

Enterprise IT-GRC Best Practices

(Podcast Transcript, Feb 26th 2009)

In this executive panel discussion, Aberdeen Group's Stephen Walker moderates an intriguing dialogue with CA's Chris Fox, eFortresses John Dimaria and Aline's Roland Mosimann, on Enterprise IT-GRC Best Practices.

Please note that readers may submit questions regarding the topics discussed today in the member's forum at www.itgrcforum.com, and your questions will be fielded to the relevant participants.



Moderator: Stephen Walker, GRC Specialist, Aberdeen Group.

Stephen is primarily focused on the interconnections and impact Governance, Risk management, and Compliance (GRC) solutions have on organizations in today's increasingly risky and regulated global market. Stephen is now focusing on diving deeper into the rapidly growing GRC market and covering a variety of topics including: Enterprise Risk Management (ERM), IT GRC, internal auditing and identity and access management.



Panelist: Chris Fox, Senior Principal of GRC, CA.

Part his role is to get involved in the evolution of GRC, provide CA thought leadership and to translate new developments into requirements for future versions of our software. He became interested in GRC through work he performed at the Australian Securities Exchange, and furthered his interest working as a Director at PwC in banking regulatory projects and management assistance in large Sarbanes-Oxley projects



Panelist: John DiMaria, Director of Professional Services, eFortresses.

John DiMaria (Co-Author of "How to Deploy BS 25999") is a management system professional, Six Sigma Black Belt and certified Holistic Information Security Practitioner (HISP). He was responsible for overseeing development, education and expertise for BSI Americas regarding all information security and business continuity activities including ISO 27001, ISO 20000 and BS 25999 and he is the president of HISPI.



Panelist: Roland Mosimann, CEO, Aline

Roland provides clients with globally-recognized thought leadership and 25 years of industry experience. Most recently, he drove the launch of the Aline™ platform for on-demand Governance, Risk, Compliance. Roland is also a co-author of "The Multidimensional Manager: 24 Ways to Impact Your Bottom Line in 90 Days," and "The Performance Manager: Proven Strategies for Turning Information into Higher Business Performance."

Partners



IT-GRC Market Overview

SW: I would like to welcome everyone onto today's podcast on IT Governance and Risk Management Compliance, otherwise known as IT-GRC, and thank in advance our expert participants from 3 leading GRC Vendors. My name's Stephen Walker, I'm the GRC Specialist at Aberdeen Group inside the Governance, Risk Management and Compliance practice.

To quickly set the stage and provide everyone a sense of what this discussion will entail, I'll begin by briefly providing some overall market context and trends in the GRC space, detail some of the high level business pressures that are driving organizations to implement GRC solutions, and identify some of the strategic actions that these companies are taking to address and overcome these challenges. We'll then jump right into the panel discussion with a Q&A session designed to offer actual recommendations on addressing the risk and compliance business challenges that are facing so many organizations in today's risky and increasingly regulated global market.

Before I provide the introductory market context I'd like to quickly explain where the fact based information that I'll be discussing comes from. As a primary fact based Research Company, Aberdeen Group extensively surveys and benchmarks the end user community on their experiences in and use of a variety of technologies and services designed to improve business performance. In particular the information I will be discussing comes from a benchmark study I'm in the process of conducting entitled; IT-GRC Aligning Risk and Compliance processes to Business Strategies. The survey for this study is the data from which serves the foundation and cornerstone for the upcoming report. It will publish at the end of this month and has already been taken by over 90 global organizations. If any of our readers or listeners want to participate in this survey you can access the survey online at the IT GRC Forum website.

How Aberdeen Group goes about conducting its research is designed around what we call our PACE methodology. Essentially what this means is we're really trying to understand what the high level business pressures are that are driving organizations to engage in IT-GRC initiatives and implement IT Risk Management and Compliance Solutions. We also want to understand what actions they will be taking and strategically; how they will set themselves up to put in place organizational framework, and how they design a plan to ensure that any solutions will be effective and drive business performance. We also want to understand what the organizational capabilities are that they both have in place now and that their also looking to put in place over the next 12 or 24 months, as well as the technology and service enablers themselves, and specifically what are those technologies companies are using to drive forward their performance improvements.

