

Quency Advisory & Training

GRC Training Portfolio

GRC
Governance
Risk and
Compliance



This page has been left intentionally blank

OVERVIEW

Dear GRC Professional,

Organisations across the world are under increased pressure to meet waves of regulatory changes and adopt cumbersome new standards, while improving organisational performance and ensuring key-stakeholder value. Efforts to meet these requirements have created a culture of silo management — a fragmented approach that undermines the interdependency of oversight activities — which can lead to operational inefficiencies, ineffectual maintenance of compliance initiatives, and increased costs.

GRC is a global initiative of convergence that aims to integrate discrete management assurance functions into a unified framework for corporate governance, risk management, regulatory compliance and assurance. Its objective is to unify the silos that divide corporate oversight, standardise processes, increase communication, decrease operational cost, and secure competitive advantage. GRC is rapidly becoming an intrinsic part of the corporate landscape — as a governance, risk or compliance professional you can't afford to fall behind in the integrative efforts underway!

Quency Advisory & Training Services has brought together with international organisation to provide practical solutions and answers to your most pressing issues and questions regarding this most important and timely subject in your business today. Our in-house and public programs workshop will address your challenges and provide the applicable insights required to make your GRC implementation efforts a resounding success.

Move Away from Silo Management and towards Convergence and Efficiency These workshops will show you how to tackle GRC integration within your organisation. All aspects of your business operations will be targeted during the workshop that highlight the integrative efforts and components that GRC must align: governance, risk, and compliance. You can customise your workshop to accommodate your most pressing concerns and issues and bring your whole team to share ideas and prepare to meet common goals.

Gain valuable best practice insight and practical information on the design and implementation of innovative practices that will improve the enterprise-wide effectiveness of your governance, risk, and compliance functions —Please contact us for more information by calling me at **+2783 251 8430** or e-mail us at ***info@quency.co.za***.

Sincerely

Jayen Vyravene

Quency Advisory & Training Services (Pty) Ltd

Contents

OVERVIEW	2
GRC PROGRAMS	
GRC BOOTCAMP FOR BOARD OF DIRECTORS	3
GRC – STRATEGIC & IMPLEMENTATION WORKSHOP	4
OCEG GRC PROFESSIONAL INTENSIVE WORKSHOP	9
RISK MANAGEMENT PROGRAMS	
RISK MANAGEMENT: CONCEPT, TOOLS & TECHNIQUES	11
MASTERING RISK MANAGEMENT: TOWARD RISK CONVERGENCE	12
ERMA - ERM CERTIFIED PROFESSIONAL	15
COMPLIANCE MANAGEMENT PROGRAMS©	
CORPORATE COMPLIANCE – ESTABLISHING AN EFFECTIVE COMPLIANCE PROGRAMS	20
CORPORATE COMPLIANCE – OPTIMIZING YOUR PROGRAM	23
IT GRC PROGRAMS	
INFORMATION TECHNOLOGY (IT) GOVERNANCE	25
IT COMPLIANCE, RISK & SECURITY MANAGEMENT	27

GRC PROGRAMS

GRC BOOTCAMP FOR THE BOARD OF DIRECTORS – THE BUY IN APPROACH

½ Day Session - Inhouse

Who should attend!

Board members, Non-Executives members, Audit & Risk Committee members, Governance Committee members.

AGENDA

GRC Overview: Where Are We Going and How Do We Get There?

- Introduction to goals and intentions of GRC implementation
- How GRC is different from current governance, risk and compliance assurance methods

GRC: What's the Business Case for Change?

- How public companies are benchmarking the business impacts of GRC programs?
- Common reasons for not integrating GRC, and the real reasons why your organization should!

Achieving GRC Buy-In at the Top and Establishing Clear Roles and Responsibilities

- Challenges to getting buy-in from corporate and business areas involved in the process
- Achieving buy-in from senior executives and a clear demarcation of c-level responsibilities
- The place of IT in the GRC process
- Defining roles and accountabilities of key stakeholders (board, executives, management, compliance, audit, etc)
- The factor of selling it to c-level executives to get buy-in and mobilization
- Importance of clear visibility of information from anywhere in the organization

Enterprise-Level View of GRC: Importance of Sharing Information with Stakeholders

- Providing role-based information and real-time analytics to key stakeholders through and GRC dashboard
- How the reliability of data in GRC dashboards will help increase usage and impact decision-making
- The GRC Maturity Model

THE STRATEGIC & IMPLEMENTATION APPROACH

2 DAY BOOTCAMP

Who Should Attend!

CEO's, COO's, Chief Risk Officer, Chief Compliance Officer, Chief Information Officer, Chief Audit Executives and other Senior Executives.

