

GRC (Governance, Risk and Compliance) and IT (Information Technology) GRC – an Interview with Dave Anderson, Director of Marketing at SAP

Listen to Podcast [here](#).

Brian Contos: Welcome to the Imperva Security podcast. I'm Brian Contos, chief security strategist for Imperva. If you would like to learn more about this subject and Imperva, visit Imperva.com, check out our [blog](#), follow us on [Twitter](#), or send us an e-mail at blog@imperva.com.

Joining me today is Dave Anderson, director of marketing for SAP Business Objects, Governance, Risk, and Compliance Solutions. He has 15 year of experience in information security, risk management, and compliance at several leading companies including: SAP, ArcSight, KPMG, and VeriSign.

During this time he developed and managed marketing and product solutions that integrate risk, compliance, strategy, and performance into unified governance and compliance frameworks. Dave's experience also includes: Implementing and auditing IT governance solutions based on COSO, COBIT, ISO 27001, and ITIL Standards. He is a certified information systems auditor.

Well welcome to the show Dave.

Dave Anderson: Thanks very much Brian. I'm very happy to be here today.

Brian Contos: Dave, before we get started I just kind of wanted to get an update from you. What's new and what are you working on these days?

Dave Anderson: Well, you know there's a lot of activity going on in the GRC market today. A lot of this activity that I see, it's kind of in direct response to a lot of the economic conditions that are going on. The companies are building out a lot of more robust risk management, policy management type of activities.

But I also see a lot of companies starting to really shift their focus of GRC, and starting to look at GRC in a new way. And they're really moving away from GRC. You know, really focused on being this tactical compliance type of an activity.

And moving more towards how to use GRC to enable strategic performance. I think a lot of this is really being driven by the ability of GRC, of really an enterprise GRC solution, to provide that deeper level of context and understanding into performance objectives.

And to how a company is performing across a particular strategic initiative. Across a business objective for instance. How GRC can really provide this context into the risks associated with a strategic initiative, let's say.

GRC with Dave Anderson

You know, good for, possibly, international expansion. There's a strategic initiative around international expansion. How can GRC actually help provide value into that type of a strategic initiative?

You know, moving away from just providing compliance capabilities for that strategy or for that business objective. But how GRC can actually help a company better perform and better execute against that strategy, by allowing them to see their risks in a deeper way. And specifically to see the impact of those risks against that strategic initiative.

Brian Contos: Dave, for some of our listeners, perhaps you could give a little bit of background. What's GRC? Sometimes we hear about ITGRC. And what are the differences? What do these terms mean exactly?

Dave Anderson: Absolutely. First let me define, really, what GRC is really about. And if you break down GRC into its three components. First is the governance piece. And governance really is providing the strategic direction and the policies for an organization. And really the means and the processes that an organization uses to implement and execute their strategy.

The risk layer. You know, risk is really how company defines their level of tolerance to risk exposure for all types of risk across an organization. Not just financial risks but all types of business risk. How a company mitigates the risk. How a company responds to specific risk events across their organization.

And then really the compliance piece is the functions and the processes that ensures that the corporate policies or internal policies and procedures, as well as both regulatory or legal mandates, are actually followed and can be evidenced across that organization.

If you look at ITGRC... You know, I really look at ITGRC as simply a proof point or more of a subset of GRC. And what I mean by that is: ITGRC really addresses the specific needs around how an organization's IT infrastructure is managed. And this includes all the processes, all the people that operate an IT infrastructure across that IT environment within an organization.

Kind of the general capabilities within ITGRC look at how these systems are configured, who accesses these systems, making sure that those individuals are authorized to access those particular systems and applications. And how they're managed and how they're operated on a day to day basis.

But ITGRC is, again, a specific proof point or a subset of an overall GRC structure. There's multiple types of these proof points within a company, such as how GRC capabilities help them address their financial needs and their financial challenges. More towards financial GRC capabilities.

There is also additional supply chain GRC capabilities within a supply chain environment. How does a company actually leverage capabilities around risk and compliance management to address their supply chain operations?

So I look at GRC as a large, really a large enterprise set of capabilities that allows a company to built the proper level of governance, to manage their risks and their controls across their enterprise. And then that extends down into these individual subsets, or proof points, for a particular line of business.

Brian Contos: Who are the early adopters for this type of... Actually I was just going to say technology, but who are the early adopters of GRC type solutions? Is it generally the very large enterprises or is it broader than that?

