

# Governance, Risk and Compliance Training Course



This comprehensive 2 day Course provides an overview and analysis of a range of public and commercially-oriented models, frameworks and methodologies in the Governance, Risk Management, Compliance and Information Security arenas. It furthermore investigates the legislative compliance imperatives applicable to South African organisations alternatively companies trading in South Africa.

## Course Description

There are a range of models, frameworks, and methodologies available to both private and public organisations to help address enterprise risk management and compliance with legislative requirements. Despite the abundance of information at hand, there is still confusion amongst many professionals as to which model is best suited for their organisation or particular industry and which is not.

There is furthermore a shortage of time or resources to research all these models, frameworks and methodologies and often a difficulty in grasping the key concepts that each has to offer. This first day of the workshop aims to empower the relevant employees in each organisation with an accurate summary of the major international standards and frameworks.

The second day of the workshop expands on aspects of critical legislative compliance that impact an organisation's methodologies to achieve comprehensive governance and risk management. Key topics such as "records management," "interception of communications," "data privacy" and "electronic evidence procedures" will be discussed. The second day further addresses the challenges of translating legislation into action steps by suggesting best practice and integration of legal compliance within new or existing risk and governance frameworks.

## Approach, Deliverables and Method

### **Course Deliverables:**

- Comprehensive course notes and advice on further sources of information.
- Certificate of attendance upon completion of the course

### **Delivery Method:**

- Classroom style - combining lecture, discussion and exercises utilising course materials, digital projector and flipchart

## In-house Training

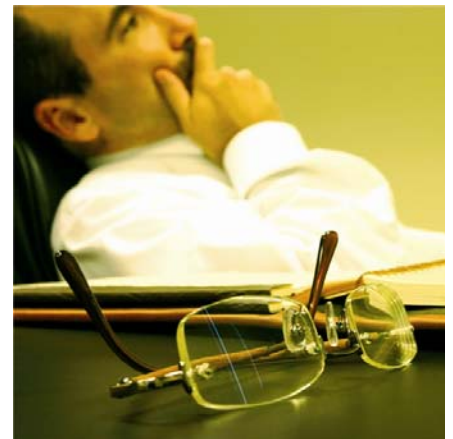
All Analytix Courses are available in-house, should your organisation have a number of people or multiple sets to train. The cost advantages and the ability to discuss and resolve organisational issues are two major attractions of such training.

## Consulting services

Analytix also offers consulting services to support the implementation of GRC.

## Who will benefit?

- CIO's / IT Directors / IT Managers
- Information Security Professionals
- Risk / Legal / Compliance departments
- IT & Information Security Auditors
- Business continuity / Disaster Recovery staff members
- Sales executives / Consultants



## What you will learn

On completion of the course, delegates will be able to:

- Understand the main drivers forcing companies to look into Governance, Risk management, Compliance and Information Security solutions
- Differentiate between a Framework, Methodology and Standard
- Gain an understanding of over 20 international frameworks and standards;
- Appreciate the key benefits and differences of each and determine which are relevant for their particular organisation or industry;
- Appreciate current and imminent legislation pertinent to ICT governance, risk management and compliance;
- Appreciate critical internal compliance duties relevant to organisations;
- Draw from the policies and procedures discussed to compile an action plan for organisational compliance.



[www.analytix.co.za](http://www.analytix.co.za)

## Course Content



### Day 1:

1. Introduction to Governance, Risk management, Compliance & Information Security (GRCI)
2. What are the main drivers forcing companies to look at GRCI
3. Understanding the difference between Frameworks, Methodologies and Standards

### Overview and analysis of:

#### Risk Management

- COSO Enterprise Risk Management
- OCTAVE

#### Information Security

- ISO 27001 / ISO 17799
- Information Security Management Maturity Model (ISM3)
- Payment Card Industry (PCI) data security standard
- ISF Standard of Good Practice
- NIST SP 800 series
- Systems Security Engineering Capability Maturity Model

#### IT Governance

- Control Objectives for Information and related Technology (COBIT)
- Statement on Auditing Standards (SAS 70)
- ITIL / ISO 20000
- The IIA Generally Accepted IT Principles (GAIT)
- ISACA Standards for IS Auditing

#### IT Security

- COBIT DS5
- ISO 13335 - IT security management
- Open Source Security Testing Methodology Manual (OSSTMM)
- US Cyber Security Checklist
- Common Criteria
- ISO 18043 – Selecting & operating an IDS
- ISO 18028 – Security techniques

#### Industry or Country specific

- Basel II, The New Accord
- SB1386 Senate Bill
- Sarbanes Oxley Act (SOX)
- Health Insurance Portability and Accountability Act (HIPAA)
- Minimum Information Security Standards (MISS)
- An overview of intelligence operations in South Africa

#### Business Continuity

- Security Incident Policy Enforcement System
- Business Continuity Management (BS 25999-1)

### Day 2

- An overview of the King II Report as an introduction to the duty to comply with legislative imperatives
- Compliance duties when communicating and transacting electronically:
  - Website Compliance;
  - Email Compliance;
  - Mobile Compliance; and
  - Organisational Policies pertaining to employee use of electronic communications equipment and systems.
- Records Management:
  - Differentiation between management of paper and electronic records:
  - An overview of "Electronic Evidence and Legal Discovery" legislation and its implications on records management;
  - An overview "Data Privacy and Protection" legislation and its implications on records management; and
  - An organisation's records management obligations in relation to the Promotion of Access to Info Act (PAIA).
- Interception of Communications:
  - Defining "Interception"
  - When may an organisation lawfully intercept employee communications?
  - When may an organisation lawfully intercept third party communications with the organisation?
  - The balance between an organisations duty to protect its assets/ verses individual privacy
  - Procedures and Policies pertaining to Interception of Communications
- Legislation covered:
  - Electronic Communications and Transactions Act 25 of
  - Regulation of Interception of Communications Act 70 of
  - Protection of Personal Information Bill
  - Companies Act 1973 / Amendment Act 20 of 2004)
  - Promotion of Access to Information Act 2 of 2000
  - King II Report on Corporate Governance
  - JSE Listing Requirements

## Register Today

To register, or for more information, please contact us:

**Tel: 0861 ANALYTIX or 0861 262 598**

**Fax: +27 (011) 447 4192**

**Email: [info@analytix.co.za](mailto:info@analytix.co.za)**

**Web site: [www.analytix.co.za](http://www.analytix.co.za)**

### ANALYTIX

MLC House • 1st Floor • 50 Sixth Road • Hyde Park • 2196

PO Box 413988 • Craighall • 2024

[www.analytix.co.za](http://www.analytix.co.za) • [info@analytix.co.za](mailto:info@analytix.co.za)