The objective is to give you an insight and practical strategies for your Governance, Risk and Compliance integration by:

- Defining progressive governance, risk, and compliance roles and responsibilities to move forward from silo management
- Fulfilling regulatory requirements while achieving a real ROI
- Increasing productivity and capital by putting an end to silo management
- Leveraging your current IT systems to integrate GRC
- Gaining an in-depth view into key risk metrics and policy compliance to improve your risk control and self-assessments

About the Workshop

The workshop provides an introductory overview of this new global groundswell of GRC, including discussion of the challenges organizations will face and business case that will drive this new movement.

Topics covered include:

- An introduction to GRC: the new corporate “must have”
- Explanation of an integrated GRC system
- How is GRC different from current governance, risk, and compliance assurance methods?
- Building your business case
- What current laws require: a global perspective on “bare minimum” compliance, how the corporate governance bar continues to move upwards
- Integrated GRC: what parts must be assembled, bought, wired up, or rented to build one? What cultural changes are required to make it work?
- Setting up and staffing an integrated GRC system
- Overcoming barriers and avoiding pitfalls
- Maintaining and sustaining your GRC and measuring its benefits

AGENDA: THE STRATEGIC APPROACH

GRC Overview: Where Are We Going and How Do We Get There?

- Introduction to goals and intentions of GRC implementation
- How GRC is different from current governance, risk, and compliance assurance methods

GRC: What's the Business Case for Change?

- How public companies are benchmarking business impacts of GRC programs?
- Common reasons for not integrating GRC, and the organization, real reasons why your organization should!

Achieving GRC Buy-in at the Top and Establishing Clear Roles & Responsibilities

- Challenges to getting buy-in from corporate and business areas involved in the process
- Achieving buy-in from senior executives and a clear demarcation of c-level responsibilities
- The place of IT in the GRC process
- Defining roles and accountabilities of key stakeholders (board, executives, management, compliance, audit, etc)

Practical Strategies for Implementing GRC

- Integrating GRC and practical experience of the challenges and opportunities
- Managing qualitative aspects and quantitative aspects of GRC
- Handling GRC as a fundamental business practice, not just in a reactionary and short-term way

Establishing the Desired Enterprise-Wide Culture

- Ensuring GRC benefits impact behavior
- Assessing your organization's current culture
- Defining or redefining the culture to meet your desired ends
- Communication GRC initiatives throughout the organization
- Promote the new culture enterprise-wide

Business Objectives & Drivers

- Understand all dimensions of business objectives and risk, and compliance assurance methods drivers, how they effect and affect GRC initiatives
- How to design and adapt initiatives and approaches to the existing implications across levels (firm wide, business unit, work unit, and individual) within your organization.

Risk & Opportunities

- Understand key long-term and short-term single and cumulative risks and opportunities and the events that trigger them.
- Define your risk culture
- Define methodology for risk identification and assessment
- Analyse and prioritize your risk within a GRC framework

Plan & Design

- Designing your GRC initiatives roadmap to achieving your business objectives
- Define your GRC initiatives plan, change management, methodology and resources

AGENDA: THE IMPLEMENTATION APPROACH

GRC Overview: Where Are We Going and How Do We Get There?

- Introduction to goals and intentions of GRC implementation
- Building your business case – From “As is” to “To Be” Situation

Seeing the “Big Picture”

- What are your capabilities to set your business company objectives – Strategic, Operational, Customer, Compliance and reporting throughout the organization?
- What are your business models in place – Strategy, People, Process, Technology and infrastructure?
- What are your boundaries – Mandatory & Voluntary?
- What are the obstacles that impede your organization towards achieving objectives?

Governance, Risk Management, Compliance & Internal Control Approach – Standards, Guidelines and Regulatory Requirements

- ❖ **Governance** – King III, Sarbanes-Oxley (SOX), OECD, European Directives
- ❖ **Risk** – ISO 31000, COSO, ASNZ 4360, Basel I, Solvency II
- ❖ **Compliance** – SA Companies Act, SOX, FCPA, National & International Regulatory Requirements
- ❖ **Audit** – COSO Internal control, IFRS, AS 5, SAS 99
- ❖ **Ethics & Culture** – Various CSR Frameworks, AA 1000, SA 8000, OCDE
- ❖ **IT Governance & Security** – COBIT, ISO 20000, ISO 27001, NIST
- ❖ **Quality** – ISO 9001, ISO 14000, Six Sigma

Integrated Approach Programs: The three core principles

- Integration of governance, risk management, ethics and compliance from interdisciplinary approach guided by principles, enacted by processes, implemented by practice, conducted by people, and enabled by technology
- Integration link to value, to effectively coordinate people, process and technology so that an integrity-driven performance strategy is embedded in the fabric of the organization
- Measured by metrics and indicators, characterized by along a maturity model and integration index, enabled by technology components and creating or transforming deliverables

Building your organization GRC Framework: Establishing the Desired Enterprise-Wide Culture

- Ensuring GRC benefits impact behavior
- Assessing your organization’s current culture – Ethical, Risk, Governance Workforce & Technology culture
- Defining or redefining the culture to meet your desired ends
- Communicating GRC initiatives throughout the organization
- Promote the new culture enterprise-wide

