

---

## How to Implement an Integrated GRC Architecture



---

**White Paper**  
**January 2008**

## Background

Risk Management, Compliance and Governance reforms that followed the corporate failures of the past decade have dramatically changed today's business environment. Organizations worldwide are coping with a proliferation of new regulations and standards, and are challenged to do so in a way that supports performance objectives, upholds stakeholder expectations, sustains value and protects the organization's brand.

Recent studies indicate that Fortune 1000 corporations are subject to 35-40 different regulatory mandates and the management of regulation and compliance has become a serious risk factor in itself. Complying with each individual regulation is always complicated, lengthy and costly. Managing the burden of complying with multiple and overlapping regulations is becoming increasingly difficult and expensive. The need for an integrated GRC (Governance, Risk Management and Compliance) platform in today's business environment is obvious. Despite the hype around this topic, only a few organizations have succeeded in implementing a truly integrated GRC platform due to the complexity of the GRC environment.

## GRC Complexity

In order to implement an integrated GRC platform, organizations need to cope with the following complexity:

- 1 Multiple Regulations:
  - o Vertical Industry Regulations  
(e.g. Banking: Basel II, Insurance: Solvency)
  - o Horizontal Regulations (e.g. Sox)
  - o Internal Corporate Governance
  - o International Regulations
  - o Regional Regulations
  - o Local Regulations
- 2 Different Scope
  - o Operational Risk
  - o Internal Audit
  - o Financial Control
  - o IT Governance
  - o Anti-Fraud Management
  - o Business Continuity Planning
  - o Information Security Risk
- .4 Different Consulting Firms involved in each project
- .5 Different Objectives for each project
- .6 Different Methodologies and Diverging Workflows
- .7 Different Data Architecture Requirements
- .8 Diverse Participants
  - o Business Executives
  - o Risk & Compliance Officers
  - o Business Unit and Process Managers
  - o Employees
  - o Contractors
  - o Consultants

o Business Partners

Due to this complexity, most organizations still manage GRC projects in silos, adopting different methodologies and different software point solutions for each project. As a result of this approach, organizations face the following difficulties:

- Inconsistency among the different projects
- Lack of a unified view of risk and compliance that limits management's decision making process
- Lack of scalability from an enterprise wide prospective
- Duplication of activities and overlapping efforts that increase cost, internal overhead and external consulting expenses

Owing to the complex regulatory environment, GRC related costs in enterprises are skyrocketing. For example, according to a recent SIA study, the cost of compliance in the U.S. securities community alone has nearly doubled in three years reaching \$25 billion in 2006.

*"Companies that select individual solutions for each regulatory challenge they face will spend 10 times more on IT portion of compliance projects than companies that take on a proactive and more integrated approach."*