To get a better understanding of how companies can either begin a GRC program for the first time or optimize an existing initiative is essentially the end goal for this research. Taking a look at the high level business pressures driving companies to incorporate GRC solutions and the challenges facing these companies, some of the top challenges are:

- the need to better manage and mitigate the variety of technology and operational risks facing these companies
- Improve operational program efficiencies and reduce the cost of risk management activities
- the new and changing regulatory demands coming from governmental as well as industry specific regulatory bodies
- the need to provide enterprise wide visibility into risk management compliance activities for improved decision making

In terms of the actions that companies are looking to take; they're looking to develop and improve corporate IT governance frameworks, they need to establish and enforce consistent policies and procedures for risk and compliance activities, their also looking to engage professional services firms and consultancies for initial ongoing assessments and advice, and develop a comprehensive and continuous compliance infrastructure. To get a better sense of how these actions are going to be translated into an actionable plan and essentially implemented within that company we'll now jump into the Q&A.

Roland, how do you approach helping your customers understand what the business needs are and how they're going to be addressed through a comprehensive GRC program?

RM: This is actually a key point for us. We find that Enterprise Risk Management which we're seeing emerge as a big topic within GRC right now, starts with just trying to get their heads around what that should mean for them. When you look at typical risks companies are assessing it's not unusual to find 70% or more of those risks are usually business related or risks of non performance. So by getting to know what they already know and feel about the business, getting that aligned across different points of view, and getting that clearly agreed upon, we see as a great starting point for companies because from that vantage point they can then begin prioritizing some of the deep dives that might be needed. For example, you're familiar with the heat maps and grids etc, so the top quadrant of biggest impact and likelihood concern is where you want to dig deeper into what exactly you have in your environment to mitigate those risks.

SW: John, do you find that most organizations have a good handle on evaluation risks, and if they don't where do they fall short?

JD: What we're finding is rather than meeting risks head on and despite increased efforts to promote sound risk management processes, most of the clients we see in the industry as a whole tend to be in denial whether risks exist. If they do have a risk based system there are a lot of issues to how they should go about addressing them. So as a result, symptoms that organizations are not effectively managing risk management continue to flourish and include a continuous state of product instability. We're seeing constant firefighting, multiple schedule interruptions because of re-occurring surprises and the constant attacks of operating in this high stress management environment. So what we try to do is put forward a formal risk management process that provides continuous improvement and systematically addresses risk throughout the product and process lifecycle, so that risk can be introduced in the very early stages of the cycle, through a process of continuous improvement by having a system in place that continues to update the rest of the organizations changes. We're finding that a lot of organizations don't have an effective process in place and tend to be more in the crisis management mode involving risks.

SW: What's interesting John, it is very prevalent now that companies are at that 'putting out fires' stage of managing risks. It's difficult for them to think strategically about these initiatives because there are so many immediate issues for which they need to address.

Chris, for the companies that don't really have an ERM framework in place but they're looking to go there how would they get started on putting that Enterprise Risk Management methodology in place?

CF: Well it's a good question; there are a number of things you need to look at, one of the things you may want to do to start with is to start small by doing something that's fairly easy in implementing it rather than going for the big bang and putting a big methodology in place to start with. So, I'd look at something where you could see there would be some

good payback, it could be automating Sarbanes, it could be another regulatory area, it could be looking at my regulatory framework. I know that as the president said the other day, there's going to be a lot more regulation coming in the future. We did a study on how you address risk and it determined you really need some sort of risk library, and it recognized people view risk in the short term on what they know. When we developed our risk library it became very holistic. And interestingly enough we also found that 70% or 80% of the risks weren't financial risks but were operational risks.

