

Prepared By:



Michael Rasmussen
*Risk & Compliance
 Lecturer, Writer, & Advisor*

Effective management of compliance requires data and visibility across the business. This requires that the organization deploy an infrastructure and supporting processes that deliver real-time compliance transparency across the business and its relationships.

www.Corp-Integrity.com
 research@Corp-Integrity.com
 +1.888.365.4560

Foundations of GRC: Streamlining Compliance

Executive Summary

Organizational exposure to compliance risk is rising while the cost of compliance soars. Additionally, the ad hoc, reactive approach to compliance brings complexity, forcing business to be less agile. Organizations typically address compliance as singular issues and obligations; as a result they have multiple initiatives working in isolation to respond to each regulatory requirement. These isolated compliance initiatives tend to rely on manual processes burdened with costly assessments managed through spreadsheets, often proving costly and unreliable. This modus operandi is not proactive and makes it difficult to adapt to new regulatory requirements while increasing pressure and anxieties on management, employees, and business relationships.

Without a holistic and streamlined view of compliance, organizations will continue to be burdened with the data overload and complexity of compliance data for management reporting. Organizations need complete visibility into a portfolio of compliance obligations spread across distributed, complex business processes and relationships.

Table of Contents

- Executive Summary 1
- Organizations strain under the burden of regulations2
 - Ad hoc compliance no longer works.....3
 - Streamlining compliance management4
- Develop a streamlined regulatory framework and architecture.....4
 - Value achieved in an integrated risk-based approach to compliance5
 - Structure the regulatory framework.....6
 - Build an integrated compliance platform6
- Conclusion7
- About this paper8
- About Corporate Integrity8
- About Michael Rasmussen8

Compliance management is ultimately about maintaining oversight and control of business processes, transactions, relationships, and information. Organizations are beginning to provide an integrated view across specific compliance requirements that roll up into a broader compliance management program.

Success in compliance management begins with a strategy – how to effectively manage compliance across the organization. Ultimately, the organization needs to identify and prioritize major risks resulting from regulatory mandates as well as maintain oversight and control over business processes to mitigate these risks. This requires the organization to deploy an infrastructure and supporting processes that deliver real-time compliance transparency across the business and its relationships. A streamlined compliance architecture is one in which accountability and compliance are effectively managed and the business has a system of record to understand and manage the diverse complexity of compliance issues.

By integrating a common regulatory and control framework with other business applications, an organization can deliver automation in control monitoring and remediation processes. This integration results in efficiency of controls and minimizing the time between the occurrence of an issue (control failure, fraud incident, etc.) and its identification, thus reducing overall risk and minimizing future issues. It allows issues to be detected quickly and dealt with in a timely manner, and provides better visibility on compliance risks across different mandates and methods of mitigation. Failures can be treated individually as well as aggregated to track areas of weakness and to implement remediation more efficiently.

The outcome is an organization delivering streamlined compliance management through control optimization that enables and does not encumber corporate performance.

Organizations strain under the burden of regulations

As regulations increasingly burden business, the average executive remains unaware as to just how burdensome they have become. It appears nearly impossible to get a full understanding of regulatory impact upon business. The Competitive Enterprise Institute reports that U.S. federal regulatory compliance costs hit an estimated \$1.157 trillion in 2007.¹ This is just one trajectory of the burden business has to bear in regulatory compliance. This figure does not include U.S. state and local regulations, nor does it include the impact of regulations from other countries around the world. Business is dynamic and global; maintaining regulatory compliance across distributed business operations and relationships around the world remains an elusive goal for many organizations. Organizations face regulations that at times can be harmonized, yet in other situations they conflict (as with conflicting data privacy and whistleblower rules between the United States and European Union).

In most countries and industries, regulations are continuously multiplying and evolving – putting increased pressure on companies to keep up and to maintain compliance. Organizational exposure to compliance risk is rising while the cost of compliance soars. Additionally, the ad hoc, reactive approach to compliance brings complexity, forcing business to be less agile.

