

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

Waheed Alkahtani, CFE and CCEP

November 2017



SOCIETY OF CORPORATE
COMPLIANCE AND ETHICS



Saudi Aramco: Company General Use

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

Saudi Aramco: Company General Use

1

How it was started

To comply or not to comply?

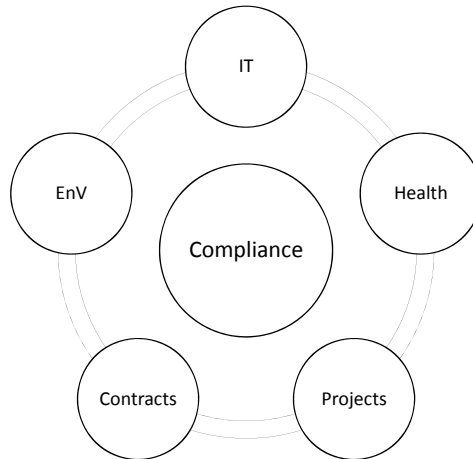
Saudi Aramco: Company General Use

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.

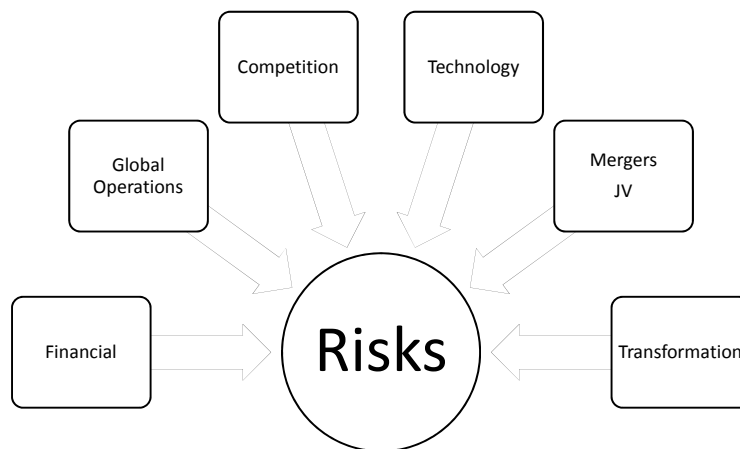
Saudi Aramco: Company General Use

Compliance-related Offices

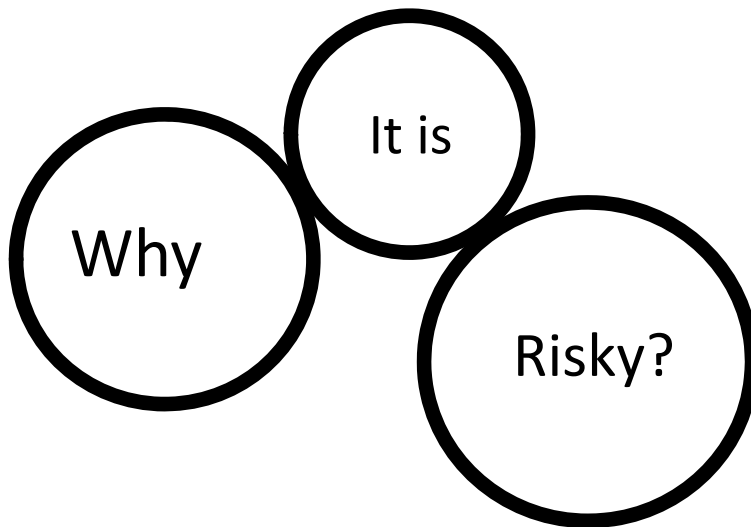


Saudi Aramco: Company General Use

Organizational Risks



Saudi Aramco: Company General Use



Saudi Aramco: Company General Use

The “carrot and stick” philosophy

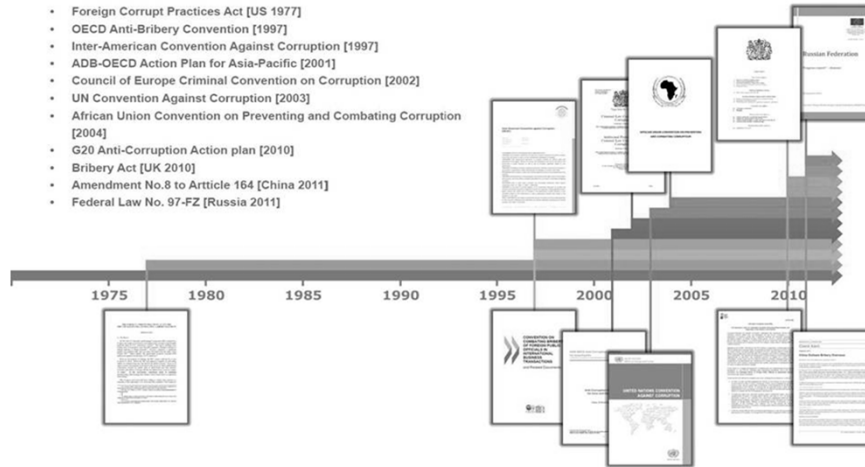
US Organizational Sentencing Guidelines (1991)

- “Corporations can, and should, be incentivized to self-police, and with respect to compliance and ethics”

Saudi Aramco: Company General Use

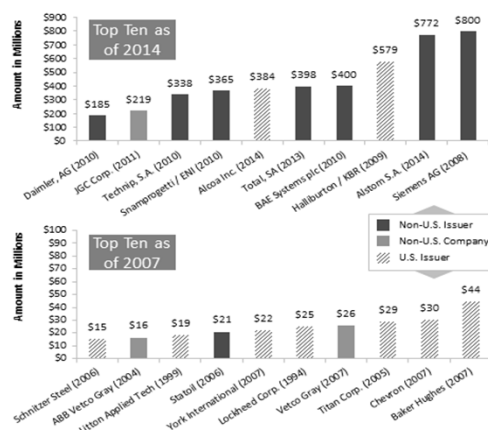
Trend: Legislation and Regulation is increasing