Oversight Personnel

- Define board structure, committees and responsibilities
- Defining roles and accountabilities of key stakeholders (board, executives, management, compliance, audit, etc)
- GRC training program for board members

Leaders and Champions

- Defining leadership and champion responsibilities
- Screening & Selecting program leadership and champions

Strategic Personnel

- Defining strategic personnel structure and responsibilities
- Screening & Selecting strategic personnel

Operational Personnel

- Defining operating personnel structure and responsibilities and specific reporting line to strategic personnel
- Establish training programs to educate operating personnel

Plan & Organize the GRC Implementation

- Define scope, stakeholders, planning methodology and team
- Define organization objectives – mission/vision/values
- The GRC framework from current to desired state
- Identification of organization structure, including major entities, business units, departments and the way these groups interrelate.
- Identification of boundaries – mandatory & voluntary
- Control, policies, procedures in place
- Training programs
- Workforce management
- Physical infrastructure

OCEG GRC CERTIFY INTENSIVE WORKSHOP – 4 Day

Overview

OCEG affiliate **GRC Certify** offers the GRC Professional Certification (GRCP) that provides an opportunity to gain a globally recognized qualification that is portable across all industries. To prepare applicants for the GRCP exam, Quency offers an innovative program that provides excellent career development opportunities and the chance for participants to enhance their GRC knowledge. The **GRC Professional Intensive Workshop** is designed to provide practical tools for participants to utilize in their role, whilst obtaining formal recognition for their professional excellence and competencies as a GRC professional.



GRC Certification demonstrates to the marketplace and your employer that you have the skills to integrate governance, performance, risk, internal control and compliance management to achieve principled performance.

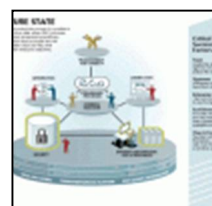
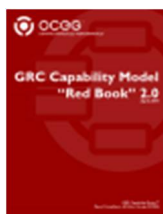
The benefits from being Certify

- Ensure your understanding of the GRC Capability Model (OCEG Red Book).
- Add the GRCP credential to your resume.
- Demonstrate to your current and potential employers that you have knowledge of GRC process standards.
- Include your name in the GRCP Directory.
- Be prepared to lead GRC projects in your organization

You get...

Attendees of the GRC Intensive Workshop will gain a practical understanding of the following learning objectives:

- Aligning risk and compliance in the context of business objectives
- Understanding, defining, and enhancing organizational culture as it relates to GRC
- Implementing GRC processes that increase stakeholder confidence
- How to prepare and protect the organization while preventing, detecting, and reducing adversity
- Strategies to motivate and inspire desired conduct
- Improve responsiveness and efficiency of GRC processes
- Optimizing the economic and social value of the organization
- Understanding technologies role in GRC
- How to develop a GRC strategic plan
- Ongoing monitoring of GRC activities through metrics and measurement



Agenda

Introduction to GRC and the Principle of Performance®

Understanding and defining GRC & Principled Performance®

GRC Fundamentals

GRC Capability Model (Red Book):

8 Integrated Components & 8 Universal Outcomes

Detailed review of the OCEG GRC Capability Model & Red Book:

- Culture & Context
- Organize & Oversee
- Assess & Align
- Prevent & Promote
- Detect & Discern
- Respond & Resolve
- Monitor & Measure
- Inform & Integrate

Continued review and implementation of the OCEG GRC Capability Model & Red Book 2

Defining and executing a GRC strategy in your organization

Implementing metrics, measurement, and improvement of the GRC program

The Critical Role of Information Technology in GRC Management

The GRC Reference Architecture: Utilizing the GRC Technology Guide 2.1®

Conducting a GRC Technology Assessment

Developing Your GRC IT Roadmap & Action Plan

Case Study

Exam

RISK MANAGEMENT PROGRAMS

RISK MANAGEMENT: CONCEPTS, TOOLS & TECHNIQUES

2 Day Workshop

OBJECTIVES

Participants will be able to:

- Describe key concepts that modernise risk management - stakeholder focus, risk perception, risk tolerance, and integrated (Enterprise) Risk Management (IRM/ERM);
- Develop and use key tools (e.g. Risk Matrix and Risk Tolerance Model) for more structured risk management; and
- Participate in, and contribute to, structured risk management techniques.

ABOUT THE WORKSHOP

Day one explores the strengths, weakness, and objectives inherent in the most commonly used risk management processes so participants may make informed decisions about the best process for their organization. Participants also learn proven strategies for implementing IRM/ERM. In addition, participants are introduced to two critical components in the suite of risk management techniques - Risk Factoring (for day to day management of operational risks) and Strategic Risk Assessment (for managing the strategic risks of major initiatives, programs and the organization overall).

