

M a n a g i n g
B u s i n e s s
P e r f o r m a n c e
t h r o u g h
g o v e r n a n c e , r i s k
a n d c o m p l i a n c e



Written by: John Conaghan • Managing Director, Securac Europe • john.conaghan@riskgovernance.com



Introduction

The mere mention of Governance, Risk and Compliance (GRC) is likely to glaze the eyes of many a senior executive in today's corporate world – for others it will serve as a timely prompt to check that they didn't forget to send their lawyer a birthday card. Although the importance of GRC is well recognised, it is usually thought of as an unwelcome cost to the business and something that often 'gets in the way of delivering the results'. Sadly, in many cases it does, but this needn't be so. Indeed, we argue that the appropriate attention to Governance, Risk and Compliance is essential to maximise business performance results. It's been said before but...

good management = good risk management.

As sure as death and taxes, GRC is now an item that has to be taken very seriously. Whether it is Sarbanes-Oxley, the Combined Code in the UK, HIPAA, Basel II, industry-specific regulators, or simply shareholder pressure, companies and their officers need to turn these elements into strategic and economic value.

No-one is advocating eliminating risk altogether. That would be akin to throwing the baby out with the bath water. After all, risk creates opportunity; opportunity creates value and wealth. Responsible management of risk is key to unlocking business value and creating wealth for shareholders.

The important thing is to turn GRC into a value-generation activity. The potential for this is tremendous and absolutely dwarves the benefits that can be derived from other management techniques such as balanced scorecard and management by objectives.

Most popular performance management techniques are backwards looking. In other words, they compare historic results against targets and objectives. Although this is a commendable thing to do, because you can learn from mistakes and continuously improve your business performance, isn't it better to focus attention on activities that will positively influence the results?

Business performance is eroded by a series of events that contrive to diminish your corporate effectiveness: your top sales team is recruited by your competitor; your new product line is six months late; there's a sustained hike in global energy pricing; your core market is disrupted by a new technology appearance.

All of these events are material threats to your business. In today's world, every corporate officer has a duty to consider all material threats to their business and put in place controls and actions to mitigate those risks; and to ensure that there is an embedded, sustainable process for identifying, assessing and managing risk. This is what good Enterprise Risk Management is all about.

One of the difficult challenges is to introduce the right sort of culture, the right sort of systems and processes to make sure that your GRC efforts do not 'get in the way of delivering the results'. Simply loading additional reporting bureaucracy on already busy people will have the opposite effect to the desired one. Finding a way to gain enthusiastic and painless participation in the process is the key to unlocking the benefits and value that are there to be realised.

Executed properly, an embedded GRC process will give early warnings of risks and will minimise the impact of any that materialise – keeping business performance levels high.



Steps towards value from GRC

GRC spend has rocketed in recent years; fuelled by events and corporate disasters such as 9/11, Enron and a whole catalogue of others. Sarbanes-Oxley, Basel II, The Combined Code...etc have created a consulting industry feeding-frenzy not seen since the days of Y2k. The leading companies in the US are spending a minimum of \$3m to address their Sarbox initial filing requirements with many spending as much as \$10m.

This level of spending on consulting fees is not sustainable. Companies must seek to embed the right sort of culture, systems and processes to ensure that governance and risk management are part of the fabric of the organisation. In other words, take the output from the consulting phase of work and encapsulate it within a flexible system (most likely software) that will introduce a standard vocabulary and method for identifying and managing risk within a performance management framework.

In broad terms, there are a number of steps that an organisation must take to ensure that they are getting business value out of their GRC efforts. They include:

- ✔ Ensuring that there's a coherent set of business objectives that permeate throughout the business;
- ✔ Ensuring that all material assets, physical or non-physical are identified and their value is understood;
- ✔ With objectives and assets as the focal point, identify material threats and vulnerabilities (i.e. risks) that could interfere with your ability to protect those assets or meet those objectives;
- ✔ Involve risk owners (as well as risk experts) in the process by approaching the subject from their perspective – in other words from a business objectives perspective;
- ✔ Adopt a 'light touch' to the risk assessment piece. Serious risks can be isolated for more detailed analysis, but unless they're identified properly in the first place, you won't even know that many of them exist;
- ✔ Seek to embed a risk-aware culture throughout the organisation. Provide accessible help through on-line knowledge and policy information in order to raise the average level of risk-competence;
- ✔ Over time, develop localised Loss Expectancy information that will inform future predictions and continuously improve the accuracy of reporting;
- ✔ Manage compliance issues in the same way as other risks. Compliance breaches after all represent a risk to the business;
- ✔ Ensure that there are clear and unambiguous lines of responsibility and communication around objectives, risks, controls, compliance and governance issues;
- ✔ Set thresholds for early warnings and for escalation of issues up the management hierarchy;
- ✔ Avoid deluging people with information. Seek out the key reporting items and present them intuitively and graphically – a picture tells a thousand words.

Realisable Benefits from GRC

The list of benefits below relates to benefits that can be realised from the introduction of sound governance and risk management processes and is drawn from a list compiled by the Institute of Chartered Accountants of England & Wales (ICAEW). These have been echoed by almost every professional body since the late 1990s. They include:

- ✓ greater likelihood of achieving objectives;
- ✓ higher share price over the long-term;
- ✓ greater likelihood of successful change initiatives;
- ✓ lower cost of capital;
- ✓ early mover into new business areas;
- ✓ reduced insurance premiums;
- ✓ reduction in cost of remedial work and firefighting;
- ✓ achievement of competitive advantage;
- ✓ less business interruption;
- ✓ achievement of compliance/regulatory targets.

These benefits go to the very heart of business performance. Can you imagine the impact it would have on your business if even only two or three of these benefits were realised?

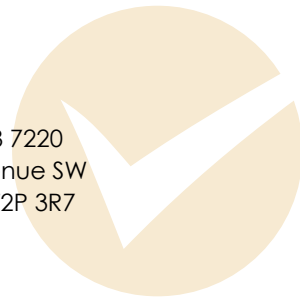
Earlier we listed the steps necessary to gain value from your GRC efforts. Some of these steps are discussed in more detail below and we draw upon considerable experience in the design and deployment of GRC solutions for Global 1000 companies in outlining these steps. If you would like to understand how such a process could be started or improved within your own environment or, if you would like to understand what the costs and financial payback could be from implementing a world-class GRC solution, then we would be delighted to share our expertise with you. You may contact us as follows:

Securac (Europe) Limited
Surrey House
34 Eden Street
Kingston-upon-Thames
Surrey KT1 1ER
United Kingdom

t: +44 (0)208 481 3883
f: +44 (0)208 481 3884
e: jconaghan@securac.net

Securac Inc.
2500, 520 – 5th Avenue S.W.
Calgary, Alberta
T2P 1V6
CANADA

t: +1 403 225 0403
toll free: 1. 877. 328 7220
2500, 520 - 5th Avenue SW
Calgary, Alberta T2P 3R7



Setting and Managing Objectives

An organisation's activities are usually guided by its desire to achieve a number of strategic objectives – hopefully within the parameters of legal and regulatory restrictions! These objectives are often publicly announced or re-enforced through the company's annual report, and will deal with issues such as shareholder value, contribution to global and local communities, innovation, environmental husbandry, and employee welfare. Enlightened organisations will ensure that the corporate level objectives drive the goals and activities of other parts of the business; down through divisions, country locations, individual departments and even down to project or personal objective setting. Sadly, it has been our experience that such 'joined-up' companies are hard to find and it is commonplace to find objectives in one part of an organisation that actually work against the corporate goals.

Organisations have varying levels of sophistication when it comes to implementing methods to achieve their desired and committed business objectives. Some organisations will have comprehensive regimes established for setting and then monitoring performance against business objectives; whilst others will barely consider what their objectives are from one year to the next.

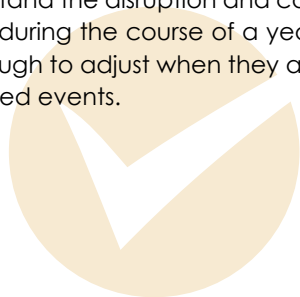
Some organisations will diligently go through an annual 3- or 5-year rolling planning process but then fail to ensure that the updated targets or objectives are mirrored in the activities from the top to the bottom of the organisation. Even the best of companies, who clearly define and communicate their overall objectives, and who ensure that all parts of the machine are contributing to the achievement of those objectives, will often under-perform because they failed to understand the disruption and cost of events that confront them during the course of a year; or they will not be flexible enough to adjust when they are confronted by such unexpected events.