- Foreign Corrupt Practices Act [US 1977]
- OECD Anti-Bribery Convention [1997]
- Inter-American Convention Against Corruption [1997]
- ADB-OECD Action Plan for Asia-Pacific [2001]
- Council of Europe Criminal Convention on Corruption [2002]
- UN Convention Against Corruption [2003]
- African Union Convention on Preventing and Combating Corruption [2004]
- G20 Anti-Corruption Action plan [2010]
- Bribery Act [UK 2010]
- Amendment No.8 to Article 164 [China 2011]
- Federal Law No. 97-FZ [Russia 2011]



Saudi Aramco: Company General Use

Foreign Corruption Practices Act (US 1977)



FCPA top ten penalties in 2014 vs 2007

Saudi Aramco: Company General Use

The Cost of Not to COMPLY

Company Name	Penalty	Year
Siemens (Germany)	\$1.6 billion	2009
Alstom (France)	\$772 million	2014
KBR / Halliburton (USA)	\$579 million	2009
BAE (UK)	\$400 million	2010
Total (France)	\$398 million	2013

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

Saudi Aramco: Company General Use

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

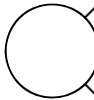
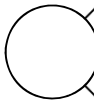
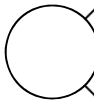
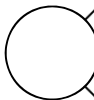
It's a Global Trend

It Could Happen
Here: when was
the last time you
checked?

It's Not Optional

Saudi Aramco: Company General Use

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

Saudi Aramco: Company General Use

2

Internal Audit are Compliance Best Friend

Frist who and then where

Saudi Aramco: Company General Use

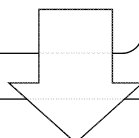
Internal Auditing

- 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.

Saudi Aramco: Company General Use

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. .

Saudi Aramco: Company General Use

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**.

IIA Webinar: How Internal Audit can Provide a Leadership Role in GRC

Saudi Aramco: Company General Use

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 Function can be effective partners.
- Serve as a member of the Compliance Committee.
- Finally, compliance is part of our audit plan, and it is good to be aware

AUDITED

Saudi Aramco: Company General Use

Compliance Office Role

How similar this Role to IA?

- 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.

Saudi Aramco: Company General Use

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

Saudi Aramco: Company General Use

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.

Saudi Aramco: Company General Use

Knowing the Difference

Internal Audit

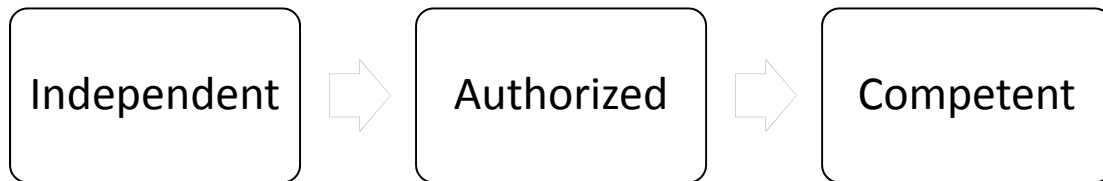
- 🔗 Risk Based Audit Plan
- 🔗 Independent of Management
- 🔗 Assessing Internal Control System
- 🔗 Looking at the past and present to provide assurance
- 🔗 Expertise in controls, risk management, and governance processes
- 🔗 After-the-fact
- 🔗 Considers strategic, operations, reporting, and compliance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

Internal Auditing
Saudi Aramco: Company General Use

Who Carries the Compliance FLAG?



Best Practice ACFE, AICPA, IIA, and SCCE

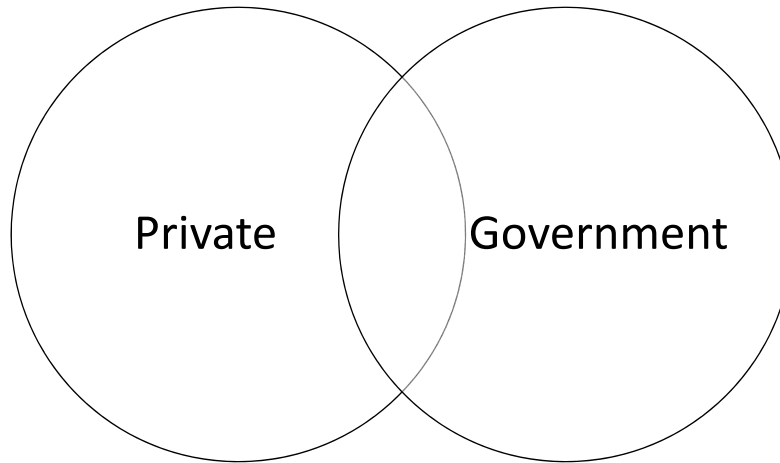
Saudi Aramco: Company General Use

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

Saudi Aramco: Company General Use

Oh, one more thing



Saudi Aramco: Company General Use

3

The Basics

Compliance Basic Elements

Saudi Aramco: Company General Use

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

Saudi Aramco: Company General Use



The is no one size fits all



Saudi Aramco: Company General Use

The Way Forward



7 Basic Elements

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



5 Main Stages

Policies and procedures (including a Code of Conduct)
Oversight and accountability
Education and awareness
Enforcement and incentives
Hotline and Escalation



3 Core Entities

Policies and procedures
Education and awareness
Hotline and Escalation

What is the most critical function in the Compliance Process?

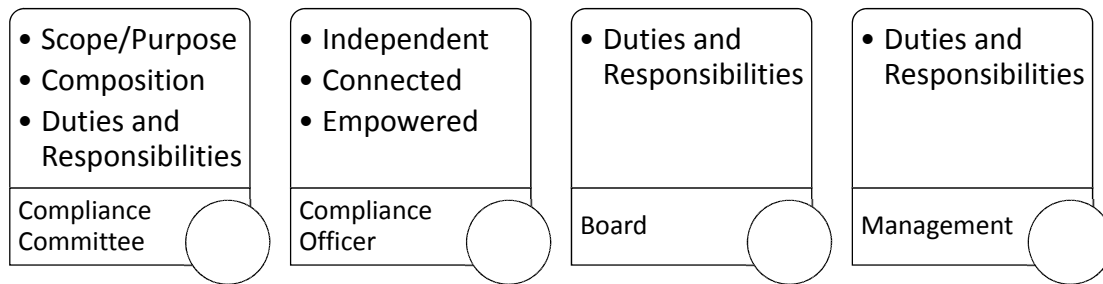
Saudi Aramco: Company General Use

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.