The burden of compliance upon business includes:

- **Horizontal (cross-industry) obligations.** Companies need to comply with “horizontal” regulations for compliance that span vertical industries. These include areas of listing requirements, financial governance (for example, Sarbanes-Oxley, E.U. 8th Company Law Directive), employment/labor laws, anti-corruption, and privacy.
- **Vertical obligations.** Organizations face industry-specific regulatory requirements. Financial service organizations are driven to enhance risk management while complying with Basel II, “know your customer” or anti-money-laundering laws, transaction monitoring, and other requirements. Life sciences organizations are encumbered with oversight across research, clinical trials, manufacturing, sales, and marketing.² Utilities face mounting regulations across opera-

1 The \$1.157 trillion federal regulatory burden is calculated by economist Mark Crain, and is referenced in the Competitive Enterprise Institute’s report “Ten Thousand Commandments: An Annual Snapshot of the Federal Regulatory State,” 2008 Edition by Clyde Wayne Crews Jr. (http://cei.org/cei_files/fm/active/0/10KC_2008_FINAL_WEB.pdf)

2 Global pharmaceutical companies strictly regulated under the FDA in the US (21CFR...) and local equivalents in many developed countries. They are also increasingly subjected to environmental, health, and safety regulations and often comply with financial mandates such as SOX in parallel.

tions and distribution.³ Other industries face growing regulatory pressure in global trade, environmental, health and safety, quality, and more.

- **Contractual obligations.** Business relationships have become increasingly complex as business has become distributed and global. Organizations have a complex web of business relationships comprised of business partners, supply chain, outsourcers, service providers, and contractors. Where an organization might not have had a regulatory requirement, they are finding one is imposed on them because of a business relationship. Organizations face significant risks to their reputation and brand when their business partners fail in compliance – such as the case with Nike⁴ and Primark⁵ when they have struggled with child labor issues across business relationships.
- **Strategic objectives.** Compliance and control is more than just meeting regulatory requirements; it is about maintaining visibility and control of the organization so that the organization can meet business objectives. Strategic objectives as well as regulatory requirements define an organization's culture that is portrayed in its policies, procedures, and control environment. Organizations need not only to properly identify controls, but also to understand that there is a point of over-control as well as under-control. Streamlining compliance involves finding the right balance of control (for example, risk versus cost of control), and integrating and automating controls within business processes to relieve the burden of control on the business while maintaining its benefits. Optimized controls deliver value in mitigating risk (for example, fraud) through prevention or timely detection – keeping the organization on track to hit strategic objectives.

Ad hoc compliance no longer works

Organizations typically address compliance as singular issues and obligations; as a result they have multiple initiatives working in isolation to respond to each regulatory requirement. These isolated compliance initiatives tend to rely on manual processes burdened with costly assessments managed through spreadsheets, often proving costly and unreliable. This modus operandi is not proactive and makes it difficult to adapt to new regulatory requirements while increasing pressure and anxieties on management, employees, and business relationships.

Approaching aspects of compliance as isolated programs is a significant concern, and one that needs to be addressed. Compliance information and processes house some of the most sensitive and critical information of an organization. Those relying on manual processes supported by desktop applications as their compliance backbone will find that their compliance program:

- **Lacks integrity.** How can you ensure that the manual process or ad hoc application has complete and accurate information, functions consistently as intended, and is protected from inappropriate change? Did someone change his or her response at a later date to cover a trail?
- **Misses on nonrepudiation.** Can you be sure that the person who answered a control or compliance question really was that person?
- **Does not deliver business continuity.** Do you have effective backup procedures so that compliance is not at risk in the event the desktop data is lost?
- **Suffers with data overload.** Can you adequately integrate, digest, and report on the volume of individual files from manual processes?
- **Is highly inefficient.** How do you demonstrate that compliance does not constrain the business by introducing bottlenecks and inefficiency?

³ In the United States alone, that can involve complying with requirements from the NERC (Nth American Electric Reliability Corp.), FERC (Federal Energy Regulation Commission), NRC (Nuclear Regulatory Commission), EPA (Environmental Protection Agency) and OSHA (Occupational Safety and Health Administration).

⁴ <http://www.independent.co.uk/news/world/americas/nike-admits-to-mistakes-over-child-labour-631975.html>.

⁵ <http://www.guardian.co.uk/business/2008/jun/23/primark.children>.

Organizations have struggled with as many as 40,000 spreadsheets for a single compliance purpose. Managing this volume of data overload while maintaining nonrepudiation, audit trail, and integrity has become infeasible. The growing number of audit exceptions that companies face around these issues and the cost of going back to validate compliance is causing organizations to reconsider their approach. They are starting to look for ways to drive economies into compliance while increasing the integrity of compliance processes. Further, the fragmented approach does not provide the visibility management needs into key risks and – due to the absence of a consolidated view – into areas of weakness in the organization, which accumulate control failures across different areas of compliance.