Day two concentrates on hands-on practice with Risk Factoring and Strategic Risk Assessment. Tools such as Risk Assessment Toolkit are used as a learning aid and can be adopted or adapted by participants for their organisation. Participants will also learn about tools (Risk Register) and strategies for reporting and monitoring risks (Risk Indicators).

Agenda

- Introductions, Objectives, Agenda
- Key Risk Management Concepts - Cementing the Basis of Common Understanding
- Understanding Stakeholders, Risk Perception & Tolerance
- Understanding Integrated Risk Management in Modern Public Sector Organizations
- Understanding the Systematic Risk Management Process
- Practicing Risk Management - Preparing a "Context" before starting a risk assessment session
- Review of the Systematic Process
- Practice using the Risk Assessment Toolkit
- Post Risk Assessment Session Strategies and Techniques
- Topical Issues and Evolving Risk Management Concepts

MASTERING RISK MANAGEMENT: TOWARD RISK CONVERGENCE

2 DAY WORKSHOP

Who Should Attend!

This workshop is designed for executives and senior managers in business, industry or government wishing to understand and apply leading risk management processes to their work, or those wishing to extend their risk management capabilities.

It will be of particular instant benefit and value to:

- ❖ Chief Risk Officer
- ❖ Compliance Officer
- ❖ Risk Managers
- ❖ Internal & External Auditors
- ❖ Senior IT Professionals
- ❖ Senior Managers in Planning, Finance, Marketing, Project, HR, etc
- ❖ Consultants & Business Advisors

Key Issues:

- Why is the discipline of GRC important, what challenges do organizations face?
- What are some best practices to consider when performing risk assessments?
- What action steps can organizations take to perform better risk assessments?
- Why and how to integrate performance measures and risk measures – The Key Indicator Trio, KRI, KPI, and KCI?

Course Background

Managing risk and compliance in silos is both cumbersome and costly. For each new regulation or risk discipline, organizations typically implement a new technology point-solution. This fragmented approach limits an organization's ability to streamline risk and compliance processes and reduce costs. It also obscures the opportunity to integrate risk and compliance to gain a holistic view of the firm's risk landscape.

This new, two-day workshop provides the framework for a successful GRC program. No two organizations will implement Risk Management in the same way; let our expert instructor help you customize a plan that will work for your organization.

In addition to acquiring the knowledge to full understand the RM process; this workshop will demonstrate practical ways of putting theory into practice by using case studies, check-lists and hands-on exercises.

AGENDA

Introduction to Governance, Risk Management, Compliance & Ethics

What is “Risk” Convergence?

Looking at the “Big Picture”

Introduction to Risk Assessment

An Overview of COSO ERM, AS/NZ 4360 – 2004 & ISO 31000

Traditional v/s Modern Risk Management

Challenges with Risk Assessment

- Different Standards & Guidelines
- Organization Silos

GRC Risk Convergence – Key Issues

- Why is the discipline of risk assessment important and what challenges do organization face?
- What are some best practices to consider when performing risk assessments?
- What action steps can organizations take to perform better risk assessments?

Risk Convergence Defined

- Where are we exposed?
- What can go wrong?
- What can go right?
- How likely is it to happen?
- How bad can it be?
- What can cause it to happen?
- What are the consequences?
- Who gets to decide?

Assessing Risks Using a Consistent Methodology

- Assess business context
- Assess business process
- Identify process risk
- Assess process risk
- Identify issues
- Create action plan
- Assess performance result
- Certification of process

Developing a Common Shared Context

- Strategic objectives
- Organizational structure
- Process hierarchy

Assessment of Context Exposure

- Defining the Problem
- Formulating the Hypothesis
- Collecting the Facts

Control v/s Risk Focus

- Control assessment
- Risk assessment

Understanding the Anatomy of Risk

- The concepts: RMA approach
- Root cause
- Consequence
- Downstream effect
- Control/Failure
- Risk Event
- Control issue

The DNA of Risk Management

Building your Risk Taxonomy

- Use a common taxonomy to categorize risks

The Key Indicator Trio:

- Key Risk Indicator
- Key Control Indicator
- Key Performance Indicator

Risk Assessment Methodology

- Critical Analytical Thinking
- Scenario Analysis

Risk Assurance

- The Role of the Internal & External Auditor

Internal Audit Methodology

Building your Business Case

- The Context
- Risk Convergence
- Risk Taxonomy
- Methodology
- Indicators
- Reporting & Assurance

ENTERPRISE RISK MANAGEMENT CERTIFIED PROFESSIONAL - ERMCP



4 DAY WORKSHOP + EXAM

ERMA - Enterprise Risk Management Academy

ERMA is a global learning centre for professionals and practitioners in the field of Enterprise Risk Management (ERM). The Academy is established to facilitate collaboration efforts of ERM professionals and practitioners around the world, promoting and practicing ERM at their workplace.

With several hundreds members from more than 65 countries, spread in America, Europe, Middle East, Asia Pacific and Africa, our members comes from a wide variety of professional background, from CEOs and Chief Risk Officers, to graduate and under graduate students. They all share one thing in common. The same passion in ERM.