*Gartner*

## The Integrated GRC Approach

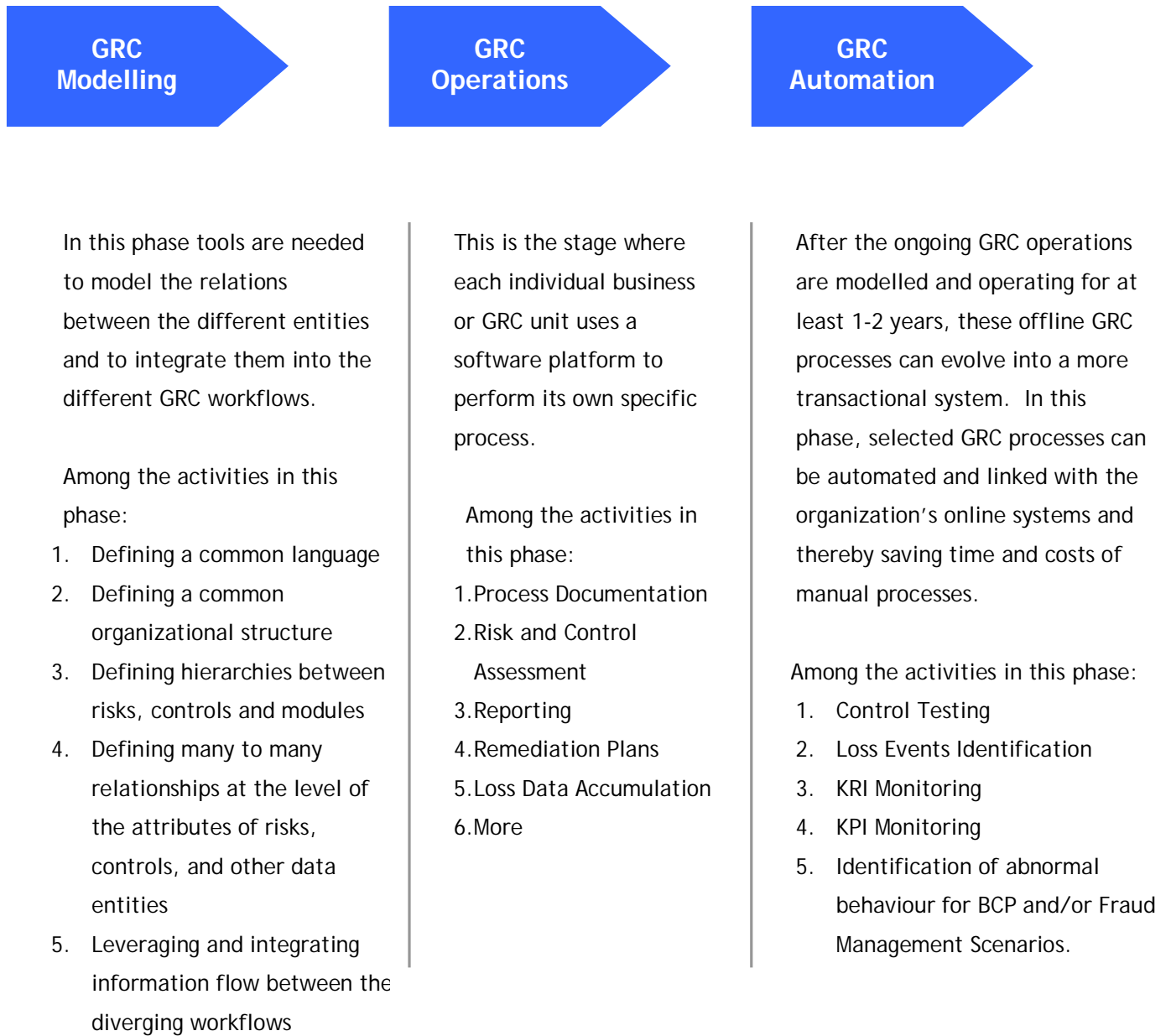
An integrated GRC strategy must provide an environment that on one hand allows each GRC process to be fully managed independently, while providing tools for defining complex relationships and the sharing and linking of information between the different regulations and standards.

Dynasec has defined a series of mandatory steps for managing multiple GRC processes in harmony which we call GRC Modelling.

- Definition of a single GRC terminology. Adopting a common language is a crucial step to avoid misunderstandings within the organization.
- Creation of a unified organizational structure. Variant organizational structures often inadvertently cause mistaken assessments that are based on erroneous risk and control calculations up the organizational tree.
- Granularity at the level of risk and control attributes. It is common knowledge that there are many-to-many relationships between risks and controls. This is indeed necessary, but not enough to support an integrated GRC environment. The organization must be able to define different, distinct attributes for common risks and controls shared by multiple GRC processes. A common control that occurs in two separate regulations might be critically important for one regulation and less important in the other. The ability to define this level granularity is critical for the success of an integrated approach.

- Defining hierarchical, complex relationships between controls. In order to reduce the duplication of controls between separate compliance procedures, the organization needs tools to define control dependencies intelligently. For example, a high level control in a regulation may be identical to a combination of 5 controls in another standard. The ability to define such smart links and multi-level hierarchies between risks, controls and GRC processes is vital to reducing the overhead of managing and testing controls across the enterprise.
- Leveraging information between separate GRC workflows. Each GRC unit has its own individual workflow that might consist of periodic control tests, multi-year audit plans or collected loss events. In order to achieve an overall view of the organization's risk; information must be shared between the different processes. For example, the Internal Audit team should receive status of control tests for determining how to build its audit plans. Loss event information collected by the operational risk group should be shared with other GRC functions.

