

GRC *Perspectives*

*Achieving a Sustainable and Effective IT
Risk & Compliance Program*

September 2008

Prepared By: Michael Rasmussen

Corporate Integrity, LLC
research@Corp-Integrity.com
www.Corp-Integrity.com

Corporate
Integrity™
strategic direction for GRC →

Executive Summary

IT departments scramble as they react to multiple initiatives demanding greater oversight of IT risk and compliance across IT infrastructure, identities, and information. The web of stakeholders with varying risk and compliance requirements appears to introduce a complex IT tug-of-war with opposing priorities. However, the scenario is not so gloom. There is significant redundancy in requirements, technologies, and processes across risk and compliance issues impacting IT.

Sustainability of IT risk and compliance is achieved through defining common processes and technologies that different stakeholders can utilize for their individual requirements as well as for collaboration and sharing. Organizations need to be intelligent about what processes and technologies they deploy – the goal is to define once and comply with many regulations while managing a range of risks. A sustainable risk and compliance technology architecture is in place when . . .

Content management is the cornerstone of a risk and compliance architecture

Workflow enables and streamlines risk and compliance management

Infrastructure and asset discovery and classification identifies a baseline for analysis

Automated and continuous monitoring of the IT environment is analyzed against policies

Identity management provides the core of understanding risk and compliance access issues

Change/configuration management and remediation maintains compliance as business evolves

Problem management and remediation streamlines identification and management of issues

Automated protection and enforcement of business rules reduces risk and enforces compliance

Reporting and metrics provide proof of IT risk and compliance

The realm of risk and compliance is diverse with many intricacies and issues ready to frustrate the organization. This requires that the organization discover what they have in place, what they have to comply with, and then analyze the environment to identify what needs to change. Selecting the right technology vendors that provide the integration and enterprise control of risk and compliance is a critical step that organizations should not take lightly.

Table of Contents

TABLE OF CONTENTS.....	2
EXECUTIVE SUMMARY	2
PUTTING OUT THE FIRES OF IT GOVERNANCE, RISK, AND COMPLIANCE	4
APPEASING A CROWD OF IT STAKEHOLDERS WITH VARYING MOTIVATIONS.....	4
<i>Mitigating threats while staying compliant, . . .</i>	4
<i>Streamlining the impact on IT management, and . . .</i>	5

<i>Using oversight to remain aligned with business goals.</i>	5
REACTING TO REQUIREMENTS IS A LOSING STRATEGY.....	5
1 - Higher expense.....	5
2 - Inability to align with the business.....	6
SUSTAINABLE IT RISK & COMPLIANCE IS BUILT UPON A COMMON ARCHITECTURE	6
CRITICAL INGREDIENTS TO A SUSTAINABLE IT RISK AND COMPLIANCE STRATEGY	7
DEFINING A COMMON ARCHITECTURE FOR IT RISK AND COMPLIANCE	7
<i>Content management is the cornerstone of a risk and compliance architecture</i>	8
<i>Workflow enables and streamlines risk and compliance management</i>	8
<i>Infrastructure and asset discovery and classification identifies a baseline for analysis</i>	8
<i>Automated and continuous monitoring of the IT environment against policies</i>	8
<i>Identity management provides the core of understanding risk and compliance access issues</i>	9
<i>Change/configuration management and remediation maintains compliance as business evolves</i>	9
<i>Problem management and remediation streamlines identification and management of issues</i>	9
<i>Automated protection and enforcement of business rules reduce risk and enforces compliance</i>	10
<i>Reporting and metrics provide proof of IT risk and compliance</i>	10
WHERE TO START?	11
ABOUT THE AUTHOR.....	12
MICHAEL RASMUSSEN, PRESIDENT	12
CORPORATE INTEGRITY, LLC	13

Putting out the fires of IT governance, risk, and compliance

IT departments scramble as they react to multiple initiatives demanding greater oversight of IT risk and compliance across IT infrastructure, identities, and information. Most organizations have approached these issues in reactive mode -- putting out the fires of IT wherever the flames are the hottest. It is now time for IT to step back and think strategically; to figure out how to streamline resources and use technology efficiently and effectively to manage and monitor IT risk and compliance.

The challenge facing IT stems from multiple mandates requiring organizations to demonstrate . . .