Certification Programs

ERMAP or Enterprise Risk Management Associate Professional is given to professionals who are comparatively less experienced in the field of enterprise risk management, but are able to demonstrate an integrated and comprehensive knowledge of the essential principles and fundamental concepts required for managing enterprise-wide risks.



ERMCP (Enterprise Risk Management Certified Professional) is given to professionals who are well experienced in the field of enterprise risk management and can demonstrate their knowledge, experiences and skills in managing the ERM process, which consists at least the following processes: setting the context, identifying risk, assessing risk, mitigating risk, and monitoring it.



EBA - Exam-Based Assessment

EBA or Exam-Based Assessment, is part of the ERMA Certification Pathways, which will enable a candidate to participate in a professional assessment, leading to one of ERMA's professional designations.

In the EBA, the assessment will be focused on Technical Competency, as well as the Behavioural Competency.

AGENDA

ERMA's workshop structure is focused on providing a strong fundamental understanding on Enterprise Risk Management, with special reference to ISO 31000. The workshop uses a combination of instructor-led training and real-world case study analysis. It consists of the following four primary modules:

Introduction to ISO 31000

- Why ISO 31000
- Scope of ISO 31000
- Terms & definitions

Risk Management Principles

- Principles of ISO 31000
- Case Study

Risk Management Framework

- Overview of risk management framework
- Mandate & Commitment
- Design of framework for managing risk
- Implementing risk management
- Monitoring & Review of the framework
- Continual improvement of the framework
- Case study

Risk Management Process

- Overview of risk management process
- Communication and Consultation
- Establishing the context
- Risk Assessment
- Risk Treatment
- Monitoring and review
- Recording the risk management process
- Integrated case study

Module Structure

MODULE I: Introduction to ISO 31000

Despite being newly introduced, ISO 31000 is more systematically structure and easy to understand for implementation, especially when compared to other risk management standard. The first module is designed to give the course participants an overview of the primary components of ISO 31000, its advantages, and how it can effectively be used as a framework for managing risks faced by any organization.

Why ISO 31000?

An overview of what is ISO 31000, and how it can be used as an effective framework for managing risk.

Scope of ISO 31000

Generic guidelines on how ISO 31000 is applicable to public and private organizations in terms of a wide range of activities, which could be strategic or operational, or pertain to decision making or projects, etc.

Terms & Definitions

This module is focused on familiarizing the audience with specific terminologies relating to risk management, and specifically to ISO 31000

MODULE II: Risk Management Principles

The eleven principles of the ISO 31000 for managing risk, act as a guideline for effective risk management at all levels. These principles are aimed at changing the mind-set of an organisation's management and staff, with the objective of creating a new behavior in risk management, increasing risk awareness and making risk management an inseparable part of their daily job.

Principles

The module thoroughly explores each principles of ISO 13000, which are:

Principle 1: Risk Management creates and protects value

Principle 2: Risk Management is an integral part of all organizational processes

Principle 3: Risk Management is part of decision making

Principle 4: Risk Management explicitly addresses uncertainty

Principle 5: Risk Management is systematic, structured and timely

Principle 6: Risk Management is based on the best available information

Principle 7: Risk Management is tailored

Principle 8: Risk Management takes human and cultural factors into account

Principle 9: Risk Management is transparent and inclusive

Principle 10: Risk Management is dynamic, iterative and responsive to change

Principle 11: Risk Management facilitates continual improvement of the organisation

Case Study

The module is also equipped with a case study aimed at describing how each of ISO 31000's principles is applied in real-world scenario.

MODULE III: Risk Management Framework

The success of risk management highly depends on the effectiveness of the risk management framework, which provides the foundation and the arrangements that will embed it within the organization. The framework assists in managing risks effectively through the application of the risk management process at various levels and within the specific context of the organization.

The third module will explain how the risk management framework provides the foundation for risk governance structure, which consists of structural, operational and maintenance aspects.

Overview of risk management framework

An overview of what risk management framework is, and how it is applied.

Mandate & Commitment

- Corporate laws and regulations (Continental Law and Common Law)
- One-tier board system
- Two-tier board system
- Duty of the Board of Directors
- Duty of the Board of Commissioners

Design of a framework for managing risk

- Understanding the organization and its context
- Establishing risk management policy
- Accountability
- Integrating with organizational processes
- Resources
- Establishing internal communication and reporting mechanism
- Establishing external communication and reporting mechanism

Implementing risk management

- Implementing the framework for managing risk
- Implementing risk management process

Monitoring & Review of the framework

- Determine the gap between plan versus actual, and then analyze it for improvements (to close the gap)
- Performance measurement
- Effectiveness of existing risk controls
- Effectiveness of the framework
- Regularity in reporting
- Monitoring external changes and trends, which could have an impact on the achievement of the organisation's objectives.