Dealing with the Unexpected

Too often, the Business Plan, which may have consumed months of the top executives' time to produce, will lie undisturbed in a locked filing cabinet until it is time to repeat the planning cycle 12-months later. If a company spends expensive executive time to set out a realistic set of business goals, and then makes a commitment to their staff and shareholders to pursue those goals, then it is surely their duty to (i) diligently manage towards them, (ii) track performance against them and (iii) plan ahead to ensure that expected or unexpected obstacles can be safely navigated with the minimum of disruption. If they are confronted by a threat or risk, expected or unexpected, they should react in unison and in a controlled way.



Everyone can probably visualise a shoal of fish swimming along in quite stunning co-ordination. Each member of the shoal seemingly understands the purpose and direction of the group and, collectively, they behave as one. When risk is sensed or identified, the shoal reacts immediately and in unison and, in so doing, minimises the impact of the risk whilst protecting its safe existence. Like the shoal of fish, we need to get our organisations to the point where they understand precisely the risks and vulnerabilities that threaten them, such that, when the inevitable does happen, they react quickly and cohesively, and don't fall apart through chaotic, random behaviour. Once sensible business plans have been made and the necessary resources have been correctly applied, risk, and our reaction to it, remains the biggest obstacle to achieving our business performance objectives.



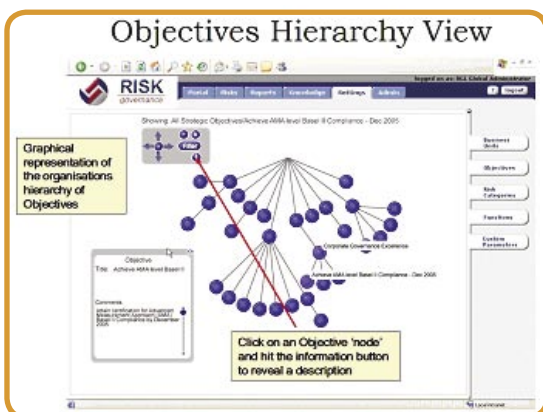
Harmonised Objectives

As suggested above, one of the first jobs we must do if we're to turn GRC into a force-for-good is to create a set of harmonised business objectives, starting from the very top of the organisation. At each level down from the Group Headquarters, we need to articulate what the objectives are for the entity at this level. They will likely be different from those at the level above but one would hope that they are at least making a contribution to the greater corporate goal and that there is a fairly obvious mapping from the corporate objective down to objectives at the lower level.

Eventually, we will be able to draw a hierarchical map of business objectives. From the strategic, high-level corporate ones right the way down through the organisation to the furniture re-fit project in the sales demonstration area of the Melbourne office. If we cannot make such a link between a lower-level objective and its higher-level precedents – then just maybe we shouldn't be considering that objective at all.

Now that we have identified the objectives that will drive our core activity we have the perfect perspective from which to start identifying risks. What are the things that will likely threaten my ability to achieve this objective?

This question also resonates better with the people that we need to involve in the process – the risk owners. Ask this same group of people to attend a risk identification workshop and all of a sudden that 4-hour car trip to your most difficult customer starts to sound attractive!

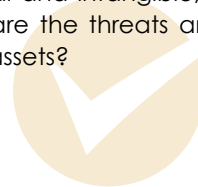


Asset Identification

Another key area of consideration when implementing a framework for good GRC practice is to identify all material assets owned or under the control of the business. These assets might be physical things e.g. a nuclear reactor or a back-up generator or they might be less tangible assets such as a license to trade or a brand value. Either way, the asset has a value to the business and, if it were a material asset, its loss would cause us financial, reputational or other types of problems. Many companies do a very thorough job of tracking and protecting their physical assets. The same cannot be said for the less-tangible assets. A certain large audit firm allowed a scandal with one of its clients, involving only a handful of Partners, to destroy the reputation of what, to that point, was one of the world's most successful audit firms. The speed with which the meltdown occurred was frightening and much of the damage could have been prevented had they had better controls and effective mitigation strategies to deal with such reputational threats.