1. **Effectiveness of IT governance.** The IT organization faces a range of internal governance demands that push the organization to manage resources, validate ROI on new and existing initiatives, and oversee a web of IT management priorities.
2. **Adherence to frameworks, best practices, and industry standards.** Adding to this is the complexity of achieving compliance with a variety of frameworks and standards (e.g., ISO/IEC 21000, ISO/IEC 14000, ITIL, COSO, COBIT). This becomes an ongoing, or recurring, challenge of demonstrating parity with these common industry practices in a constantly changing IT environment.
3. **Compliance with regulations and standards.** The IT acronym soup has moved beyond technical terms to include things such as SOX, HIPAA, GLBA, PCI, PIPEDA, and others. IT struggles to meet compliance with cross-industry requirements as well as industry specific requirements. Healthcare, for example, is a mess of compliance acronyms such as HL-7, DICOM, IHE, and XDS. When it comes to non-compliance, IT has become familiar with corporate integrity agreements, deferred prosecution, and consent decrees. The range of regulatory compliance initiatives facing IT spans from a host of security and data protection initiatives, disaster recovery, retention and e-discovery, to demonstrating accessibility on websites for the disabled.
4. **Conformity to business relationship/contract requirements.** IT organizations also face a complex web of business relationships and resulting contractual control requirements for connectivity and access. It is not uncommon in large IT shops to have half of the user identity population in the environment stem from 3rd party relationships and not the traditional employee base.

Appeasing a crowd of IT stakeholders with varying motivations

The mixture of IT stakeholders vested in IT risk, and compliance is diverse and complex. Sustainability in IT strategy and operations requires collaboration across roles responsible for varying aspects of risk and compliance. These include roles focused on . . .

Mitigating threats while staying compliant, . . .

- **Security.** The traditional view of IT Security has been buried in IT operations and aimed at responding to hackers, viruses, and worms and attempting to avoid risk. Unfortunately, there are still many organizations that have failed to let their IT security organization mature beyond this. This role has been focused on minimizing exposure to the business through risk elimination or avoidance strategies, which comes at a high cost to the business as mandatory controls are placed on systems and information with little thought given streamlining investment for other risk and compliance purposes.

- **Risk.** Organizations have seen their IT security function split to include an IT risk management discipline. Risk management aims at understanding and modeling the various threats, likelihoods, and business impacts to the organization to select and prioritize IT controls aimed to bring systems and information in line within acceptable levels of risk tolerance.
- **Compliance.** Facing many regulations impacting information systems, IT organizations have begun to develop their own internal legal acumen and are aggressively defending the organization by demonstrating compliance to laws and regulations impacting IT. IT compliance officers aim to avoid the penalties of non-compliance by passing audits and remediating compliance gaps, supported through aggressive reporting and analysis of the state of controls in the IT environment.

Streamlining the impact on IT management, and . . .

- **Governance.** IT governance aims to align IT with business requirements and expectations. The strategy of IT governance professionals is: to aggressively pursue alignment of IT to the business; to report on metrics and monitor IT key-performance and risk indicators; and, demonstrate that IT is on-time, on-budget, and meeting service level agreements.
- **Operations.** Meanwhile, IT operations seek to enhance visibility and control of the IT infrastructure to improve system operations and avoid downtime. Operation's priorities include obtaining visibility into IT system and infrastructure performance, simplifying compliance analysis, enforcing controls to demonstrate compliance, remediating deficient controls, continuous monitoring of controls in a dynamic business and technology environment, and reducing incidents around the IT infrastructure.

Using oversight to remain aligned with business goals.

- **Audit.** The world of internal audit has expanded significantly over the past five years – credit for this growth goes to the demand placed on the organization because of SOX and other regulations. IT has been the primary expansion point of the internal audit department as the business aims to validate that policies, procedures, and controls within the IT department are not only defined but also implemented and effective.
- **Line of business.** IT is in place to support the business – thus many stakeholders in IT risk and compliance fall outside of IT. This role represents the business process, or information owner, whose neck is on the line when there is too much risk inherent in business processes supported by IT. They face the scrutiny when business processes are encumbered by a legion of poorly defined, and at times unnecessary, controls. Striking a balance between risk avoidance and burdensome controls is a fine line the business owner of IT systems and processes has to maintain.