Saudi Aramco: Company General Use

2- Oversight and accountability



Saudi Aramco: Company General Use

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

Saudi Aramco: Company General Use

32

4- Enforcement, discipline and incentives

Internal Investigation Policy	Disciplinary actions	Rewards
<ul style="list-style-type: none"> • Who is responsible • Hotline 	<ul style="list-style-type: none"> • None retaliation • Employees vs None employees and Vendor 	<ul style="list-style-type: none"> • Informants • Suspects

Saudi Aramco: Company General Use

5- Reporting and Escalation

Objective	Categories	Escalation Procedure
<ul style="list-style-type: none"> • Develop a Communication strategy to inform management and form a measurement tool 	<ul style="list-style-type: none"> • Periodic/Ad hoc • Internal/External • Status vs studies 	<ul style="list-style-type: none"> • Selection criteria • Framework

Saudi Aramco: Company General Use

6- Auditing and Monitoring

Compliance Program Risk Inventory

Forensic Accounting	Conflicts of Interest	Antitrust/Competition law	Document Management/Retention
<ul style="list-style-type: none"> • Financial statements • Books and records/off-books accounts • Revenue/cost manipulation 	<ul style="list-style-type: none"> • Gifts and gratuities • Entertainment • Ownership interests • Outside employment and job offers • Corporate opportunities 	<ul style="list-style-type: none"> • Collusive conduct (e.g., price-fixing, market allocation) • Unfair practices/business offences (disparagement, inducing breach of contract, infringing) • Monopolization/abuse of dominant position • Price discrimination 	<ul style="list-style-type: none"> • Retention of documents during investigations • Retention of required records

Saudi Aramco: Company General Use

7- Ongoing Improvement

- Evaluating Effectiveness
- Program indicators
- Surveys, focus groups, testing
- Self and external assessment
- Periodical Benchmarking



Saudi Aramco: Company General Use

Bonus 3 - The most critical function in the Compliance Process



Reporting and Escalation

Saudi Aramco: Company General Use

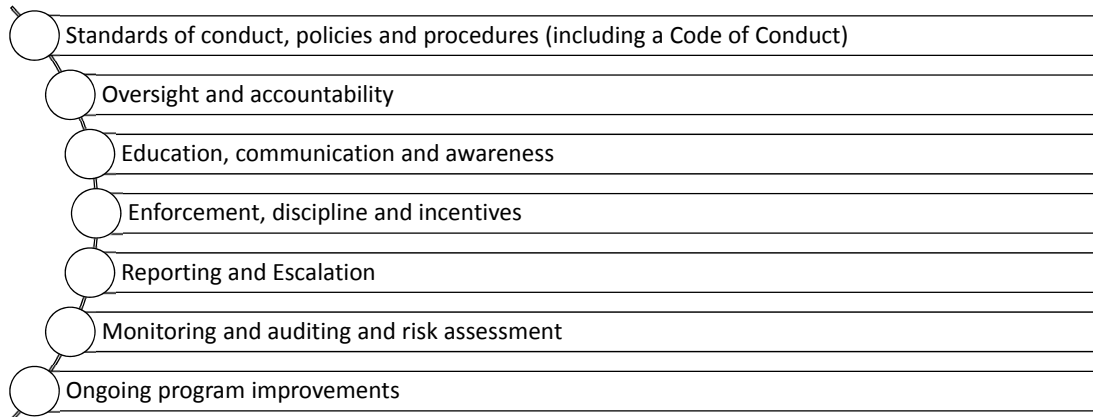
4

The HOW question?