SW: Interesting, you know a study that Aberdeen conducted over the last several months and the report we're publishing in the next few days was on Risk Management and it really found that the overall maturity levels of ERM programs and even comprehensive GRC programs are still very low. The companies that were more mature are in fact driving significant business improvements from these programs but there is a lot of hesitancy and we're just now getting over the 'wait and see' mentality that was kind of rampant throughout the marketplace.

Roland, how do you help these companies address their maturity and narrow down for them what they can be doing immediately versus a three to five year plan and an ongoing framework?

RM: As I'm sure many of my colleagues do we try and get them to think in terms of these levels of maturity to help them manage their own priorities and expectations. What we try to do is like Chris was saying get them to start small, we try and get them to a win that they can do quickly and one of the things we've looked at is how they could meet some of the expectations that have been set, be it by Standard and Poor's or be it by some of these emerging standards like the Australian standard or the ISO standard around a program. We believe if you can show the program and be effective in communicating that program the actual scope or depth of what you're doing doesn't have to be as great. So we kind of think of that as getting to a repeatable page within a couple of months if not even a couple of weeks, to get something that you can show and build on, use that as your foundation and then lay out the longer term plan against some key parameters. So we typically look at process, people, systems and information and try and lay out some of the strengths and weaknesses in their operating environment to see how they might ultimately align some of their investments be it into people or into systems and make sure that they are really going to reinforce and strengthen some of the risk management issues that have been flagged.

SW: I noticed that one of the emphasis points that you made Roland was the people component and it is sometimes one of the most overlooked elements. When companies are thinking about this it's sometimes from a very technology centric standpoint and what the research that I've been doing has clearly showed is that the companies that really are approaching this in a comprehensive fashion and able to drive not only sustainable but significant improvements in both their risks and compliance activities are those that really have the people component locked down, and it's an organizational culture that's both risk and compliance thought process first. There are a lot of companies claiming that they have a GRC program in place but it's very clear that the companies that are top performing have the upper level management buy-in for the program. That's one of the biggest concerns.

John, how do these problems exist with upper management buy-in and how can you attack this issue?

JD: We see that a lot of things get overlooked aspect of regulatory compliance is the buy-in of top level management. Getting management buy-in is relatively a simple matter of discussing economics and the negative impact of non-compliance on businesses and the ROI cost benefit analysis and so on. To get that management buying we use an analysis using Six Sigma methodologies where we go and analyze organizations compliance processes, and then bring to the forefront for management what impacts non-compliance can have on the organization, how they can achieve more

ROI by having a controllable holistic program and minimize the negative financial impact that comes with non-compliance. Just as important is showing management where they can reduce cost over-runs by integrating redundant processes that gives them a better ROI, allows them to control their compliance programs and therefore increase the buy-ins to put forward a formal process in their organizations.

SW: It's very interesting that you have targeted in on the compliance issue, the passage of SOX has been one of the most troublesome and revenue sucking areas that these companies are dealing with. Giving what's going on in the global market place in particular the financial markets in the recent turmoil and upheaval there's been multiple regulatory demands made from top political activists from both sides. The has really been an increased focus on not only tightening the regulatory framework that exists right now but also adding new and more targeted regulations to ensure that financial viability is not left up in the air.

Chris, what can GRC do to help address this increased regulatory framework that organizations are now competing in?

CF: One of the things that I like to do is take a balanced scorecard approach where we look at the balanced scorecard and we look at things like customer perspective and financial perspective, and we look at compliance against what are we doing to achieve those goals and what are we complying with to achieve those goals. For example for customer loyalty are we measuring employee's commitment to service and how important it is. On the regulatory side my experience is that the best way to deal with regulatory issues is to be proactive. I've been involved with the IT banking regulatory world assisting banks to put together work plans to comply with federal requirements, and I've been heavily involved with SOX in writing a book on Sarbanes. What we know is if you're not proactive it will cost you a lot of money and a lot of resources. One thing about the current environment is we need to have the resources focused on the business goals. Yes regulation is important but we need to manage it in an efficient way so we can also use those resources elsewhere. I think things and going to get more important if we look from the regulatory side, we've seen this week with the European Union proposing to regulate all financial institutions including the rating agencies, Standard and Poor's will find themselves regulated. We're finding much more accountability as far as the board and senior management is concerned and I'm expecting to see much more of a trend for risk management; do we know where the risks are and are we addressing the risks.

