Compliance Risk Assessment and Management Workshop

Society of Corporate Compliance and Ethics and
Health Care Compliance Association

1

1

RISK RESPONSE AND MITIGATION

Gwendolyn Lee Hassan, JD, CCEP
gwenhassan@yahoo.com
708-932-6437

2

2

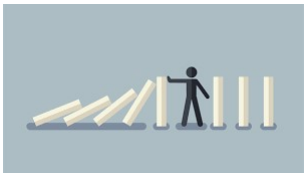
Overview

- The difference between remediation and mitigation
- Types of controls
- Three Lines of Defense
- Cost Benefit Analysis of Controls
- Root Cause Analysis
- Remediation Plans

3

Remediation and Mitigation

- Remediation = Elimination of a threat
- Mitigation = Limiting and minimizing the damage from a threat



4

Preventive v. Detective Controls

- Preventive Controls are designed to prevent a loss
  - Separation of duties
  - Documentation
  - Limiting physical access to assets
  - Requiring authorizations
- Detective Controls, on the other hand, are designed to detect or discover a loss that has already occurred
  - Reconciliations
  - Audits
  - Variance reviews

Why have controls?

- What do these controls accomplish?
- Are we seeking to reduce the likelihood of a particular risk?
- Are we seeking to reduce the impact of a particular risk?

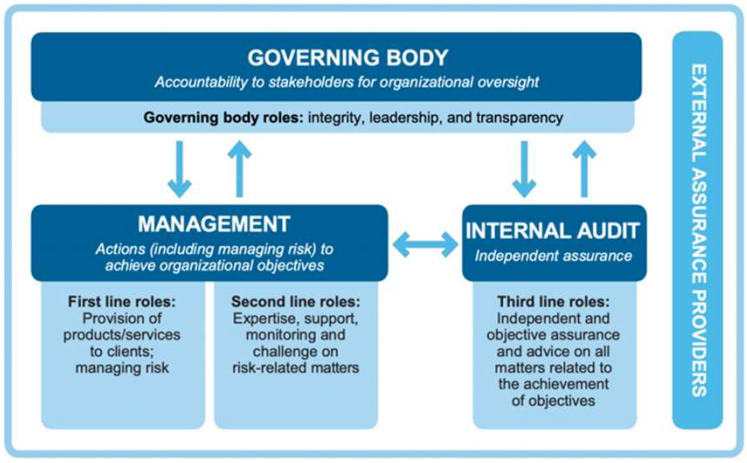
The three lines of defense

- Who "owns" risk within an organization?
- Who is responsible for preventive controls?
- What about detective controls?

7

Three lines of defense

The IIA's Three Lines Model



8

Who should create controls?

- Compliance
- The business unit involved
- Internal audit team
- ERM team
- SOX controls team
- All of the above

Residual risk

- Does your control reduce likelihood or impact or both?
- How do you estimate risk reduction?
- Can a risk ever be completely controlled?

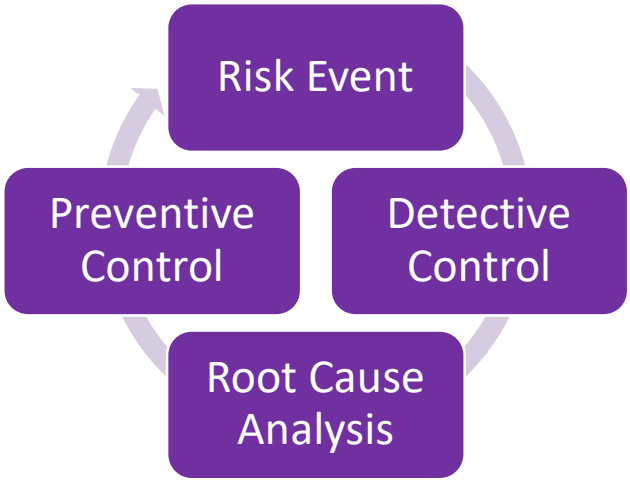
Trial and error

- Document the rationale behind your estimate
- Test it out!
- Monitor risk trends and occurrences over time to test the effectiveness of your control
- Benchmark with others to see how effective their controls have been

Control Cost-Benefit Analysis

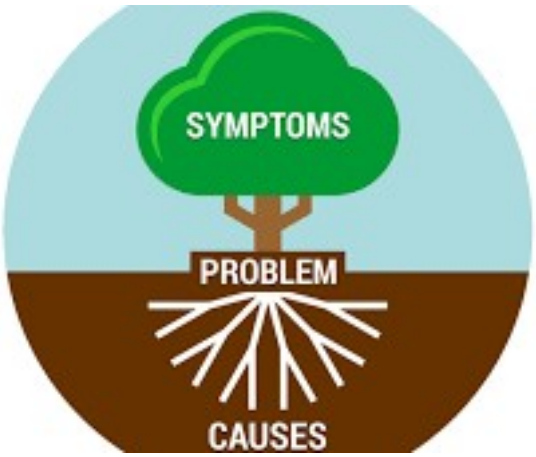
- Is it "worth it" to attempt to completely eliminate risk?
  - Keep your organization's risk tolerances in mind
- Risk controls have an opportunity cost
  - Make sure the cost of controls in terms of lost opportunity doesn't outweigh the potential benefit

