ASSESSING THE EFFECTIVENESS OF INTERNAL CONTROLS OVER COMPLIANCE

Caroline McMichen, CCEP, CIA

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

1

Polling Question

Does your organization evaluate the effectiveness of internal control activities to reduce risk as part of its overall risk management or Sarbanes-Oxley compliance process?

- Yes
- No
- I don't know

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

2

Assessing Effectiveness of Internal Controls

In the session, we will discuss:

- internal control concepts and definitions
- the different types of internal controls
- how internal controls can be used to reduce compliance risk
- how monitoring and auditing can be used to assess effectiveness of internal controls

We will also put what we learned to use in a group exercise.

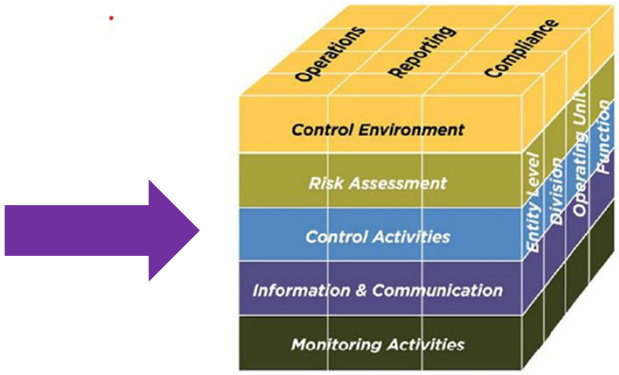
Key Concepts and Definitions*

Internal Control is "a *process*, effected by an entity's board of directors, management, and other personnel, designed to provide *reasonable assurance* regarding the *achievement of objectives* relating to *operations, reporting, and compliance*."

*COSO Internal Control – Integrated Framework

Key Concepts and Definitions*

Internal Control consists of five integrated components working together:



*COSO Internal Control – Integrated Framework

5

5

5 Integrated Components	17 Principles
Control Environment	1. Demonstrates commitment to integrity and ethical values 2. Exercises oversight responsibility 3. Establishes structure, authority, and responsibility 4. Demonstrates commitment to competence 5. Enforces accountability
Risk Assessment	6. Specifies suitable objectives 7. Identifies and analyzes risks 8. Assesses fraud risk 9. Identifies and analyzes significant change
Control Activities	10. Selects and develops control activities 11. Selects and develops general controls over technology 12. Deploys control activities through policies and procedures
Information and Communication	13. Uses relevant information 14. Communicates internally 15. Communicates externally
Monitoring Activities	16. Conducts ongoing and/or separate evaluations 17. Evaluates and communicates deficiencies

Adapted from the COSO "internal Control – Integrated Framework

6

6

Control Activities

Within the system of internal control, ***control activities*** are developed to mitigate risks to the achievement of the organization's objectives, including compliance risks.

There are two types of control activities:

1. ***Preventive Controls*** are designed to keep errors and irregularities (or compliance violations) from occurring.
2. ***Detective Controls*** are designed to detect errors and irregularities (or compliance violations) that have already occurred.

Control activities are performed at all levels of the organization, throughout business processes and systems and can be automated or manual.

Control Activities

Control Activities are evaluated on both their ***design*** and ***operating effectiveness***.

- ***Design*** – Is the control activity designed to mitigate the risk of an error, irregularity or compliance violation to an acceptable level if operating effectively?
- ***Operating Effectiveness*** – Is the control properly implemented and functioning as designed?

Control Activities - Example

Process: Procurement

Risk: Unauthorized payments are made to third parties

Control Activity: All transactions must be approved by someone with the appropriate authority as indicated in the Company's approval matrix. Approval limits are tied to user credentials in the system. An automated preventive control exists in the system to operate on every transaction. If user does not have appropriate authority, the transaction is routed to the next appropriate level for approval.

Control Activities – Polling Question

What if the control activity in the previous example was a manual control? How might that affect its operating effectiveness?

