Compliance Best Practices

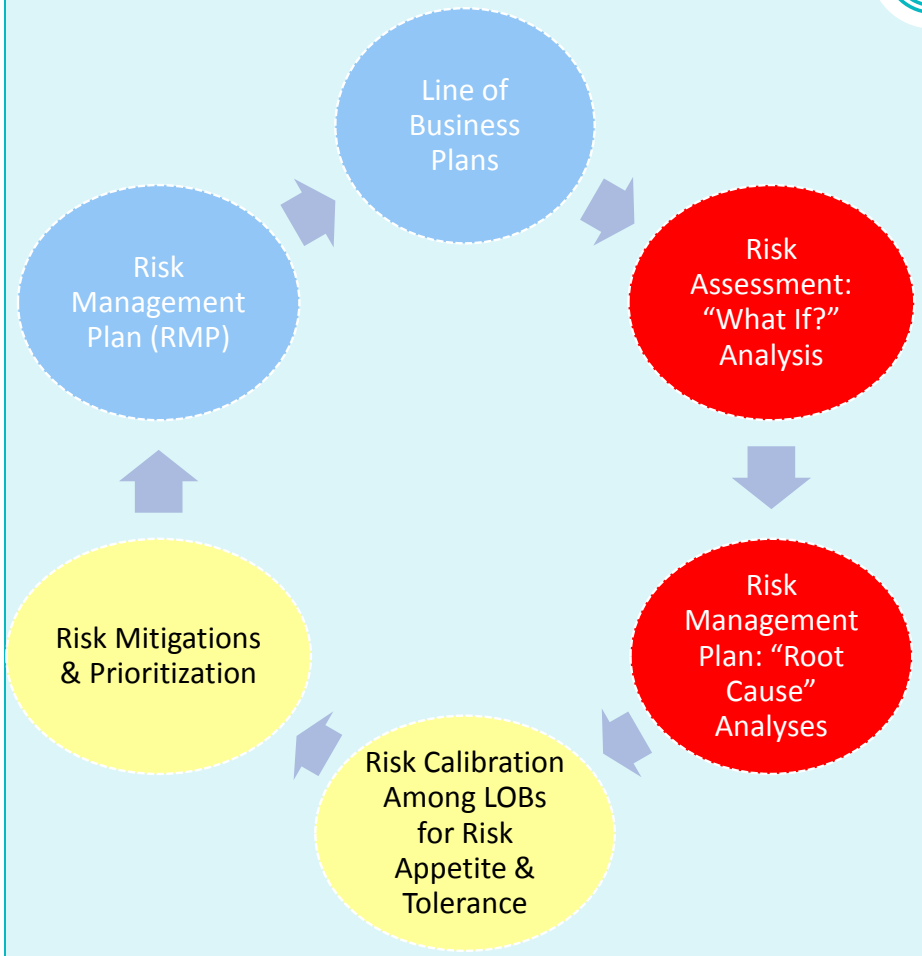
Fabiana Lacerca-Allen
2016

Compliance Program Best Practices

- Risk Assessment
- Program Governance & Resources
- Guidance Documents
- Compliance Controls
- Communications/Training
- Monitoring & Auditing
- Investigations & Response
- Enforcement, Discipline & Incentives

Risk Assessment

3



- Red actions are **Risk Assessment** and **Management** (mitigation) related.
- Consider Business plans. Ask "What if things do not go as planned; what is the impact and what is the likelihood of such?"
  - This identifies risks. Once Risks are identified Risk Mitigations are formulated.
- To determine mitigations, use **Root Cause Analysis**. Here, relationships among risks are identified. Ask: "If we take the action to reduce Risk X, will it also reduce the related Risks Y and Z?"
- Strong risk mitigations **address multiple risks** because they address the Root Causes of related risks.

Risk Assessment Best Practices

- Follows a clearly stated process
- Is aligned with the compliance strategy
- Includes senior members of the leadership team
- Is regularly validated and updated

Program Governance & Resources

- The compliance group is organized to enhance accountability, insight and access to both leaders and members of the organization regarding ethics and compliance matters
- The right people are in the right places, resourced appropriately and fostering an environment where issues are raised without fear of retaliation
- The organization has the right “tone at the top,” that makes integrity and ethics integral parts of doing business.