Reacting to requirements is a losing strategy

These varied roles pressuring IT for risk and compliance is the root cause many IT organizations have moved to reactive mode aimed at putting out the fires of IT control. A reactive approach to IT risk and compliance is not sustainable, as something will eventually burn through - a recipe for disaster, which leads to . . .

1 - Higher expense

- **Wasted and/or inefficient use of resources.** Silos of IT risk and compliance lead to wasted resources. Instead of leveraging how controls and resources can be defined and

implemented to meet a range of requirements, they are developed independently with no thought for leverage. The IT department ends up with different internal processes, systems, controls, and technologies to meet individual risk and compliance needs.

- **Unnecessary complexity.** Multiple and different IT risk and compliance approaches introduce greater complexity into the IT environment. With complexity comes an increase of inherent risk. Controls are not streamlined and managed consistently introducing more points where controls can fail or go unmonitored. Inconsistency in controls also means inconsistency in documentation of those controls, which further confuses IT, regulators, and the line of business.

2 - Inability to align with the business.

- **Lack of flexibility.** Complexity drives inflexibility. The IT organization becomes so wrapped up in spinning individual risk and compliance plates that IT performance, development, and support of the business is degraded. Developers and the business become bewildered in a maze of varying methodologies and control requirements that have not been approached with any sense of consistency or logic.
- **Vulnerability and exposure.** A reactive approach finally leads to greater exposure and vulnerability. This is a fruit of complexity: everyone is focused on their silo of compliance and no one sees the big picture. No one is looking at IT risk and compliance holistically. The focus is on what is immediately before them and not what the business needs to protect itself in the long run. Varying and independent efforts of IT risk and compliance leads to difficulty in demonstrating enforcement and confusing audits and assessments.

Sustainable IT Risk & Compliance is Built Upon a Common Architecture

Risk and compliance burdens are not getting simpler – they are growing in number and complexity. It is no longer about an annual audit; it now involves continuous monitoring as business changes. Business evolves rapidly – particularly within the IT department. User identities are added, they change roles, and they are terminated. New business partner connections are established – others are torn down. IT infrastructures and applications are patched and configurations change. Sensitive information has become distributed and pervasive throughout the organization. Risk and compliance needs to be sustainable as an ongoing and integrated part of IT processes.

Continuously monitoring risk and compliance has become imperative but it's only cost effective if the organization has a strategic approach to managing controls across risk and compliance initiatives. IT is in an awkward position of reacting to mandates where it should be proactively managing IT controls and risk. The web of stakeholders with varying risk and compliance requirements appears to introduce a complex IT tug-of-war with opposing priorities. However, the scenario is not so gloom. There is significant redundancy in requirements, technologies, and processes across these risk and compliance issues impacting IT.

Sustainability of IT risk and compliance is achieved through defining common processes and technologies that different stakeholders can utilize for their individual requirements as well as for collaboration and sharing. A sustainable IT risk and compliance strategy is one that has a symbiotic influence on the variety of IT stakeholder roles and their common requirements.

Critical ingredients to a sustainable IT risk and compliance strategy

Sustainable risk and compliance programs are built upon a common process and technology architecture designed to meet a range of requirements impacting IT. Organizations need to be intelligent about what processes and technologies they deploy – the goal is to define once and comply with many regulations while managing a range of risks. A sustainable approach to risk and compliance results in an IT organization that is looking to the future and mitigating risk in the course of business as opposed to putting out fires by reacting to risk and control issues as they arise.

To achieve sustainability in risk and compliance an organizations needs to adopt a solution that is . . .

- **Unified.** All the stakeholders in risk and compliance need to be playing out of the same playbook. If different parts of the organization are going in different directions, risk and compliance will not be able to achieve the economies that a sustainable IT risk and compliance architecture achieves. The goal is to provide sustainability and efficiency through a unified view of the different aspects of risk and compliance. An organization should be able to look through a single lens to see the complete view of risk and compliance as well as focus in on specific areas of interest.
- **Automated.** IT infrastructure is vast and rapidly changing. The only way to achieve effective risk and compliance is to select and deploy technologies that help the organization automate risk and compliance processes and enforce controls within the environment. Only through automation can an organization achieve continuous risk and control monitoring as opposed to the point-in-time spot checks of the past.
- **Integrated.** A lot of time is wasted in deploying islands of technology that do not work together. Multiple points of management that span different areas of the infrastructure are costly to manage, do not provide a holistic view into the enterprise, and cannot correlate their analysis to provide more definitive conclusions. Sustainable risk and compliance leverages an architecture that is integrated to facilitate management and reporting across the enterprise.
- **End-to-end.** The IT environment is complex and distributed, which requires end-to-end management of risk and controls across identities, infrastructure, and information in the IT architecture. When it gets down to it – information is the center of risk and compliance initiatives, and an organization needs an end-to-end strategy to define the confidentiality, integrity, and availability of information.