Continual improvement of the framework

Continual improvement should give more assurance in achieving the organisation's, objectives, by increasing the ability to mitigate the risks.

Case Study

MODULE IV: Risk Management Process

The fourth and final module of the coursework will focus on:

- a) Tailoring risk management to the business process of the organization;
- b) Risk management as an integral part of management, in achieving the objectives;
- c) Embedding risk management in the culture and practices of the organization.

Overview of risk management process

An overview of what is the process of risk management

Communication and consultation

Communication is an exchange of information, which can flow horizontally forward and backward, or vertically upward or downward. In many cases communication act as a lubricant for the system. The sub-module will focus on how communication should be managed to achieve effective results.

Establishing the context

In establishing the context, the risk assessment objectives, risk criteria and risk assessment program are determined and agreed.

The context to be established is:

- a) External context
- b) Internal context
- c) Risk management context
- d) Risk criteria

Risk assessment

- a) Risk identification
- b) Risk analysis
- c) Risk evaluation (tools for risk evaluation)

Risk treatment

This sub-module will explain about risk treatment, and how it helps modify a risk to become acceptable.

Monitoring and review

Through this topic, participants get to understand how monitoring and review ensure that the risk management process leads to the targeted performance, and assure that the organisation's objectives are achieved.

Recording the risk management process

- a) Risk Management plan
- b) Record the implementation of the risk management plan

Integrated case study

COMPLIANCE MANAGEMENT PROGRAMS

CORPORATE COMPLIANCE: ESTABLISHING AN EFFECTIVE COMPLIANCE PROGRAM

2 DAY WORKSHOP

Who Should Attend!

This workshop is designed for executives and senior managers in business, industry or government wishing to understand and apply leading compliance management processes to establish an effective compliance program, compliance risk assessments and the role of the compliance officer and corporate counsel.

It will be of particular instant benefit and value to:

- ❖ Risk Officer
- ❖ Compliance Officer
- ❖ Ethic Officer
- ❖ Senior Managers in Planning, Finance, Marketing, Project, HR, etc
- ❖ Consultants & Business Advisors

Upon successful completion of this course, you will be able to:

- Comprehend and maintain awareness of compliance requirements
- Organise and monitor the operation of compliance management system
- Implement processes for the management of breaches in compliance requirements
- Provide education and training on compliance requirements and systems
- Promote and liaise on compliance requirements, systems and related issues
- Promote compliance with legislation
- Support performance management process
- Identify risk and apply risk management processes
- Undertake compliance audits

AGENDA

Why have a Compliance Program!

- Risk Minimization
- Better Image, Improved Relationships, Greater Trust
- External Pressures
- Reduced Fines and Penalties
- Greater Efficiency and Improved Outcomes

The Seven Elements of an Effective Compliance & Ethic Program

- ❖ Element 1 - Establish Policies, Procedures and Controls

- ❖ Element 2 - Exercise Effective Compliance and Ethics Oversight
- ❖ Element 3 - Exercise Due Diligence to Avoid Delegation of Authority to Unethical Individuals
- ❖ Element 4 - Communicate and Educate Employees on Compliance and Ethics programs
- ❖ Element 5 - Monitor and Audit Compliance and Ethic Programs for Effectiveness
- ❖ Element 6 - Ensure Consistent Promotion of the Program and Enforcement of Violations
- ❖ Element 7 - Respond Appropriately to Incidents and Take Steps to Prevent Future Incidents

Compliance Framework

- Define 'compliance' and the roles at each level of an organisation to deliver a compliance framework.
- Articulate the elements of the AS/NSZ 3806: 2006 and how they are used to develop a compliance framework.
- Discuss the relationship between compliance and risk management.
- Apply the structural elements of the Risk Management standard ISO 31000 to assess, treat and monitor compliance risks.
- Develop a compliance risk register and supporting compliance plan on how to treat the risks.

Culture of Compliance & Ethics

- Define and describe compliance culture, integrity, ethics and values
- Articulate the importance of ethical decision-making
- Outline strategies and compliance programs in order to impact the organisation's standards and values

Compliance Obligations, Legislation and Regulation

- Describe compliance obligations; particularly the impact of the legislative and regulatory environment.
- Articulate the steps of a legislative and regulatory change program.
- Outline engagement issues which influence the development of legislative and regulatory reform.

Awareness, Communication and Training

- Define and describe the three key elements of an effective compliance, communication program – Awareness, Communication and Training
- Develop an 'ACT' plan
- Consider and assess critical factors that contribute to the success of implementing an 'ACT plan', including budgets, internal and external resources, and supporting audiences

Issues and Breach Management

- Describe the elements of a consequence management program
- Design and develop an issues and breach management process
- Establish a standard process to investigate breaches and manage the outcomes

Managing Compliance Projects

- Define what is a compliance project and when it is required
- Describe the elements of each stage in a project lifecycle
- Identify the specific responsibilities of a compliance officer in a project

Compliance Monitoring

- Define compliance monitoring and why it needs to be performed
- Outline the difference between compliance monitoring and audit function audits
- Articulate the steps of a compliance monitoring program
- Outline how to undertake an individual compliance monitoring plan
- Develop final reports on findings and recommendations

CORPORATE COMPLIANCE: OPTIMIZING YOUR PROGRAM

2 Day Workshop

Who Should Attend!

