



Compliance Track Compliance Framework

Version	Date	Author	Email	Comments
1.0	Jan 5, 2011	J Cyriac	john@compliancetrack.com	

Agenda

1. Introduction	3
2. Rules Management.....	3
2.1. Rules Management – Excerpts from Frameworks	3
2.2. Rules Management using Compliance Track	4
3. Compliance Risks & Controls	5
3.1. Compliance Risks - Excerpts from Frameworks	5
3.2. Controls - Excerpts from Frameworks.....	6
3.3. Risk and Control Assessment- Excerpts from Frameworks.....	8
3.4. Compliance Track – Risks & Controls.....	10
4. Policy Management, Audit & Compliance Monitoring	10
5. Summary.....	12

1. Introduction

Compliance Track is a feature rich GRC (Governance, Risk & Compliance) platform. It is designed for flexibility and ease of use. A compliance manager can use the product in a variety of ways for realising his objectives. He can implement a compliance framework suitable for his organisation without any system mandated restrictions.

This document is an attempt to consider some areas of the major compliance frameworks around the world and introduce Compliance Track from a framework perspective .

2. Rules Management

2.1. Rules Management – Excerpts from Frameworks

Rulebook applicable to a company may be 1) Best Practice 2) Contracts (example- contract with a supplier) 3) Law (Statute or Case Law) or 4) Sector Regulation. A compliance manager should know the rulebooks applicable to his firm and he should assess the impact of the rules within those rulebooks to the various activities of his company's business. This section shows few relevant excerpts from some of the major compliance frameworks in the world advocating the need for having Rules Management as part of a company's compliance framework.

Australia AS 3806-2006 [Rules Management]

PRINCIPLE 5 - Compliance obligations are identified and assessed
(Sections 3.5.1 & 3.5.2)

- Identify Obligations
- Assess impact on business activities
- Process to identify changes in obligations

BASEL Compliance Framework [Rules Management]

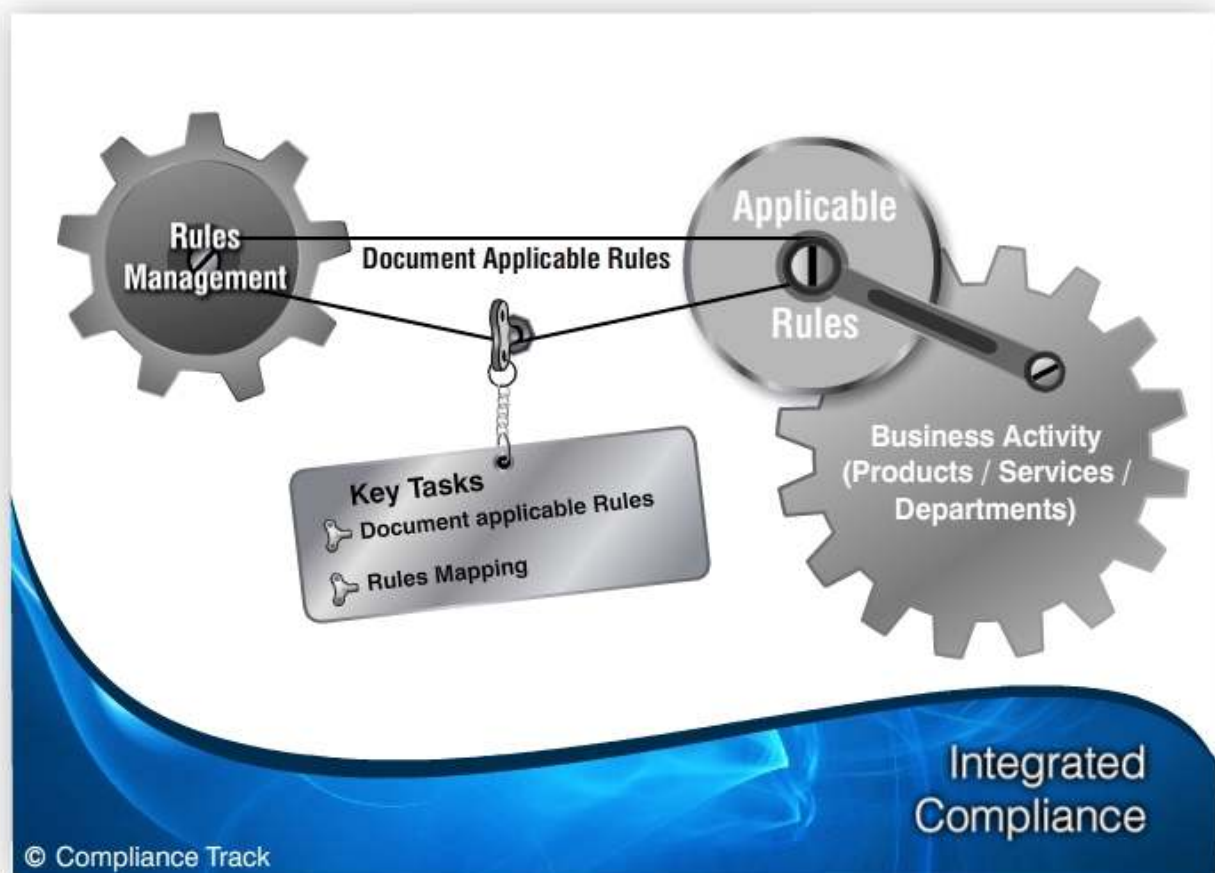
- Clarity and transparency may be promoted by making a distinction between general standards for all staff members and rules that only apply to specific groups of staff. (*Principle 3, Section 16*)
- Compliance function staff should have a sound understanding of compliance laws, rules and standards and their practical impact on the bank's operations. (*Principle 6, Section 33*)

