



Corporate Integrity, LLC

Strategic Direction in Governance, Risk, & Compliance

RSA, The Security Division of EMC

Developing a Sustainable and Cost Effective IT Compliance Program

April 2008

Prepared By: Michael Rasmussen
President

Corporate Integrity, LLC
Waterford, Wisconsin 53185
Phone: +1.262.534.9188
E-Mail: mrasnussen@Corp-Integrity.com
Web: www.Corp-Integrity.com

Table of Contents

EXECUTIVE SUMMARY	3
COMPLIANCE IMPACTS IT	4
IT SECURITY HAS EVOLVED	5
IT PLAYS A DUAL ROLE IN GOVERNANCE, RISK, AND COMPLIANCE	6
MOVING FROM REACTIVE TO PROACTIVE IT COMPLIANCE	7
PROACTIVE IT COMPLIANCE STREAMLINES IT AND REDUCES COST	8
PROACTIVE IT COMPLIANCE LEADS TO RISK AND REGULATORY INTELLIGENCE	9
PROACTIVE IT COMPLIANCE REQUIRES A COMMON FRAMEWORK	10
DEFINING THE FRAMEWORK.....	10
END GAME OF IT COMPLIANCE – DEFINE ONCE AND COMPLY WITH MANY	11
APPROACHING PROACTIVE COMPLIANCE WITH ISO 27002	11
WHERE DO YOU START IN DEVELOPING A SUSTAINABLE AND EFFECTIVE IT COMPLIANCE PROGRAM?	14
ABOUT THE AUTHOR	16
MICHAEL RASMUSSEN, PRESIDENT	16
CORPORATE INTEGRITY, LLC.....	16
ENDNOTES.....	17

© 2008, Corporate Integrity, LLC. All rights reserved.

This research piece was commissioned by RSA, The Security Division of EMC. RSA, The Security Division of EMC is granted full distribution rights to this research and the material it contains.

Reproduction in any form is strictly prohibited without express permission. For reproduction rights, usage information, and to purchase reprints contact: research@Corp-Integrity.com. Information is based on best available resources. Opinions represent judgment at the time and are subject to change.

www.Corp-Integrity.com

Executive Summary

Complying with laws and regulations is an increasing burden for organizations, from the board of directors down to the trenches of business. Over the past ten years there has been a significant and growing impact of regulatory compliance specifically on the IT department. In a nutshell: business is complex and global, and the demand upon IT to comply with an array of laws and regulations is requiring IT to change and adapt. The compliance challenges burdening IT are legion; this has put IT in an awkward position of reacting to regulations where it should be proactively managing IT controls and risk.

A reactive approach to IT compliance is a recipe for disaster and leads to escalated costs in compliance, lack of visibility of the control environment as a whole, wasted or inefficient use of resources, unnecessary complexity, a lack of flexibility, and vulnerability and exposure.

A proactive approach to compliance means seeing the big picture. Whereas the reactive approach to IT compliance leads to greater exposure, complexity, and higher costs for compliance, a proactive approach to compliance leads to a stronger IT department with reduced risk of exposure and efficient use of resources.

A proactive approach to IT compliance leads to an 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. An effective IT compliance program has to be centered on a single framework and work in harmony with others. The most flexible framework for a proactive approach to IT risk and compliance is ISO/IEC 27002:2005 (ISO 27002). The purpose of a common framework to define the control architecture for an IT compliance program is to define controls once and demonstrate compliance with a range of requirements and regulations. This also allows an organization to continually monitor risk in the dynamic and extended business environment imposed upon business today.

Developing a sustainable and effective IT compliance program is not achieved overnight. An organization needs to have a strategy. Organizations looking to develop a proactive IT compliance program focused on sustainability and effectiveness should follow the following five steps:

1. Establish your IT risk and compliance charter.
2. Develop your IT risk and compliance framework and policy.
3. Assess the current state of IT compliance.
4. Determine the desired state of IT compliance.
5. Measure, assess, and report.

© 2008, Corporate Integrity, LLC. All rights reserved.

This research piece was commissioned by RSA, The Security Division of EMC. RSA, The Security Division of EMC is granted full distribution rights to this research and the material it contains.