Consequentially, we believe that the deployment of a comprehensive, integrated GRC strategy is composed of 3 phases:



## Easy2comply™ - Integrated GRC Approach

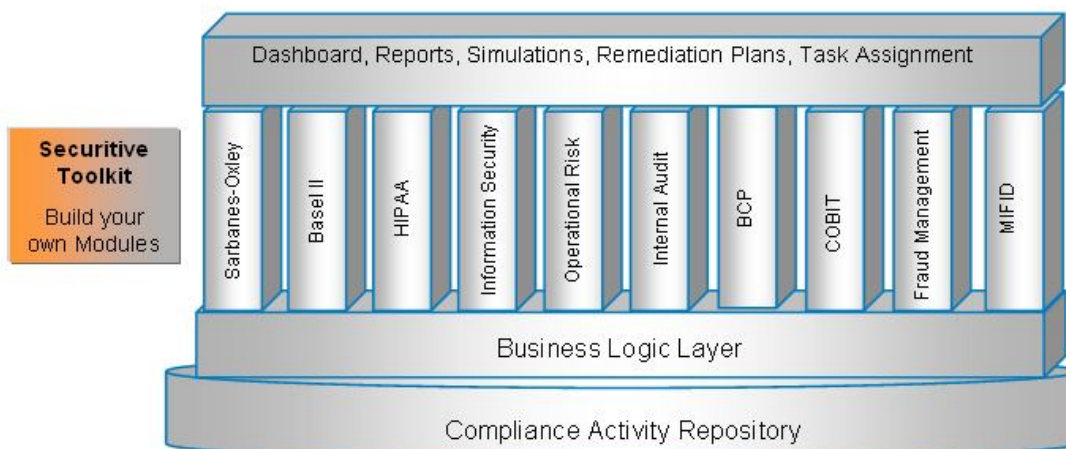
easy2comply™ is a web based software platform that enables companies to continuously manage and control compliance, corporate governance and risk management processes with built-in tools for GRC modelling.

There are 5 groups of GRC applications supported:

1. **Operational Risk Management** (ORM) including modules such as general ORM, Basel II, Solvency II, Arrow, BilMoG, MaRisk, etc.
2. **Internal Control Management** (ICM), including modules such as general ICM, SOX, JSOX, MiFID, Turnbull, Tabaksblat, etc.
3. **IT Risk and Governance** (ITG) including modules such as: CobiT, ITIL, ISO27001, ISO17799, Business Continuity Planning (BCP), BCM (25999), Information Security.
4. **Internal Audit Management** (IA)
5. **General Compliance** (GC) for special needs such as corporate governance and procedures, strategic projects, privacy and local laws, and more.

easy2comply™ provides the tools and functionality required to design the integrated workflow and data relationships between the different GRC projects, while providing each software module with its own full set of functionality, unique workflow and if relevant, best practices data.

easy2comply™'s unique data model is composed of 4 logical layers built as a single data model. It is this architecture that enables the intelligent sharing of information between the different GRC projects, the elimination of redundancy between risks and controls and enabling each project to be managed separately according to its specific time frame, methodology, workflow and reporting needs.



- The bottom layer is a repository that stores all the entities that are part of the GRC projects such as: organizational units, processes, sub-processes, systems, risks, controls, loss events, scenarios and others.
- The second layer provides tools that enable GRC modelling - the creation of complex relations between the data entities and workflows thereby facilitating the integrated multi-regulatory concept.

- The third layer is the applications layer for the different GRC modules. Each application is composed of the relevant methodology, functionality and workflow needed for its specific requirements.
- The fourth layer is a shared management layer that enables communication, coordination, and measurement of GRC processes. Authorized users can create and view reports, dashboards, remediation simulations and plans, warnings and notifications, and more. .

## About Dynasec

Dynasec Ltd. is a leading provider of Governance, Risk Management and Compliance (GRC) solutions. Our flagship product, easy2comply™ is the perfect answer for businesses of all sizes seeking to simplify their compliance and risk management processes.

easy2comply™ can be deployed either on-demand (SaaS) or on-site to suit each customer's preferred configuration. We serve customers in many markets including: financial institutions, telecom, energy, and government, pharmaceutical, healthcare, commercial organizations.

easy2comply™ - Practical Compliance Solutions  
affordable. reliable. easy2deploy.  
[www.easy2comply.com](http://www.easy2comply.com)