Dave Anderson: I think initially it was probably more the large enterprises, the companies that were subject to very particular regulatory requirements over the last three, four, five years. Sarbanes-Oxley was definitely a big driver for larger companies to start to adopt GRC solutions. What I see here is much more process focused industries, highly regulated industries that have built this initial foundation of compliance for their regulation, for their internal policies that they have to comply with. But they're now starting to move away from just using GRC to comply with these sets of regulations and are now starting to focus on really the other two acronyms: the G and the R components of GRC. And are focusing on building out higher level much more strategic governance activities. Ones that are tied to performance objectives that are tied to how a company actually operates their strategies and executes their strategies as well as how they're managing their risk associated directly with their strategic initiatives. So it's been an interesting shift where a lot of the large companies, the process industries themselves have started to move away from just the compliance focus that they've had for the last three to five years and are now starting to refocus their attention within GRC onto, really as an enabling technology an enabling solution set for performance.

Brian Contos: Do you think it would be fair to say that because such an investment was made in trying to address either one form or multiple forms of regulatory compliance that because of all that baseline work was done, now a number of organizations are saying "Well in addition to just sort of satisfying the auditors we can use all this great work we've done to really enable our business to be more effective and that sort of a transition that you mentioned to the governance and the risk side of things and not just C, not just the compliance side?"

Dave Anderson: Yeah I think absolutely, I think one of the drivers for that is companies have spent a lot of time and resources building out the individual GRC solutions and capabilities over the last number of years, and I think part of that is organizations are realizing that a single individual point solution that they've built out for one requirement combines with a point solution that they've built up for another requirement and you know extending that across their enterprise they have multiple sets of point solutions that don't integrate, that don't talk with each other and are very, very, costly and operated with manual processes and manual controls. And because of the lack of alignment, because of that lack of unification across those technologies that they've deployed there is a much better way to actually leverage that and refocus those capabilities into much more of an enterprise perspective that does bring together these types of technologies and these types of capabilities and then leverage what they already know from a regulator perspective that feed up into a higher level of GRC solutions that aligns these underlying solutions that aligns these underlying technologies gives them much much deeper context and understanding into what all that lower evidence, kind of an evidentiary layer information actually means. And then how they can extend that into driving the performance of their organization because they understand that lower level detail, that lower level information much better now.

Brian Contos: So Dave, for organizations out there that are interested in addressing either the large umbrella GRC or maybe even the subset ITGRC or supply shade GNC, what kinds of solutions out there to help enable them in this process?

Dave Anderson: Well, there's about a million of them the last time I checked, multiple, multiple solutions. Many of these are still focused on individual point solution capabilities: things like policy management, document repository, even disaster recovery, kind of business continuity. Those types of solutions are still, companies still argue that those are a collective GRC solutions are GRC capabilities. But I think that any company that's looking to implement a GRC solution, whether it be to manage their IT processes, their supply chain processes. They really start looking to this enterprise approach to GRC, solutions that can actual integrate and provide integrated functionality across all those lower level functionality. They can align how risk are identified, how risk are managed, how control is managed across individual lines of business. Those are the types of solutions that are going to return the quickest investment, going to give companies the quickest return and allow them to much, much more effectively align their GRC processes to their strategy. And I think that's really what companies are focused on today need to continue to focus on is how do you take GRC and allow that to drive your strategy and allow that to build and enable your performance.

Brian Contos: So what are some of the biggest gaps that you see, and I suppose I can look at it from two directions the technology that people are trying to leverage these solutions or just the general process which people are taking. Where are the big pitfalls, where are the gaps in technology? What are the problems that are apparent when trying to address GRC?

Dave Anderson: Well I think from both of those perspectives initially there's a cultural gap in terms of how companies are leveraging these types of solutions these type of capabilities to build a culture across their enterprise, across their entire organization to allow the business to take ownership of risk management and compliance and control activities. And that's a big shift within organizations today. GRC has really been holistically owned by the IT organization over the last several years. I'm starting to see a shift up into the business, that's a big cultural shift where companies can use this technology and use these solutions to embed GRC if you will into the business process, and into how business processes are operated and executed every single day. And it's definitely a cultural shift, we are starting to see a lot of good movement into that and I think the companies that have started to build up that culture and build GRC into their business they're seeing some very significant value added to their performance and to how their organizations are operating.

I think one of the primary gaps that a lot of GRC solutions do not provide (And companies could find themselves in a pitfall where they're implementing GRC solutions without this particular capability.) is the ability to monitor across multiple sets of IT... Really across the heterogeneous IT infrastructure and across different lines of business.