Reproduction in any form is strictly prohibited without express permission. For reproduction rights, usage information, and to purchase reprints contact: research@Corp-Integrity.com. Information is based on best available resources. Opinions represent judgment at the time and are subject to change.

www.Corp-Integrity.com

Compliance Impacts IT

Organizations face a broad array of regulatory challenges. Complying with laws and regulations is an increasing burden for them, from the board of directors down to the trenches of business. Regulators across the globe have focused regulations in numerous areas: employment/labor, global trade, anti-corruption, financial/accounting controls – the list goes on. Several industries – such as life sciences, banking, insurance, and utilities – also receive a higher degree of regulatory scrutiny.

Many areas of the business have been impacted by regulatory compliance. Over the past ten years, the impact specifically on the IT department has been significant and growing. The more extended and distributed the business, the more challenging the risk and compliance demands upon IT become. Chief Information Officers (CIOs), along with their Chief Information Security/Risk Officer (CISO/CRO) reports, have become bewildered in trying to manage compliance with a complex array of requirements.

Compliance drivers impacting on IT include:

- **Governance demands.** There is scrutiny as to how business is run. Much of this attention has been focused on financial accounting practices in the wake of regulatory schemes like Sarbanes-Oxley, King II, Turnbull, J-SOX, and EU Directives. Much of the attention upon accounting practices has an effect on IT controls, because IT supports the underlying accounting systems and processes.
- **Information privacy.** Organizations around the world have been bewildered by privacy regulations. Many of these regulations stem from the Organization for Economic Cooperation and Development (OECD) Privacy Principles, with its fruits being found in the EU Directive on Data Protection (95/46/EC, "Directive"), Canada's Personal Information Protection in Electronic Documents Act (PIPEDA), and Japan's Personal Information Protection Act (PIPA). In contrast, the U.S. has not responded with broad sweeping privacy laws and regulations. Instead it has focused attention upon specific verticals such as healthcare and financial services, passing the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach Bliley Act (GLBA). Additionally, a majority of U.S. states have implemented varying, and at times conflicting, degrees of privacy legislation in the form of mandatory disclosure laws.
- **Government oversight.** Regulations typically have not moved IT to respond without the government wielding a stick.ⁱ This has been a significant issue in the U.S. Legislators first passed HIPAA in 1996, but hospitals were slow to respond until the U.S. Health and Human Services (HHS) took action against an Atlanta hospital this past year.ⁱⁱ In the meantime financial services has been quick to respond to similar requirements in GLBA because the U.S. financial regulators have been aggressive in evaluating IT compliance.ⁱⁱⁱ Government organizations, such as the U.S. Federal Trade Commission, have been quick to ensure IT diligence in security and privacy, across vertical markets, through a range of consent decrees. A CISO at one mid-sized bank had an extra desk set up in his office,

© 2008, Corporate Integrity, LLC. All rights reserved.

This research piece was commissioned by RSA, The Security Division of EMC. RSA, The Security Division of EMC is granted full distribution rights to this research and the material it contains.

Reproduction in any form is strictly prohibited without express permission. For reproduction rights, usage information, and to purchase reprints contact: research@Corp-Integrity.com. Information is based on best available resources. Opinions represent judgment at the time and are subject to change.

www.Corp-Integrity.com

because odds were good that, on any given day, a financial regulator was going to be conducting some regulatory review and would need a work space close to his own.

- **Litigation.** The greatest fear of non-compliance does not come from government fines and sanctions. Organizations are dreadfully scared when regulators establish a way of measuring negligence that can be used against them in civil actions. There is a growing concern that the organization may face litigation over data loss and privacy breaches – the peak of this concern is a fear of a potential class-action lawsuit should the loss be widespread across many defendants.
- **Business partners.** Pressure to demonstrate compliance does not come from regulators alone but also from business partners. Organizations are challenged not only to demonstrate their own compliance with laws, but their business partners' compliance as well. Even where regulations are not currently present, there is a growing tendency to ensure that business partners in supply chains can demonstrate an adequate level of security control. A security manager at a leading high-tech manufacturing firm was having difficulty getting his management to buy into the need for intellectual property protection, but he was able to change that perception when he started discussing the intellectual property protection of a significant business partner.
- **Geographic distribution.** It is challenging enough to comply with a complex array of laws and regulations when operations are within a single jurisdiction or country. The task becomes truly daunting as organizations face expanding business, globalization, and a web of business partner relationships distributed around the world. One major retailer is trying to define how it is going to keep up with laws and regulations that change on a regular basis and affect its IT operations in fourteen countries around the world. The matter becomes even more challenging when differing regulatory environments have conflicting requirements, as exemplified over the past few years in the issues raised between Canada's PIPEDA and the U.S. PATRIOT Act.

