documenting Processes and Controls

## Handout 2 – Entity-level Controls Questionnaire

A logical place to begin any comprehensive evaluation of internal controls is at the top—entity-level controls that might have a pervasive effect on the organization. This includes a consideration of factors in each of the five components of internal control that can have a pervasive effect on the risks of errors or fraud (i.e., control environment, risk assessment, information and communication, control activities, and monitoring). Documenting and evaluating internal control at the entity level does not by itself provide a complete perspective of internal control of an entity. However, it is an important starting point because the assessment of entity-level controls—particularly when weaknesses are identified—can have a significant effect on the overall assessment of the effectiveness of internal controls and procedures for financial reporting.

This questionnaire provides points to consider for each of the five components of internal control as part of documenting an organization's entity-level controls. These considerations serve as a guide to help gain an understanding of the culture and operating style of the agency. These points are not all-inclusive, and not all the points listed will apply to every entity. While a “no” response to an individual point does not necessarily mean that the entire component is ineffective, a “no” response should heighten awareness to potential weaknesses in internal control and indicate areas where management should focus attention.

**Note: This questionnaire is not required, but merely included as a guide for considering entity-level controls.**

<b>Control Environment</b>
Does management show concern for integrity and ethical values? Is there a code of conduct and/or ethics policy and has it been adequately communicated?
Is management’s commitment to integrity and ethical behavior communicated effectively throughout the organization, both in words and deeds? Does management lead by example?
Are those in top management hired from outside made familiar with the importance of high ethics and controls?
Does management take appropriate disciplinary action in response to departures from approved policies and procedures or violations of the code of conduct?
Do rewards, such as bonuses, foster an appropriate ethical tone (i.e., not given to those who meet objectives but, in the process, circumvent established policies, procedures, and controls?)
Is the management structure appropriate (i.e., not dominated by one of a few individuals) and is there effective oversight?
Is there a mechanism in place to regularly educate and communicate to management and employees the importance of internal controls, and to raise their level of understanding of controls?
Does management give appropriate attention to internal control, including the effects of information systems processing?
Does management set realistic financial targets and expectations for operating personnel?
Do personnel appear to have the competence and training necessary for their assigned level of responsibility or the nature and complexity of the entity’s business?
Does management possess broad functional experience (i.e., management comes from several functional areas rather than from just a few)?
Does management demonstrate a commitment to provide sufficient accounting and financial personnel to keep pace with the growth and/or complexity of the business environment?

# Module 6 – Documenting Processes and Controls

## Handout 2 – Entity-level Controls Questionnaire

Are there standards and procedures for hiring, training, motivating, evaluating, promoting, compensating, transferring, and terminating personnel that are applicable to all functional areas (e.g., accounting, information systems)?
Are there screening procedures for job applicants, particularly for employees with access to assets susceptible to misappropriation?
Are policies and procedures clear and are they issued, updated, and revised on a timely basis?
Are there written job descriptions, reference manuals or other forms of communication to inform personnel of their duties?
<b><i>Additional IT Considerations</i></b>
Has management prepared strategic plans for IT that align business objectives with IT strategies? Does the planning approach include mechanisms to solicit input from relevant internal and external stakeholders affected by the IT strategic plans?
Does the IT organization communicate its IT plans to business process owners and other relevant parties across the organization?
Does IT 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?
Does the IT organization monitor its progress against the strategic plan and react accordingly to meet established objectives?
Do IT managers have adequate knowledge and experience to fulfill their responsibilities?
Have relevant systems and data been inventoried and their owners identified?
Are roles and responsibilities of the IT organization defined, documented and understood?
Do IT personnel understand and accept their responsibility regarding internal control?
Have data integrity ownership and responsibilities been communicated to appropriate data/business owners and have they accepted these responsibilities?
Has IT management implemented a division of roles and responsibilities (segregation of duties) that reasonably prevents a single individual from subverting a critical process?
Has the IT organization adopted and promoted the entity’s culture of integrity management, including ethics, business practices and human resources evaluations?
Does IT management provide education and ongoing training programs that include ethical conduct, system security practices, confidentiality standards, integrity standards and security responsibilities of all staff?
<b>Risk Assessment</b>
Are key elements of the entity’s strategic plan communicated throughout the entity so all employees have a basic understanding of the entity’s overall objectives?
Is a process in place to periodically review and update entity-wide strategic plans?
Does the entity-wide strategic plan include IT or is there a separate IT strategic plan that addresses the technology needs of the entity to effectively and efficiently meet its strategic plan?
Does internal audit (or another group within the entity) perform a periodic (at least annual) risk assessment? If yes, does management review the risk assessment and consider actions to mitigate the significant risks identified?

