The Establishment of the Compliance Function: The Framework and the Role of Internal Auditing

Waheed Alkahtani, CFE and CCEP

November 2017

Outlines

1. Why Compliance: to Comply or not to Comply?
2. The Role of Auditing in the Compliance Function
3. The basic elements of a compliance function
4. The Framework and Implementation Strategies
5. Key References
How it was started
To comply or not to comply?

Corporate Compliance Organization

The Corporate Compliance Organization is a centralized, enterprise-wide organization charged to help the Company and its global network of companies comply with laws, regulations, rules, industry codes, and organizational policies and standards that promote and reinforce a corporate culture of adherence to the highest ethical and legal standards.
Compliance-related Offices

Organizational Risks
Why

It is

Risky?

The “carrot and stick” philosophy


• “ Corporations can, and should, be incentivized to self-police, and with respect to compliance and ethics”
Trend: Legislation and Regulation is increasing

- Foreign Corrupt Practices Act (US 1977)
- OECD Anti-Bribery Convention (1997)
- Inter-American Convention Against Corruption (1997)
- UN Convention Against Corruption (2003)
- G20 Action Plan Against Corruption
- Bribery Act (UK 2010)
- Amendment No. 8 to Article 164 (China 2011)
- Federal Law No. 97-FZ (Russia 2011)

Foreign Corruption Practices Act (US 1977)

FCPA top ten penalties in 2014 vs 2007
The Cost of Not to COMPLY

<table>
<thead>
<tr>
<th>Company Name</th>
<th>Penalty</th>
<th>Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Siemens (Germany)</td>
<td>$1.6 billion</td>
<td>2009</td>
</tr>
<tr>
<td>Alstom (France)</td>
<td>$772 million</td>
<td>2014</td>
</tr>
<tr>
<td>KBR / Halliburton (USA)</td>
<td>$579 million</td>
<td>2009</td>
</tr>
<tr>
<td>BAE (UK)</td>
<td>$400 million</td>
<td>2010</td>
</tr>
<tr>
<td>Total (France)</td>
<td>$398 million</td>
<td>2013</td>
</tr>
</tbody>
</table>

In 2014, 10 companies paid $1.56 billion to resolve FCPA cases.

Making a Business Case: Selling Compliance to Management

- Protect the Company, the Board, the Brand and Reputation
- Avoiding the Big Legal Stick if someone blow the whistler
- It’s a Global Trend
- It Could Happen Here: when was the last time you checked?
- It’s Not Optional
Do you have management agreement?

- Get going immediately: Get the foundations in place ASAP.
- Get it in writing, such a document will be important as proof of board support if the integrity of the program is ever challenged.
- Awareness: make sure everyone affected in the company is notified, and make sure you, or whoever is meant to run the program, have the authority to do what needs to be done.
- You are now on your way!.....Good luck

2

Internal Audit are Compliance
Best Friend
Frist who and then where
Internal Auditing

• Auditing is an independent examination and evaluation of something performed to provide an objective second opinion.
• Effective auditing enhances confidence in management and accountability processes.
• Internal Auditing is management oriented.
• Internal auditors are management team members who report to the CEO/senior management and Audit Committee and who are responsible for assuring that the CEO/senior management are in a position to make optimally informed decisions.

Overview

IA assist the Board and Management in effective corporate governance, business risk management and internal control.

We provide objective, independent, professional and risk-based ASSURANCE and ADVISORY services designed to help achieve Saudi Aramco’s business objectives.
Assurance and more...

- Stakeholder expectations of internal audit’s role within governance, risk, and compliance (GRC) have evolved from a control assurance function to one of leadership and guidance for focusing the organization’s efforts.

- The broad cross-functional nature of internal audit’s work uniquely qualifies the department to “connect the GRC dots” across the organization and provide guidance in the design and implementation of the GRC operating approach.

- Few areas within any organization can efficiently and cost effectively provide the coordination, collaboration, and integration needed to develop and maintain GRC effort like internal audit.