UK BS 8453, Financial services compliance framework [Rules Management]

The compliance function shall keep up-to-date with actual or potential changes in regulation, and communicate these to the relevant areas, such as business lines, risk management, senior managers and the governing body. (Section 4.6.7)

2.2. Rules Management using Compliance Track

Rules Management module in Compliance Track provides a simple and powerful way for the compliance manager to implement the concepts outlined in the above mentioned compliance frameworks. It provides interfaces to document and manage the rulebooks applicable to a firm and map the rulebooks to the right product or service or department within the firm. Compliance Track provides a variety of ways to import rulebooks into the product and manage rulebook changes.



3. Compliance Risks & Controls

3.1. Compliance Risks - Excerpts from Frameworks

The primary motivation behind the concept of Compliance Risk is to shortlist the applicable rules and prioritise them based on the apparent risk. If there are hundreds of rules applicable to a firm, it makes sense to prioritise those rules in the context of the business and the market place and monitor them closely. Nowadays, risk based compliance is a commonly accepted approach. This section shows relevant excerpts from some of the major compliance frameworks in the world on the topic of Compliance Risks.

Australia AS 3806-2006 [Compliance Risks]

(PRINCIPLE 5) Prioritisation *Section 3.5.3*

Prior to the implementation of its compliance program an organization should identify compliance risks and rank the likelihood and consequences of potential compliance failures and allocate resources for their treatment accordingly.

Notes:

The risk of compliance failure should be reassessed whenever there are—

- new or changed activities, products or services;
- changes to the strategy of the organization;
- significant external changes; or
- changes to compliance obligations.

BASEL Compliance Framework [Compliance Risks]

The compliance function should, on a pro-active basis, identify, document and assess the compliance risks associated with the bank's business activities (*Principle 7, Section 37*)

The compliance function should also consider ways to measure compliance risk (e.g. by using performance indicators) and use such measurements to enhance compliance risk assessment. (*Principle 7, Section 38*)

UK BS 8453, Financial services compliance – Framework [Compliance Risks]

Risk factors, which might include the following, are routinely identified.

1. The type of client with which the business deals.
2. The nature of the services the firm offers
3. Current regulatory requirements and concerns.
4. The extent to which the business or sector in question has had compliance issues in the past.
5. On each determination, the risk factors are applied to the different business areas to assess the level of compliance risk currently faced by each business.