IT Security Has Evolved

In a nutshell: business is complex and global, and the demand upon IT to comply with an array of laws and regulations is requiring IT to change and adapt.

Security is not just about keeping the hackers, viruses, and worms away – it has evolved into a complexity of risk-management and compliance processes. It involves protecting intellectual property and trade secrets, managing IT compliance, monitoring information risk, and validating controls within business relationships.

This change within IT has caused an evolution in how security is defined and approached within the wider business. Security is evolving from a technical department buried within IT operations to one with significant risk-management and legal acumen – one that not only understands technology but also the business, legal, and risk contexts it operates within. Where yesterday's security manager was a techie, today's manager requires business and legal proficiencies. Traditional IT security departments are now often being referred to as information risk departments.

© 2008, Corporate Integrity, LLC. All rights reserved.

This research piece was commissioned by RSA, The Security Division of EMC. RSA, The Security Division of EMC is granted full distribution rights to this research and the material it contains.

Reproduction in any form is strictly prohibited without express permission. For reproduction rights, usage information, and to purchase reprints contact: research@Corp-Integrity.com. Information is based on best available resources. Opinions represent judgment at the time and are subject to change.

www.Corp-Integrity.com

IT Plays a Dual Role in Governance, Risk, and Compliance

Both business and IT are also responding to a trend of increased collaboration across the business on governance, risk, and compliance (GRC). IT is a significant player in, and enabler of, GRC initiatives within organizations. The role of IT in GRC is a dual role where, on the one hand, IT has to manage its own GRC issues and, on the other hand, IT becomes an enabler and automator of GRC for the business.

This has given rise to an outlook and relationship between enterprise GRC and IT-GRC. Enterprise GRC involves the GRC issues that impact on the business outside of IT – these are the things that keep business executives (e.g., CRO, CCO) up at night but that IT can help to automate and monitor. Then there are the GRC issues that fall in the lap of the CIO and CISO and keep them up at night – that is where IT-GRC starts.

IT risk management/security plays an interesting role today in this GRC dichotomy – it ends up being the intersection point connecting IT-GRC to enterprise GRC.

© 2008, Corporate Integrity, LLC. All rights reserved.

This research piece was commissioned by RSA, The Security Division of EMC. RSA, The Security Division of EMC is granted full distribution rights to this research and the material it contains.

Reproduction in any form is strictly prohibited without express permission. For reproduction rights, usage information, and to purchase reprints contact: research@Corp-Integrity.com. Information is based on best available resources. Opinions represent judgment at the time and are subject to change.

www.Corp-Integrity.com

Moving From Reactive to Proactive IT Compliance

The compliance challenges burdening IT are legion – and this has put IT in an awkward position of reacting to regulations where it should be proactively managing IT controls and risk. In order for IT security to play an efficient and effective role in IT compliance, it becomes necessary that IT builds a solid foundation to manage and automate IT risk and compliance processes.

A reactive approach to IT compliance is a recipe for disaster and leads to:

- **Escalated costs in compliance.** When the organization is busy putting out individual fires of IT compliance, costs begin to skyrocket. Money is thrown at individual issues to keep the auditors and regulators at bay, with no thought as to how those resources could be spent wisely to meet a range of IT compliance needs. No one is seeing the big picture and looking towards ‘fire prevention’ through a proactive approach to IT compliance.
- **Lack of visibility.** A reactive approach to compliance leads to siloed compliance initiatives that never see the big picture. No one is thinking about how IT controls could be architected to meet a range of compliance needs. The result is poor visibility across the IT organization and its control environment, with no consistent framework or architecture for managing controls within.
- **Wasted or inefficient use of resources.** Silos of IT compliance lead to wasted resources. Instead of leveraging controls and resources to meet a range of compliance needs, they are developed independently with no thought for leverage. The IT department ends up with different internal processes, systems, controls, and technologies to meet compliance. Many of these processes and controls could have been streamlined with a common framework approach to IT risk and compliance control.
- **Unnecessary complexity.** Varying IT compliance approaches introduce greater complexity to IT. With complexity comes an inherent increase in risk. Complexity probably means that controls are not streamlined or managed consistently, and it introduces more points where controls can fail. Inconsistency in controls also means inconsistency in documentation of those controls: which further confuses IT, regulators, and business partners.
- **Lack of flexibility.** Complexity causes inflexibility. The IT organization becomes so wrapped up in spinning a multitude of compliance plates that IT performance, development, and support of the business is degraded. Developers and the business become bewildered in a maze of varying approaches 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 further fruit of complexity: everyone is focused on their silo of compliance and no one sees the big picture. No one is looking at controls holistically. The focus is on what is immediately before