The Framework and Implementation Strategies

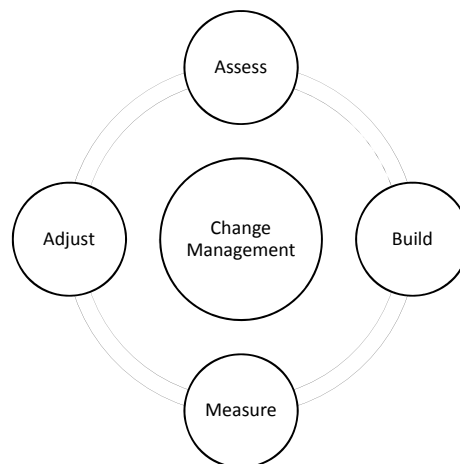
Saudi Aramco: Company General Use

Seven Essential Elements of the Compliance Program developed by SCCE



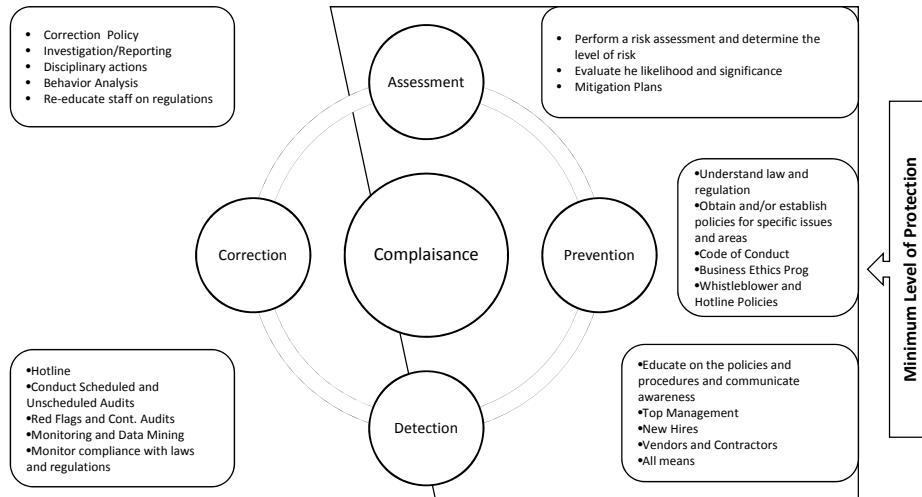
Saudi Aramco: Company General Use

Change Management Theory



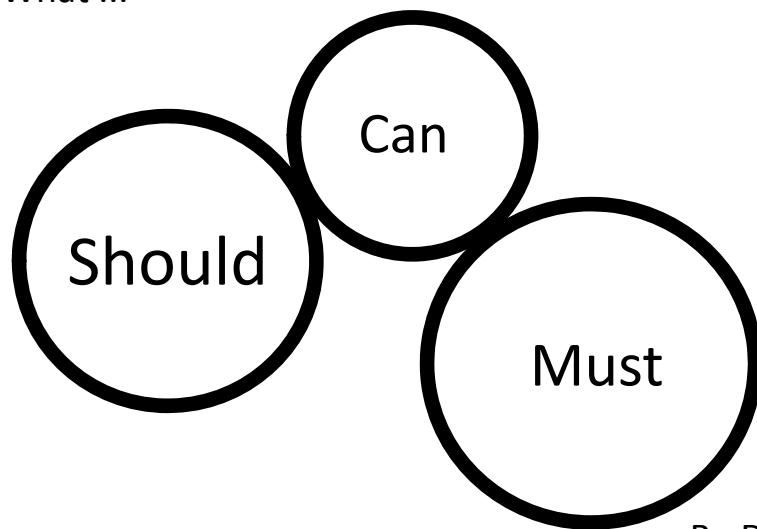
Saudi Aramco: Company General Use

The Compliance Framework



Saudi Aramco: Company General Use

What ...



Saudi Aramco: Company General Use



Set the Tone from the Top

First, get the green light

Saudi Aramco: Company General Use

Set the Tone from the Top



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



Saudi Aramco: Company General Use

The Challenging Elements

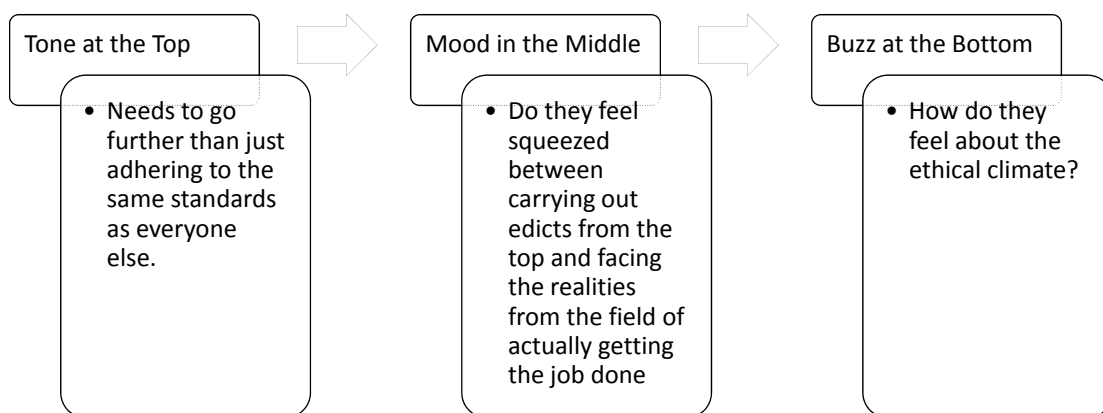
Actions speak
louder than
words.

Leading by Example

People follow
what you say
without
following the
intent

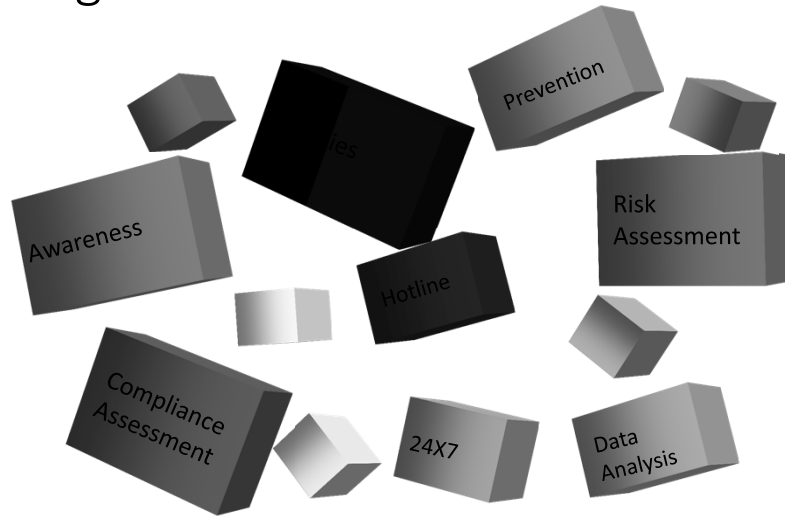
Saudi Aramco: Company General Use

What the Corporate Rhythm?



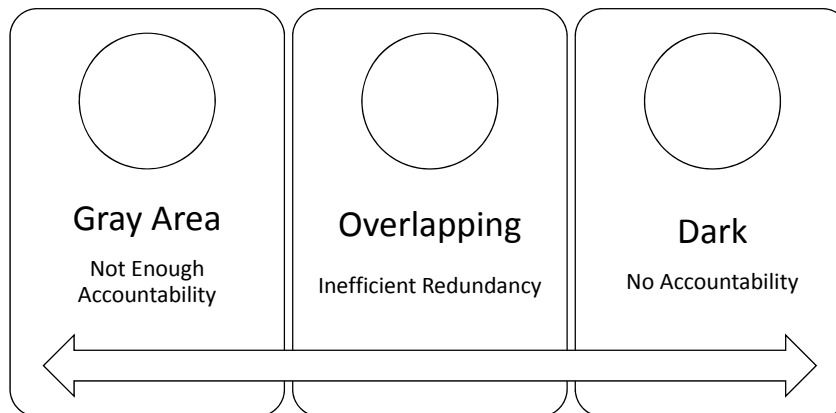
Saudi Aramco: Company General Use

Building Blocks



Saudi Aramco: Company General Use

Gap Analysis Methodology



Saudi Aramco: Company General Use

Policies and Procedures

Module ONE

Saudi Aramco: Company General Use

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

Saudi Aramco: Company General Use

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

Saudi Aramco: Company General Use

Polices and Procedures

- | | |
|---------------------------------|-------------------------------------------|
| 1. Code of Conduct | 11. Participation in political activities |
| 2. Competition and Fair Dealing | 12. Insider Trading |
| 3. Sexual Harassment Policy | 13. Risk Management Policy level |
| 4. Whistle Blower Policy | 14. Risk Management Effectiveness |
| 5. Hot line Policy | 15. Corrupt practices |
| 6. Legal Compliance Policy | 16. Financial Disclosure Practices |
| 7. Safety Policy | 17. Conflicts of Interest |
| 8. Record Maintenance Policy | 18. Proper Use of Company Assets |
| 9. Compliance Policy | 19. Corporate Governance Code |
| 10. Gifts and Gratuities | 20. Non-Disclosure Agreements |