A robust risk rating methodology, which is not necessarily complex, is applied regularly on a consistent basis.

3.2. Controls - Excerpts from Frameworks

The term Controls or Internal Controls is often associated with financial controls. It is applicable in a compliance framework where one consciously applies a mechanism to mitigate a compliance risk. Controls can be categorized as 1) preventive 2) corrective or 3) detective. For example, an audit test or compliance monitoring test is a detective type of control whereas a documented policy or a procedure is a preventive control. Corrective control refers to any activity to correct the errors that have already occurred. This section shows relevant excerpts from some of the major compliance frameworks in the world referring to Controls as part of a company's compliance framework

Australia AS 3806-2006 [Controls]

PRINCIPLE 9 - Controls are in place to manage the identified compliance obligations and achieve desired behaviours.

(Section 4.4)

Controls should be identified for the prioritised compliance obligations (Compliance Risks).

BASEL Compliance Framework [Controls]**Principle 8: Relationship with Internal Audit**

The scope and breadth of the activities of the compliance function should be subject to periodic review by the internal audit function.

Compliance risk should be included in the risk assessment methodology of the internal audit function, and an audit programme that covers the adequacy and effectiveness of the compliance function should be established by testing of controls (*Principle 8, Section 44*)

3.3. Risk and Control Assessment- Excerpts from Frameworks

The process of Risk and Control Assessment is known by various names. Some call it Risk Assessment. It is also referred to as Risk and Control Self Assessment (RCSA). This does not refer to an Auditor's annual audit test or the regular monitoring conducted by the compliance function. This is a point in time assessment of Risk posed by a specific area of the business. This is normally conducted with a lot of involvement with the business, not just the Risk & Compliance executives. The result of this process affects the Risk & Compliance efforts. For example, an area that is rated as high risk may need a daily or weekly monitoring by the compliance function. In addition, the risk rating may affect the way in which processes are created and managed in the business. This section shows relevant excerpts from some of the major compliance frameworks in the world discussing the need for risk assessment as part of a company's compliance framework.

Australia AS 3806-2006 [Risk Assessment]

rank the likelihood and consequences of potential compliance failures and allocate resources for their treatment accordingly. (*PRINCIPLE 5 Section 3.5.3*)

controls should be maintained and evaluated periodically to ensure their continuing effectiveness. (*PRINCIPLE 9 Section 4.4*)

BASEL Compliance Framework [Risk Assessment]

It is the responsibility of the internal audit function to conduct testing of controls commensurate with the perceived level of risk. The audit function should, of course, keep the head of compliance informed of any audit findings relating to compliance. (*Principle 8, Section 44,45*)

UK BS 8453, Financial services compliance – Framework [Risk Assessment]

(Section 4.2) On each routine assessment of the current risk factors and application of the rating methodology to the firm's businesses, the firm has a current measure of the compliance risk associated with each activity. This may be used to inform:

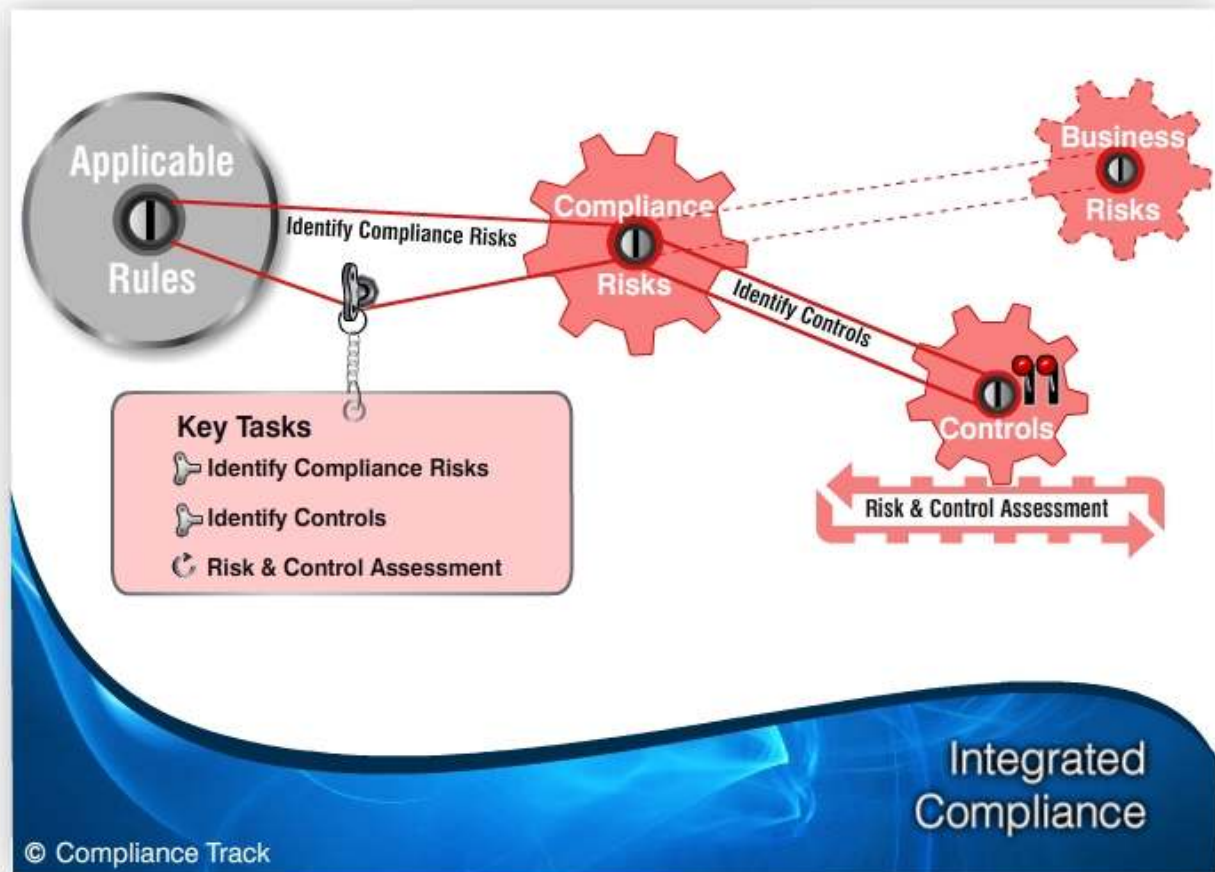
the level of compliance advisory resource to be allocated to that business line;
the amount and level of compliance monitoring to be applied to transactions and products in that business line;
the amount and type of training to be provided to that business line.

Notes:

The frequency and the way of compliance monitoring test is dependent on the outcome of a Compliance Risk Assessment. We need to consider how to link this. In an ideal scenario, while conducting a Risk assessment, one should be able to say how often it should be monitored.

3.4. Compliance Track – Risks & Controls

Compliance Track provides all the features necessary to incorporate Risks & Controls into a compliance framework as depicted in the following image.