© 2008, Corporate Integrity, LLC. All rights reserved.

This research piece was commissioned by RSA, The Security Division of EMC. RSA, The Security Division of EMC is granted full distribution rights to this research and the material it contains.

Reproduction in any form is strictly prohibited without express permission. For reproduction rights, usage information, and to purchase reprints contact: research@Corp-Integrity.com. Information is based on best available resources. Opinions represent judgment at the time and are subject to change.

www.Corp-Integrity.com

them, not on what the business needs to do to protect itself in the long run. Varying and independent IT compliance efforts lead to difficulty in demonstrating enforcement and audit compliance.

The preceding issues of a reactive approach to IT compliance build upon one another. The lack of visibility leads to wasted and inefficient use of resources. Wasted resources, because of varying approaches to IT compliance, lead to complexity. Complexity and inflexibility result in greater vulnerability and exposure for the organization.

Proactive IT Compliance Streamlines IT and Reduces Cost

A proactive approach to compliance involves seeing the big picture – seeing the forest past the trees. Whereas the reactive approach to IT compliance leads to greater exposure and complexity, a proactive approach to compliance leads to a stronger IT department with reduced risk of exposure.

Organizations looking to build a proactive IT compliance program can expect to manage IT compliance costs through:

- **Sustainability.** IT compliance demands are not getting simpler – they are growing in number and complexity. Compliance is no longer about an annual audit; it now involves continual monitoring as business changes. Business changes rapidly – particularly within the IT department. Users are added, they change roles, and they leave. New business partner connections are established – others are torn down. IT infrastructure and applications are patched and configurations change. Compliance needs to be an ongoing part of IT processes. This is only possible if the organization has a strategic approach to managing controls across compliance initiatives. A proactive approach to monitoring and enforcing compliance leads to sustainable IT risk management and compliance.
- **Consistency.** A proactive approach to IT compliance builds a foundation for consistency of compliance controls across the enterprise. The big picture is kept in view. The proactive IT compliance program maps controls into a common framework, leveraging existing implemented controls, and avoiding redundant controls and processes. This leads to an organization that finds compliance easier to approach, interpret, and manage.
- **Efficiency.** Consistency leads to efficiency. As the organization looks to leverage existing IT controls and processes for the sake of consistency, there is a reduction in resources needed to meet compliance requirements. The business also finds compliance to be easier, because it has a consistent view into IT compliance processes and faces reduced demands for IT compliance assessments.
- **Transparency.** A proactive IT compliance program built upon a common framework for IT compliance leads to greater transparency. Reporting on compliance becomes a streamlined process rather than a maze of reports on redundant and inconsistent approaches to compliance.

© 2008, Corporate Integrity, LLC. All rights reserved.

This research piece was commissioned by RSA, The Security Division of EMC. RSA, The Security Division of EMC is granted full distribution rights to this research and the material it contains.

Reproduction in any form is strictly prohibited without express permission. For reproduction rights, usage information, and to purchase reprints contact: research@Corp-Integrity.com. Information is based on best available resources. Opinions represent judgment at the time and are subject to change.

www.Corp-Integrity.com

Proactive IT Compliance Leads to Risk and Regulatory Intelligence

A proactive approach to IT compliance leads to an 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. Risk and regulatory intelligence is a key component of proactive IT compliance as organizations aim at getting ahead of the regulatory environment.