Some organizations have invested in specialized software for specific types of compliance, which is better than relying on spreadsheets. However, this still maintains a level of fragmentation when different specialized applications are not integrated and do not scale across the enterprise. Without a holistic and streamlined view of compliance, organizations will continue to be burdened with the data overload and complexity of compliance data for management reporting.

Streamlining compliance management

Organizations are in an ongoing effort to achieve sustainability, consistency, transparency, accountability, and efficiency across compliance initiatives. In fact, organizations need complete visibility into a portfolio of compliance obligations spread across distributed, complex business processes and relationships. Regulatory compliance has a large impact on the ability of organizations to produce and deliver goods and services to clients profitably.

Old paradigms of managing compliance do not work. Tackling each compliance requirement as a single entity is doomed to failure. This method introduces greater risk as the organization lacks visibility across silos within the business. Failure to understand the interrelationship of compliance obligations and risk causes greater uncertainty in business and increasing exposure to loss. The organization is quickly beaten down and defeated, realizing it cannot keep up with growing compliance burdens in a fiercely competitive, global, distributed, and risky business climate.

Develop a streamlined regulatory framework and architecture

Compliance management is ultimately about maintaining oversight and control of business processes, transactions, relationships, and information. Organizations are beginning to move beyond managing compliance as separate processes with little oversight to a streamlined compliance program that has a common process and technology architecture. Their goal is to provide an integrated view across specific compliance requirements that roll up into a broader compliance management program.

One of the most difficult tasks in compliance is the apparently simple one of knowing what one must comply with. Someone has to own the identification of new or changed compliance requirements. Someone needs to take responsibility for determining the impact on the organization (which may affect existing compliance requirements), establish ownership, assess the risk of noncompliance, and manage the response. The next tough task then relates to communicating and training everybody who has to know or comply with the new requirements.

Success in compliance management begins with a strategy: how to effectively manage compliance across the organization. The seven core elements of a compliance management strategy are:⁶

1. **Established compliance standards and procedures.** Policy and procedure development, control definition, workflow, and accountability management
2. **Organizational leadership.** Enterprise visibility and reporting, system of record, and accountability and responsibility for compliance

⁶ Adapted from the United States Sentencing Commission Organizational Sentencing Procedures compliance requirements.

3. **Delegation of authority/screening.** Screening and provisioning controls, procedures around authorizations and access, as well as role and responsibility management
4. **Training and education.** Role-based policy and procedure attestations, delivery of e-learning modules, and surveys
5. **Monitoring and auditing.** Monitoring of performance, ongoing control assessment, reporting across standardized risk and control frameworks, and action-items management
6. **Enforcement.** A single core process for enforcing controls and managing events
7. **Response and improvement.** Ongoing analysis of loss, root cause analysis, and accountability management

Value achieved in an integrated risk-based approach to compliance

Surrounding all seven core elements is risk management. Ultimately, the organization needs to identify and prioritize major risks resulting from regulatory mandates as well as maintain oversight and control over business processes to mitigate these risks.

This requires the organization to deploy an infrastructure and supporting processes that deliver real-time compliance transparency across the business and its relationships. Today, organizations manage compliance in different systems and with spreadsheets that are not integrated, resulting in a struggle to get a full picture of compliance and the risk it represents to the organization. Developing a strategic and integrated approach to compliance management aims to achieve:

- **Sustainability.** Business requires a sustainable process and infrastructure for ongoing management of compliance on a continuous basis. Compliance risk is highly volatile and requires continuous monitoring and validation. The dynamic nature of business, supply chains, and relationships demands that an organization develop a sustainable compliance management program.
- **Consistency.** Compliance has historically been managed ineffectively across silos that do not integrate into a holistic view of compliance risk. The complexity of business requires that compliance management be part of an integrated compliance management architecture.
- **Efficiency.** The line of business is fighting back because of redundant and nonintegrated compliance processes that handicap operational objectives. Streamlined compliance aims to ease the burden leveraging common control monitors, processes, assessments, and information.
- **Transparency.** Ultimately compliance management needs to require greater transparency into key risk indicators so that the organization can monitor its compliance health, enhance corporate culture, avoid fraud, and avert or mitigate infractions.
- **Accountability.** In the end, someone is accountable for managing compliance. The organization brings all of this together to measure the effectiveness of compliance management and to provide accountability (whether positive or negative) to those who oversee it.