Saudi Aramco: Company General Use

Enforcement and Investigation

Module TWO

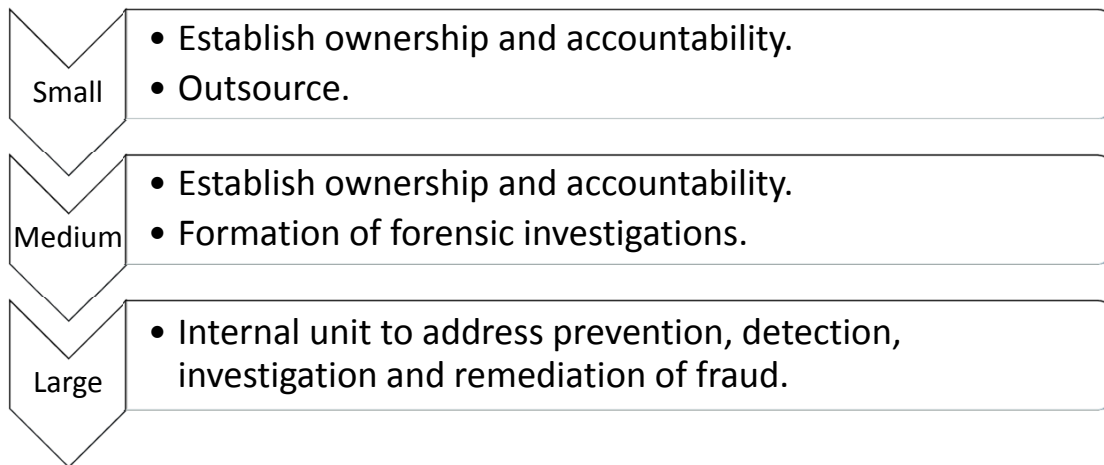
Saudi Aramco: Company General Use

ACFE In-House Fraud Investigation Teams: 2017 Benchmarking Report



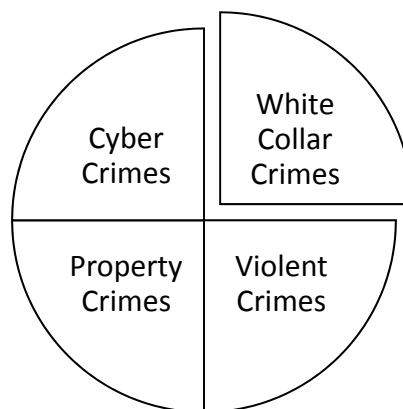
Saudi Aramco: Company General Use

How to respond to an incident



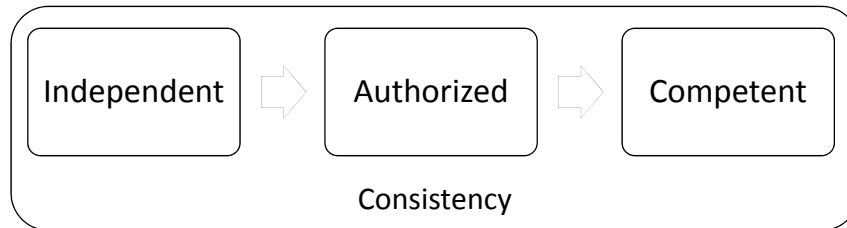
Saudi Aramco: Company General Use

Who Investigate and Examine Fraud?



Saudi Aramco: Company General Use

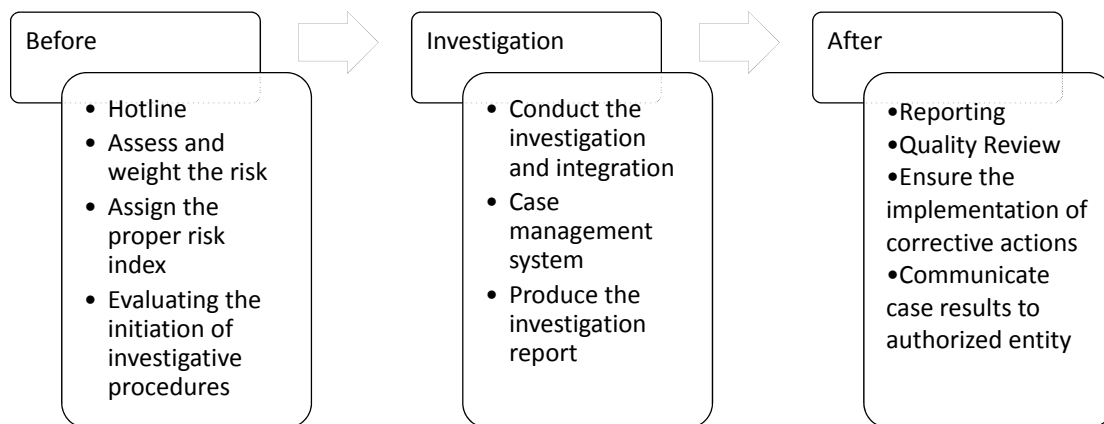
Who Investigates Irregularities?