Reactive organizations don't know what the next set of regulations will look like. In the absence of a proactive compliance program, they are forced to respond in one of two ways:

1. React to new requirements as they appear, or
2. Be taken off guard by something of which they are completely unaware.

Organizations with a proactive IT compliance program are looking to where things are heading. They understand the short-term tactical issues but also have the ability to look towards the long-term strategic issues. A proactive compliance program continually monitors the external environment that impacts on its business, such as pending legislation, court cases, geo-political risks, and new threats appearing on the horizon. This makes IT a valuable element of enterprise risk management. IT is an enabler that proactively assists the organization to deal with whatever may come.

© 2008, Corporate Integrity, LLC. All rights reserved.

This research piece was commissioned by RSA, The Security Division of EMC. RSA, The Security Division of EMC is granted full distribution rights to this research and the material it contains.

Reproduction in any form is strictly prohibited without express permission. For reproduction rights, usage information, and to purchase reprints contact: research@Corp-Integrity.com. Information is based on best available resources. Opinions represent judgment at the time and are subject to change.

www.Corp-Integrity.com

Proactive IT Compliance Requires a Common Framework

A good house is built upon a solid foundation. In the case of IT compliance, a proactive approach requires a solid foundation built upon a common framework. If everyone building a particular house had a different blueprint, the result would be a disaster. The way to achieve IT compliance sustainability, consistency, efficiency, and transparency is to architect IT control and compliance processes upon a common architectural framework.

From an enterprise point of view, there is no one framework that can meet the full range of compliance needs across the organization. For an organization to achieve a vision of GRC that spans the enterprise, it is necessary for the IT compliance framework to fit into other business frameworks – such as the COSO Internal Control and Enterprise Risk Management Frameworks, or the Australia/New Zealand 4360:2004 standard, varying ISO standards, as well as frameworks used by auditors. What is achieved is not a single framework, but a hierarchy of frameworks built to work in harmony with each other.

Not only does an IT compliance framework need to work with risk-management and compliance frameworks within the business, it also needs to work with related frameworks within IT. The frameworks related to IT-GRC include:

- **ISO/IEC 27002:2005.** This is the leading framework used for managing IT risk and compliance and has the broadest approach and acceptance.
- **COBIT.** Provides the framework most favored by auditors. For IT risk management and compliance to be effective it is necessary that the IT framework show relationships to COBIT control objectives.
- **ITIL.** Delivers a structure for managing and delivering IT processes.

Defining the Framework

While there are different but related frameworks involved in an expansive view of IT-GRC, an effective IT compliance program has to be centered on a single framework and work in harmony with the rest.

The most flexible framework to date for a proactive approach to IT risk and compliance is ISO/IEC 27002:2005 (ISO 27002). Organizations should consider building their IT risk and compliance programs upon ISO 27002 because it:

- **Offers the greatest flexibility.** The standard was not built for a single purpose, industry, or size of organization. It offers IT organizations a significant amount of flexibility to define how compliance operates within an organization's unique demands.

© 2008, Corporate Integrity, LLC. All rights reserved.

This research piece was commissioned by RSA, The Security Division of EMC. RSA, The Security Division of EMC is granted full distribution rights to this research and the material it contains.

Reproduction in any form is strictly prohibited without express permission. For reproduction rights, usage information, and to purchase reprints contact: research@Corp-Integrity.com. Information is based on best available resources. Opinions represent judgment at the time and are subject to change.

www.Corp-Integrity.com

- **Avoids being prescriptive.** It was built to give guidance on how to see the big picture, while recognizing that different organizations of varying cultures, industries, and size will have varying requirements for IT risk and compliance management.
- **Provides a common approach.** ISO 27002 is internationally recognized and used by a variety of organizations around the world. This is significant for organizations that are impacted by the extended enterprise while managing a range of business partner connections and relationships. A common framework to define and assess compliance between business partners is critical.
- **Utilizes best practices.** ISO 27002 is focused on structure and best practice. It gives guidance by defining control structure and implementation guidance.
- **Emphasizes the need for risk assessment.** Compliance involves assessing risk. The regulatory environment has moved away from a focus on checking boxes to a focus on organizations demonstrating that they understand their internal and external operational environments and that they manage compliance in proportion to the risk they face.^{iv}
- **Offers a certification track.** For those inclined to seek a certification of compliance with a framework, ISO 27002 has a corresponding certification standard in ISO/IEC 27001.