A streamlined compliance architecture is one in which accountability and compliance are effectively managed and the business has a system of record to understand and manage the diverse complexity of compliance issues. Companies can better respond to the multiplication of regulations and the constant evolution of their regulatory environment by putting in place a central compliance framework to do the following:

- **Structure regulatory information.** By developing a regulatory framework, an organization can get a holistic and transparent view of the requirements it faces. This framework should map requirements, controls, risks, and policies within the environment. This allows the organization to systematize regulation information by providing a centralized and cross-referenced framework of all relevant compliance documentation and structure. This facilitates the identification and management of compliance requirements and maps the content to controls, ensuring that compliance can be

enforced and maintained in a dynamic business environment. The goal is to bring together all mandates, whether they are regulatory or internal policies, and map them to controls in order to maximize efficiency in compliance.

- **Assign accountability.** Organizations are to develop an accountability matrix for compliance. This matrix takes each requirement and identifies who is responsible for compliance to ensure that there are no gaps in compliance control and that there is a focus on reducing redundancy in controls and compliance processes.
- **Optimize compliance through a risk-based approach.** Using a process to evaluate and prioritize compliance risks helps optimize compliance management while ensuring that there are adequate (and not excessive) controls in place to address risks. The intent is to manage compliance risk through mitigation and avoidance of risks that are inherent to the lack of controls, duplicated controls, or poorly defined controls in the business environment. This approach also allows the organization to utilize corporate resources to invest in controls in the most critical areas of exposure.
- **Architect an integrated compliance platform.** Using a strong, integrated governance, risk, and compliance system provides an integrated compliance and control platform that leverages technology to automate the monitoring, testing, and enforcement of compliance controls within the environment. Automating the testing of controls and implementing continuous monitoring procedures is a powerful means of reducing risks as well as the cost of compliance.

Structure the regulatory framework

Streamlining compliance efforts begins by managing regulatory risks, controls, and actions. The idea is to maximize synergy between compliance initiatives while leveraging compliance processes, technologies, and best practices across the business. This involves the following three steps:

1. **Gather relevant content** and store it centrally, with an understandable structure that identifies and links relevant components. For example, for each regulation this means identifying, documenting, and organizing in a central repository key mandates and sub-mandates that require attention – such as representing a compliance risk for the company and calling for action. The structuring of this central regulatory framework helps identify regulation overlaps and reduce the number of action items and controls needed to ensure compliance. Certain controls can also be shared among different regulations as they perform the same checks, simplifying testing and monitoring.
2. **Relate regulation mandates to key compliance risks**, while assessing and prioritizing these risks. Each regulation implies a number of risks, which can sometime span other regulations. It is important to have a central view of these compliance risks and evaluate them to identify the most critical areas and priorities for action. In particular, this is important for companies that take an approach based on risk and materiality (scoping) to determine key controls and to optimize their compliance practice.
3. **Implement controls used to ensure compliance** to multiple regulations and to reduce risk. By centralizing the controls in a unified environment and moving away from fragmentation across various systems, redundancies can be removed. Additionally, a number of key controls that fulfill similar requirements originating from different regulations can be shared – maintained and tested in only one place, for example.

Build an integrated compliance platform

Consolidating all this compliance data to provide reports and management dashboards can be complex and time consuming, preventing executives from tracking critical items in real time or making decisions based on complete, consistent, and up-to-date information. By integrating a common regulatory and control framework with other business applications, an organization can deliver automation in control monitoring and remediation processes. This integration results in efficiency of controls and minimizing the time between the occurrence of an issue (control failure, fraud incident, etc.) and its identification, thus reducing overall risk and minimizing future issues. It allows issues to be detected quickly and dealt with in a timely manner, and provides better visibility on compliance risks across different mandates and methods of mitigation. Failures can be treated individually as well as aggregated to track areas of weakness and to implement remediation more efficiently.