Defining a common architecture for IT risk and compliance

Organizations face an array of technologies to consider as the foundation of their risk and compliance architecture. The challenge IT professionals have is sorting through the maze of IT vendors, all hawking their risk and compliance technologies. These days it would appear that every IT vendor on the planet has a risk and compliance message, so the task of sorting through this and selecting the right vendor to build a sustainable risk and compliance architecture can be overwhelming.

To approach the maze of IT vendors, organizations should consider the range of risk and compliance requirements impacting IT and select the vendor(s) that have the strongest integrated solution to manage these requirements on a consistent ongoing basis. The right technology architecture lays a strong foundation for a sustainable risk and compliance strategy.

Content management is the cornerstone of a risk and compliance architecture

The foundation of any risk and compliance strategy starts with content. The organization is swimming in business content that introduces exposure to risk and regulatory requirements -- personal information, financial results, trade secrets -- as well as compliance specific content such as policies, procedures, and controls. You boil down any regulation or area of risk and at its core it gets to information that needs to be stored, assessed, communicated, and analyzed within the enterprise. Further, the organization is challenged to ensure integrity, security, and accessibility of business critical information. Whether looking at risk and compliance from a business or IT perspective, the organization is required to document and communicate how they will be compliant. However, organizations are exposed to significant risk when content is inaccessible and/or out of date. Many of the nightmares of risk and compliance come from silos of content that are redundant, out of date, non-existent, or even in conflict with each other.

Organizations require a robust content management strategy to define, communicate, execute, and enforce corporate policies, procedures, and controls. It is also necessary to manage and share information across the organization for enhanced productivity while at the same time control and secure sensitive information, and provide audit trails to prove adherence to corporate policies.

Workflow enables and streamlines risk and compliance management

After an organization tackles the content management puzzle of risk and compliance, they next need to get a handle on developing and managing IT risk and compliance processes. This starts with integrating workflow to build risk and compliance processes that integrate with the organization's content management backbone.

Workflow processes ensure that steps and tasks are properly defined and managed and it streamlines the overall management of risk and compliance processes. Workflow and process management technologies drive the oversight and efficiency that organizations seek in order to reduce the impact risk and compliance processes have on the business.

Infrastructure and asset discovery and classification identifies a baseline for analysis

Managing and controlling risk and compliance requires a detailed and accurate picture of IT assets and infrastructure. This includes understanding the network, server, application and storage infrastructure, and information assets -- identifying their use, relationships, and establishing both IT and business process owners.

Organizations should look for technology solutions that are continuous, automated, and provide real-time discovery of enterprise information assets. Automatic discovery and classification of sensitive information assets and infrastructure according to policy is a critical component of a sustainable IT risk and compliance architecture. Essential to the success of managing enterprise assets is the mapping of relationships and dependencies as well as and the ability to provide visibility across assets in both the physical and virtual business environments.

Automated and continuous monitoring of the IT environment against policies

Critical to a sustainable risk and compliance strategy is the ability to automate the ongoing monitoring and analysis of the IT environment for adherence to or violation of policies. This is a significant area where IT can drive efficiencies in risk and compliance and relieve the burden upon business -- providing a lower cost to managing risk and maintaining compliance.

Automated control monitoring requires that an organization have the ability to describe a compliant environment, apply policies to the environment, analyze current infrastructure and systems against the policies, track changes over time, and alert IT operations of violations in storage, networks, application infrastructure, servers, and data. Success hinges on technology with the ability to model policies that

are easy for both IT and the business to understand and can be automated to continuously monitor policies, provide detection of unauthorized changes, and alert when violations are detected.

Identity management provides the core of understanding risk and compliance access issues

A large number of risk and compliance issues can be boiled down to understanding who has (or had) access to what systems, information, and processes. This becomes particularly challenging in the extended enterprise when third party relationships complicate monitoring and evaluating access to systems and information.

