

# 10 steps to a sustainable integrated GRC architecture

As firms struggle to keep up in an ever-changing regulatory environment, Mati Ram, CEO at Dynasec, presents 10 practical techniques that can help organisations to build a sustainable integrated GRC architecture

Organisations today are facing increased risk and regulatory pressures. The risk management, compliance and governance reforms that followed the corporate failures of the past decade have dramatically changed today's business environment. Organisations 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 organisation'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. 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.

To address these issues, organisations have invested in multiple risk and compliance initiatives, with little co-ordination between them. Working in silos causes a substantial amount of duplicated control activities, which results in high cost and inefficiency. The lack of consistent methodology among the multiple GRC initiatives causes a limited visibility at upper management and board levels. Executive management is unable to obtain a comprehensive view of risk and compliance.

## The challenge

In many cases promoting an integrated GRC initiative in organisations requires dealing with the natural scepticism of some of the staff members. Claims that integrated GRC is nice in theory but will not work in practice are common.

In fact, there are many good reasons for this scepticism. To implement an integrated GRC platform, organisations need to find a way to manage the following complexity:

1. Multiple regulations and standards.
2. Various regulators.
3. The differing scope of each regulation and standard.
4. Various concepts.
5. Different reporting due dates.
6. Different workflow for each project.
7. Different data architecture requirements.
8. Diverse participants within the organisation.

The fact that in many cases several consulting firms are involved in the different projects, bringing different methodologies to the table, combined with the natural internal politics within organisations, makes the challenge of building an integrated GRC architecture even more complicated. Besides the professional challenges, there are serious cultural barriers to be considered. Building the architecture is just the first stage of working in an integrated fashion. This architecture cannot be implemented successfully without ensuring

a convenient platform for co-ordination between all the participants.

Another common barrier comes from the world of IT – the existence of information existing in diverse platforms such as MS-Excel files, MS-Word documents, Access databases or other dedicated applications. Managers are afraid of losing the information and time invested in accumulating this information during the migration process to a new architecture and system. Automating the data import of legacy and existing information must be accounted for to overcome this IT barrier.

Due to the complexity mentioned above, most organisations still manage GRC projects in silos, adopting different methodologies and different software point solutions for each project. As a result of this approach, organisations 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 perspective.
- Duplication of activities and overlapping efforts, which increases cost, internal overhead and external consulting expenses.

As Gartner, the IT research and advisory firm, said: "Companies that select individual solutions for each regulatory challenge they face will spend 10 times more on

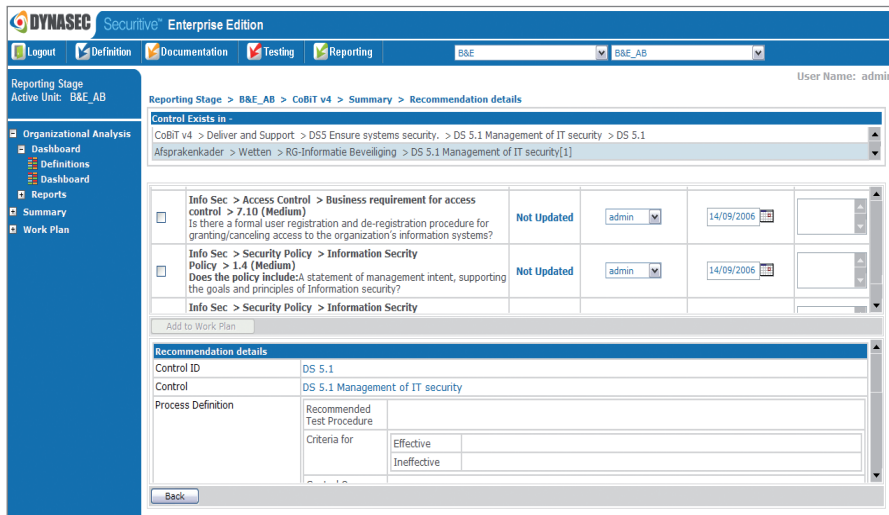


Figure 1: Dynasec Enterprise Software

the IT portion of compliance projects than companies that take on a proactive and more integrated approach.”

### Building an integrated GRC architecture

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

The goal is not only to generate a maintainable and reusable framework, but to ensure, over time, compliance with a list of changing legislative, regulatory, quality and internal control requirements.

Based on our experience in implementing dozens of risk and compliance projects in large and fragmented enterprise organisations, we have applied our accumulated know-how and expertise to design a step-by-step, practical process for building and implementing an integrated GRC architecture.

The process is suitable for any type of organisation but was specifically developed for large enterprises where multiple GRC audit groups and processes were created separately over time, and where

these disparate GRC functions continued to evolve in parallel, with little interaction between them.