Controls are only part of the story



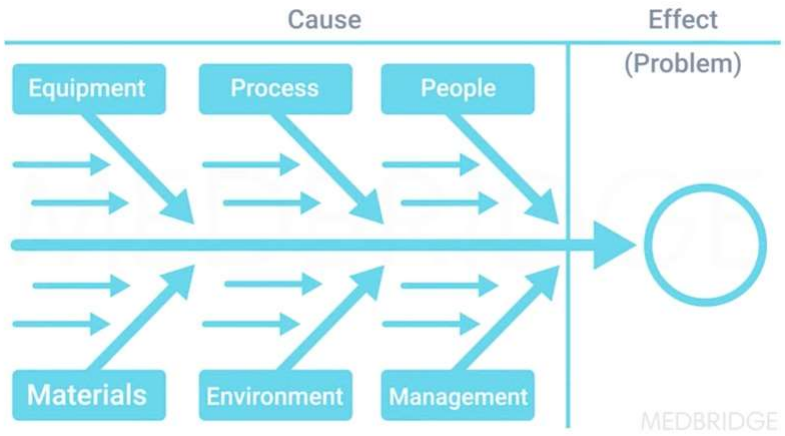
13

Root Cause Analysis



14

Fishbone Analysis



15

The 5 Whys

16

Polling Question

- An employee in a far-flung satellite office needs to renew a government permit of some sort to keep that local office's business registration current and compliant. They apply for the permit and wait and wait and wait for it to be renewed with no response. They take money out of petty cash and pay a bribe to the local official who immediately issues the license. What is the "root cause" of this issue?

A. Availability of petty cash
B. Allowing local permitting issues to be handled locally
C. Lack of proper bribery prevention training
D. Local government inefficiency and corruption
E. Failure to build-in proper waiting time into renewal process

Risk remediation plan

- Discussion of the risk event
- Agreement upon the root cause of the risk, can it be eliminated?
- Consensus on recommended improvements to:
  - preventive controls
  - detective controls

Risk remediation plan

- How will you know your risk remediation plan is working?
- Build in the measures or data you will use to determine effectiveness in advance
  - Make sure you follow-up and test
- What if it doesn't work as intended? How will you fix?
  - Remediating your remediation plan!

Timing of a risk remediation plan

- Don't wait!
- Target of 30 days cadence between:
  - risk event and remediation plan development
  - plan development and full implementation
  - implementation and testing/verification
- All risks fully remediated in 90 days

Reporting about risk remediation plans

- Who should receive reports?
- How often?
- What should the report include?
  - Risk events
  - Owner
  - Root cause
  - Remediation plan

21

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

21

Test your plan

- You can't develop and implement a risk remediation plan and then forget about it!
- You must determine if it was effective in remediating risk
  - Did it work as intended?
  - How will you know?

22

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

22

Exercise

Risk Event: Helpline call alleges favoritism towards female subordinate by male boss.

- Investigation reveals employees are married, did not disclose marriage to rest of team or compliance but did tell department VP who "approved".

Existing controls:

- Preventive: Employees required to report potential conflicts annually in written certification. Conflicts of Interest policy prohibits family members from reporting to each other. Bi-annual training on conflicts.
- Detective: Automated conflict of interest reporting system encourages employees to report violations through global helpline.

- What is the root cause of this issue? Are these controls effective? What remediation plan would you suggest? What other information would be helpful?

Exercise Results

- Root Cause
- Effectiveness of Controls
- Remediation Plan
- Other information that would be helpful

Exercise

Risk Event: Third party intermediary being paid commission rate that is 200% higher than any other intermediary in the region.

Existing controls:

- Detective: Discovered through variance review of general ledger payments outside of certain limits
- Preventive: Third Party Intermediary Policy requires all commission amounts above a certain percentage must be approved in writing by local sales leader. Global helpline.

What is the root cause of this issue? Are these controls effective? What remediation plan would you suggest? What other information would be helpful?

Exercise Results

- Root Cause
- Effectiveness of Controls
- Remediation Plan
- Other information that would be helpful

Wrap-Up

- Root cause analysis is crucial
- In order to respond to risk, you need to determine effectiveness of controls
- Your remediation plan:
  - Develop it with the risk owner (remember 3 Lines of Defense)
  - Do it promptly
  - Test your remediation plan – did it work?
    - If not, why (root cause analysis!)
    - Do you need to remediate your remediation plan?

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association