As a result, an IT risk and compliance strategy is to include the implementation of a comprehensive identity and access management solution that provides for provisioning, de-provisioning, centralizing the view of identities and their entitlements, role and rule management, as well as monitoring and enforcement of segregation of duties. A complete identity and access management solution will also include a range of authentication and authorization capabilities to protect access to information and processes commensurate with the risk faced.

Change/configuration management and remediation maintains compliance as business evolves

Organizations are dynamic and fluid – constantly changing. Risk and compliance is not a point in time assessment but is required as business changes. Validating that a configuration management process is in place is a critical step in passing audits and regulatory inspections. Change and configuration management provide for a sustainable IT risk and compliance strategy ensuring that audit and remediation policies are in synch and that changes are consistently maintained while reducing errors in translating audit results to remediation. A robust change and configuration management strategy will not only help the organization maintain compliance and control risk but will also streamline the audit process with an integrated strategy for assessing changes and controls.

A sustainable risk and compliance strategy requires monitoring changes when business connections are setup; users are provisioned, re-provisioned, or de-provisioned; when configurations are changed; and new systems are deployed. Organizations should look to utilize change and configuration management technology to find issues and automatically feed them into the appropriate remediation response to bring the element back into compliance. Change and configuration management technologies are also utilized to remediate control deficiencies by automatically bringing infrastructure and systems back into a state of compliance.

Problem management and remediation streamlines identification and management of issues

Automated discovery, control/environment monitoring, and change and configuration management provide for the ongoing analysis and discovery of risk and compliance issues that the organization has. However, open and unresolved issues pose a liability to the organization that needs to be remediated. Problem management and remediation comes into play when something breaks. This requires that the organization gain a firm hold on problem management through the deployment of systems to monitor, document, and manage the remediation process.

Organizations need solutions to aid them in automated root cause analysis with correlation across the various technology domains (e.g., applications, servers, networks, and storage). This provides sustainability by streamlining the process of bringing the organization back into a state of control, it and minimizes the mean-time-to-repair and maintain compliance. Control is brought to the organization as incidents impacting business operations are evaluated to identify what happened, the impact/loss to the organization, and provide root cause analysis of detected problems so they are addressed in the correct manner.

Automated protection and enforcement of business rules reduce risk and enforces compliance

Because organizations have multiple points of access into information and systems, they have become quite porous. Being able to control what authorized recipients can or cannot do with information they receive provides a stronger level of security than just ensuring that the correct recipient received the information.

This requires that organizations deploy technologies to monitor and enforce controls across endpoints, the datacenter, and network perimeters to prevent information leakage. When sensitive information and communications are involved, it becomes necessary, and often required by regulations and third party requirements, for the organization to utilize encryption technologies to protect that information in transit and at rest. Additionally, when sensitive information and intellectual property are shared with other parties, the organization needs to have in place the appropriate information rights management technology to mitigate risk.

Reporting and metrics provide proof of IT risk and compliance

Deploying a range of technologies to define policies, monitor change, remediate control deficiencies, and automate enforcement of controls helps provide for risk and compliance sustainability. However, it is not complete unless the organization can document and report on the state of risk and compliance.

Organizations need to ensure to auditors, regulators, stakeholders, and third parties that risk is managed, controls are in place and effective, and that systems and information are in compliance with policy. This requires that an organization implement integrated solutions that provide real-time monitoring of the environment, reporting on controls and policy violations, and supporting the remediation and response to incidents discovered.

Where to start?

The realm of risk and compliance is diverse with many intricacies and issues ready to frustrate the organization. Organizations that attempt to build an IT risk and compliance strategy alone are often left in the dark and are boxed into a view of the world that they may find limiting down the road.

To get started, organizations are to . . .

