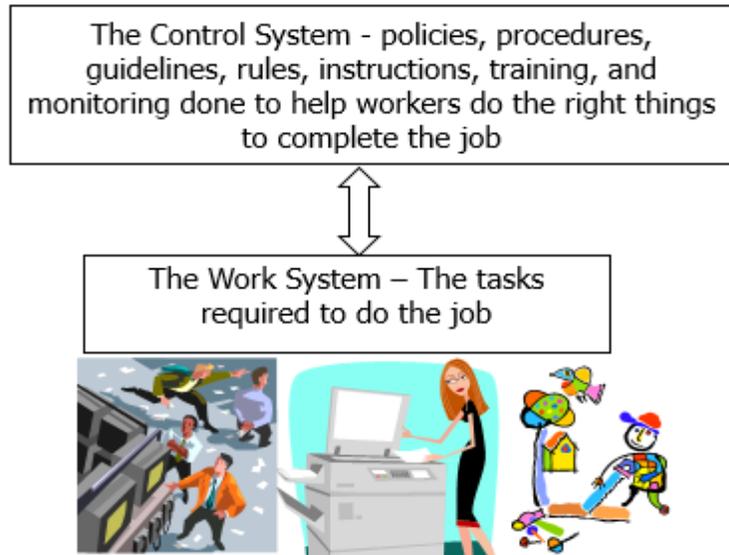


Larry's Cheat Sheet – Internal Controls

“Control” is the key to auditing – controls see that things get done, and are a key management responsibility. Controls are where auditors focus their attention, and can be simply defined as things management puts in place to be sure activities and work are done correctly.

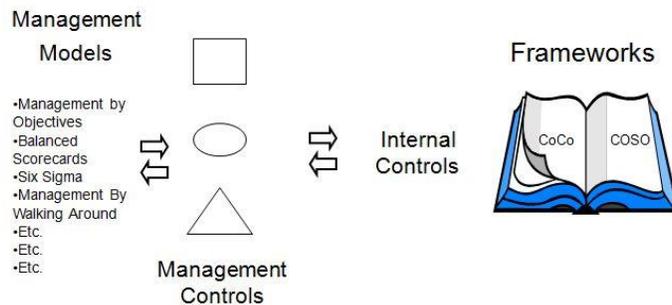
Every activity has two levels:

- the work system, which are the tasks required to do a job
- the control system, which overlays the work and are the policies, procedures, objectives, guidelines, rules, instructions, training and monitoring that management establishes to help be sure the job is done correctly and objectives are achieved.



Control Frameworks

Auditors see many different operations and managers, and must evaluate them all objectively. So, auditors need common criteria against which to evaluate for reporting to the board or senior management. That's where an internal control framework or model comes in. Think of “internal controls” as common criteria, and “management controls” as specific to a particular manager and management technique. Auditors are almost never expert enough in a business activity to determine the controls management should have in place without the use of a framework that defines good controls.



What Controls are not

Controls are not the actual steps required to do a job, so auditors do not (or should not) critique how people do the job. Controls are above that, and help people do the job right. That's where auditors focus.

Sometimes, controls are "part of the process" because of the way the process has been designed. For instance, obtaining credit approval before shipping products to a new customer is "part of the process" in some organizations. The reason it is called a "control" is that credit checking is not part of the actual shipping of the product - it is embedded in the shipping process, but it was put there by management to ensure the shipping and collection activities work right. A company could sell to anybody and just hope to get paid, but instead they do credit checks as a control to increase the probability of getting paid. Many steps, such as reconciliations and approvals and balancing, are embedded in business processes - but they are put there by management to help "control" the process and be sure the process works as planned.



Some Really Specific Things about Controls ...

- Controls are actual mechanisms – there is no such thing as a “soft” control.
- Management controls and internal controls are different things.
- Controls are nouns, not verbs (controls don't end with “ing”).
- Control frameworks are for auditors.
- Internal controls and risk management are both processes.
- A control does more than just respond to a risk.
- Risk assessment is a control.
- Setting objectives is a control.

A Simple Control Identification Approach

Control identification is the major effort in planning an audit. Here is a simple approach that works.

Based on the audit objectives, identify the major activities within the audit scope. (Activities are the major “things” the audit area does for the organization.) Then for each activity:

1. Identify the "steps to do the job" - that is, the major, unavoidable steps in the actual business process or activity. Three or four at most even for a major process.
2. Identify the controls embedded directly in the process flow (the Process Flow Controls) that are in place to be sure the process works right, for instance approvals, reconciliations, edits
3. Identify the people-based controls (Non-Process Flow Controls), such as training, policies and procedures, objectives, roles and responsibilities, measurements to be sure the people do their jobs related to the activity.
4. Identify any important risks that could occur, despite the controls above, and cause the process or activity to have a problem (residual risks). Always consider the risk of fraud here.
5. If you want to determine objectively if the control design is adequate, compare the above list of controls to the COSO framework.

Standard 2201- In planning the engagement, internal auditors must consider:

- The objectives of the activity being reviewed and the means by which the activity controls its performance;
- The significant risks to the activity, its objectives, resources, and operations and the means by which the potential impact of risk is kept to an acceptable level;
- The adequacy and effectiveness of the activity's governance, risk management, and control processes compared to a relevant framework or model; and
- The opportunities for making significant improvements to the activity's governance, risk management, and control processes.

Standard 2210.A3 - Adequate criteria are needed to evaluate governance, risk management, and controls. Internal auditors must ascertain the extent to which management and/or the board has established adequate criteria to determine whether objectives and goals have been accomplished. If adequate, internal auditors must use such criteria in their evaluation. If inadequate, internal auditors must work with management and/or the board to develop appropriate evaluation criteria.