The Role Of Auditing In The Compliance Function

- Can COMPLIANCE be born from the womb of Auditing
- Internal Audit can add value to the compliance FUNCTION.
- Internal Audit and the Compliance Office can be effective partners.
- Serve as a member of the Compliance Committee.
- Finally, compliance is on your audit plan, and it is good to be aware
Compliance Office Role

- To develop, implement, and monitor an effective compliance function to coordinate organization-wide initiatives to prevent, detect, and respond appropriately to compliance risks.
- Independent, objective evaluator, consultant, and advisor.
- Compliance Office is management oriented.
- Compliance Officers are management team members who report to the CEO/senior management and Compliance Committee and who are responsible for assuring that the CEO/senior management are in a position to make optimally informed decisions.

IA and Compliance

- Internal auditors provide an independent and objective assessment of the effectiveness and efficiency of a company's operations, specifically its internal control structure. The internal audit function helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.
- The scope of internal auditing is broad and may involve the efficiency of operations, IT controls, the reliability of financial reporting, deterring and detecting fraud, and compliance with laws and regulations.
- Internal Auditors may also conduct compliance and operational audits, offering solutions for weaknesses in internal controls and verifying that all laws and regulations are upheld.
Same or Different Roles and Responsibility

- Twenty-two comparative categories were identified:
- Requirement, purpose, **reporting**, internal authority, span of responsibility, **Professional standards**, level of focus, **primary focus from a risk standpoint**, activity focus, Relationship to management, training responsibility, monitoring, impact on internal audit plan, follow-up, **investigation**, hotline, information systems, and internal controls.

### Knowing the Difference

**Internal Audit**
- Risk Based Audit Plan
- Independent of Management
- Assessing Internal Control System
- Looking at the past and present to provide assurance
- Expertise in controls, risk management, and governance processes
- After-the-fact
- Considers strategic, operations, reporting, and compliance objectives

**Compliances Functions**
- Schedule based
- Part of Management
- Detecting violations and correcting action
- Looking at the present and towards the future
- Expertise in industry-specific requirements, standards, and practices
- Continuous and (near) real-time
- Focus on compliance objectives
Who Carries the Compliance FLAG?

- Independent
- Authorized
- Competent

Best Practice ACFE, AICPA, IIA, and SCCE

Who, and then where?

- The compliance officer and the compliance committee
- The reporting structure
  - CEO/CFO
  - General Counsel vs General Auditor
  - The Board
- Shape the compliance committee and develop the charter
- Appoint the CCO: Duties and responsibilities
Oh, one more thing

Private

Government

The Basics
Compliance Basic Elements
Seven Essential Elements of the Compliance Program developed by

- Standards of conduct, policies and procedures (including a Code of Conduct)
- Oversight and accountability
- Education, communication and awareness
- Enforcement, discipline and incentives
- Reporting and Escalation
- Monitoring and auditing and risk assessment
- Ongoing program improvements

The is no one size fits all
1- Establish policies for specific issues and areas

- Assessment of the existing Policies and review of present procedures, which are an essential part of the Integrated Policy Framework, and suggest changes / modification in the existing policies and also recommend additional policies, if any that the company needs to develop and implement which may not be presently followed or documented.

What is the most critical function in the Compliance Process?
2- Oversight and accountability

- Scope/Purpose
- Composition
- Duties and Responsibilities
  - Compliance Committee

- Independent
- Connected
- Empowered
  - Compliance Officer

- Duties and Responsibilities
  - Board

- Duties and Responsibilities
  - Management

3- Education and Awareness

**How**
- Email/Posters
- CBT and eLearning
- Public Presentations

**When**
- The proper launching date
- Time frame
- Special occasion/event

**Who**
- Managers & other supervisors
- General employee
- Functions: Engineering, Procurement, Inspection
- Vendors, contractors & suppliers
4- Enforcement, discipline and incentives

- **Internal Investigation Policy**
  - Who is responsible
  - Hotline

- **Disciplinary actions**
  - None retaliation
  - Employees vs None employees and Vendor

- **Rewards**
  - Informants
  - Suspects

5- Reporting and Escalation

- **Objective**
  - Develop a Communication strategy to inform management and form a measurement tool

- **Categories**
  - Periodic/Ad hoc
  - Internal/External
  - Status vs studies

- **Escalation Procedure**
  - Selection criteria
  - Framework
6- Auditing and Monitoring