- **Take a top-down approach.** This requires that the organization discover what it has in place, what it has to comply with, and then analyze the environment to identify what needs to change. From there, the organization can identify any needed solutions and technologies, and then move into continuous control monitoring to validate and prove the implementation and effectiveness of risk and compliance processes. Prioritization of risk and compliance activities needs to be decided at a business level so that IT clearly knows what to work on. This can be difficult as silos of risk and compliance can function buried within different functions of IT and the business. To overcome this and facilitate a top-down approach, a sustainable risk and compliance strategy requires that the organization get executive buy-in and support. This provides endorsement of the effort and overcomes obstacles of silos wanting to work independently and do things their own way.
- **Seek advice and experience from experts.** A successful risk and compliance strategy starts with seeking outside help from consultants and integrators that have been through the process before and can benefit the organization by providing a range of insight into common and leading practices. To facilitate a risk and compliance strategy, organizations should look to engage professional services that have experience in their industry; that understand the intricacies of their business processes; and that have developed sound methodologies for managing risk and compliance, in order to help the organization define or review policies, procedures, and controls.
- **Start with the greatest gaps.** Risk and compliance is not new to organizations. The problem is that there have been multiple independent projects and systems put in place to monitor and manage IT risk and compliance. Getting started on a sustainable IT risk and compliance strategy requires that the organization get a current assessment of where they are today, determine what is already in place and deployed, identify redundancies in technology, and find areas that might have been addressed but where the solutions are not scalable or manageable at an enterprise level. The gap analysis is aimed to not only identify the current state but also to help the organization prioritize its roadmap going forward.

One thing is certain – risk and compliance burdens are not going away. Government regulators continue to influence control upon organizational practices through tighter regulation. Business partners are requiring stronger controls within their relationships. The globalization of business introduces significant risk with more points of vulnerability and exposure to the organization. The time is now for organizations to define and implement a sustainable risk and compliance strategy that drives consistency, efficiency, and transparency of risk and compliance across the organization. Selecting the right technology vendors that provide the integration and enterprise control of risk and compliance is a critical step that organizations should not take lightly.

About the Author



Michael Rasmussen, President

Michael Rasmussen is the authority in understanding Governance, Risk, and Compliance (GRC). He is a sought after keynote speaker, author, and collaborator on GRC issues around the world and is noted for being the first analyst to define and model the GRC market for technology and professional services.

With more than 15 years of experience, Michael's objective is to assist organizations in defining GRC processes that are sustainable, consistent, efficient, and transparent. His thought leadership is tuned to:

- Educate GRC professionals within corporations to identify, understand, and analyze GRC strategies, drivers, trends, and best practices;
- Assist technology providers with alignment of their product and marketing strategies to the needs and requirements of GRC professionals; and
- Collaborate with professional service firms on their portfolio of GRC service offerings to better equip them to serve their respective clients.

A leader in understanding risk and compliance standards, frameworks, regulations, and legislation - Michael aims to improve corporate integrity through advancing GRC initiatives. He has served in leading roles in public policy contributions to US Congressional reports and committees, interacted with organizations around the world on GRC, and currently serves on the Leadership Council and Steering Committee of the Open Compliance and Ethics Group. Michael has been quoted extensively in the press and is respected for his commentary on broadcast news channels.

In June 2007, *Treasury & Risk* recognized Michael as one of the 100 most influential people in finance with specific accolades noting his work in "*Governance and Compliance: Saving the Planet and the Corporation.*"

Michael can be contacted at:

+1.888.365.4563 (office)

mrasnussen@corp-integrity.com (email)

<http://blog.corp-integrity.com> (blog)

Corporate Integrity, LLC

Corporate Integrity, LLC is a strategy & research advisory firm providing education, research, and analysis on enterprise governance, risk management, and compliance.

Through ongoing research, interactions, and analytics, Corporate Integrity is the authority in understanding how organizations can foster a culture that “walks the talk” – where integrity is central to governance, risk and compliance (GRC) practices. Corporate Integrity educates organizations and GRC professionals within those organizations on achieving sustainability, consistency, efficiency, and transparency in their corporate GRC practices to maintain a position of integrity aligned with corporate values and business performance.

In addition to helping organizations understand and improve their internal GRC processes, Corporate Integrity assists technology providers and professional service firms in aligning their sales, product, service, and marketing strategies to the requirements of the roles responsible for GRC.

With the deepest GRC expertise and understanding available in the market, Corporate Integrity has developed a range of service offerings to assist organizations, GRC professionals, technology vendors, and professional services firms focused on GRC.

Corporate Integrity, LLC

Tel: +1.888.365.4560

Fax: +1.888.365.4561

Email: research@Corp-Integrity.com

www.Corp-Integrity.com

Thank you for supporting Corporate Integrity's research by purchasing this document. For hard-copy or electronic reprint rights, contact Corporate Integrity research staff at +1.888.365.4560 or research@Corp-Integrity.com.

Please send feedback or ideas to research@Corp-Integrity.com!