Straight Talk Book No. 8

Growing confidence

(The smart way to manage governance, risk, and compliance)

As is the gardener,
so is the garden.

Straight Talk Book No. 8

Growing confidence

(The smart way to manage
governance, risk, and compliance)

Orchid
(Phalaenopsis)

Contents

Venus Flytrap
(Dionaea muscipula)

“I never saw it coming”

Have you ever wondered why so many companies are unprepared for the barrage of risks they’re facing these days? Or why otherwise capable leaders often get caught looking the wrong way when big opportunities come along?

Threats are everywhere. From meltdowns in the mortgage industry and lead paint in toys to foreign corruption and willful wrongdoing by executives. Opportunities are just as diverse. Disruptive innovation, new market openings, competitor missteps. If you can imagine it – and even if you can’t – it could happen.

Fortunately, organizations no longer have to live at the mercy of unforeseen events. The solutions needed to take control of risk have finally matured to the point where becoming a risk-intelligent enterprise – one that takes risks by design and not by default – is well within reach.

The payoff? Better decisions, improved performance, greater confidence, and increased value.

Apple
(Malus domestica)

Orange
(Citrus sinensis)

Apples and oranges?

This book is both a call to action and an action plan. It's about taking better control of literally thousands of governance, risk management, and compliance activities that companies struggle with every day.

It might be tempting to think that these activities are really different from one another, like apples and oranges. But that would be a mistake. They are fundamentally interconnected, each driven by and dependent on the exact same processes, people, and data. By getting them under control, you'll have access to the reliable information you need to make more confident decisions and manage risks more effectively.

Cactus
(Echinocactus grusonii)

Ouch!

Few companies have a good handle on the wide range of policies and processes that are intended to manage risk and compliance. That's because they approach the functions separately, tacking them *on top* of the business rather than embedding them *into* the business.

The result is a prickly tangle of controls and practices buried inside functional or geographic silos with hundreds – or even thousands – of isolated activities. This approach creates bewildering complexity and duplication, even as it leaves major gaps uncovered and fails to deliver the desired results.

A manager can get requests from compliance one day and from internal auditors, legal counsel, or regulators the next – each seeking essentially the same information in slightly different forms. And if that weren't bad enough, leaders still don't have a sufficiently clear view of risks. They can't see the faint warning signals of problems on the horizon, and they can't respond as quickly as they should to opportunities.

Your current approach might *look* orderly from a distance, but when you get up close, you may be facing some thorny challenges. Confusion across business units, functions, and geographies can lead to big inefficiencies – and even bigger risks to the enterprise.

Bottom line? A fragmented approach is expensive – and still doesn't work very well.

The squeeze is on

After collectively spending billions on compliance activities over the years, many companies are suffering from "compliance fatigue." And though it's tempting to just leave it all behind, that's probably not a good idea.

In fact, many companies are looking at *increasing* demands for compliance, especially if they're extending operations into new markets around the world.

Sarbanes-Oxley was just the start. It triggered a massive effort to improve the quality of financial reporting, and for many organizations, it is working. Financial restatement rates have started to decline, and financial reporting risk has decreased for many.

Yet some executives still feel they're in the dark when it comes to non-financial information and risks. Many have little understanding of what they currently spend in all these separate areas – let alone how they all roll up together. It's no wonder scandals continue to erupt, with executives often blindsided by bad news.

Lemon
(Citrus limon)

The squeeze is on

After collectively spending billions on compliance activities over the years, many companies are suffering from "compliance fatigue." And though it's tempting to just leave it all behind, that's probably not a good idea.

In fact, many companies are looking at *increasing* demands for compliance, especially if they're extending operations into new markets around the world.

Sarbanes-Oxley was just the start. It triggered a massive effort to improve the quality of financial reporting, and for many organizations, it is working. Financial restatement rates have started to decline, and financial reporting risk has decreased for many.

Yet some executives still feel they're in the dark when it comes to non-financial information and risks. Many have little understanding of what they currently spend in all these separate areas – let alone how they all roll up together. It's no wonder scandals continue to erupt, with executives often blindsided by bad news.

Making lemonade

Every company has to invest resources in governance, risk management, and compliance – *GRC* for short. That's a fact of life. So why not do it in a way that creates more value and a bigger payoff?