Best Practice ACFE, AICPA, IIA, and SCCE

Saudi Aramco: Company General Use

Proposed Investigation Process



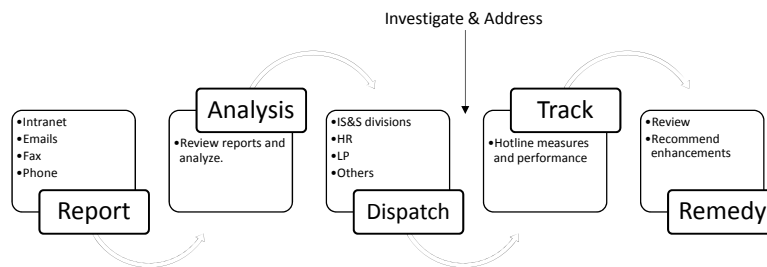
Saudi Aramco: Company General Use

The result of the screening process



Saudi Aramco: Company General Use

Reported issue Processing



Saudi Aramco: Company General Use

60

From Good to Great

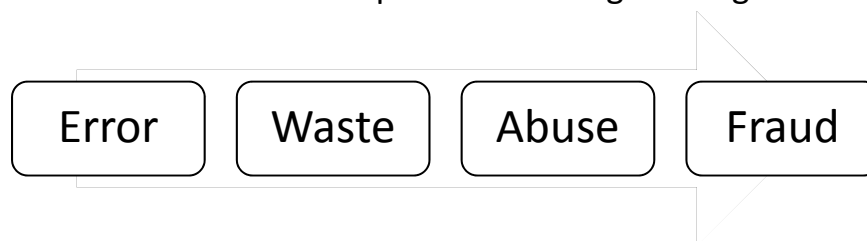
mining for
hotline gold

all that glitters
is not gold

Saudi Aramco: Company General Use

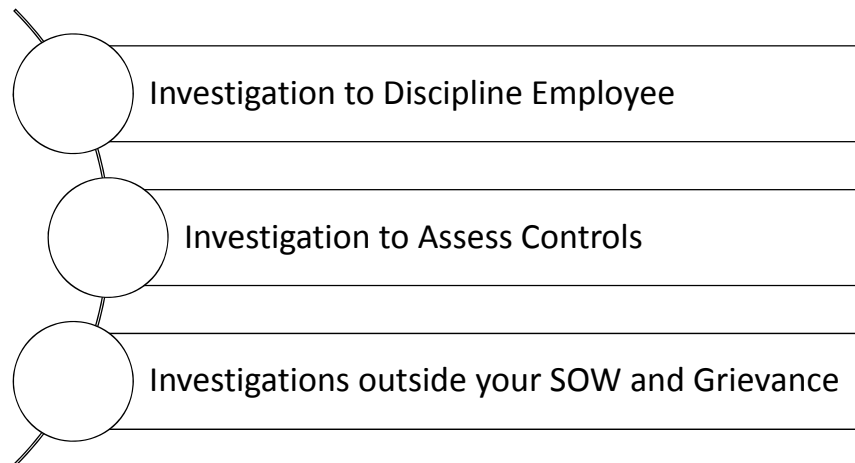
Top questions that you need to answer

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?