Risk Officer, Compliance Officer, Legal Counsel, Internal Auditor and other Senior Managers

AGENDA

How do we Measure the Performance of Compliance

Key Aspects of Compliance Performance

- Responsive
- Efficient
- Effective

Who is interested in which aspects!

- Government and Enforcement
- Compliance, Control & Internal Audit
- Business Operators
- Board

Challenges

- Compared to What!
What generally accepted and vetted standard can be used to judge a program? Not just “in principle” but at a practical and operational level?
- Who Decides!
What types of internal and external professionals have the skills to evaluate and judge the effectiveness of a program?
- How Often!
How often can we (should we) put a stake in the ground so that if we need to go back in time, we can present evidence of effectiveness?

How effective, responsive and efficient processes will deliver measureable program outcomes for the organization

- ❖ Responsive to change - The system should be able to absorb changes in the external environment (e.g., new laws and regulations) and internal environment
- ❖ Responsive to events - The system should detect noncompliance and adverse events in a timely manner so that action can be taken.
- ❖ Efficient use of financial capital - The system should efficiently use financial capital and seek to reduce operational costs over time
- ❖ Efficient use of human capital - The system should efficiently use human capital, most importantly senior executive time, and look for ways to reduce the amount of time required to perform management activities.
- ❖ Effective design - Are reasonable and sound structures in place to address risks?
- ❖ Effective operation - Does the system operate as designed?

Performance Measurement Process

- ❖ Define – Objectives, Outcomes, Indicators, Targets and tolerances
- ❖ Measure – Data from existing systems and from specific systems
- ❖ Analyse – Relationship between indicators and outcomes and define opportunities for improvement
- ❖ Improve – Optimize the program and improve measurement
- ❖ Verify & Control – Verify improvements that are in place and improve the control of the compliance and ethics program

Indicators - SMART

Specific/Simple

- Is it exactly what is being measured! Is it easily understood?
- Does the indicator isolate the true event?
- Does the indicator avoid “mixed messages”?

Measurable

- Is it accessible and worth the cost to obtain the data?
- Can it be quantified?

Actionable

- Are the underlying processes that can affect this indicator under our control?
- Once we understand the value of the indicator and any trends, will it be possible for us to take meaningful action?

Relevant

- Does the indicator capture the essence of the desired outcome?
- Will tracking this indicator drive the appropriate behaviour – or generate unintended consequences?

Timely

- Can it be frequently updated?
- Will the indicator reveal itself in time to take appropriate action?

Compliance Maturity Model

- Degree to which the organization anticipates and influences the boundaries to which it is subject and communicates or incorporates compliance into the rules by which it runs the organization
- Limits imposed upon the conduct of an organization and its employees either voluntarily (values, standards, internal policies) and by mandate (laws and regulations)
- Degree to which the structure of the organization sustains and promotes accountability for compliance

Case Study – XYZ Ltd

IT GRC PROGRAMS

INFORMATION TECHNOLOGY (IT) GOVERNANCE

2 DAY WORKSHOP

Who should attend?

This workshop is designed for IT executives and senior managers in business, industry or Government wishing to understand and apply leading governance management practices to their work, or those wishing to extend their risk management capabilities.

Objectives

This course fills that need in the marketplace and gives you structured and practical solutions using the best of the best principles available today. The three critical pillars necessary to develop, execute and sustain a robust and effective IT governance environment are:

- Leadership and proactive people and change agents,
- Flexible and scalable processes and
- Enabling technology

We also cover these action-oriented elements:

- ❖ Demand management and alignment (the why and what of IT strategic planning, portfolio investment management, decision authority, etc);
- ❖ Execution management (includes the how – Program/Project Management, IT Service Management with IT Infrastructure Library (ITIL) and Strategic Sourcing and outsourcing);
- ❖ Performance, risk and contingency management (e.g. includes COBIT, the balanced scorecard and other metrics and controls); and
- ❖ Leadership, teams and people skills

AGENDA

Introduction to IT/business governance

- Defining enterprise governance, business and IT governance
- Purpose and scope of IT governance
- Linking the role of the CEO to creating an effective governance and compliance environment
- Overview of the integrated IT governance framework Steps in making IT governance achievable and real

Overview of comprehensive IT governance framework and related industry best practice frameworks

- Limitations to existing models, standards and frameworks
- Integrated IT governance framework and roadmap

- Overview of models, frameworks and standards including: ISO 38500, COSO, ITIL, PMBOK, PRINCE2, Six Sigma and Lean, COBIT, ISO/IEC 20000, ISO 17799 and many more