An integrated approach to GRC can give even the most complex organizations the power of discipline and the benefits of efficiency:

- Core processes that flow smoothly across organizational boundaries
- An integrated technology platform for controls, risk monitoring, and performance management
- A consistent risk framework throughout the organization
- Improved awareness and understanding of risk at all levels
- An ethical culture

With integrated GRC, different functions rely on the same core information, technology, and processes. The same set of rules guides all risk management activities. Everyone gets timely access to the information they need in the right format to help make better decisions. And the whole system is buttressed by a culture that values good corporate behavior and rewards people for doing the right thing.

What's your story?

There's no shortage of reasons companies use to avoid the obvious improvement opportunities that come from integrated GRC. How many of these sound familiar to you?

- This is a long-term problem in a short-term world
- No one owns it
- We're not really spending that much
- We couldn't *begin* to tackle this
- It works better when things bubble up from the bottom
- The technology isn't mature – and it costs too much
- I'll worry when there's a crisis
- Change? We're too busy putting out fires

These excuses might have made sense back when there was less scrutiny and lower stakes. Back when executives and board members had little personal risk. But that was then, and times have definitely changed.

What to expect from an integrated approach to GRC

Sustainable cost reductions
Improved risk management
Quicker response opportunities
More shareholder confidence

More value

Nine ways you can start taking action today

1. Take the long view
2. Don’t delegate this one
3. Make the business case
4. Start where you are
5. Getting ahead of risk
6. Work from the top
7. Overcoming inertia
8. Automate
9. Get to the heart of the matter

Now that you know what you don’t know

Chinese Privet
(Ligustrum Sinensis)

Take the long view

Your fragmented approach to governance, risk management, and compliance wasn't designed with a master plan in mind. It evolved over time, driven by practical needs in reaction to ever-changing requirements. Things are going to keep evolving too, and the pace at which threats and opportunities emerge will only increase.

- Companies operating in multiple countries or with complex global supply chains face growing risk and compliance challenges every year.
- Employment regulations pose new risks, especially with workforces scattered around the world.
- Outsourcing and offshoring bring special threats because they cut across cultures as well as borders.
- Advanced technologies give individuals unprecedented power, including the power to misbehave.
- Regulators not only want to know what you're doing, they want to know *how* you're doing it – and why. Documentation matters.
- Customers, communities, and even investors have higher expectations for corporate responsibility.

All of this means that you can't expect to achieve GRC nirvana overnight. An integrated, risk-intelligent approach requires a long-term focus and investment in underlying infrastructure.

First things
Recognize the new realities around you.
Champion the wisdom of doing things better.

A CEO's options for handling GRC

	Pros	Cons
Ignore it	No investment or action required	Unacceptable risk Problems don't go away, but get steadily worse
Delegate it	It's not much fun Somebody else could do a decent job You have more important things to do	Only the CEO has the clout to make GRC integration real Fragmented leadership can drive incremental improvements, but the overall piecemeal approach remains When things blow up, it's still your problem
Take charge	Reduced costs, improved performance Improved quality and efficiency through integration and standardization Reduced risk Increased board confidence	Requires an upfront investment of time, money, and resources – and personal involvement from the top

Don't delegate this one

You've heard the adage "When everyone's responsible, no one's responsible." Well, that's especially true here. Until you have a sustainable framework in place, getting ahead of the GRC challenge will have to be CEO-driven.

- GRC cuts across every operational area of a business. Expect turf battles in the overlaps. Expect to find holes where ownership needs to be assigned. Be prepared to mandate an enterprise perspective. And don't buy it when people say, "We already have this handled."
- Unless the CEO signals the importance of an integrated enterprise approach, it won't happen. "Tone at the top" is a prerequisite, but hands-on leadership is even more critical.
- Only the CEO can engage the board. As board members confront the reality of their personal exposure and risk, they need to know exactly how the company is approaching GRC integration.

One more thing. Don't spend a lot of time worrying about lines and boxes on your org chart. That's not what matters most. Effective GRC is about the knowledge, information, and tools to do the right things – not about fine-tuning organizational structures.

First things
Make it clear that you don't intend to wait for a major crisis to improve how your organization manages governance, risk management, and compliance.

The narrow view	The bigger picture
GRC is about policy.	GRC is about people and behavior.
If legal says it's okay, it's okay.	Just because something adheres to the law doesn't mean there's no risk.
The main role of IT is to automate transactions.	IT delivers information that leads to insight and good decisions. Automation helps.
GRC is just about tone at the top.	Integrated GRC runs deep.
Controllable risks are the only risks worth worrying about.	You can't prevent uncontrollable risks, but you can control the damage.
GRC might discourage people from taking necessary risks.	GRC allows businesses to take *intelligent* risks and still keep control.
GRC is a fad.	Good governance and compliance are here to stay.
Boards get involved and cause problems.	Boards don't get involved – and cause bigger problems.
We're private. GRC doesn't apply.	Any company can lose value or tarnish its reputation.
Excellent GRC = Expensive GRC.	Streamlining GRC improves effectiveness and cuts costs.