Conclusion

Organizations looking to streamline compliance should start with:

1. **Understanding their compliance requirements and objectives**, including the risks of noncompliance
2. **Establishing a program that will ensure** the prompt identification and assessment of new or changed compliance requirements, and that changes are appropriately and promptly communicated to those responsible for compliance.
3. **Mapping various compliance requirements** to ensure there is clear ownership and accountability for compliance and related assurance activities
4. **Identifying all risks to compliance** and assessing adequacy of existing compliance programs and processes, identifying gaps, and assigning corrective actions
5. **Reviewing the processes and controls** identified in the previous step and identifying opportunities to improve efficiency through:
 - Eliminating redundant or unnecessary activities
 - Simplifying and standardizing, where possible, on shared processes and tools
 - Increasing the level of automated controls, replacing manual controls
 - Increasing the level of automated control testing
 - Assessing the value and opportunity to simplify by potentially centralizing policy and document management
6. **Establishing a program of continual improvement**, where compliance systems and processes are regularly reevaluated to ensure that they remain efficient as the business and regulatory environment change

Effective management of compliance requires data and visibility across the business. This requires that the organization deploy an infrastructure and supporting processes that deliver real-time compliance transparency across the business and its relationships.

Today, organizations manage compliance in different systems that are not integrated – or even manually. In this scenario, organizations will struggle to get a full picture of the compliance risk they face. An isolated view prevents an organization from looking at the entire exposure in a consolidated manner.

Core to streamlined compliance is the ability to provide multi-regulatory, cross-enterprise compliance management. An organization benefits from a common platform for compliance management to monitor compliance across requirements, provide integration and visibility, and as a result produce greater transparency into intricate control relationships.

Organizations need to consider compliance platforms that have a holistic and integrated view across requirements. The goal is to:

- **Reduce risks and improve the efficiency of controls.** This streamlined structure facilitates the identification and evaluation of key regulatory risks, and the efficient control environment powerfully contributes to mitigate these risks. This framework also brings together both external mandates and internal policies, helping optimize the control environment and provide a unified response to the complete set of requirements. Fewer controls and less duplication of effort allows reduction in cost and, to go even further, the monitoring of many of these controls into source systems that can be automated. The result is a reduction in errors and cost while speeding the detection of failures. The goal is not to over-control the business – since more control does not mean better control – but to optimize the level of control.

- **Provide flexibility to accommodate evolving requirements.** This framework needs to provide flexibility and scalability so that new regulations or major changes can be integrated quickly. It also involves working closely with advisors or partners with strong knowledge of their industry and experienced with regulatory requirements to optimize the process on an ongoing basis. A compliance platform should flexibly adapt to evolving requirements while maintaining an accurate historical perspective for regulatory reporting and management.
- **Enable real-time visibility on the status of risk and compliance.** Centralizing and rationalizing regulatory, risk, and control information makes it much easier to consolidate key data and extract real-time information in an intelligible format. Management thus gets clear insight at any time into the status of compliance and risk management, which helps them make the right decisions. With proper linkage to risks, action plans, and controls, management gains a clear view of the status of compliance, the location of key risks, and the methods of mitigation and monitoring. They can use ad hoc reports and dashboards, both globally and by business area or compliance initiative. The end game is not just complying with law but developing a level of control and insight into business process to help manage risk and achieve strategic objectives.

The outcome is an organization delivering streamlined compliance management that supports and enables corporate performance.

About this paper . . .

This white paper is brought to you by SAP.

For more information, please visit <http://www.sap.com/sapbusinessobjects/grc>

About Corporate Integrity . . .

Corporate Integrity is a research advisory firm providing leadership in education, research, benchmarking, and analysis on the issues and corresponding solutions for corporate governance, enterprise risk, and compliance management.

Through ongoing research, interactions, and benchmark 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 on achieving sustainability, consistency, efficiency, accountability, and transparency in their corporate GRC practices.

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.

About Michael Rasmussen . . .

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.

Foundations of GRC: Streamlining Compliance

With more than 15 years of experience, Michael's objective is to assist organizations in defining GRC processes that are sustainable, consistent, efficient, transparent, and accountable. 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." Most recently, in October 2008, he was recognized as a "Rising Star in Rocky Times: Corporate America's Outstanding Executives Under the Age of 40."

During his career, Michael has worked in the market analyst, consulting, and enterprise sectors. Prior to founding Corporate Integrity, Michael was a Vice-President and top analyst at Forrester Research, Inc. Before Forrester, he led the risk consulting practice at a professional services firm in the Midwest. Earlier, his career included industry experience in healthcare as well as manufacturing.

Michael's educational experience includes a Juris Doctorate as well as a Bachelor of Science in Business.