Embrace This Acronym: IT GRC. It Could Save Banks a Bundle
Conte, Patrick
American Banker Magazine; Nov 2007; 117, 11; ABI/INFORM Complete
pg. 62

OpEd

Embrace This Acronym: IT GRC. It Could Save Banks a Bundle.

By Patrick Conte
CEO, Agiliance

THE FINANCIAL-SERVICES INDUSTRY, LIKE EVERY OTHER, IS awash in acronyms, and one that's been gaining ground lately is GRC. Used to describe the interdependent disciplines of governance, risk and compliance, GRC refers to the people, processes and technology banks invest in to comply with regulations and manage risk as part of effective corporate governance. GRC connects the dots between many of other acronyms—SOX, FFIEC, GLBA, PCI DSS—not to mention every other regulation and mandate that touches the bank.

In fact, GRC has already produced an "offspring" of sorts—IT GRC (information-technology governance, risk and compliance.) IT GRC augments and complements the overarching GRC landscape by addressing the unique role information technology plays in GRC.

With respect to compliance and risk, IT consumes the majority of bank employees' time and effort. A whopping 80 percent is spent on developing, implementing and testing controls and remediating issues related to failed controls, according to IDC. Managing information, applications, systems and networks is complex, requiring sophisticated and integrated technology and processes. IT GRC addresses technology's specific challenges, providing methodologies and technology that IT can effectively use to cut time and costs while improving the quality of risk and compliance information.

Banks and other financial institutions are no strangers to regulations, and currently face three challenges that, together, are driving them to understand and invest in IT GRC to create and automate processes to manage compliance and security risk in a systematic, quantitative and comprehensive fashion. These challenges include a shift by regulators to risk-based compliance; a growing regulatory focus on an institution's accountability for third-party service providers; and the breakdown of compliance and risk-assessment processes that can't scale to support multiple regulations and mandates, especially with respect to information technology.

Changes in how regulators are approaching compliance have a significant impact on IT and also provide opportunities to improve efficiencies and the quality of compliance and risk activities and information.

For example, it used to be good enough to choose a small number of critical business applications to include for risk assessment as part of the Sarbanes-Oxley compliance audit cycle. But now regulators no longer accept these small samples as adequate or representative.

Quite simply, they do not provide an enterprise perspective of the information-security risks that banks face. It is not uncommon for large financial institutions to have to scale risk-assessment activities immediately from a sample of 15 to more than 400 or 500 high-risk applications. The challenge IT faces is how to scale. How well they solve it impacts the entire business.

The upside is that, if they do it right, managers throughout the entire organization can use this new risk information to make better business decisions that could ultimately result in a meaningful competitive advantage.

Another area of significant impact on information governance, risk and compliance is the dependency of banks on outsourcing critical aspects of the business to third-party service providers. As banks strive to control costs, outsourcing has provided a useful tool.

But that tool comes with a cost. More third-party relationships increase the complexity of managing compliance and security risk across outsourced operations and present new accountability challenges. Where is the bank's data and who has access? Are information assets safe? How can the risks be most effectively managed? According to TPI, an outsourcing consulting company, such an approach increases the governance burden, estimated at between eight percent to 15 percent of the project's cost.

A final area of concern is the unwieldiness and expense of current approaches to managing IT compliance and risk, espe-

OpEd

cially as the number of regulations and mandates continues to grow. With the imposition of each new regulation, the common approach has been simply to add a new compliance team with a new mission and scope.

The final result? Many different teams with many missions ask the same questions, create significant inefficiencies, and hamper banks from comprehensively understanding their risk position.

Redundant policies and controls are common. Teams interpret the same risk data differently. Compliance and risk information is siloed with no ability to see the big picture. Teams often cannot see redundancies across regulations or share a common interpretation of risk information, either across compliance and risk teams or management at large. IT GRC provides a means to eliminate those redundancies, improve the consistency and quality of risk data, save time and reduce the demands on managers.

As these trends continue to apply pressure, banks should assess whether their current processes can scale. As risk assessment becomes a center point for compliance, bank managers need to ask whether their institutions are ready to scale from tens to hundreds of assessments overnight.

Second, banks should review their current approach to managing their third-party vendors and ensure that compliance and risk data can be encapsulated and aggregated with the bank's own data easily to draw a comprehensive risk picture and provide evidence of compliance in line with regulatory expectations. If the bank is still relying on emails and spreadsheets, perhaps the bank needs to take a closer look at its approach.

Finally, banks should review their approach to compliance. Understanding the overlaps among policies relating to separate regulations can be a real eye opener. Why absorb the time and employee expense of implementing and testing the same control many times, when once would suffice to meet the requirements of all relevant regulations?

IT GRC allows banks to effectively manage information-technology assets and processes with respect to compliance. It provides the means to consolidate and integrate the plethora of technical data and to systematically gather, quantify and prioritize security-risk data across assets, operations and regulations, thereby improving risk mitigation.

Finally, it provides a means to control the cost of IT compliance—a significant sliver of the $6 billion spent in 2006 to comply with SOX—the ability to understand which security risks really matter, and the tools to communicate what those risks mean in business terms that every manager can understand. In an age of increasing information overload that may be the greatest gift IT GRC delivers—a way to map all the regulatory acronyms back to one—ROI.