End Game of IT Compliance – Define Once and Comply with Many

The purpose of a common framework defining the control architecture for an IT compliance program is to define controls once and demonstrate compliance with a range of requirements and regulations. This also allows an organization to monitor risk continually in the dynamic and extended business environment faced by organizations today.

Utilizing ISO 27002, an organization should aim to map the controls defined within the framework to compliance requirements in the regulatory environment, as well as to requirements stemming from corporate policies and procedures. The organization monitors the IT control environment to make sure that risk is managed within the boundaries of risk tolerance and risk appetite.

Approaching Proactive Compliance with ISO 27002

ISO 27002 provides the ideal structure for defining a complete set of IT controls. Organizations find the standard is thorough in its breadth while giving them the flexibility to adapt it to their specific requirements.

- **Risk Assessment and Treatment.** The strength of ISO 27002 starts with its initial focus on the need for risk assessment and treatment. For IT controls to be effective in managing, mitigating, and avoiding IT risk, it is necessary that an understanding of risk be established. Only from an understanding of the risk the business faces can appropriate controls be selected to manage and mitigate that risk. Regulatory guidance also requires that risk assessment processes be established. A proactive compliance program is one that is continually assessing and treating risk.

© 2008, Corporate Integrity, LLC. All rights reserved.

This research piece was commissioned by RSA, The Security Division of EMC. RSA, The Security Division of EMC is granted full distribution rights to this research and the material it contains.

Reproduction in any form is strictly prohibited without express permission. For reproduction rights, usage information, and to purchase reprints contact: research@Corp-Integrity.com. Information is based on best available resources. Opinions represent judgment at the time and are subject to change.

www.Corp-Integrity.com

- **Security Policy.** Accountability for security and IT controls is not for IT alone – it extends in some capacity to every user in the environment. ISO 27002 provides a solid foundation for managing IT risk and controls by delivering guidance on the structure of a broad information security policy that is supported by management while being communicated and attested to by the range of users in the environment. The security policy document should be maintained and reviewed on a regular basis to make sure it is consistent with changing requirements within the business. It is this document that sets the context for the definition and enforcement of IT controls for compliance. A proactive compliance program is one that has a defined and communicated policy.
- **Organization of Information Security.** ISO 27002 provides the context for the management of information security by empowering the security organization to define and enforce IT controls and compliance. This includes management's support and commitment to information security, allocation of responsibilities, and relationships with internal and external parties.
- **Asset Management.** Fundamental to compliance is the definition of controls within the context of protecting organizational assets. ISO 27002 lays the foundation for IT compliance by defining responsibility for, or ownership of, assets; as well as the requirements for maintaining an ongoing inventory of both tangible and intangible assets – such as hardware, software, information, and business relationships. When assets are defined properly, they can then be classified or labeled: compliance requirements and supporting controls can be mapped to their specific contexts and relationships. A proactive compliance program is one that understands the range of organizational assets and has mapped controls and requirements to those assets.
- **Human Resources Security.** The human element is the hardest factor to control in IT security. ISO 27002 lays the framework for compliance by clearly defining the need to address roles and responsibilities for IT security, risk, and compliance across the user base. This includes employees, contractors, third parties, and even temporary workers. All users should understand policy and be adequately trained in their roles and responsibilities. The standard also gives guidance for the control of access rights throughout the relationship process – from hiring through termination of contract. A proactive compliance program is one that recognizes that the human element is the greatest risk to compliance, and communicates, manages, and controls compliance within the context of employment and business relationships.
- **Physical and Environmental Security.** The security and control of IT hardware, software, and information is subject to the security of the broader physical environment. ISO 27002 recognizes this dependency and provides guidance to secure the physical environment and assets of the organization and to provide for environmental protection and precautions. A proactive compliance program is one that will enable a holistic view of controls that spans physical and logical protection of corporate assets.
- **Communications and Operations Management.** A majority of IT control and compliance requirements deal with the details of managing IT operations and the broader communication environment. ISO 27002 provides guidance on the control within IT operations, development,

© 2008, Corporate Integrity, LLC. All rights reserved.

This research piece was commissioned by RSA, The Security Division of EMC. RSA, The Security Division of EMC is granted full distribution rights to this research and the material it contains.