Saudi Aramco: Company General Use

Business-focused investigation



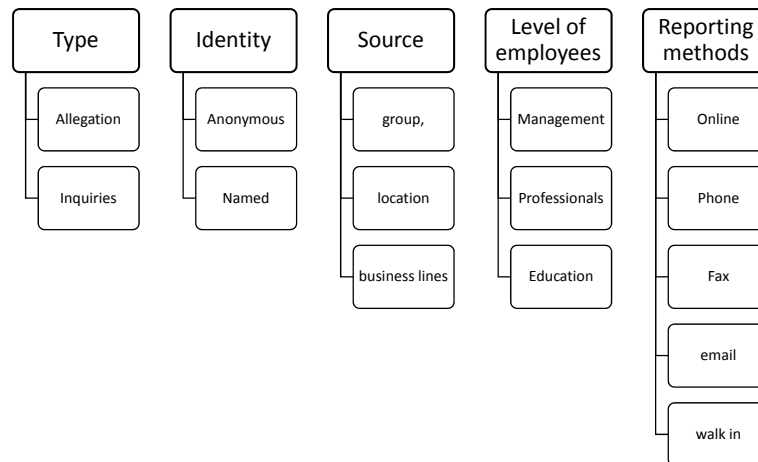
Saudi Aramco: Company General Use

What is Final Decision



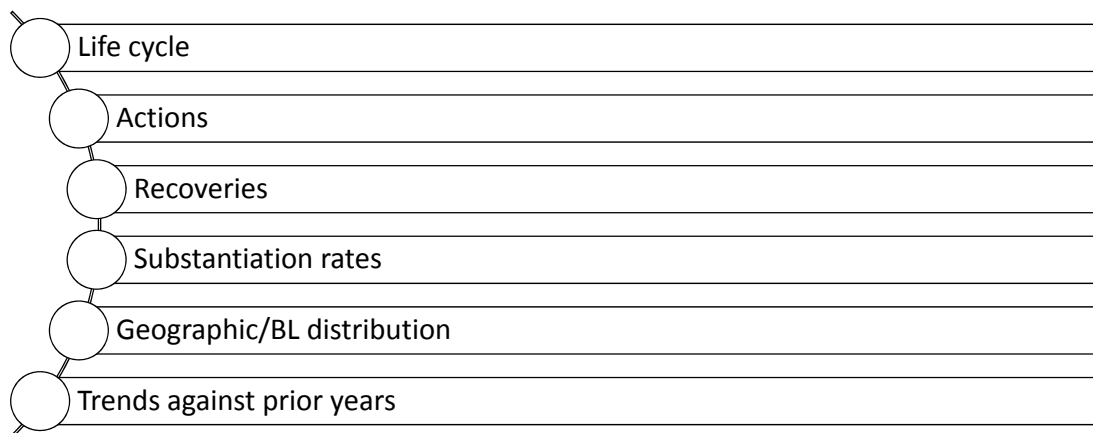
Saudi Aramco: Company General Use

Investigation Measuring and Key Performance Indicators



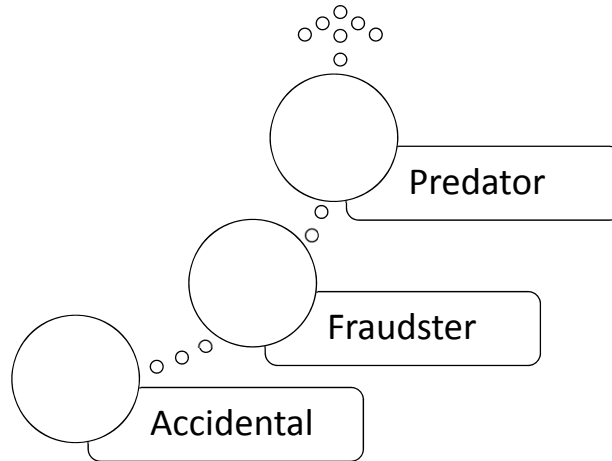
Saudi Aramco: Company General Use

Other useful measures



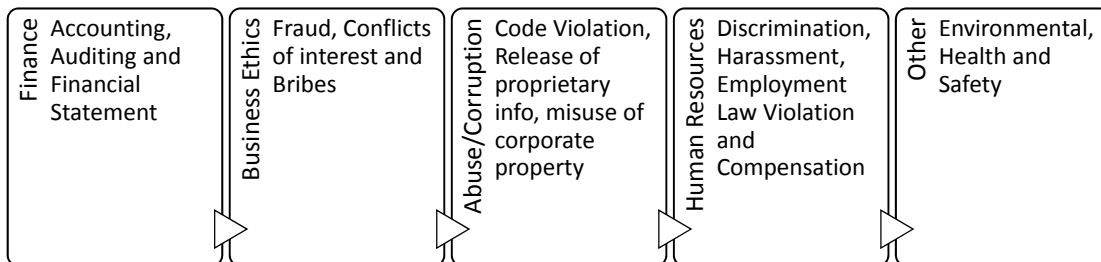
Saudi Aramco: Company General Use

Define your module and Profile you suspect



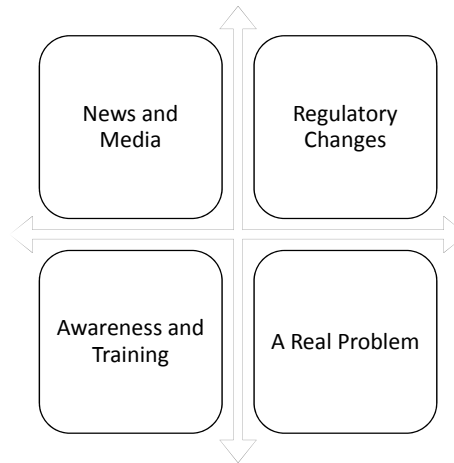
Saudi Aramco: Company General Use

Investigation categories



Saudi Aramco: Company General Use

What may cause changes



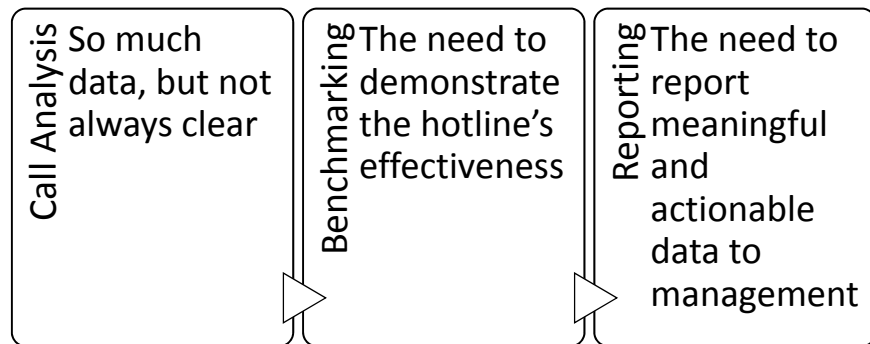
Saudi Aramco: Company General Use

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.

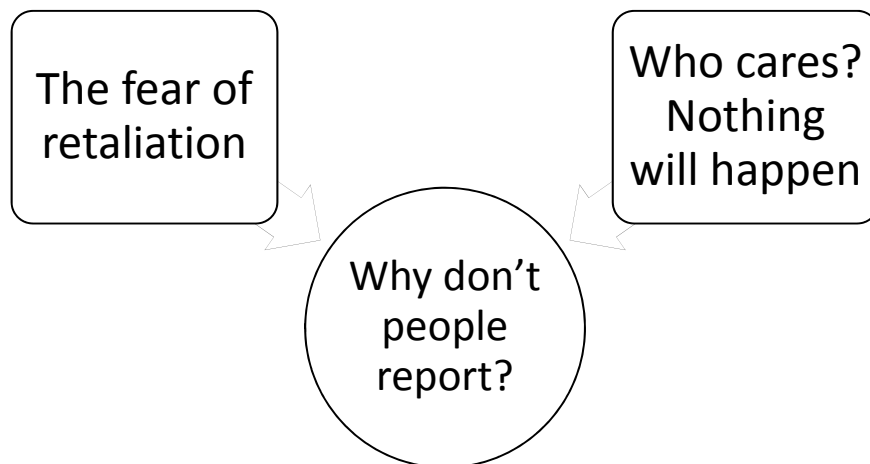
Saudi Aramco: Company General Use

Other Challenges



Saudi Aramco: Company General Use

Final thought



Saudi Aramco: Company General Use

5

Reference and Templates

Global Bodies and International Associations

Saudi Aramco: Company General Use

Global Bodies



Saudi Aramco: Company General Use

Sample Policies and Procedures

- The Complete Compliance and Ethics Manual from the SCCE



Saudi Aramco: Company General Use

Auditors Red Flags and Breaking Points 1

CCO and The CO

☐

- ☐ Lack of direct line to the CEO and board of directors
- ☐ Lack of authority to enforce disciplinary action
- ☐ Outsourcing of compliance responsibilities
- ☐ Conflicts of interest and/or lack of independence

Policies and Procedures

☐

- ☐ Lack of, or lack of proper dissemination of, policies and procedures
- ☐ Inaccurate, highly theoretical, non-tailored, out-of-date policies and procedures

Oversight and accountability

☐

- ☐ Compliance Committee are not briefed regularly
- ☐ Immediate remediation of problem not taken
- ☐ No reporting mechanism or published Hotline

Education, communication and awareness

☐

- ☐ Poor/incorrect/inadequate
- ☐ Lack of variation in education (training sessions, memos, postings, one-on-one instruction, Web-based training, etc.)
- ☐ No logs or tracking sheets

Saudi Aramco: Company General Use

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

Saudi Aramco: Company General Use

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%

Saudi Aramco: Company General Use

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

Saudi Aramco: Company General Use

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)