SW: Sometimes there are a lot of questions floating around on who is regulating the regulators. Of course compliance is not only a regulatory concern but it's been identified in past survey's I've conducted that internal compliance policies and practices are some of the most important and top of mind for these companies. Those that are able to structure internal policies and internal compliance requirements in a comprehensive fashion and map them back to not only the business goals of the company but also to the overall regulatory framework and requirements that they're held accountable for are finding that if they approach it the right way, the outside regulations almost take care of themselves and really start to generate some positive returns both in terms of the speed and the quality of the deliverables to their customers. For both Internal and external compliance some of the most critical organizational members that play a role in achieving these compliance requirements are of course the Internal Auditing team. These can be broken down into essentially two groups; those that are more of a checkbox mentality approach, and those that are really using the internal audit function to drive performance improvements across the enterprise.

Roland, what's your strategy around ensuring or trying to get to that second group of internal auditors and helping them to drive not only organizational change but an approach that's based on consistency and business performance?

RM: That's a very interesting question as we're seeing a lot of things happening right now. I think if you look back a few years traditionally internal audit had a lot of operational and environmental audits etc, and that was a clear and

somewhat steady path and then SOX comes along and there's a lot of disruption, not the very least being the available resources on internal audit get sidetracked on trying to get SOX done and managing the testing and everything else, and now we get to a point where they have a chance to get back to their roots but with an extra plus. We're seeing in some ways they are one of the only departments that have a very deep and broad view of the business, so they're very well positioned to help out on these risk agendas and bridge some of the priorities at the top with some of the operational reality at the bottom. So I'd say that internal auditors have a critical role to play and are almost like internal consultants, particularly those that have a good understanding of the business can provide a lot of value to the company.

SW: A lot of companies are trying to incorporate the different standards and methodologies and there have been a variety of more well known and established methodologies like the COSO framework as well as ISO and some of the newer frameworks that have been designed to help organizations grasp GRC programs and implement them in a holistic fashion, the OCEG GRC framework is a good example.

John, One of the challenges these organizations are facing is that there are different levels of acceptability across particularly global multi-national organizations who are not only struggling with requirement issues but also governmental and cultural issues. Is there one approach that stands out to you in particular that seems to be most accepted both on a national and international basis?

JD: We have found very good tie-ins with a lot of the international standards specifically ISO 27001. We find this very helpful because in general what we're seeing is most organizations have a silos approach to GRC, and because of all the different regulations they have to adhere to they don't have one integrated solution. So in order to reduce costs and really be a multinational organization a good umbrella which is acceptable in most international environments is a good way forward. The common perception is that GRC is expensive and going to take a major realignment and large database integration effort in most cases, but we found that taking a top down approach and integrated control method, and using a holistic approach such as ISO 27001 which is not prescriptive allows that umbrella approach to eliminate silos and have a good integrated system will help control and minimize costs while bringing more control to the organization and be more international friendly.

SW: John you alluded to what the data that I've been collecting over the past few months is really highlighting is there is a lot of uncertainty around GRC in the overall marketplace, not only from not really comprehending and understanding what it means but also from what it can do and how to start it. Particularly this is prevalent from when applying GRC to IT.

Chris, what are some of the common pitfalls companies fall into concerning IT-GRC and how do they establish and determine not only where to start the journey but how to ensure it is going to be able to continue on the path.

