Governance, risk, compliance

Experts discuss what governance, risk and compliance is and how it affects companies

Alaa Abdulnabi from EMC's security division RSA, says that GRC is fairly new to the enterprise landscape.

Governance, risk and compliance is something fairly new to the IT landscape and GRC automation software is just emerging in the region.GRC is an integrated set of processes and technologies that allow companies to improve business decision making, increase risk awareness and increase accountability.

To break it down further, governance is the culture, policies, processes, laws, and institutions that define the structure by which companies are directed and managed, risk is the effect of uncertainty on business objectives; risk management is the coordinated activities to direct and control an organisation to realise opportunities while managing negative events, and compliance is the act of adhering to, and demonstrating adherence to, external laws and regulations as well as corporate policies and corporate procedures.

"Governance, risk management, and compliance or GRC is a term that reflects the approach for organisations that adopt an integrated view to these aspects of their business. This is done by aligning and integrating the governance, risk and compliance activities and initiatives across the organisation," says Alaa Abdulnabi, regional pre-sales manager, Turkey, emerging Africa and Middle East, for EMC RSA, experts in GRC solutions.

GRC is fast becoming essential for enterprises, especially for those that are doing business globally and are struggling to keep up with the regulatory requirements in each country and manage the greater risks associated with more complex business and IT environments.

While many IT GRC programmes are showing significant value however, there is often a substantial gap between the efforts undertaken within the enterprise IT department and the expectations that are understood by business professionals.

"Regulatory compliance continues to be a major driver in the adoption of a wide variety of products that automate risk-relevant tasks, but it is increasingly being replaced by a more business-oriented risk management approach. The use of automation to manage risk- and regulatory-relevant processes is a common practice in many enterprises. Complex organisations, especially those that are heavily regulated, use a wide variety of process management and decision support tools to manage risk, govern their activities, and ensure regulatory compliance," says Biswajeet Mahapatra, research director at international technology research organisa-

"Ongoing risk and compliance concerns regarding privacy, fraud prevention, business continuity, intellectual property protection, and other top enterprise risk and compliance concerns will continue to put more pressure on IT. They will also, however, offer IT the chance to elevate their service and value to the business."

ALAA ABDULNABI, REGIONAL PRE-SALES MANAGER, TURKEY, EMERGING AFRICA AND MIDDLE EAST, RSA.

By implementing eGRC solutions, companies experience Improved Efficiency:

Organisations are tackling a specific compliance initiative, such as PCI or Privacy Mandates, as one-off projects. Rather than asking the question once of your business and IT teams and reusing that information across several compliance initiatives. By asking once and answering to many regulations you can reduce the time it takes to show compliance and reduce the number of assessments sent to the business and IT teams.

Automation:

Compliance data is often stored in several spreadsheets and only represent this data at one specific point in time. The data is instantly out of date. Using automated tools you can pull this isolated data into one system of record transforming one-off processes into a sustainable, consistent process that is used by all within the organisation.

Accountability:

Many organisations lose track of exceptions to policies that they have grant to specific areas of the organisation. Untracked, these exceptions often result in risks to the business. Managing the exception process including status and expirations improve the overall transparency and accountability of the process within the organisation.

Partnerships:

Multiple business units track compliance data across the organisation.

Collaboration across these silos enables you to consolidate this critical data to provide better insight of threats and risk across the entire organisation.

Visibility:

One of the most difficult challenges manager face is the ability to prioritise the growing number of threats they must address based on their impact to the business.

With an eGRC solution, organisations can assess the impact a particular threat has on your operational infrastructure and business hierarchy and easily track the resolution.

tion Gartner. Companies such as RSA have developed EGRC solutions that automate the GRC process, making it easier for companies to comply across a host of regulations, as well as ensuring that the company's data is up-todate and allowing greater visibility into threat impacts.