Saudi Aramco: Company General Use

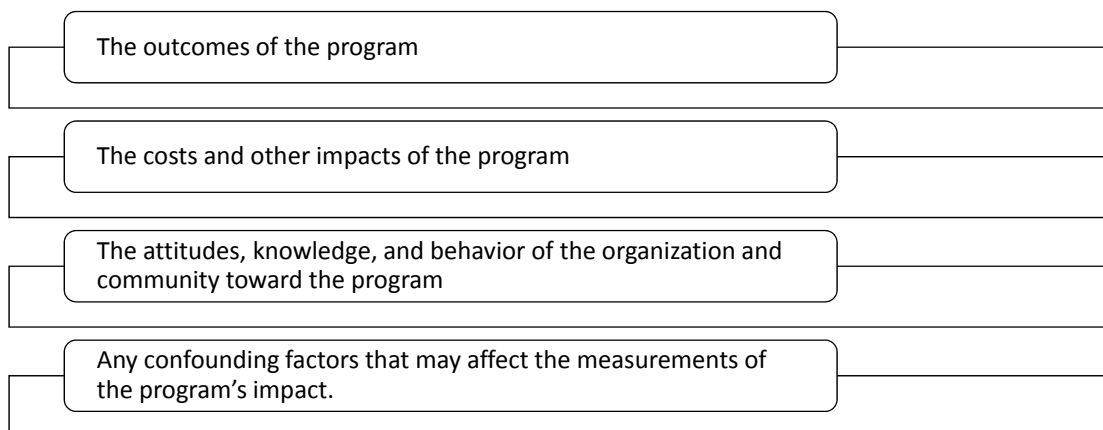
Other Recommendations

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.”

Saudi Aramco: Company General Use

Measuring the effectiveness -1

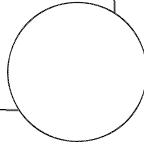


Saudi Aramco: Company General Use

Measuring the effectiveness -2

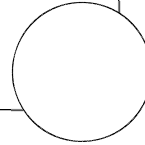
- the presence of compliance and ethics activities
- staff, management, board, and community understanding of risk areas and ongoing compliance and ethics activities.
- Early detection of illegal and improper activities due to the efforts of the compliance and ethics program

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

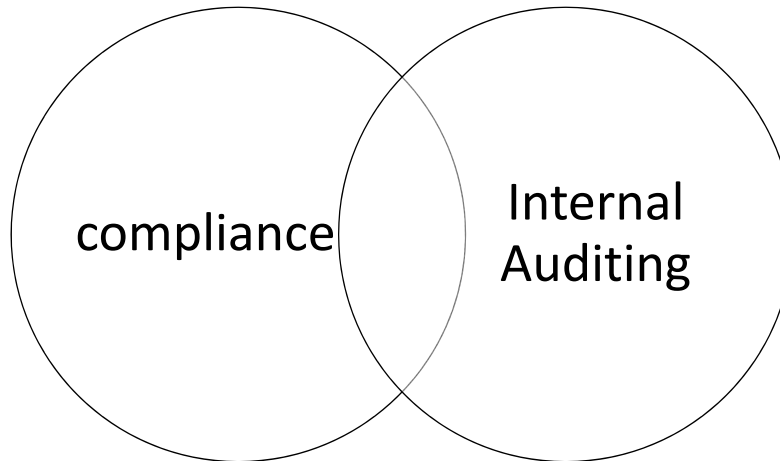


Saudi Aramco: Company General Use

In Conclusion

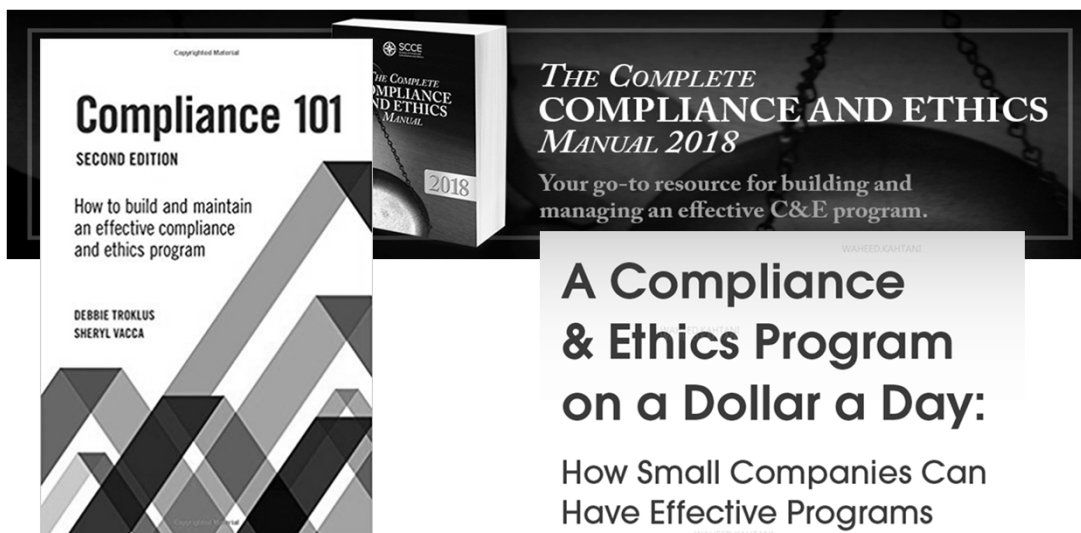
Saudi Aramco: Company General Use

Integrating Disciplines within the Risk Management Framework



Saudi Aramco: Company General Use

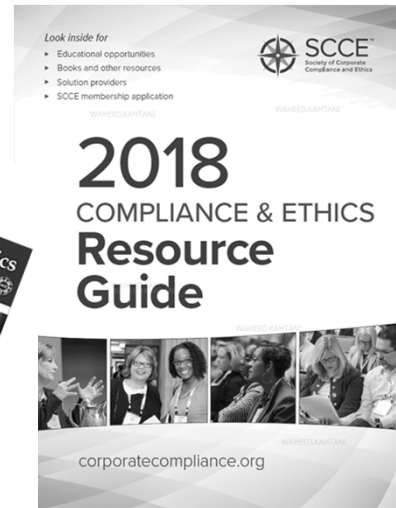
Free available resources for IA



Saudi Aramco: Company General Use

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



Saudi Aramco: Company General Use

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

Act NOW



Saudi Aramco: Company General Use

THANKS

Q&A

Saudi Aramco: Company General Use