Compliance Program Risk Inventory

<table>
<thead>
<tr>
<th>Forensic Accounting</th>
<th>Conflicts of Interest</th>
<th>Antitrust/Competition law</th>
<th>Document Management/Retention</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Financial statements</td>
<td>• Gifts and gratuities</td>
<td>• Collusive conduct (e.g., price-fixing, market allocation)</td>
<td>• Retention of documents during investigations</td>
</tr>
<tr>
<td>• Books and records/off-books accounts</td>
<td>• Entertainment</td>
<td>• Unfair practices/business offences (disparagement, inducing breach of contract, infringing)</td>
<td>• Retention of required records</td>
</tr>
<tr>
<td>• Revenue/cost manipulation</td>
<td>• Ownership interests</td>
<td>• Monopolization/abuse of dominant position</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Outside employment and job offers</td>
<td>• Price discrimination</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Corporate opportunities</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

7- Ongoing Improvement

- Evaluating Effectiveness
- Program indicators
- Surveys, focus groups, testing
- Self and external assessment
- Periodical Benchmarking
Bonus 3 - The most critical function in the Compliance Process

Hotline

Reporting and Escalation

4

The HOW question?
The Framework and Implementation Strategies
Seven Essential Elements of the Compliance Program developed by SCCE

- Standards of conduct, policies and procedures (including a Code of Conduct)
- Oversight and accountability
- Education, communication and awareness
- Enforcement, discipline and incentives
- Reporting and Escalation
- Monitoring and auditing and risk assessment
- Ongoing program improvements

Change Management Theory

- Assess
- Build
- Measure
- Adjust

Change Management
The Compliance Framework

- **Assessment**
  - Perform a risk assessment and determine the level of risk.
  - Evaluate likelihood and significance.
  - Mitigation Plans.

- **Compliance**
  - Understand law and regulation.
  - Obtain and/or establish policies for specific issues and areas.
  - Code of Conduct.
  - Business Ethics Program.
  - Whistleblower and Hotline Policies.

- **Correction**
  - Hotline.
  - Conduct Scheduled and Unscheduled Audits.
  - Red Flags and Cont. Audits.
  - Monitoring and Data Mining.
  - Monitor compliance with laws and regulations.

- **Prevention**
  - Educate on the policies and procedures and communicate awareness.
  - Top Management.
  - New Hires.
  - Vendors and Contractors.
  - All means.

- **Detection**
  - Monitor compliance with laws and regulations.

Minimum Level of Protection

What ...

What Should, Can, Must Be Done?
Set the Tone from the Top
First, get the green light

You must be the change you wish to see in the world.
The Challenging Elements

Actions speak louder than words.

People follow what you say without following the intent

Leading by Example

What the Corporate Rhythm?

Tone at the Top
- Needs to go further than just adhering to the same standards as everyone else.

Mood in the Middle
- Do they feel squeezed between carrying out edicts from the top and facing the realities from the field of actually getting the job done

Buzz at the Bottom
- How do they feel about the ethical climate?
Building Blocks

Gap Analysis Methodology

Gray Area
- Not Enough Accountability

Overlapping
- Inefficient Redundancy

Dark
- No Accountability
Polices and Procedures
Module ONE

Establish policies for specific issues and areas

• Review of existing policies, which are an essential part of the Integrated Policy Framework.
• Suggest changes / modification in the existing policies and also recommend additional policies.
• Document the List of policies to be reviewed
Policy Setting – Drafting & Finalization

- Clarity on principles and coverage regarding policies
- Discussions with Process Owners and key personnel
- Draft policy preparation
- Discussion with quality board
- Final approval

Polices and Procedures

1. Code of Conduct
2. Competition and Fair Dealing
3. Sexual Harassment Policy
4. Whistle Blower Policy
5. Hot line Policy
6. Legal Compliance Policy
7. Safety Policy
8. Record Maintenance Policy
9. Compliance Policy
10. Gifts and Gratuities
11. Participation in political activities
12. Insider Trading
13. Risk Management Policy level
14. Risk Management Effectiveness
15. Corrupt practices
17. Conflicts of Interest
18. Proper Use of Company Assets
19. Corporate Governance Code
20. Non-Disclosure Agreements
Enforcement and Investigation
Module TWO

ACFE In-House Fraud Investigation Teams: 2017 Benchmarking Report
How to respond to an incident

Small
- Establish ownership and accountability.
- Outsource.