On the other hand, a world-leading airline consistently acts with military precision in the event of one of their aircraft being involved in a disaster. The Director of Risk for the airline said, "We know exactly what will happen to our share price in the event of a disaster. It will fall quickly by up to 15% but within 10 days it will stabilise at a level higher than it was before the disaster. It's because we react quickly and with the right messages and are seen to be doing the right things. People take confidence from that and they realise that there are no systemic problems." I'm not sure however, that I'd like to be in the air just as the CEO of the airline needs a couple of points on the share price to meet the annual target!

Once again, having identified the key assets, both physical and intangible, we might now ask the question; What are the threats and vulnerabilities associated with those assets?



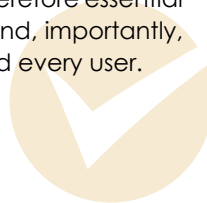
Risk Identification and Assessment

Here we are at the detailed grind part of the exercise, but heh! There's a difference. Whereas before I used to get twice yearly, or yearly questionnaires asking me what controls I was affected by and what risks I was using the controls to manage. Someone is now saying to me, "These are your objectives (or assets); tell me the things that can materially hurt your efforts to achieve your objectives." So the whole exercise has taken on a performance-centric approach. I articulate the objectives for my area; I, with the help of my team, determine what the material risks and threats are; and with the help of the risk practitioners, we will choose, develop or modify controls to make sure that we're successful. If we're still not happy, we'll identify further actions that will improve the strength of the control even further and help me make my targets. Now the dog's properly wagging the tail and playing havoc with the competitors' cats.

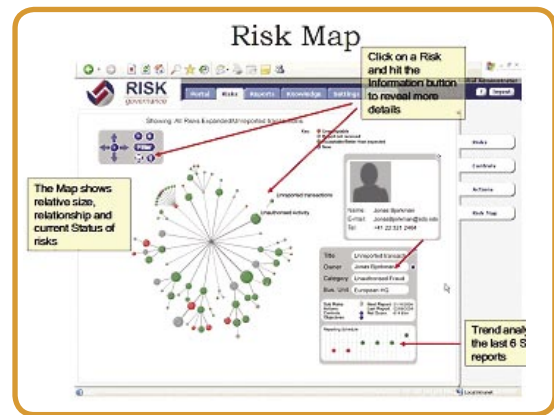
Recent Government and professional body edicts have, in essence, said that risk management has to become part of the very fabric of the organisation in order for it to become compliant. The challenge is to encourage the enthusiastic participation of risk owners (i.e. business executives and managers) in the process of risk management. In short, move the issue out of the minds of the few, into the hands of the many.

Tools are available now that will let risk owners (who after all are not risk experts) make a good and off times accurate guess at the financial impact and probability of a particular risk. Simple point and click scoring grids, and status reporting with on-screen expert guidance can make the job fast and accurate.

By necessity, these tools need to be deployed widely; to risk owners [possibly hundreds or thousands] in addition to risk experts [most likely a few dozen]. It is therefore essential that they are attractive and easy to use and, importantly, give back considerable value to each and every user.



Risk professionals can drill down further into individual risks and do far more detailed assessments, and various different analyses as they see fit. The results of these more detailed assessments, often using a geo-industry specific set of annual loss estimates as a baseline for the predictions, can then be reviewed with the risk and/or control owner before agreeing to update the risk score.



Compliance Issues

Guess what! My compliance issues have largely been addressed through the exercises above. If I'm operating in a highly regulated industry then falling foul of the rules is a risk that I have to manage, just like any other risk. If the consequence of falling foul of a particular regulator's rule is likely to be material, then it should have been identified in the Risk Identification phase and there should have been controls and actions identified to make sure that breach of this regulation could not adversely affect my objectives.

What's more, if I can allow my regulator a controlled view into my GRC platform then I can make their job easier and run the chance of winning serious credit with regulators – which may even get me some competitive edge.