CF: I think from the IT perspective common pitfalls are; a, trying to do too much, and B, looking at it just as IT. The reality of today is that IT is really the circulatory system and lifeblood of a company. All communication goes through IT, if you want to achieve a business objective it goes through IT, and I'd view IT as an integral part of GRC. Over the next few years I expect GRC to be mandatory even if people now see it as expensive. As far as IT's concerned I think you need to sit down with your users and your own people and possibly be facilitated by consultants to identify what the objectives of GRC are. Once you assess your objectives you can then start addressing your current situation so you then start moving to the objective.

SW: As you mentioned Chris the applicability of these issues is certainly not confined to the IT department but they're very much overall revenue impacting issues. Looking at some of the more advanced and mature companies that have

implemented ERM and GRC programs there are some clear commonalities that occur. One of the best in class trade score and most consistently employed organizational activities that are finding success is an approach that is based on flexible and not rigid consistency across their functional areas and divisions.

Roland, What in your mind are some of the most important elements of that consistent approach and how can companies start on incorporating that consistent approach and driving it down from the top of the company?

RM: As mentioned by the others today I think it starts with having a unified view of how it all fits together. Very often consistency problems begin with things being described as apples and oranges when they're actually the same thing. So, making sure that you have visibility in all the different areas and how they fit is a simple point but important and often tricky one because of all the different sources of information that you're bringing together. So having this in an integrated and single repository is very important. Also, having a methodology and approach that is proven and repeatable will help. How you define the criteria for different levels of impact, how you define the factors that really drive likelihood, whether it is external or internal to you, and if you have a sense of how things are interdependent, are all important elements that are really helpful in trying to get consistency. Lastly a simple but powerful point, if you can improve the communication and sharing of the different results that you're getting this will help you get consistency as well. Often you start with two different points of view on something and then get people in a room to start talking about their differences and you will either end up with two bits of new information (that is helpful) or you'll end up with alignment.

SW: You mentioned that one of the main challenges that companies are often in the process of trying to work through is the fact that frequently they'll be referring to the same thing but calling it something different. These organizational and operational silos' that do exist make it very difficult to put a common risk based language into place. Another challenge is to get those individuals into the same room to begin with and start those conversations however once you do the data is showing that the visibility is much more clearly enabled and the consistent approach is much more likely to occur.

John, do you have any strategies in particular on gaining that organizational buy-in from individuals that don't want any organizational change and are concerned about where they'll play a role in the new organizational foundation and culture?

JD: I think companies need to take the strategy of figuring out where they have gaps in the organization to help build a cost effective roadmap and build that holistic security compliance program so that all the stakeholders know where they're at and how they can make a difference. This all starts with getting a good evaluation of the existing organization and how the people pull all that together. I think my colleagues will agree that a lot of people have an issue when they hear the word consultants but consultants can help them define their objectives, inventory their environment and recommend a course of action. This allows them to build their roadmap and get buy-in from stakeholders as everyone knows where they stand within their organization and this all becomes part of their job, not just something they do when their day job is over. So this really is value, companies really need to show how they work together, supports GRC practices and deliver that ROI so that you have a consolidated effort that you can be applying to the entire enterprise, and this will save significant expenditures over time. I can tell you as also being the President of the Holistic Informational Security Practitioners Institute; our members are really driving down this road of having this approach within their organizations and making sure that everyone knows their goal. It becomes a process not a program, and they get the help necessary to enable them align their environment with the objectives of the organization, so it's a moving process and not just words that management is throwing out there.

SW: One of the critical components is getting the organizational buy-ins and having the risk and compliance programs that are put in place not be an afterthought, but rather the goal is to infect those processes within the organizations DNA so it's not something that they're thinking about and having to remind themselves to do, but rather build into the company mindset that we're taking a risk and compliance approach towards our business activities.

Chris, how does a 'risk based' approach to GRC affect the design and implementation of not only the supporting IT infrastructure but also the technologies that these companies are looking at?