Reproduction in any form is strictly prohibited without express permission. For reproduction rights, usage information, and to purchase reprints contact: research@Corp-Integrity.com. Information is based on best available resources. Opinions represent judgment at the time and are subject to change.

www.Corp-Integrity.com

testing, backup procedures, configuration management, and communications/networking. A proactive compliance program is one that monitors the communications and operations environments and makes sure that proper controls and segregation of duties are in place within IT operations.

- **Access Control.** The heart of IT compliance is: “*who* has access to *what*?” Access control is an essential component of ISO 27002. It addresses the controls of user provisioning, the granting and reviewing of access to information and systems, the revocation of access, user authentication, and privilege management. A proactive compliance program monitors and enforces access controls within IT infrastructure and applications.
- **Information Systems Acquisition, Development, and Maintenance.** Controls that are integrated into IT (as opposed to control 'band-aids') are more effective. ISO 27002 enforces compliance by providing a control perspective throughout the IT acquisition, development, and maintenance processes. A proactive compliance program identifies exposure points and vulnerabilities in the acquisition and development stages; and implements controls to meet compliance requirements and control risk before systems are deployed.
- **Information Security Incident Management.** The best-laid control plans are still susceptible to occasional failure. Compliance programs are often measured on the ability of the organization to detect and respond swiftly to violations of controls and to unethical conduct. The organization that does not have a response plan in place is headed for serious compliance difficulties. ISO 27002 provides a holistic perspective on reporting, managing, and investigating incidents within the IT environment. A proactive compliance program is one that is ready to respond when control violations or malicious behavior are reported.
- **Business Continuity Management.** A significant compliance and control point is the ongoing availability of systems to provide for the continuity of business operations. ISO 27002 manages risk and controls by establishing proper procedures for disaster preparedness and disaster recovery. A proactive compliance program is one in which the organization has established business continuity plans and remains agile in the face of incidents and disasters.
- **Compliance.** ISO 27002 directly addresses the oversight and management of compliance with legal, business, and technical requirements. The protection of personal information and intellectual property are critical components of IT control. A proactive compliance program is one in which compliance enforcement and monitoring plans are in place for the range of IT controls established within the ISO 27002 framework.

© 2008, Corporate Integrity, LLC. All rights reserved.

This research piece was commissioned by RSA, The Security Division of EMC. RSA, The Security Division of EMC is granted full distribution rights to this research and the material it contains.

Reproduction in any form is strictly prohibited without express permission. For reproduction rights, usage information, and to purchase reprints contact: research@Corp-Integrity.com. Information is based on best available resources. Opinions represent judgment at the time and are subject to change.

www.Corp-Integrity.com

Where Do You Start in Developing a Sustainable and Effective IT Compliance Program?

A sustainable and effective IT compliance program cannot be developed overnight. An organization needs to have a strategy. Organizations looking to develop a proactive IT compliance program focused on sustainability and effectiveness should follow these five steps:

1. **Establish your IT risk management and compliance charter.** A proactive IT compliance program starts with understanding what IT is trying to achieve. The organization is best served by first establishing the vision, mission, and principles for IT risk management and compliance.

Part of this charter process is also identifying the roles involved in IT risk management and compliance. Because IT enables much of the business, business liaisons should be engaged in to define the IT charter for risk management and compliance. This should include the roles of audit, finance, line-of-business, developers, architecture, corporate compliance, enterprise risk, and physical security as stakeholders in developing a proactive IT risk management and compliance charter.

2. **Develop your IT risk management and compliance framework and policy.** After establishing your IT risk management and compliance charter, the next step is selecting your framework for IT risk management and compliance. As discussed, ISO 27002 is the most agile and thorough framework for managing IT risk and compliance within the IT department.

Link IT governance and compliance requirements to the framework, as well as existing IT policies, procedures, and controls. IT controls should be cataloged within the framework and cross-referenced to information classes for structured and unstructured information.

3. **Assess the current state of IT compliance.** The next step is to understand where you are. In order to move from reactive IT compliance to a proactive program that is sustainable and effective, it is necessary to understand the current state of the IT control environment, processes, and applications. Organizations are to inventory and assess their structured and unstructured information assets as part of the assessment process so that controls can be applied appropriately.
4. **Determine the desired state of IT compliance.** Working from the current state assessment, the organization can determine gaps in controls, as well as identifying overlapping but varying controls and processes, in order to begin laying the foundation for a roadmap towards proactive compliance.