The primary purpose of any Enterprise GRC (EGRC) platform is to automate much of the work associated with the documentation and reporting of the risk management and compliance activities that are most closely associated with corporate governance and strategic business objectives. The primary end users include internal auditors and the audit committee, risk and compliance managers, legal professionals, and all accountable executives.

GRC software provides enterprises with a method to improve compliance with retention policy, reduce legal risk, and streamline the operational process of managing unstructured information, according to Darren Lee, vice president, Governance and Archiving at cloud-based GRC solutions provider Proofpoint.

Some of the products available in this space include IBM OpenPages, Thomson Reuters Enterprise GRC, Oracle GRC, EMC – RSA Archer, SAP Risk Management and Process Control, SAS Enterprise GRC, Nasdaq – Bwise and many more.

According to Atul Kamat, head of Technology Service Delivery, at data centre and cloud provider eHosting DataFort, the EGRC platform market has expanded from a tactical focus on regulatory compliance to a strategic focus on enterprise risk management. Many vendors are looking toward the next market phase, which includes adding or integrating with business performance management and score carding capabilities.

The major advantages of GRC programs in any organisation are:

Improving board's risk oversight
Responding to regulatory changes
Strengthening corporate governance
Restructuring corporate risk tolerance
Strengthening anti-fraud compliance programs.
Extending corporate social responsibility and philanthropic activities.
Renewing Green IT policies

Biswajeet Mahapatra, research director, Gartner says that the use of automation to manage risk- and regulatory-relevant processes is a common practice in many enterprises.

"Complex organisations, especially those that are heavily regulated, use a wide variety of process management and decision support tools to manage risk, govern their activities, and ensure regulatory compliance."
BISWAJEET MAHAPATRA, RESEARCH DIRECTOR, GARTNER.

GRC IN THE MIDDLE EAST:

There are currently a large amount of GRC initiatives in the region, although it is still early days. According to Gartner, companies have only just realised the importance of GRC and have begun adopting best practices, standards and tools to make their IT environment more secure.

"Many organisations are coming to realise the importance of having a GRC programme in place, and are now looking at enhancing their current processes. Compliance with regulations is the major driver for governance, risk and compliance in the Middle East, which drives focus to other areas of the givernance, risk, compliance space such as risk management, Business continuity management and audit management," states Abdulnabi.

GRC is of major importance in government, banks and financial institutions but slowly will become one of the top three priorities in most of the large and medium enterprises, says research firm Gartner. According to Chuck Hollis, VP Global Marketing CTO EMC Corporation, if you're a company or an organisation of any type, you want to avoid bad things happening. You want to understand what the risks might be, their potential impact, what can be done to mitigate those risks, and what the relative costs might be. To do this, enterprises need a group of people and some process to go look at those things, understand them, and make recommendations. In a nutshell, that's governance.

Once the recommendations are made, enterprises need people and process to go do what was recommended, measure the results, and be able to prove what you've done. That is enterprise compliance.

"You'll find GRC-type thinking emerging everywhere: legal, finance, HR, IT, engineering, research, healthcare, energy exploration. Each sub-segment faces a very different risk profile, so GRC is thought of differently depending on who you're talking to. HR risks aren't the same as legal risks aren't the same as engineering risks, and so on," according to Abdulnabi.

DEPLOYMENTS:

IT GRC programmes are still relatively new, but they have already shown great success and even more promise in many organisations. Working to align efforts with business expectations will help assure IT that projects aren't perceived to be wasted efforts, helping solidify the collaboration and support that is required from the business in order to achieve ongoing success.

"IT professionals should take heart that their efforts are seen as important and valuable to business professionals. Where previously there has been a distinct divide between the two groups and little understanding between them, the changing nature of the corporate environment is creating opportunities for understanding and collaboration. Ongoing risk and compliance concerns regarding privacy, fraud prevention, business continuity, intellectual property protection, and other top enterprise risk and compliance concerns will continue to put more pressure on IT. They will also, however, offer IT the chance to elevate their service and value to the business," explains Abdulnabi.