And the importance of doing that is... I mean, no company today that I know of runs a single ERP platform or a single CRM platform. Every company has some set of proprietary or even legacy applications that all, in some degree or another, help them operate their business, help them operate their financial processes, and even their IT processes.

You have to have with the GRC solution, the ability to touch and to integrate with all of those different types of disparate IT systems. Just implementing a risk and a control program over an SAP system and not addressing your Oracle system, PeopleSoft ERP system, or any of the other legacy or proprietary apps that all are used to support that business process; that doesn't provide any value at all.

You have to be able to not only address and to integrate with all of the different types of IT infrastructure that you have, but you also have to monitor those systems going forward. So

that as you identify a risk, as you mitigate a risk, as you build a control, you have an ability to do real time monitoring at any point in time.

And make sure that risk event does not occur. Or that you can at least proactively identify that a risk might be occurring based on monitoring underlying indicators, monitoring underlying transactional systems, and so forth.

So that you can actually go in and you can address that risk and mitigate that risk, or address that potential control violation before there's an impact to your business. Before your performance gets dinged. Before you experience some of the negative impact against your strategic objective.

Brian Contos: And that's why I think it makes a lot of sense to your previous point that the myopic perspective, if you will, of ITGRC: Once you start thinking about it as the larger umbrella of GRC, the fact that it would even be conceived to live in IT makes zero sense.

Of course IT needs to be involved in it. There are certainly functions that overlap with the underlying technologies. But certainly when you look at business risk, these are generally decisions that are made by people within the CFO organization and other leadership positions such as that.

It certainly seems like it's... As you get deeper and deeper into the capital R of risk, it seems like a smaller percentage of this really stays within the IT group.

Dave Anderson: Yeah, absolutely. I think the more that the business side starts to take ownership and starts to drive decisions around, obviously, how the business is operating and how they want to manage the risks associated across their business unit; IT simply becomes an enabler of those decisions.

So the business side still drives and still operates the organization. They still manage their own set of risks and how they address their controls and their control requirements. IT simply provides a forum to enable the business side to actually execute upon those decisions.

Brian Contos: So Dave, we have about time for one more question. And I'd really like to get your perspectives on: What do you see as the future of GRC? And what kind of closing comments might you have around that?

Dave Anderson: You know, I think the future that I see is (We've hit upon this a little bit to a small degree.) companies moving to a degree where they can start to embed GRC into this business process. Where it becomes much more of a business oriented approach. Where GRC is almost, if you will, almost becomes table stakes within how a business process is operated and executed.

It's not a fragmented, kind of separate approach that has to be... You know, it's not a "check the box activity" by any means, or something that has to be validated before a process can be executed. It just becomes part of that process.

Every individual within an organization across a process manages their risk. Manages the effectiveness of the controls that they're responsible for, to make sure that process is operating in a compliant way against their policies. Against their regulatory requirements, and addresses their strategic performance objectives.

And I think just to close off, I think that is really the key within GRC solutions going forward, is this movement towards really enabling GRC to help drive performance. And moving GRC from just the focus on compliance, but allowing companies to understand how these types of capabilities around monitoring risk, around monitoring control effectiveness, and then aligning risks and controls directly up into a strategic initiative.

And how that alignment can help a company optimize their performance. Increase how they're actually... Increase their ability to execute a business process in a much more efficient, much more productive way.

Brian Contos: It goes along with the saying that nobody is in business to be compliant. The fact that you're spending these resources and time, and running these projects. And if you can leverage them appropriately to your point, increase performance. Increase revenue. Increase sales. It all goes down just to general business momentum, doesn't it?

Dave Anderson: Absolutely. Companies are expected to be compliant. And what their looking for right now are solutions that can obviously deliver that, but that can help them increase their performance. And you can tie back to the bottom line about how that business is operating.

Brian Contos: Dave, this was a real pleasure. Thank you so much for joining us on today's podcast.

Dave Anderson: Thank you very much Brian.

Brian Contos: If you would like to learn more about this subject and Imperva, please visit Imperva.com. And as always, if you have any questions or comments please email us at Blog@Imperva.com.



North America Headquarters
3400 Bridge Parkway
Suite 101
Redwood Shores, CA 94065
Tel: +1-650-345-9000
Fax: +1-650-345-9004

International Headquarters
125 Menachem Begin Street
Tel Aviv 67010
Israel
Tel: +972-3-684-0100
Fax: +972-3-684-0200