Make the business case

With GRC – as with anything – return on investment matters. But you have to make sure you're looking at the whole picture, not just "check-the-box" compliance.

And don't limit your thinking to how a project will reduce costs in one particular silo. Scale is at play here. To motivate change, you'll need a broad business case that considers overall cost reductions as well as specific operational improvements.

Better GRC improves culture, performance, and value. It enables business agility by allowing companies to assess problems quickly – before they become crises – and to respond rapidly to market opportunities. It also allows you to redeploy talent to focus on risk management, not just traditional compliance.

Getting a reliable cost baseline will be hard. Most managers understand only the most readily apparent costs. Embedded costs are tricky to recognize. But until you see the whole picture, you won't have the information you need to make a smart decision about investing.

First things
Focus on specific changes that can drive performance improvements. Look closer, look deeper. The benefits are there.

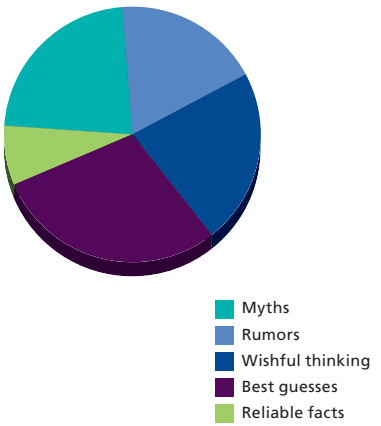
Start where you are

Knowing what you're currently spending on governance, risk management, and compliance is a critical first step – to be quickly followed with an understanding of what you're getting in return. That knowledge is essential in building the business case for change.

Know how you're allocating capital – both financial and human. Get a clear picture of the amount of time spent by senior executives on compliance busy work that could be better done using automation.

Find out what you're losing, too. What fines, reputation costs, and other liabilities can be traced to your fragmented approach to risk management and compliance?

What does your leadership team *really* know about GRC costs?



First things
Kick off the assessment. Don't strive for perfection – just get an initial look at what's getting done and who's responsible.

Getting ahead of risk

Early detection is a big deal in GRC. But accurate predictions are even better. And they require mapping risks to uncover interdependencies between things that at first blush seem unrelated. For example, risk-mapping can show how risks related to employee privacy affect areas such as information technology, legal, and operations.

Smart companies define clear lines of authority for managing different types of risk. This helps decision-makers understand threats associated with each major risk – and choose the most effective risk management strategy.

Seeking. Intelligently pursuing risks with significant upside – strategic initiatives such as new markets, new products, mergers, and acquisitions.

Avoiding or transferring. Choosing to avoid the risk entirely or to take a hedging strategy.

Accepting. Consciously deciding not to take action – accepting the risk as is, with eyes wide open.

Managing. Using GRC principles to take an integrated approach. This involves clearly defining responsibilities, monitoring procedures, and tracking key performance indicators and triggers.

First things
Put someone in charge of finding the best ideas for risk management in your organization. Use them to create an internal education blueprint.

Sunflower
(Helianthus annuus)

Work from the top

Business people like to debate whether certain things should be top-down or bottom-up. When it comes to GRC, there's not much room for discussion. If you don't start at the top, you won't get anywhere worth going.

An integrated approach starts with business strategy and moves steadily toward the front lines of the organization. Along the way, risks get prioritized in terms of impact and probability. Focus first on areas where exposure is high, and build your strategy to make sure those risks are effectively managed.

In some high-risk areas, you'll want to take extra care. These critical areas may call for specialized processes and systems that provide deep protection and real-time alerts to potential problems. In other risk areas, the bare minimum may be appropriate. Do what's required, and nothing more.

Companies that approach GRC from the bottom up, or try to provide a high degree of coverage in every area, end up drowning in details or wasting time on investments that don't really pay off.

First things
Get consensus on the three largest GRC issues you're facing, and put them at the top of your to-do list.

Here's a sample e-mail you can use to get the ball rolling.

From: John
To: Leadership team
Subject: GRC initiative

We're moving forward with our plan to integrate our governance, risk management, and compliance processes. We have two goals: reduce costs and improve performance.