Program Governance & Resources Best Practices

- Robust compliance program has a seasoned Chief Ethics and Compliance officer that is responsibility for delineating and implementing an enterprise wide compliance program
- Is member of the Senior Executive Team and reports to the CEO and BoD
- Reports regularly on compliance to the senior team and chairs a Compliance Committee which includes senior members of the team
- The compliance department is well resourced and is seen as independent and unbiased
- Senior members of the organizations certify to compliance

Guidance Documents

A compliance program should have clearly stated standards and procedures, a well disseminated code of conduct and policies and procedures designed to facilitate compliance with applicable laws and regulations. There should be a system to regularly review and update policies and procedures.

Guidance Documents Best Practices

- Policies and procedures are well disseminated and readily accessible to all employees
- Adherence is part of performance reviews
- Policies and procedures are reviewed and updated according to a schedule and on time
- Employees at all levels are trained on policies and procedures
- Third parties acting on the company's behalf should adhere to the company's policies
- A process for communicating new and updated policies

Compliance Controls

- Management controls assure that work proceeds consistent with ethical, regulatory, and organizational expectations
- Controls consist of:
  - Policies
  - Procedures
  - Work Instructions/Processes
  - Reporting Relationships
  - Rewards and Sanctions
- Compliance Controls: management controls designed to assure compliance
  - Controls to assure that things happen the right way, **not** the wrong way

Compliance Controls Best Practices

- Functioning, independent compliance audit program
- Compliance indicators are integrated into regularly tracked and reported business metrics
- Functioning and fully resourced compliance investigations program
- Insight to 100% of policies and procedures companywide
- Insight to corrective and preventive action plans companywide

Communications/Training

Communications and training are key elements of the compliance program because they heighten awareness among all employees and emphasize the organization's commitment to ethical business behavior. Compliance education is essential for employees at all levels. High quality and consistent compliance messaging demonstrates a mature, high performing compliance program.

Communications/Trainings Best Practices

- Compliance training is seamlessly integrated into employee training plans
- Employees and managers are held accountable for ensuring training occurs within prescribed timing
- Live training sessions whenever possible with examples, in relevant terms
- Newsletter with frequently asked questions/best practices, success stories
- Participate in business strategy sessions: understanding objectives and potential issues early can help tailor relevant training

Monitoring and Auditing

- Audit is a key *compliance program* control
  - Audit plans and schedules control risk as part of risk management
  - Corrective and Preventive Actions (CAPA) implement compliance risk reduction
- Monitoring is a collection of *business* controls
  - Dashboards
  - Status reports
  - Employee evaluation process
  - Risk mapping and prioritization

Compliance Audit Best Practices

- Compliance Audit is separate function from Internal Audit
- Auditors are trained and resourced to execute risk-based audit plans
- Auditor teams have a mixture of dedicated and ad-hoc professionals
  - Cadre of compliance auditors lead audit teams
  - Ad-hoc auditors are trained, but staff audit teams on an as-needed basis as part of their development and to spread compliance excellence across the organization

Compliance Monitoring Best Practices

- Businesses conduct compliance monitoring as part of their routine reports
- Compliance indicators are part of business dashboards
- Both leading and lagging indicators are used in monitoring
  - Leading indicators: provide insight to how things are going
  - Lagging indictors: describe how things have gone

Investigation & Response

All potential compliance violations should be logged and investigated according to policy.

- Detailed documentation is critical:
  - A description of the content and how it was reported
  - A description of the investigative process
  - List of relevant documents reviewed
  - Employee interview questions and notes
  - Changes to policies and procedures
- The government calls for prompt reporting of misconduct to the appropriate governmental authority within a reasonable period

Investigation & Response Best Practices

- Policy that clearly states how to report potential compliance violations and how investigations will be conducted
- Possibility to anonymously report potential compliance investigations, and a policy that ensures no retaliation for reporting
- All reports should be investigated and compliance logs kept
- Investigation results should be discussed with the BoD and senior leadership
- Remediation/prevention plans should be designed and executed to address any issues encountered

Enforcement, Discipline & Incentives

- Enforcement is necessary for the compliance program to be credible
- There should be appropriate incentives to perform activities with integrity and in compliance with applicable laws, regulations and the Code of Conduct.
- There should also be clear consequences for violations of compliance, up to and including termination

Enforcement, Discipline & Incentives Best Practices

- Appropriate disciplinary measures for engaging in criminal conduct and for failing to take reasonable steps to prevent or detect criminal conduct
- Policies and Procedures (Fair, Equitable, Consistent)
- Written Policy Statement
  - Noncompliance will be punished
  - Failure to report noncompliance will be punished
  - Outline of disciplinary procedures
  - Parties responsible for appropriate action
  - Discipline should be objective, fair and consistent