4. Policy Management, Audit & Compliance Monitoring

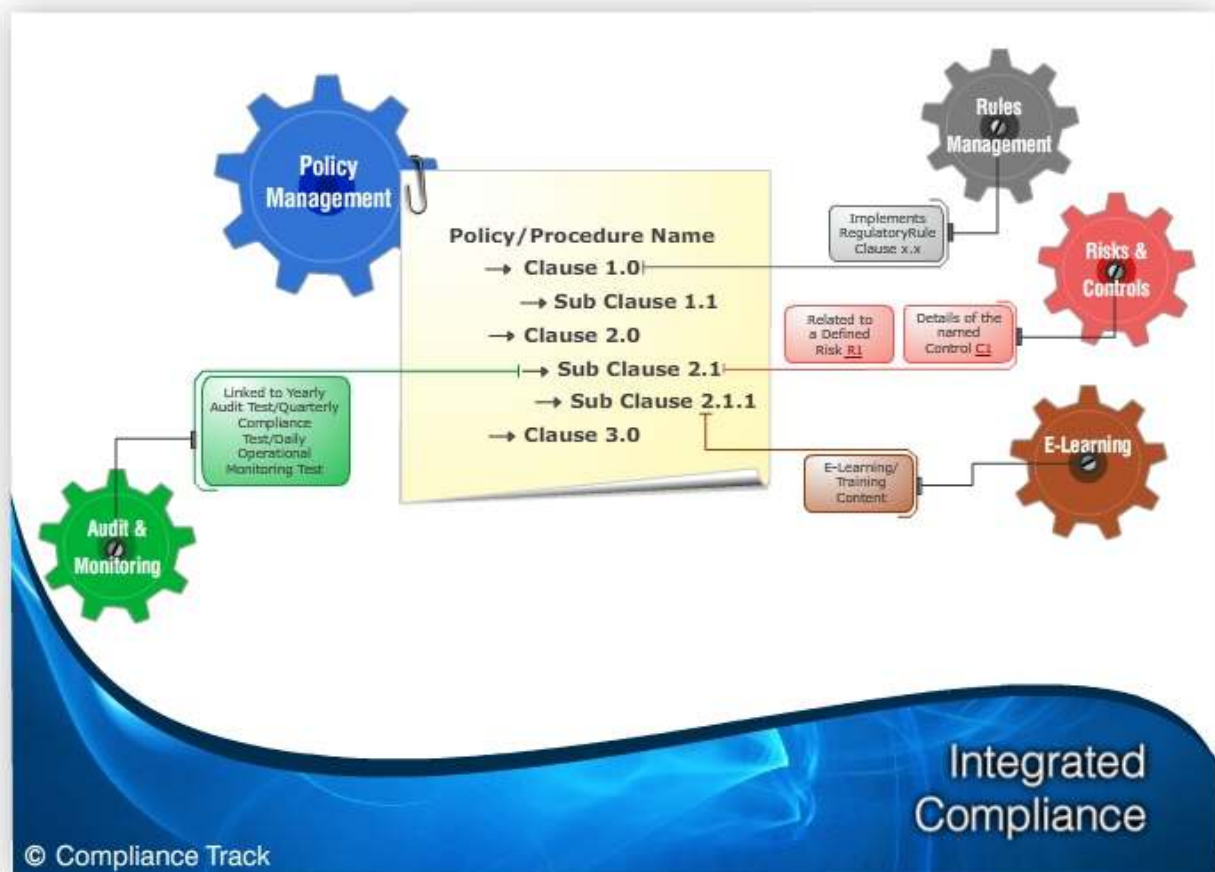
Policy Management is a widely adopted part in most organisation's compliance framework. Possible difference between companies in this area is in the nature of the adoption and the manner in which policies are created, deployed and updated.

Having a policy or a procedure is solving only part of the problem. A company needs a process to check the adherence of employees to those policies. The goal of such a process is to mitigate the possible compliance risks. The elements of such a process can be categorised as 'three lines of defence against risk'. The first line of defence is the operational monitoring. This refers to the daily per transaction monitoring, most often conducted by a customer facing employee. The second line of defence is the compliance monitoring. This is most often conducted by the compliance function at regular intervals. Audit is considered as the third line of defence and that is conducted by the audit function, less frequently compared to compliance.

All the major compliance frameworks discuss about the need for having policy management and audit & monitoring as part of a company's compliance framework.

- ✓ **Australian Compliance Framework AS 3806-2006**
- ✓ **BASEL Compliance Framework**
- ✓ **UK BS 8453 Financial Services Compliance Framework**
- ✓ **US Sentencing Guidelines – Chapter 8**

Compliance Track provides a well designed information architecture ready solution to handle the requirements related to policy management and audit & monitoring. It provides an easy to use point and click mechanism for the user to create relationship between various types of Risk & Compliance data.



5. Summary

Compliance Track is a flexible GRC platform that allows a compliance manager to adopt any compliance framework suitable for his organisation. It is highly recommended to review one's compliance framework from a strategic perspective atleast once in two years. It is definitely a plus when you have a platform like Compliance Track that is flexible to accommodate such changing requirements.