Larry's Cheat Sheet – Operational Auditing

Definition – Operational auditing evaluates the procedures management uses to plan, organize and direct work against an established framework of internal control, such as COSO or CoCo.

Operational Auditing Techniques (in order of preference):

Internal Control Framework Approach – Determine the adequacy and effectiveness of management's controls, when compared to an internal control framework such as COSO. The primary tools are a COSO Map and a Risk/Control Matrix.
Value-for-Money Approach – Use of Twelve Attributes of Effectiveness, published by Canadian Comprehensive Audit Foundation in 1994, to determine the effectiveness, economy and efficiency of a program or operation.
Control Self-Assessment – Facilitated or survey-based approach where those directly involved in a business process or activity self-assess or evaluate their activities, using an agreed framework.
Maturity Model Approach – Identify the stages of maturity of a process according to an accepted model, such as the one in COBIT 4 (Non-existent, Initial, Repeatable, Defined, Managed, and Optimized).
Process-Based Approach – Evaluating the adequacy of controls over CAATS related to the Input, Processing and Output of a business process flow.
Effective Business Process Approach – Determining the effectiveness of a business process by identifying: 1) ownership and accountability; 2) level of definition and documentation of processes; 3) control points and measurements; 4) continuous process improvement.
Management Function Approach – Using surveys or interviews to determine effectiveness of planning, organizing, directing and controlling.
Risk-Based Approach – Evaluation of management's activities related to establishing objectives, identifying risks, and responding to the important risks.

Twelve Attributes of Effectiveness:

1. Management Direction
2. Relevance
3. Appropriateness
4. Achievement of Intended Results
5. Acceptance
6. Secondary Impacts
7. Cost and Productivity
8. Responsiveness
9. Financial Results
10. Working Environment
11. Protection of Assets
12. Monitoring and Reporting

Defined by Canadian Comprehensive Audit Foundation

Things to Remember about Operational Auditing:

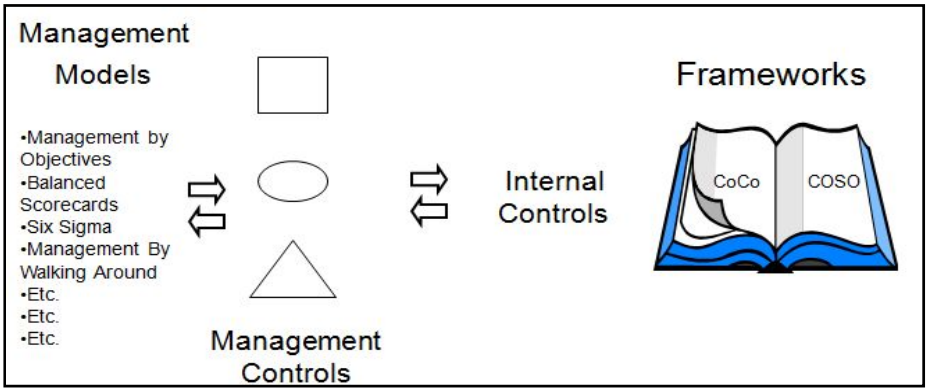
- You must have criteria to evaluate against – and it must be agreed in advance with management. "We think this is a better way" is NOT acceptable criteria.
- Operational auditing is still auditing, and is not the same thing as consulting. Consulting requires direct experience and expertise in the operation being done. Auditing requires experience and expertise in applying the agreed-upon criteria, and familiarity with the operation.
- Those doing the operation will always know more about the operation than the auditors. They are the experts.
- Other efforts, like ISO, TQM, and BSC are also part of risk assessment, ERM, and internal controls, and are great approaches to evaluating operational controls.
- Setting SMART objectives is one the most important internal controls. SMART – Specific, Measurable, Attainable, Relevant, Time-bound
- No manager uses Internal Controls to achieve objectives – they use whatever management method or models work for them.
- Internal Control frameworks are for auditors.
- "Best Practices" require evidence, and are unique to the organization.

Regarding Risks:

- You cannot flowchart risks – if you flowchart it, just look for CAATS controls over Input, Processing and Output, and then think about WCGW (What Could Go Wrong).
- Most risk responses are part of I/T process flows.
- In Risk Assessment the discussion IS the value.
- Be specific about risks – a generic list of risks is a starting point, not an end result.
- Don't spend time trying to predict the future – you cannot.