I already have the results of the recent risk assessment completed by internal audit, but I'd like you independently to list the top three risks in your area – the risks that are causing you the greatest concern.

Use this chart to keep your feedback focused. Please return it to me by 5 pm next Monday.

Area of risk	Describe the monitoring or compliance processes related to this risk

Overcoming inertia

Imagine your organization as a well-oiled machine. Your processes and systems are purring along, helping you prevent, detect, and correct activities happening outside established boundaries of acceptable conduct. Policies and procedures are congruent, execution is consistent. Performance, risk management, and compliance are integrated, embedded, and managed seamlessly.

Sounds pretty great, right? Maybe so, but getting there is tough. It requires overcoming the dead weight of inertia. People like their silos and their spreadsheets. Many are not interested in integration, standardization, or automation if it takes them out of their comfort zones. And they don't care about enterprise benefits if they only see costs in their silos.

The key to overcoming inertia is to focus on value creation. You have to make the case that integrated GRC creates competitive advantage. You have to explain how it will help attract and retain the best talent.

Remember, integrating GRC is not something you have to do. It is not a legal or regulatory requirement. It is something companies choose to do because it makes good business sense.

Some organizations need a catastrophic event before real change is possible. That particular form of motivation may well cost more than you want to spend.

First things
Clarify reasons for change.
Clearly communicate the vision.

Automate

It's impossible to have an effective GRC program without the right information technology. And the hard truth is, your current IT assets may not be well-aligned with today's needs.

It's time to address that gap – and there's good news. Fresh ideas about "services thinking" and services-oriented architecture make operational improvements possible without having to invest in large-scale changes to your current enterprise technology.

But no matter what technology you use, the priority should be improving visibility – so business leaders have early warning signals and can address problems before they become crises. That requires automation and integration. There are simply too many moving parts to do it any other way.

Don't buy into the myth that you have to work out all your processes before you think about automation. Some processes can't even be prototyped without technology as an enabler – which means the IT side and the process side must be co-developed.

Finally, don't start choosing tools without a blueprint and an integrated plan. Otherwise you'll just end up with the kind of fragmented approach you already have.

First things

Bring your IT and business professionals to the table. That's the only way to get to a plan that aligns IT strategy, systems, and processes with your needs.

Get to the heart of the matter

CEO leadership can get a GRC initiative moving, but it won't go far unless you touch the hearts of employees and engage them. That doesn't happen until they see leaders adhering to ethical principles each and every day. People aren't just looking at the results you achieve, they're also looking at *how* you achieve them. And frankly, talk is cheap.

Building a risk-intelligent culture is challenging work. It involves an ongoing process of communicating with, educating, and rewarding individuals for their performance. Here are some tips for getting that done:

- Engage HR leadership throughout the process
- Add assessments of character and behavior into recruiting and performance management
- Engage business leaders and managers in developing your own language for GRC
- Build expectations for compliance into job descriptions and performance evaluations
- Assess your ethical culture and tone at the top to determine potential gaps as well as communication and training needs
- Include GRC "aptitude" when you're developing your leadership pipeline

First things
Make sure business leaders are amply and publicly rewarded for good GRC behavior.

Artichoke
(Cynara scolymus)

Just ask

Treating risk management and compliance challenges as an opportunity to control costs and improve performance requires stepping back to get a good look at the overall landscape. Then it's about making choices that work for your organization's own unique style and goals.

It won't be easy. Your company has governance, risk management, and compliance functions spread all over the place – and just getting a handle on everything currently happening is a big job by itself.

Fortunately, the potential for savings and performance improvements is significant – and relatively easy to quantify.

Integrated GRC does not need to be an all-consuming initiative. You can earn as you go, focusing first on those areas of greatest strategic importance or potential cost savings. As your successes build, your GRC initiative will take root. Your integrated enterprise approach will become a distinguishing characteristic of your management system and a source of competitive advantage.

Getting started is as simple as sending the e-mail on page 25. And if you need more copies of this book to share with your leadership team during your kick-off meeting, just ask.

Notes

About this book

Growing confidence (The smart way to manage governance, risk, and compliance) is the eighth in a series of books dedicated to helping companies improve performance. To request additional copies of this book or to order previous editions, go to *deloitte.com/straighttalk*.

Talk to us

We look forward to hearing from you and learning what you think about the ideas presented in this book. Please contact us at growingconfidence@deloitte.com.

A member firm of
Deloitte Touche Tohmatsu