grc 20/20

April 2018

ACL Compliance Maps

Innovation in User Experience for Compliance Management

EXPERIENCE 2017 grc 20/20

SOLUTION**PERSPECTIVE**

Governance, Risk Management & Compliance Insight

The information contained in this publication is believed to be accurate and has been obtained from sources believed to be reliable but cannot be guaranteed and is subject to change. GRC 20/20 accepts no liability whatever for actions taken based on information that may subsequently prove to be incorrect or errors in analysis. This research contains opinions of GRC 20/20 analysts and should not be construed as statements of fact. GRC 20/20 disclaims all warranties as to the accuracy, completeness or adequacy of such information and shall have no liability for errors, omissions or inadequacies in such information. Although GRC 20/20 may include a discussion of related legal issues, GRC 20/20 does not provide legal advice or services and its research should not be construed or used as such.

Table of Contents

TALK TO US . . .

We look forward to hearing from you and learning what you think about GRC 20/20 research. GRC 20/20 is eager to answer inquiries from organizations looking to improve GRC related processes and utilize technology to drive GRC efficiency, effectiveness, and agility.

ACL Compliance Maps

Innovation in User Experience for Compliance Management

Compliance Bears Down on the Organization

Compliance in Dynamic and Distributed Business

Organizations operate in a field of ethical, regulatory, and legal landmines. The daily headlines reveal companies that fail to comply with regulatory obligations. Corporate ethics is measured by what a corporation does and does not do when it thinks it can get away with something. Compliance management boils down to defining – and maintaining – corporate integrity.

Compliance is not easy. The larger the organization the more complex its operations and corresponding compliance obligations are. Adding to the complexity of global business, today's organization is dynamic and constantly changing. The modern organization changes by the minute. New employees start, others change roles, some leave the organization. New business partner relationships are established, others terminated. The business enters new markets, opens new facilities, contracts with agents, or introduces new products. New laws are introduced, regulations change, the risk environment shifts (e.g., economic, geo-political, and operational), impacting how business is conducted.

The dynamic and global nature of business is particularly challenging to a corporate compliance and ethics program. As organizations expand operations and business relationships (e.g., vendors, supply chain, consultants, and staffing) their compliance risk profile grows exponentially. To stay competitive, organizations need systems to monitor internal and external compliance risk. What may seem insignificant in one area can have profound impact on others.

In an ever-changing business environment, how does your organization validate that it is current with legal, regulatory, policy, and ethical obligations?

Compliance obligations and ethical risk is like the hydra in mythology—organizations combat risk, only to find more risk springing up. Executives react to changing compliance requirements and fluctuating legal and ethical exposure, yet fail to actively manage and understand the interrelationship of compliance data. To maintain compliance and mitigate risk exposure, an organization must stay on top of changing requirements as well as a changing business environment, and ensure changes are in sync. Demands from governments, the public, business partners, and clients require your organization to implement defined compliance practices that are monitored and adapted to the demands of a changing business and regulatory environment.

The Inevitable Failure of Compliance Silos

Compliance activities managed in silos of technology often lead to the inevitable failure of an organization's governance, risk management, and compliance (GRC) program. Reactive, document-centric, and siloed information and processes fail to manage compliance, leaving stakeholders blind to the intricate relationships of compliance risk across the business. Management is not thinking about how compliance processes can provide greater insight into the state of the integrity of the organization. This ad hoc approach results in poor visibility across the organization and its control environment.

A non-integrated approach to compliance information results in these phenomena, each one feeding off the last:

- **Redundant and inefficient processes.** Managing compliance in silos hinders big-picture thinking. Little thought goes into how resources can be leveraged for greater effectiveness, efficiency, and agility. The organization ends up with a variety of processes, applications, and documents to meet individual compliance mandates. The result: a major drain of time and resources.