Medium
- Establish ownership and accountability.
- Formation of forensic investigations.

Large
- Internal unit to address prevention, detection, investigation and remediation of fraud.

Who Investigate and Examine Fraud?

Cyber Crimes

White Collar Crimes

Property Crimes

Violent Crimes
Who Investigates Irregularities?

- Independent
- Authorized
- Competent

Consistency

Best Practice ACFE, AICPA, IIA, and SCCE

Proposed Investigation Process

Before
- Hotline
- Assess and weight the risk
- Assign the proper risk index
- Evaluating the initiation of investigative procedures

Investigation
- Conduct the investigation and integration
- Case management system
- Produce the investigation report

After
- Reporting
- Quality Review
- Ensure the implementation of corrective actions
- Communicate case results to authorized entity
The result of the screening process

Calls ➔ Complaints ➔ Cases

Level 1  Level 2  Level 3

Reported issue Processing

- Investigate & Address
- Analysis: Review reports and analyze
- Track: Outline measures and performance
- Remedy: Review, recommend enhancements

Report
- Intranet
- Emails
- Fax
- Phone
From Good to Great

mining for hotline gold
all that glitters is not gold

Top questions that you need to answer

1. Is it a human error
2. Is it violation of company policies
3. Is it violation of laws and regulations
4. Is it a type of fraud?
5. What are the consequences of doing nothing?
Business-focused investigation

- Investigation to Discipline Employee
- Investigation to Assess Controls
- Investigations outside your SOW and Grievance

What is Final Decision
Investigation Measuring and Key Performance Indicators

- **Type**
  - Allegation
  - Inquiries

- **Identity**
  - Anonymous
  - Named

- **Source**
  - group,
  - location
  - business lines

- **Level of employees**
  - Management
  - Professionals
  - Education

- **Reporting methods**
  - Online
  - Phone
  - Fax
  - email
  - walk in

Other useful measures

- Life cycle
- Actions
- Recoveries
- Substantiation rates
- Geographic/BL distribution
- Trends against prior years
Define your module and Profile you suspect

Predator

Fraudster

Accidental

Investigation categories

Finance
- Accounting, Auditing and Financial Statement

Business Ethics
- Fraud, Conflicts of interest and Bribes

Abuse/Corruption
- Code Violation, Release of proprietary info, misuse of corporate property

Human Resources
- Discrimination, Harassment, Employment Law Violation and Compensation

Other
- Environmental, Health and Safety
What may cause changes

- News and Media
- Regulatory Changes
- Awareness and Training
- A Real Problem

Investigation killing factors

- Discouraging callers with questions or requests for advice.
- Long investigation cycle.
- Failure to publish sanitized outcomes for employees.
- Neglecting trends and benchmarks.
Other Challenges

Call Analysis: So much data, but not always clear

Benchmarking: The need to demonstrate the hotline’s effectiveness

Reporting: The need to report meaningful and actionable data to management

Final thought

The fear of retaliation

Who cares? Nothing will happen

Why don’t people report?
5

Reference and Templates
Global Bodies and International Associations

Global Bodies
Sample Policies and Procedures

- **The Complete Compliance and Ethics Manual from the SCCE**

![SCCE Logo]

---

**Auditors Red Flags and Breaking Points 1**

<table>
<thead>
<tr>
<th>CCO and The CO</th>
<th>Policies and Procedures</th>
<th>Oversight and accountability</th>
<th>Education, communication and awareness</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lack of direct line to the CEO and board of directors</td>
<td>Lack-of, or lack of proper dissemination of, policies and procedures</td>
<td>Compliance Committee are not briefed regularly</td>
<td>App/incorrect/inadequate</td>
</tr>
<tr>
<td>Lack of authority to enforce disciplinary action</td>
<td>Inaccurate, highly theoretical, non-tailored, out-of-date policies and procedures</td>
<td>Immediate remediation of problem not taken</td>
<td>Lack of variation in education (training sessions, memos, postings, one-on-one)</td>
</tr>
<tr>
<td>Outsourcing of compliance responsibilities</td>
<td></td>
<td>No reporting mechanism or published Hotline</td>
<td>Instruction, Web-based training, etc.</td>
</tr>
<tr>
<td>Conflicts of interest and/or lack of independence</td>
<td></td>
<td></td>
<td>No logs or tracking sheets</td>
</tr>
</tbody>
</table>
Auditors Red Flags and Breaking Points 2