One of the critical factors that can determine the success of incorporating a culture of GRC integration in an enterprise is having a high-level, internal sponsor. Besides the functionality and technical obstacles of GRC integration, it can be politically difficult to integrate and foster co-operation between disparate audit functions in the organisation. An internal patron with enough influence can help to overcome the natural internal hardships, objections and frictions that already exist and can be magnified when trying to foster professional GRC collaboration.

The process we have designed for generating an integrated GRC approach is composed of four key phases.

The first phase is perhaps the most crucial one, in which we model the integrated architecture in a structured, 10-step process. We call this step GRC modelling.

The second phase is defining and implementing a pilot for the integrated GRC architecture. We believe that, in almost all cases, the right strategy for long-term success is a bottom-up approach. By this we mean the company should choose initially two, three

or, at most, four parallel audit processes to integrate and focus on a specific subset that is common to the chosen GRC projects.

We have often seen companies decide to implement a high-level, top-down strategy that encompasses mapping the entire organisation and design a comprehensive GRC architecture for most or all of the separate GRC functions. We understand the inclination to plan a comprehensive and long-term strategy. The danger lies in that this high-level top-down strategy can realistically take up to two years to develop, while enterprises today are subject to internal, market and regulatory pressures forcing them to be dynamic and undergo rapid change. By the time the master GRC plan is ready, the organisation and its audit processes have evolved and the strategic architecture designed no longer fits the new organisation.

After selecting the audit projects that will participate in the pilot, we must define the pilot boundaries by agreeing to:

- Define concrete pilot objectives.
- Select a subset of the organisation structure and/or sub-processes while ensuring that both business and IT processes are included.
- Select from one of several scenarios for the GRC integration .
- Define a realistic pilot timeline.
- Designate key participants from each audit process.
- Solicit (if possible) the involvement of the internal, critical sponsor.

After defining and agreeing to the pilot scope, it can begin. The designated pilot players track and/or implement the first phase of GRC modelling on the chosen subset (or scenario) based on the timeline developed.

In phase III, pilot analysis and GRC architecture modification, the pilot participants individually and as a team analyse the pilot results and perform the important, but oft-overlooked, step of modifying the GRC architecture based on the conclusions of the pilot analysis. Each participant separately analyses the pilot results from two perspectives: a) how did the pilot perform

**TABLE 1: MAPPING BUILDING BLOCKS**

	Org. units	Org. processes	Risk	Control	IT system	Loss event	KRI	Audit plan
Sox	•	•	•	•	•	•	•	
CobiT	•			•	•			
Op risk	•	•	•	•	•	•	•	•
Int. Audit	•	•	•	•	•			•

in relation to the ongoing workflow and functionality of the specific auditing group represented by the participant; and b) how did the pilot perform in relation to the overall objective of GRC integration, reducing duplications and redundancies between the selected audit groups and improving the overall GRC efficiency? The entire pilot team reviews all the participant results and then discusses together and agrees to modifications to the GRC architecture.

Phase IV is the final deployment phase of the integrated GRC architecture that was created and improved on in the pilot process throughout the organisation. Phase IV is an ongoing phase that is planned carefully by the enterprise. The company might begin by continuing to focus on the two to four selected GRC processes and expanding the deployment from the pilot subset to a wider scope. Alternatively, the organisation might decide to expand the subset of sub-processes from the initial scope of two to four audit processes to include more such groups.

We have found that, as the deployment proceeds, fewer modifications are required to the overall GRC architecture. Because it was designed with a bottom-up approach, the integrated GRC solution more easily evolves with time and the scope of the implementation widens both vertically and horizontally.

## 10 practical techniques

### 1. Scoping

As stated above, in the scoping phase we define two to four GRC processes, because the basis for the integrated GRC architecture will be built around them.

### 2. Defining building blocks

Each regulatory process is composed of main building blocks such as: organisational units, processes, sub-processes, risks, controls, loss events, IT systems, financial accounts, audit plans and scenarios.

Not all the building blocks are relevant for each regulatory requirement. After defining the building blocks, we need to assign the right building blocks to each GRC process. This mapping will be used later on to define the relations between the building blocks with regards to each risk management or compliance process.

Table 1 above presents a sample matrix mapping building blocks and GRC projects.

### 3. Defining common terminology

Due to the diversification of the GRC methodologies, adopting a common language among all GRC projects is a crucial step to avoid misunderstandings within the organisation.

Often different GRC project managers are using the same terminology for different data information. For example, when the Sox manager refers to “process”, he is referring to a different place in the architecture than the operational risk manager. Co-ordination between these two managers can prove difficult unless they define a mutual, common terminology.

When defining a common terminology, it is recommended to define a common name for each and every data field and to assign each field to one or more relevant GRC projects.