# Module 6 – Documenting Processes and Controls

## Handout 2 – Entity-level Controls Questionnaire

Are budgets/forecasts updated during the year to reflect changing conditions?
Does the accounting department have a process in place to identify and address changes prescribed by GASB, as well as for approving changes in accounting made to address such changes?
Are there processes to verify the accounting department is made aware of changes in the operating environment so they can review the changes and determine what, if any, effect the change may have on the entity’s accounting practices?
Are there processes to verify the accounting department is aware of significant transactions so they can determine whether such transactions are appropriately accounted for and disclosed?
<b><i>Additional IT Considerations</i></b>
Does the IT organization have an entity- and activity-level risk assessment framework that is used periodically to assess information risk to achieving financial reporting objectives? Does it consider the probability and likelihood of threats?
Does the IT 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?
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? Where risks have not been accepted, does management have an action plan to implement risk response?
<b>Information and Communication</b>
Is the entity able to prepare accurate and timely financial reports, including interim reports?
Does management receive sufficient and timely information to allow it to fulfill its responsibilities?
Is there a sufficient level of coordination between the accounting and information systems processing functions/departments?
Are there appropriate policies for developing and modifying accounting systems and controls (including changes to and use of computer programs and/or data files)?
Are there significant applications or transactions that are executed /processed by service organizations? If yes, has management documented the relevant controls at the service organization, the entity, or both that mitigate the risk of errors?
Are there defined responsibilities for individuals responsible for implementing, documenting, testing and approving changes to computer programs that are purchased or developed by information systems personnel or users?
Is there a current disaster recovery plan for the significant components of the IT infrastructure?
Is there a business continuity plan that incorporates the disaster recovery plan and end-user department needs for timely recovery of critical business functions, systems, processes and data?
Are the lines of authority and responsibility (including lines of reporting) within the organization clearly defined and communicated?
Are there written job descriptions and/or reference manuals that describe the duties of personnel?
Are policies and procedures established for and communicated to personnel at decentralized locations?
Is there a process for employees to communicate improprieties? Is the process well communicated throughout the entity? Does the process allow for anonymity for individuals who report possible

# Module 6 – Documenting Processes and Controls

## Handout 2 – Entity-level Controls Questionnaire

improprieties?
<b><i>Additional IT Considerations</i></b>
Does IT management periodically review its policies, procedures and standards to reflect changing business conditions?
Does IT management have a process in place to assess compliance with its policies, procedures and standards?
<b>Control Activities</b>
Are accounting and closing practices followed consistently at interim dates (e.g., quarterly, monthly) throughout the year?
Is there appropriate involvement by management in reviewing significant accounting estimates and support for significant unusual transactions and non-standard journal entries?
Is there a budgetary system?
Does management review key performance indicators (e.g., budget, profit, financial goals, operating goals) regularly (e.g., monthly, quarterly) and identify significant variances? Does management then investigate the significant variances?
Is there an appropriate segregation of duties (e.g., separation of accounting for and access to assets, IT operations function separate from systems and programming, database administration function separate from application programming and systems programming)? Are organizational charts reviewed to verify proper segregation of duties exist?
Are there processes to periodically (e.g., quarterly, semi-annually) review system privileges and access controls to the different applications and databases within the IT infrastructure to determine if system privileges and access controls are appropriate?
Has management established procedures to periodically reconcile physical assets (e.g., cash, receivables, inventories, property and equipment) with related accounting records?
Are controls in place over dial-up access to the organization’s computer resources (e.g., firewalls; centralized directories to store and manage user identities and resource privileges; automated policy-based request, approval, and fulfillment process for enterprise access)?
Is critical computer data backed up daily and stored off-site?
<b>Monitoring</b>
Are procedures in place to monitor when controls are overridden and to determine if the override was appropriate?
Are policies and procedures in place to assure that corrective action is taken on a timely basis when control exceptions occur?
Does management respond timely and appropriately to the findings and recommendations of the auditors? Internal audit?
Are the results of internal audit activities reported to management and/or appropriate parties?
Does the internal audit department develop an annual plan that considers risk in determining the allocation of resources?
<b><i>Additional IT Considerations</i></b>
Is documentation created and maintained for significant IT process, controls and activities?

## **Module 6 – Documenting Processes and Controls**

### Handout 2 – Entity-level Controls Questionnaire

Does a quality plan exist for significant IT functions (e.g., system development and deployment) and does it provide a consistent approach to address both general and project-specific quality assurance activities?
Has IT management established appropriate metrics to effectively manage the day-to-day activities of the IT department?
Does IT management monitor IT's delivery of services to identify shortfalls and does IT respond with actionable plans to improve?
Does IT management obtain independent reviews of its operations, including policies, procedures, overall IT systems and processes, and do they assess adherence to those policies and procedures?
Does the organization have an IT internal audit that is responsible for reviewing IT activities and controls, including general and application controls? Is there a follow-up process for residual actions? Is there a mechanism to allow monitoring of internal control of third-party service providers?