A. Increase effectiveness
B. Decrease effectiveness
C. No difference in effectiveness

Control Activities Impact on Risk

- ***Inherent Risk*** – "The risk to an entity in the absence of any direct or focused actions by management to alter its severity."
- ***Residual Risk*** – "The risk remaining after management has taken action to alter its severity."

Source:

A Compliance Example – Competition Law

Event: A sales representative at XYZ company plans to attend a trade show where competitors will be present.

Risk: Discussions about pricing, markets, territories or other competitively sensitive matters may take place which could violate or appear to violate Competition law.

1. What is an example of a control activity that could prevent a compliance violation from occurring in this situation?
2. What are some design considerations?
3. How might we determine if the control is operating effectively?

Control Activities – Polling Question

When evaluating residual risk following a test of the control's operating effectiveness, when would you consider residual risk to be at an acceptable level?

A. When there is no risk remaining
B. When management is willing to accept the risk that remains
C. When the remaining risk is within established tolerances

13

Control Design

Design considerations include:

Ownership, accountability	Documentation, evidence
Automated or manual	Resources Required
Frequency	Degree of risk mitigation
Significance	Cost - Benefit

A deficiency in control design exists if the control is operating as intended and yet it still does not mitigate risk to an acceptable level.

14

Assessing Operating Effectiveness

Testing plan considerations include:

- Nature
- Timing
- Extent

Tests of operating effectiveness may include:

- ***Inquiry*** of those who perform the control activity
- ***Observation*** of the control activity being performed
- ***Examination of documentation*** that provides evidence of the control being performed
- ***Reperformance*** of the control activity to verify the outcome
- Review of ***Data Analytics***

15

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

15

Assessing Operating Effectiveness - Example

Control #	Business Process / Task	Compliance Risk	Control Activity	Testing Plan
1	Procurement / Onboarding a new business partner	Corruption - Business Partner engages in illegal or unethical activity while working on our Company's behalf	All potential business partners are screened for possible compliance violations following established compliance due diligence process	• Interview procurement personnel • Review documentation to support completed due diligence for all business partners added to the system during the prior quarter
2	Same as above	Same as above	Standard Anti-corruption language must be included in all third-party contracts	• Select a sample of 25% of contracts completed during the year to determine that appropriate language was included

16

16

Assessing Operating Effectiveness

Two approaches to control testing:

Ongoing monitoring usually consists of established or regularly scheduled processes or activities generally used to determine whether internal control activities are operating as intended or to identify "red flags" that may require more detailed evaluation or auditing.

Auditing tools and techniques are typically more targeted in nature and often used for areas identified as higher risk through your risk assessment or monitoring activities.

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

17

Monitoring Examples - C&E Programs

Some common tools and techniques for ongoing monitoring of compliance and ethics control activities are:

- ***Code of Conduct or policy affirmation and disclosures***
  - Monitor % affirmed and follow up on exceptions, look for trends
- ***Training data***
  - Monitor completion rates, other available data and identify negative trends
- ***Surveys and questionnaires***
  - Measure knowledge levels, cultural issues, engagement
- ***Evaluation of hotline reporting trends***
  - Track trends in anonymous vs. identified reporting, "hot spots"

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

18

Monitoring Examples - C&E Programs

Some common tools and techniques for ongoing monitoring of compliance and ethics control activities are:

- ***Self-assessments, self-reporting***
  - Review existing internal control (SOX) assessments, online self-reporting tools (COI, G&E)
- ***Trend analysis of accounts and/or transactions***
  - Budget-to-actual reviews, G&A expense levels
- ***Automated controls embedded in business processes***
  - Approvals, workflow
- ***Review of identified risk indicators***
  - Red flags for potential corruption, cash vs credit card T&E reimbursement

19

Monitoring Examples - C&E Programs

Some common tools and techniques for ongoing monitoring of compliance and ethics control activities are:

- ***Listening to communications (internal and external)***
  - Investor/Analyst calls, town halls, sales meetings
- ***Benchmarking***
  - Hotline statistics, program elements, culture surveys
- ***Conducting Focus Groups***
  - High risk areas

20

Auditing Examples – C&E Programs

Some common tools and techniques for auditing of compliance and ethics control activities are:

- Onsite visits and interviews
- Detailed transaction testing using appropriate sampling
- Use of forensic or fraud audit techniques to identify exceptions
- Verification of monitoring results or reperformance of control activities
- Exception review and follow up

Monitoring and/or Auditing?