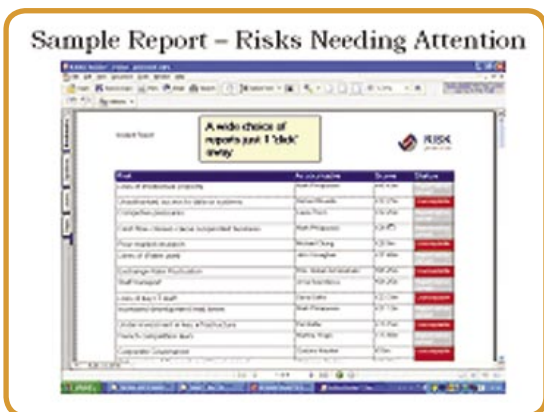
Systems for managing risk can be furnished with compliance-specific modules that will address issues such as Basel II, BS7799, ISO17799, HIPAA, and Sarbanes-Oxley for example.



Clear Communication

Now that we have mapped out our objectives and our assets (both physical and intangible) and we've identified risks and controls, it's not a bad idea to share the information with people. Naturally, objectives should be described in such a way that they are measurable and time-limited e.g. "Increase market share of Product X by 2% before the end of 2005". There should be no doubt as to what the objective means and how performance against the objective will be measured. It should also be absolutely clear as to who is responsible for the achievement of the objective or the safekeeping of the assets. These objectives and assets should have an 'owner'. Yes, they may affect or be used by many people but there has to be one person in each case who is accountable/responsible.

We've also identified the risks that threaten those objectives and we've identified the controls and actions that we will use to mitigate the risks. All these items too must have a single owner (risks, controls and actions). These owners will be responsible for maintaining the reporting regime for the risks, controls and actions that they own. If they believe a control is breaking down which will make their risk more likely to materialise then they must change the risk impact/probability score. If someone else is the owner of the control in question, they will be forced to react to the criticism and either allay the fears or improve the operation of the control to keep the risk owners happy.



Governance and Reporting

Good governance not only has to be done, it has to be seen to be done. Diligent organisations will publish policies and procedures that act as a help to the risk owners in identifying, assessing and managing their risks. Policies, procedures, knowledge bases, loss histories will all give a risk owner a strong starting point in trying to determine the likely impact of a risk. Importantly, creating powerful assets such as knowledge and policies around risk management will help to raise the average level of competence in managing risk and will embed a standard vocabulary, culture and ethos around risk that will only benefit decision-making and risk-taking.

Now that we have created a risk-intelligent organisation we have a comprehensive set of rather complex information sitting in our databases. We have risks, some of which are related in a parent-child hierarchy; we have controls, some of which are being used to manage many risks; we have a hierarchical map of business objectives; and we have people and assets that are attached to different parts of the organisational hierarchy. Making sense of all that data in such a way that consistent levels of governance can be achieved is not easy.

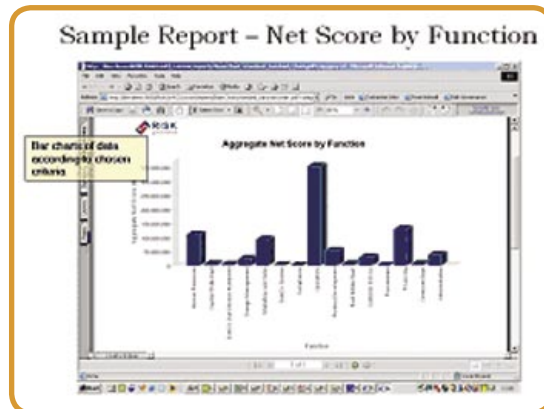
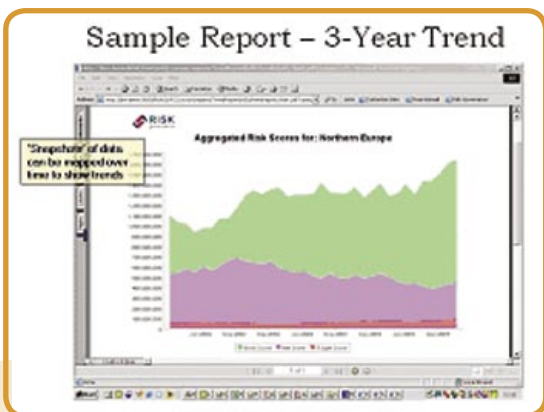
Information needs to be reported using different cuts. For instance: show me all the risks affecting this particular objective; or show me all this business unit's risks; or show me all George Bennett's risks; show me all the risks that this control is helping to manage.