Enforcement, discipline and incentives
- Not enforced when necessary and as stated
- Ensure consistent enforcement and discipline of violations
- Investigations not thorough/comprehensive/timely
- Lack of enforcement of disciplinary guidelines

Reporting and Escalation
- Not communicated or made clear to employees/contractors
- Regulated/controlled hotline by management
- Fear of retaliation or retaliation itself

Monitoring and auditing and risk assessment
- Lack of periodic risk assessment/audits
- Absence of risk inventory

Ongoing program improvements
- Lack of continued monitoring into areas of proven non-compliance

Structure, Reporting Hierarchies, and Escalation Mechanism

Standalone entity
- Where the Chief Compliance Officer (CCO) report directly to Chief Executive Officer and report indirectly (dotted line) to the Compliance Board or Board of Audit Committee

Report the to the GA
- The number of implementation has the Compliance Officer report to the General Auditor or an officer ho handles GRC

Report to the GC
- Compliance was less likely to report to legal than many would imagine. Just 20% of those not reporting to the board reported that they reported to legal, and the number in healthcare was much lower at just 12%
IA and Compliance under one Officer

Three significant benefits

- Reduction in information asymmetry
- Increased efficiency and effectiveness of both functions
- Higher level of governance over compliance risks and controls

Compliance Office and the General Counsel

- **Reporting Structure the Oversight Role:** the relationship between the CCO and the Board of Audits Committee (BAC) and the Board of Directors (BOD)
- **Governance:** the General Counsel (GC) is representing the organization from a legal perspective, which creates the potential for increased conflicts of interest and the advisory role of the GC staff doesn’t mesh well with the CCO role.
- **Competency and Skill sets:** There are key skills for a CCO that a GC may not necessarily have such as: Risk Assessment, Corporate Governance, Monitor Practice, and Investigation)
Other Recommendations

Internationally and according to a Publication of the Office of Inspector General (OIG) USA

“The OIG believes that there is some risk to establishing an independent compliance functions if the function is subordinate to the General Counsel, or comptroller or similar financial officer. The report goes on to say, “By separating the compliance function from the key management positions of General Counsel, or chief financial officer, a system of checks and balances is established to more effectively achieve the goals of the compliance program.”

Measuring the effectiveness -1

- The outcomes of the program
- The costs and other impacts of the program
- The attitudes, knowledge, and behavior of the organization and community toward the program
- Any confounding factors that may affect the measurements of the program’s impact.
Measuring the effectiveness -2

- the presence of compliance and ethics activities
- staff, management, board, and community understanding of risk areas and ongoing compliance and ethics activities.
- Early detection of illegal and improper activities due to the efforts of the compliance and ethics program

Increase

- illegal/improper activities due to the efforts of the compliance and ethics program
- the number of suspected violations actually being compliance and ethics problems
- penalties/consequence of illegal/improper activities and/or material deficiencies identified via government/external audit, whistleblower, self-audit and reporting

Decrease

In Conclusion
Integrating Disciplines within the Risk Management Framework

compliance

Internal Auditing

Free available resources for IA

Compliance 101

The Complete Compliance and Ethics Manual 2018

A Compliance & Ethics Program on a Dollar a Day:

How Small Companies Can Have Effective Programs
Education, Publications and Events

Y-Comply, a service of the Society of Corporate Compliance & Ethics, is a digital publication delivered quarterly to members. Y-Comply helps members communicate the value and purpose of compliance and ethics to the general workforce. We know you will appreciate the education and inspiration provided in the letter.

If you ever think you’re too small to be effective, you have never been in the dark with a mosquito.

Act NOW
THANKS
Q&A