UNITED STATES POSTAL SERVICE ●

Statement of Ownership, Management, and Circulation (Requester Publications Only)

1. Publication Title	2. Publication Number	3. Filing Date
U.S. Banker	0 5 2 5 - 0 5 0	October 1, 2007
4. Issue Frequency	5. Number of Issues Published Annually	6. Annual Subscription Price (If any)
Monthly	12	$ 109.00

7. Complete Mailing Address of Known Office of Publication (Not printer) (Street, city, county, state, and ZIP+4®)
One State Street Plaza, New York, NY 10004
Contact Person: Mary Mormile
Telephone (Include area code): 212-803-8830

8. Complete Mailing Address of Headquarters or General Business Office of Publisher (Not printer)
Same as above

9. Full Names and Complete Mailing Addresses of Publisher, Editor, and Managing Editor (Do not leave blank)
Publisher (Name and complete mailing address)
Liesbeth Severiens, One State St. Plaza, New York, NY 10004
Editor (Name and complete mailing address)
Holly Sraeel, One State St. Plaza, New York, NY 10004
Managing Editor (Name and complete mailing address)
Karen Krebsbach, One State St. Plaza, New York, NY 10004

10. Owner (Do not leave blank. If the publication is owned by a corporation, give the name and address of the corporation immediately followed by the names and addresses of all stockholders owning or holding 1 percent or more of the total amount of stock. If not owned by a corporation, give the names and addresses of the individual owners. If owned by a partnership or other unincorporated firm, give its name and address as well as those of each individual owner. If the publication is published by a nonprofit organization, give its name and address.)

Full Name	Complete Mailing Address
Source Media	One State Street Plaza, New York, NY 10004

11. Known Bondholders, Mortgagees, and Other Security Holders Owning or Holding 1 Percent or More of Total Amount of Bonds, Mortgages, or Other Securities. If none, check box → ☐ None

Full Name	Complete Mailing Address

12. Tax Status (For completion by nonprofit organizations authorized to mail at nonprofit rates) (Check one)
The purpose, function, and nonprofit status of this organization and the exempt status for federal income tax purposes:
☐ Has Not Changed During Preceding 12 Months
☐ Has Changed During Preceding 12 Months (Publisher must submit explanation of change with this statement)

PS Form 3526-R, September 2007 (Page 1 of 3 (Instructions Page 3)) PSN: 7530-09-000-8855 PRIVACY NOTICE: See our privacy policy on www.usps.com

13. Publication Title: U.S. Banker			14. Issue Date for Circulation Data Below: September 2007	
15. Extent and Nature of Circulation			Average No. Copies Each Issue During Preceding 12 Months	No. Copies of Single Issue Published Nearest to Filing Date
a. Total Number of Copies (Net press run)			43,441	43,518
b. Legitimate Paid and/or Requested Distribution (By Mail and Outside the Mail)	(1)	Outside County Paid/Requested Mail Subscriptions stated on PS Form 3541. (Include direct written request from recipient, telemarketing and Internet request from recipient, paid subscriptions including nominal rate subscriptions, employer requests, advertiser's proof copies, and exchange copies.)	40,095	40,216
	(2)	In-County Paid/Requested Mail Subscriptions stated on PS Form 3541. (Include direct written request from recipient, telemarketing and Internet request from recipient, paid subscriptions including nominal rate subscriptions, employer requests, advertiser's proof copies, and exchange copies.)		
	(3)	Sales Through Dealers and Carriers, Street Vendors, Counter Sales, and Other Paid or Requested Distribution Outside USPS®		
	(4)	Requested Copies Distributed by Other Mail Classes Through the USPS (e.g. First-Class Mail®)		
c. Total Paid and/or Requested Circulation (Sum of 15b (1), (2), (3), and (4)) ▶			40,095	40,216
d. Nonrequested Distribution (By Mail and Outside the Mail)	(1)	Outside County Nonrequested Copies Stated on PS Form 3541 (Include Sample copies, Requests Over 3 years old, Requests Induced by a Premium, Bulk Sales and Requests including Association Requests, Names obtained from Business Directories, Lists, and other sources)	1,583	1,624
	(2)	In-County Nonrequested Copies Stated on PS Form 3541 (Include Sample copies, Requests Over 3 years old, Requests Induced by a Premium, Bulk Sales and Requests including Association Requests, Names obtained from Business Directories, Lists, and other sources)		
	(3)	Nonrequested Copies Distributed Through the USPS by Other Classes of Mail (e.g. First-Class Mail, Nonrequestor Copies mailed in excess of 10% Limit mailed at Standard Mail® or Package Services Rates)		
	(4)	Nonrequested Copies Distributed Outside the Mail (Include Pickup Stands, Trade Shows, Showrooms and Other Sources)	857	925
e. Total Nonrequested Distribution (Sum of 15d (1), (2), and (3))			2,440	2,549
f. Total Distribution (Sum of 15c and e) ▶			42,535	42,765
g. Copies not Distributed (See Instructions to Publishers #4, (page #3)) ▶			907	753
h. Total (Sum of 15f and g)			43,442	43,518
i. Percent Paid and/or Requested Circulation (15c divided by f times 100) ▶			94.26 %	94.04 %

16. Publication of Statement of Ownership for a Requester Publication is required and will be printed in the November 2007 issue of this publication.

17. Signature and Title of Editor, Publisher, Business Manager, or Owner: Liesbeth Severiens, Publisher — Date: October 1, 2007

I certify that all information furnished on this form is true and complete. I understand that anyone who furnishes false or misleading information on this form or who omits material or information requested on the form may be subject to criminal sanctions (including fines and imprisonment) and/or civil sanctions (including civil penalties).

PS Form 3526-R, September 2007 (Page 2 of 3)