Considerations:

- Evaluate cost/benefit of each activity based on the relative risk of the particular compliance area
- Determine organizational capability
- Consider ability to work with internal or external partners

Assessing Residual Risk

Inherent Risk – "The risk to an entity in the absence of any direct or focused actions by management to alter its severity."

Target Residual Risk - "the amount of risk that an entity prefers to assume in the pursuit of its strategy and business objectives, knowing that management will implement, or has implemented, direct or focused actions to alter the severity of the risk"

Actual Residual Risk – "The risk remaining after management has taken action to alter its severity."

Source:

Consider:

- What was the impact of control activities on inherent risk?
- How might that change your compliance risk assessment?
- Is remaining risk at an acceptable level (consistent with risk appetite and within tolerance levels) or is additional remediation desired?

23

Impact on Compliance Risk Assessment

24

Group Exercise

In this exercise, we will:

- Identify risk areas
- Identify business processes associated with a risk area
- Identify internal control activities that will help to mitigate that risk
- Develop a testing plan for the internal control activities
- Analyze results and their impact on risk and the risk assessment

Group Exercise – Review Scenario

You are the new Compliance Officer of Trendsetter, a publicly traded global clothing business headquartered in the United States. Trendsetter sells clothing both in its own retail outlets and major department stores. In addition to the U.S. business, Trendsetter has recently expanded its retail outlets in Europe and India through M&A activity, acquiring new sales employees in those locations. There is a rapid growth plan in place for both of these new markets.

We have identified two areas of increased compliance risk following Trendsetter's acquisitions and growth plans:

- Data Privacy
- Bribery & Corruption

Group Exercise – Identify Business Processes

What business processes do you think create possibilities of non-compliant activities related to data privacy or bribery and corruption? Identify a business process for your selected compliance risk. Consider the following:

Data Privacy:

- What personal data have we collected on our employees and our customers?
- When and how is it collected, processed, stored?

Bribery & Corruption:

- Where are the opportunities for corrupt practices and how might you identify red flags?
- What activities within the business process could present these opportunities and where (in what systems) might they be recorded?

Group Exercise – Identify Business Processes

Compliance Risk	Business Process / Task	Control Activity	Preventive/ Detective	Testing Plan

Group Exercise – Identify Internal Controls

For your selected business process, identify an internal control that could be put in place to mitigate that risk.

Consider:

- Would the control reduce risk to an acceptable level, or would additional controls be required?
- Is the control preventive or detective?
- Is it automated or manual?
- Can it be tested?

29

Group Exercise – Identify Internal Controls

Compliance Risk	Business Process / Task	Control Activity	Preventive/ Detective	Testing Plan

30

Group Exercise – Develop Testing Plans

For your selected internal control, determine a way to test its operating effectiveness.

Consider:

- How will the control be tested for operating effectiveness, when and by whom?
- What evidence or documentation will be required?
- How frequently should it be tested?

Group Exercise – Develop Tests

Compliance Risk	Business Process / Task	Control Activity	Preventive/ Detective	Testing Plan

Group Exercise – Analyze Results

Based on the results of your control test, consider:

- Are the results acceptable based on our company's risk appetite and tolerance?
- Are additional controls or remediation efforts required to mitigate risk to an acceptable level?
- What impact might the results have on our risk assessment?

33

Impact on Compliance Risk Assessment

34