The organization should implement an action plan to address control gaps or deficiencies and build out IT controls and processes in order to meet compliance with the vision and align with

© 2008, Corporate Integrity, LLC. All rights reserved.

This research piece was commissioned by RSA, The Security Division of EMC. RSA, The Security Division of EMC is granted full distribution rights to this research and the material it contains.

Reproduction in any form is strictly prohibited without express permission. For reproduction rights, usage information, and to purchase reprints contact: research@Corp-Integrity.com. Information is based on best available resources. Opinions represent judgment at the time and are subject to change.

www.Corp-Integrity.com

ISO 27002. To move towards a state of proactive IT compliance, this stage of the process involves identifying priorities, projects, budgets, and ownership.

5. **Measurement, assessment, and reporting.** Business is dynamic and in a state of flux – therefore a proactive IT compliance program is one that is continually monitoring the external and internal business environments to measure, assess, and report on the state of compliance. Every control point within the ISO 27002 framework should have key control and risk indicators through which the organization can monitor overall compliance and enforcement.

© 2008, Corporate Integrity, LLC. All rights reserved.

This research piece was commissioned by RSA, The Security Division of EMC. RSA, The Security Division of EMC is granted full distribution rights to this research and the material it contains.

Reproduction in any form is strictly prohibited without express permission. For reproduction rights, usage information, and to purchase reprints contact: research@Corp-Integrity.com. Information is based on best available resources. Opinions represent judgment at the time and are subject to change.

www.Corp-Integrity.com

About the Author

Michael Rasmussen, President

Tel: +1.888.365.4563

Email: mrasmusen@Corp-Integrity.com

Blog: <http://corp-integrity.blogspot.com>

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 services 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, 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."

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.

© 2008, Corporate Integrity, LLC. All rights reserved.

This research piece was commissioned by RSA, The Security Division of EMC. RSA, The Security Division of EMC is granted full distribution rights to this research and the material it contains.

Reproduction in any form is strictly prohibited without express permission. For reproduction rights, usage information, and to purchase reprints contact: research@Corp-Integrity.com. Information is based on best available resources. Opinions represent judgment at the time and are subject to change.

www.Corp-Integrity.com

Endnotes

ⁱ The regulatory environment burden is not getting any easier. The Wall Street Journal reported on the increased regulatory environment within the current state of politics – Monday, March 24, 2008 “Political Pendulum Swings Toward Stricter Regulation”

(http://s.wsj.net/article/SB120631764481458291.html?mod=fpa_whatsnews)

ⁱⁱ Computer World covers this story about Atlanta’s Piedmont Hospital in the article “HIPAA: The 42 Questions HHS Might Ask”

(<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9025253&pageNumber=1>)

ⁱⁱⁱ The US financial regulators include the Federal Reserve Board, Office of the Comptroller of the Currency, National Credit Union Association, Federal Depository Insurance Corporation, and the Office of Thrift Supervision. Together they form the Federal Financial Institutions Examination Council (www.ffiec.gov) and have developed over a dozen regulator handbooks for examiners to use in evaluating IT compliance.

^{iv} “Principles-based regulation is essentially about outcomes or ends while rules-based regulation is about means. Principles-based regulation allows firms to decide how best to achieve required outcomes and, as such, it allows a much greater alignment of regulation with good business practice A more principles-based approach allows [organizations] increased scope to choose how they go about this. In short, the use of principles is a more grown-up approach to regulation than one that relies on rules.” Source: John Tiner, “Principles based regulation: the EU context” (http://www.fsa.gov.uk/pages/Library/Communication/Speeches/2006/1013_jt.shtml). “Our rules-based regulatory system is prescriptive and leads to greater focus on compliance with specific rules. We should move toward a structure that gives regulators more flexibility to work with entities on compliance within the spirit of regulatory principles.” Source: Hank Paulson, US Treasury secretary, speech to the Economic Club of New York in November 2006.

© 2008, Corporate Integrity, LLC. All rights reserved.

This research piece was commissioned by RSA, The Security Division of EMC. RSA, The Security Division of EMC is granted full distribution rights to this research and the material it contains.

Reproduction in any form is strictly prohibited without express permission. For reproduction rights, usage information, and to purchase reprints contact: research@Corp-Integrity.com. Information is based on best available resources. Opinions represent judgment at the time and are subject to change.

www.Corp-Integrity.com