Business and IT alignment, strategic/operating planning and portfolio investment management excellence

- IT alignment governance process
- Principles of aligning IT to the business more effectively
- Setting a direction for improved alignment through planning related processes
- Strategic IT investment portfolio alternatives
- IT engagement and relationship model ad roles

Principles for managing successful organizational change and developing high performance teams

- Framework for managing accelerating change
- Organizing for the IT governance initiative
- World class leadership principles and practices
- Principles for creating and sustaining high performance teams

Program and project management excellence

- Trends in program and project management
- Causes of program/project failures and challenges and how to overcome them
- Principles for achieving excellence in program/project management
- Making the choice – program and project management light or complex
- Program and project governance excellence

Strategic sourcing, outsourcing and vendor management excellence

- Defining strategic sourcing and outsourcing
- Principles and practices for outsourcing excellence
- Vender selection, contract negotiations and governance process

Performance management, management controls, risk management, business continuity and enabling technology

- Principles for achieving performance management and control excellence
- Risk assessment, management and mitigation
- Business and IT continuity and protection plan checklist
- Enabling technologies to improve IT governance

GRC Technology Assessment

- How to develop a Formal GRC Technology Assessment Policy
- How to create an Inventory of Existing GRC Technology
- Align GRC Technology Assessment Goals and Objectives with IT Governance, Strategies and Organizational GRC Requirements
- Implement a GRC Technology Assessment Methodology
- Prioritize GRC Technology Needs for the Organization
- Prepare a GRC Technology Plan

IT COMPLIANCE, RISK & SECURITY MANAGEMENT

2 DAY WORKSHOP

Every organization has a mission. In this digital era, as organizations use automated information technology (IT) systems to process their information for better support of their missions, risk management plays a critical role in protecting an organization's information assets, and therefore its mission, from IT – related risk. An effective risk management process is an important component of a successful IT security program. The principal goal of an organization's risk management process should be to protect the organization and its ability to perform their mission, not just its IT assets. Therefore, the risk management process should not be treated primarily as a technical function carried out by the IT experts who operate and manage the IT system, but as an essential management function of the organization.

Who should attend?

The workshop is designed for IT executives and senior managers in business, industry or government wishing to understand and apply leading compliance, risk management practices to their work, or those wishing to extend their risk management capabilities.

Objectives

- The ultimate roadmap for making an effective security policy and controls that enable monitoring and testing against them
- The most comprehensive IT compliance template available, giving detailed information on testing all your IT security, policy and governance requirements
- This technically based, practical map to information systems audit and assessment will show how the process can be used to meet myriad compliance issues.
- By better securing the IT systems that store, process, or transmit organizational information;
- By enabling management to make well-informed risk management decisions to justify the expenditures that are part of an IT budget; and by assisting management in authorizing (or accrediting) the IT systems on the basis of the supporting documentation resulting from the performance of risk management.

AGENDA

Information Systems Legislation

- Civil and Criminal Law
- Legal Requirements
- Electronic Contracting
- Jurisdiction
- Due Care
- Due Diligence
- E-Discovery

Security Policy

- SMART Policies
- Mission, Vision, Values
- Frameworks and Policies
- Standards and Guidelines
- Processes and Procedures
- Interpreting Policies
- Preventive and Detective Controls
- Policy Areas to be considered
- Policy Framework
- Policy Creation
- Policy Conformance
- Incident Handling
- Standards and Compliance
- Internal and External Standards

Introduction to Risk Management

- Importance of Risk Management
- Integration into SDLC

Risk Assessment

- System Characterization
 - System-Related Information
 - Information-Gathering Techniques
- Threat Identification
 - Threat-Source Identification
 - Motivation and Threat Actions
- Vulnerability Identification
 - Vulnerability Sources
 - System Security Testing
 - Development of Security Requirements Checklist
- Control Analysis
 - Control Methods
 - Control Categories
 - Control Analysis Technique
- Likelihood Determination
- Impact Analysis
- Risk Determination
 - Risk-Level Matrix
 - Description of Risk Level
- Control Recommendations

Risk Mitigation

- Risk Mitigation Options
- Risk Mitigation Strategy
- Approach for Control Implementation
 - Control Categories:
 - Cost-Benefit Analysis
 - Residual Risk

Evaluation and Assessment

- Good Security Practice
- Keys for Success

Interview Questions

Risk Assessment Reporting

Managing Risk from IT

Fundamentals

- Organization wide Perspective
- Risk-based Protection Strategies
- Trustworthiness of Information Systems
- Establishing Trust Relationships among Organizations
- Managing Risk from Supply Chains
- Strategic Planning Considerations

Process

- Risk Management Framework
- Categorizing Information and Information Systems
- Selecting Security Controls
- Implementing Security Controls
- Assessing Security Controls
- Authorizing Organizational Information Systems
- Monitoring Security State of the Organization

Managing Risks within Life Cycle Processes