Process Flow Objectives (CAATS):

- Complete
- Authorized
- Accurate
- Timely
- Safeguarded



Larry@LHubbard.com
In USA: (301) 529-8118

Larry's Cheat Sheet – Operational Auditing

A Simple Control Framework

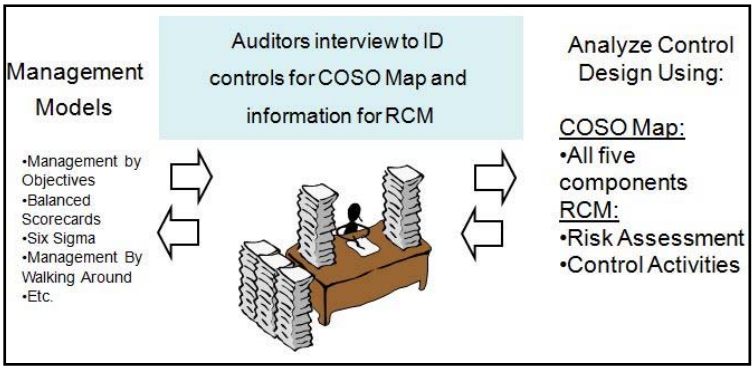
1. Identify the "steps to do the job" - that is, the major steps in the actual business process or activity.

2. Identify the controls embedded directly in the process flow - the Process Flow Controls.

3. Identify the Non-Process Flow Controls, such as training, policies and procedures, and clarity of roles and responsibilities.

4. Use a Risk/Control Matrix to identify any important risks that could occur, despite the controls above, and cause the process or activity to have a problem, and determine what to do about those risks.

5. Compare the above risks and controls to The COSO Map.



The COSO Map – Five Steps of Internal Control

1. Internal or Control Environment - the tone of the organization, which impacts and sets the basis for how objectives, internal controls and risks are viewed and addressed by the organization's people
1.1 Integrity and ethical values
1.2 Commitment to competence
1.3 Board of Directors and Audit Committee activities
1.4 Management's philosophy and operating style
1.5 Organization structure
1.6 Assignment of authority and responsibility
1.7 Human resource standards
1.8 Risk management philosophy and appetite

2. Risk Assessment - Objectives, Risks, Responses - procedures used to establish organizational objectives and analysis of relevant risks to achievement of the objectives, forming a basis for determining how the risks should be managed.
2.1 Entity-wide objective setting
2.2 Activity- and process-level objective setting
2.3 Identification and assessment of internal, external and fraud risks
2.4 Planned responses to risks: Avoid, Reduce, Share, Accept

3. Control Activities - Policies and procedures that help ensure management's directives and risk responses are carried out.
3.1 Responses that reduce or share specific risks
3.2 Responses that prevent or detect the risk of intentional or unintentional errors
3.3 Actions by direct functional or activity management
3.4 Analytical analyses
3.5 IT infrastructure controls
3.6 Top-level reviews of activities
3.7 Industry- or function- or objective-specific controls
3.8 Other management and quality initiatives

4. Information and Communication - Identifying, capturing and communicating information in a timeframe and method that enables people to carry out their responsibilities

4.1 Mechanisms that support information flow inside the organization
4.2 Mechanisms that support information flow outside the organization
4.3 Indicators and measurements
4.4 Style of communications

5. Monitoring - assessing the operation of controls over time

5.1 Ongoing monitoring of control components
5.2 Separate, periodic evaluations of control components
5.3 Reporting and correcting deficiencies in controls

The above was accumulated from Internal Control - Integrated Framework, Enterprise Risk Management (ERM) Integrated Framework, and Internal Control over Financial Reporting (ICFR), Guidance for Smaller Public Companies.

Risk/Control Matrix

Business Objective: _____

Controls Presently in Place
- Control 1
- Control 2
- Control 3
- Control 4

What could still go wrong (WCGW)	Other Controls
– Risk 1	Control 5 (exists now)
– Risk 2	Control 6 (new control)
– Risk 3	Control 2 (exists now)
– Risk 4	Accept this risk

Larry@LHubbard.com
In USA: (301) 529-8118