With such large quantities of information, and the number of links between the information, producing conventional list reports is never going to do justice to the information. Ideally, information will be able to be represented graphically and coded to depict vast quantities of facts in a seemingly simple format.



The Portal shown above is a simple way of presenting a number of different GRC-related pieces of information in a way that suits a particular user. These 'portlet' panes of information can include information from other sources e.g. an RSS News Feed or a portlet window from the organisation's ERP system. Indeed, if the organisation already has a Portal Engine such as IBM's Portal Server or SAP's NetWeaver, then individual panes of GRC-related information can be incorporated into the preferred corporate portal.

Another important capability would be to see how Risk is being managed over time. Plotting performance over a one, two, three or even ten-year period will be a valuable tool in the continuous battle for business performance improvement.



In Summary

Governance, Risk and Compliance (GRC) are issues that are here to stay. Paying them lip service or, worse still, ignoring them altogether is both bad judgement and poor management in the extreme; that could easily lead to lengthy jail sentences. The costs associated with introducing new GRC-related systems and practices can be repaid many times over if they are implemented strategically.

It's possible to start a process of performance-driven, GRC excellence in small, incremental steps. Securac, with its Acertus suite of Governance, Risk and Compliance offerings has all the pieces of the jigsaw and is perfectly equipped to partner with you on this challenge. We would welcome the opportunity to discuss your situation in more detail and share with you our experience and expertise in delivering GRC value to the world's leading companies.

About Securac Inc.

Securac is a leading global provider of enterprise governance, risk and compliance (GRC) management software and services for the public sector, financial institutions, and the Global 2000 companies. The Company has developed risk management and compliance solutions designed to enable organizations to identify, measure and manage information and physical risks, and to assess their compliance with expanding regulatory requirements and against "best practices" standards. The demand for Securac's integrated software products has been more recently spurred by the unprecedented additional compliance requirements of the Sarbanes-Oxley Act of 2002 on all publicly-owned U.S. companies.

Acertus™, Securac's integrated software platform addresses immediate, ongoing and strategic GRC needs with a process-driven approach that offers a clear roadmap to business performance and operational risk management. In addition, Acertus™ also allows its corporate users to determine compliance against national and international business practice standards including ISO17799, BS7799, HIPAA, Privacy Acts, CT-PAT, Sarbanes-Oxley and the Basel Accord.

Securac (Europe) Limited
Surrey House
34 Eden Street
Kingston-upon-Thames
Surrey KT1 1ER
United Kingdom

t: +44 (0)208 481 3883
f: +44 (0)208 481 3884
e: jconaghan@securac.net

Securac Inc.
2500, 520 – 5th Avenue S.W.
Calgary, Alberta
T2P 1V6
CANADA

t: +1 403 225 0403
toll free: 1. 877. 328 7220
2500, 520 - 5th Avenue SW
Calgary, Alberta T2P 3R7



About the Author

John Conaghan is a founder of Risk Governance Limited and a serial entrepreneur with a string of successful start-ups since the mid-1980s.

After a successful career in sales, involving director-level roles in Europe and North America, John was involved in a LAN-technology start-up on the UK's now famous Cambridge Science Park. In 1990 John created one of Lotus' premiere consulting firms, Ives & Company, and pioneered the development of CRM applications using Lotus Notes. This led to the creation of the world's most successful Lotus Notes tools developer, TeamStudio Inc, with offices in Europe, Asia and North America.

In 1993 John joined Lotus Consulting with responsibilities for a large European territory. As Managing Director, he sold and led high-impact consulting projects for some of Europe's largest corporate clients including Lloyd's of London, Svenska Handelsbanken, BP and ICI.

John, with his partner, created two further successful businesses in the 1990's including a business-led, web technology consulting firm and a highly acclaimed, innovative healthcare company. Following well publicized corporate scandals, John turned his attention in the year 2000 to the combined issues of corporate governance and enterprise risk management.

Following the acquisition of Risk Governance by Securac Inc., John is a key member of the new European operation.