- **Poor visibility across the enterprise.** Siloed initiatives result in a reactive approach to compliance. Islands of information are individually assessed and monitored. Departments are burdened by multiple compliance assessments asking the same questions in different formats. Limited visibility across the compliance risk exposure ensues.

- **Overwhelming complexity.** The lack of integrated processes introduces complexity, uncertainty, and confusion. Inconsistent processes increase inherent risk, add more points of failure, and create more compliance gaps leading to unacceptable risk. Mass confusion reigns for the organization, regulators, stakeholders, and business partners.

- **Lack of agility.** Reactive compliance strategies managed in information silos handicaps the business. Bewildered by a maze of approaches, processes and disconnected data, the organization is incapable of being agile in a dynamic and distributed business environment.

- **Greater exposure and vulnerability.** When compliance is not viewed holistically, the focus is only on what is immediately in front of each department, at the expense of enterprise-wide inter-dependencies. This fragmented view creates gaps that cripple compliance management and creates a business ill-equipped for aligning compliance initiatives to business objectives.

Today's business entity must ensure compliance is understood and managed company-wide; that its obligations are more than written policies, but part of the fabric of operations; and that a strong culture ensures transparency, accountability, and responsibility as part of its ethical environment. A strong compliance program requires a risk-based approach that can efficiently prioritize resources to risks that pose the greatest exposure to the organization's integrity.

Traditional processes of managing compliance programs (e.g., shared drives, spreadsheets, emails, etc.), can be time-consuming, error-ridden, mundane, and most importantly lacking in providing transparent insight on the state of compliance across the organization. Policies and regulations can change frequently as a result of new or emerging risks, making it increasingly difficult for organizations to identify compliance requirements, map them against organizational processes and controls, and then report on the level of compliance across the enterprise.

The organization has to be able to see the individual area of compliance as well as the interconnectedness of compliance. A compliance professional's most challenging task therefore, is developing a process or framework to understand how internal and external risks interrelate with compliance requirements, and how to evaluate organizational initiatives against these requirements.

Compliance professionals are frequently burdened with having to map a myriad of compliance requirements against organizational processes and controls to demonstrate compliance. For example, an organization may have to comply with security requirements per SOC2 and FEDRAMP standards. Both standards have similar requirements for 'password controls.' Typically, regulations-to-controls are mapped one-to-one, resulting in 'control bloat' and adding immense burden to both the business and compliance team. Inefficiencies are compounded since the typical process is administered through the excessive use of spreadsheets, emails, and out-of-sync documents which can lead to version control chaos, redundancy and overlap. This results in two controls to maintain, implement, and test. However if properly analyzed, one password control could be developed to address these overlapping requirements and then be supplemented with any unique elements from both standards.

The Bottom Line: Yesterday's compliance program no longer works. Boards desire a deeper understanding of how the organization is addressing compliance, whether its activities are effective, and how they are enhancing shareholder value and providing assurance on the integrity of the organization. Oversight demands are changing the role of the compliance department to an active, independent program that can manage and monitor compliance from the top down. The breadth and depth of compliance bearing down on companies today requires a robust compliance program operating in the context of integrated processes and information.

ACL Compliance Maps

Innovation in User Experience for Compliance Management

ACL Compliane Maps is a GRC solution that GRC 20/20 has researched, evaluated, and reviewed that is agile for use in complex, distributed, and dynamic business environments to define, align, and monitor compliance requirements. ACL delivers a new breed of GRC technology that leverages an intuitive Cloud platform to streamline compliance management and other GRC processes to make them more efficient, effective, and agile. The solution delivers significant business value and brings a contextual understanding of compliance management across an organization's distributed and heterogeneous environment. In this context, GRC 20/20 has recognized ACL's Compliance Maps with a 2017 GRC User Experience Award for the best user experience in Compliance Management.

ACL Services Ltd., headquartered in Vancouver, British Columbia, Canada, delivers technology solutions that enable governance, risk management, compliance, and audit processes. Founded in 1987, ACL employs over 300 professionals with offices across North America, Europe, and Asia with more than 14,000 customers from over 150 countries, which includes 89% of the Fortune 500.