### 4. Ensuring consistent organisational structure

One of the typical mistakes we have seen across many enterprises is the existence of different organisational structures for each GRC process. Variant organisational structures often inadvertently cause mistaken assessments that are based on erroneous risk and control calculations up the organisational tree.

Obviously, a short scoping process is needed to determine which organisational units will participate in each GRC project.

### 5. Correlate processes and units

Because organisational processes usually cross several organisational units, it is important to define which part of the process is performed in each unit. This enables organisations to analyse the information using the organisational structure perspective.

For example, we assume a human resources process creates a residual risk of 10 X.

Company A documents this process with no correlation to the actual organisational units that are running this process.

Company B divided this process into three sub-processes as follows:

	Name	Operating unit	Residual risk
A	Recruitment	Human resources	1X
B	Training	Methods and procedures	8X
C	Payment	Finance	1X
<i>Total</i>			<i>10X</i>

As opposed to company A who has only mapped residual risk to process, company B has the ability to analyse the information both from the process point of view and the organisational structure viewpoint. This can be useful when aggregating all the processes because this method easily highlights the more ‘risky’ organisational units. This technique also enables us to define more

specific and accurate key risk, contextual and performance indicators to leverage existing information for extensive analysis of the data (see point 10 below).

### 6. Enable high-resolution granularity

According to one of the most famous axioms in the GRC industry, a correlation of many-to-many between all the building blocks is required to enable integrated GRC. For example, it is common knowledge that there are many-to-many relationships between risks and controls.

This is indeed necessary, but not quite enough to support an integrated GRC environment. The organisation must be able to define different, distinct attributes for each instance of common risks and controls shared by multiple GRC processes. A common control that occurs in two separate GRC processes might be critically important for one regulation and less important in the other. The ability to define many-to-many granularity at the level of each attribute of each building block is critical for the success of an integrated approach.

Here is a sample that illustrates the need for this granularity:

**Risk:** Purchase-related transactions may not be recorded in a proper period.

This risk has several attributes, such as risk impact, risk likelihood and risk response, and is found in both Sox and operational risk processes.

The qualitative impact of risk when a purchase-related transaction is recorded on say, the January 1, 2008 instead of the correct date of December 31, 2007 is different for Sox and operational risk.

Since Sox is all about financial reporting, most companies would assign the risk impact here as high, while from an operational risk perspective, the fact that this transaction recording was delayed by one day is minor, and the impact would be classified as small.

This sample shows us that, to reduce the amount of risks being managed, each attribute of the risk should be assigned a different value in relation to other dimensions

such as GRC project, organisational process and organisational unit. This requires a high level of granularity in the database.

Companies that select a GRC system that cannot support many-to-many relations at the level of attributes will be forced to choose from one of the following bad options to overcome this limitation: either they will have to document the same risk again and again to assign the accurate attribute value for each project, process or organisational unit, or they will define this risk only once with constant attributes in a way that does not reflect the situation in practice or allow for accurate analysis and remediation.

### 7. Designing control hierarchy

To reduce the duplication of controls between separate compliance procedures, the organisation needs tools to define control dependencies intelligently.

Sometimes, a high level control in a regulation might be identical to a combination of five controls in another standard. The ability to define such smart links and multi-level hierarchies between risks, controls and GRC projects is vital to reducing the overheads of managing and testing controls across the enterprise.

For example, a detailed control objective of CobiT is ensuring network security, which is a fairly high-level objective. To ensure that this high-level objective is met in the organisation, a number of lower-level controls must be tested, most likely based on IT Security standard ISO27001. Each of the lower level ISO27001 controls might be effective or ineffective, and indicate whether the CobiT objective is met. The system should enable smart correlations of n-level hierarchy to support this capability.

### 8. Assigning roles and responsibilities

To enable and facilitate coordination between GRC participants, there is a clear need to define the rights to view, update and modify shared information.

### 9. Defining alerts and notifications

To enhance corporate internal communication, it is imperative to automate alerts and notification techniques.

Typical triggers for sending alerts and notifications are:

- organisational change;
- process change;
- redesign of shared control;
- new risk;
- successful implementation of remediation task; and
- change of process owner.

### 10. Leveraging correlative information between the GRC projects

Each GRC unit has its own individual workflow that might consist of periodic control testing, conducting multi-year audit plans or accumulating loss events. To achieve an overall organisational risk view, information must be shared between the different processes.

For example, the internal audit team should receive status of control tests for determining the frequency of audit plans by topic. Loss event information collected by the operational risk group should be shared with other GRC functions.

### Summary

The process of building the integrated GRC architecture as described in this article can help organisations improve the quality of risk and compliance information, prevent duplicated activities, decrease costs and create a long-term framework for existing and future regulatory and risk management needs.



As a risk and IT professional, Mati has personally experienced the difficulties of traditional solutions for managing risk and compliance processes and founded Dynasec to offer the GRC market a state-of-the-art software solution.