CF: There are a lot of issues there. I was on the taskforce for OCEG's Redbook involving COBIT and ISACA material, one of the big issues we had was taxonomy. We all need to use the same words that mean the same thing however a lot of people have a different definition of that. When we then apply that concept to a company we may look at risk, but what do we mean by risk? In our product we have our risk library which helps define risk. If everyone was asked to identify their risks it's very likely that they identify the same risks using different words rather than try and link them together in some way through a common library. The other think I'd expect in the infrastructure is a way that we can jump across the silo's, one of the big issues we have is a silo mentality where compliance may have one view of the world and internal audit may have another, we need to have an IT infrastructure for GRC so that; a, we can facilitate the sharing of information and b, so we can get a better appreciation of how risk is occurring throughout the organization and how risk in one part of the organization can impact another part of the organization.

SW: One of the challenges that have been identified time and again is how you put a value proposition on risk management. How do you put a dollar sign on what didn't occur because you're doing things right and particularly in this economy there has really been an emphasis on ensuring that every single implementation, service and technology buying decision is backed by the fact it is going to be able to drive business to the companies. With the escalation of these events and importance of risk and compliance and their continued and growing importance moving forward into not only 2009 but beyond, there has undoubtedly been a flurry of activity in the GRC space and we're seeing a lot of involvement, a lot of interest and frankly a lot of budgetary increases towards GRC investments and allocations.

As a wrap up question for our 3 panel participants, if you could give perhaps one or two concise statements about why companies should start GRC today what would they be?

CF: Firstly, with today's recession and previous recessions you can point to one thing that increased risk like the rise in gas prices in the 70's, and today it's almost like a perfect storm with risks coming from all over the place. I think implementing GRC will help you get a handle on these risks and what are we doing to mitigate those risks. Secondly, we are under increased pressure from regulators and government address risk more formally, so this is the time to start being proactive rather than taking on a firefighting approach as in past SOX situations where you end up spending a lot of time and effort to get things right, rather than spending the time to get it right first so when the regulatory pressure applies you can do it in a more cost effective manner.

JD: I think that GRC processes are being bought into and I believe that the enterprise segment is going to try and leverage what they've already spent to secure the infrastructure. Also I believe you must have a good management system in place as it is required and it will continue to grow. I don't think the enterprise segment is any longer going to throw dollars at the problem due to the down economy. There will be more regulations, most of them offshoots of existing regulations more detailed or less detailed. I believe more companies will spend the time to evaluate the costs of a breach against the cost of preventing them, and then make the dollars and cents business decisions on whether or not it's worth the investment and more times than not you'll see that the investment is there. So there will be a more focused and holistic approach to evaluate organizational processes that work smarter not harder.

RM: In terms of why now and how to benefit the business, I think that coming back to the people comment, however you get this done at the end of the day what you will end up with is greater visibility and greater involvement, ownership and participation into this. I'll remind about the trend back in the 80's and 90's about how we wanted to be customer centric, and over time being customer centric permeated a lot of prophecies and the like. And I think likewise here if you can push down the feeling of ownership and accountability for risk you are going to do two things, one you're going to raise visibility and understanding about opportunities because risk and opportunities are the flip side of the same coin, but also you're going to gain confidence, and at the end of the day I think confidence in what you doing is going to pay off in terms of confidence of regulators, credit rating agencies and even customers.

SW: That confidence is certainly going to help drive consistent financial integrity and an overall market uplift and that's really where the end goal is going to be for a lot of these companies. So I again want to thank all of our participants today for a very entertaining and informative podcast on IT-GRC, it's been a true pleasure to moderate.

The IT GRC Forum works with leading analysts and industry experts to produce online events for the Governance Risk and Compliance community, providing professional networking facilities and market intelligence that empower executives to make cost effective purchase decisions when managing their organization projects. Readers may submit questions regarding the topics discussed today within the member's forum on www.itgrcforum.com, and your questions will be fielded to the relevant participants.