ACL delviers a GRC technology solution that strengthens results, simplifies adoption, improves usability, and drives decisions. ACL's integrated family of products—including a cloud-based governance, risk management, and compliance (ACL GRC) solution and data analytics products (ACL Analytics) – empowers GRC professionals with data-driven decision-making that impact all levels of an organization from the C-suite to front-line audit teams. Enhanced reporting and dashboards provide transparency for organizations to focus on what matters most – identifying, managing, and mitigating risks that impact an organizations bottom line and performance.

What ACL Compliance Maps Does

GRC 20/20 has evaluated the features and capabilities of ACL Compliance Maps and finds that it delivers an agile, intuitive, and engaging solution for compliance management. Compliance Maps is an intuitive platform that modernizes how organizations manage compliance and compliance data and processes across the enterprise. It is used to collect, organize, link, report, and analyze compliance data with increased control, collaboration, transparency, and accountability.

ACL's Compliance Maps addresses common compliance management issues by:

- *Reducing the compliance burden* by centralizing management of an organizations standards and regulatory content obligations.
- *Rationalizing which regulations an organization needs to cover* and which are not applicable while avoiding doubling-up on existing processes and controls.
- *Automatically aggregating compliance test results and issues* to easily report on compliance progress in real-time.
- *Creating self-serve reports to demonstrate compliance progress* and satisfy external auditors or regulators.

When disparate controls are put together in a compliance framework, such as when compliance requirements are linked to control activities conducted across the organization through various project initiatives, it provides greater visibility for GRC professionals to identify areas that have sufficient coverage and those with gaps. ACL Compliance Maps enables an organization to streamline their activities with one control test, and understand and report on the organization's overall compliance posture holistically, in one place and in one view.

With ACL Compliance Maps, compliance professionals select the authoritative documents applicable to the organization in a compliance map. These regulations most often come in the form of nested sections with sub-sections and sub-sub-sections, leaving it up to the compliance professional to either address everything exactly as the requirement dictates and implement accordingly, or use professional judgment to rationalize and interpret the requirements. Either way, the compliance professional has full control over the internal compliance process, allowing them to make decisions as to where on the compliance spectrum they want to fall, and most importantly, decide on the compliance level they want to achieve.

Reporting on this is easily accomplished through real-time reports that communicate the status or progress of the compliance program across the organization. Reports enable users to:

- View all applicable requirements across all regulations and standards.
- View requirements that have or have not been mapped to controls.
- View requirements that have been specified as not applicable.
- View summary information about a requirement, including:
    - Extent to which the requirement is covered by controls
    - Whether or not the requirement is considered covered
    - Aggregate number of open issues associated with the requirement
    - How much work needs to be done to comply with a specific standard or regulation

In order to reduce setup and maintenance time, an ACL subscription includes content from COSO and COBIT in the projects module to help organizations kick-start their compliance program. Additional standards are also available as premium content and are packaged as follows:

- IT Compliance content includes:
    - FISMA/NIST SP 800-53 Rev 4
    - PCI DSS 3.2
    - FEDRAMP
- Banking & lending content includes:
    - IT compliance package

- BSA/AML 31 CFR Chapter X)

- Healthcare content includes:
    - IT compliance package
    - HIPAA Omnibus Final Rule 2013
    - HITECH
- Government content includes:
    - IT compliance package
    - Green Book
    - OMG-A133 Circular Compliance Supplement

Compliance Maps is a new functionality made available as part of the ACL Spring 2017 release to address the compliance grind for customers in sectors such as banking, healthcare, manufacturing, and the public sector in which they must comply with externally-imposed regulations, contractual obligations, or established internal policies & procedures.

To facilitate effective use of Compliance Maps, the user's experience is enhanced via a frameworks dashboard which works in conjunction with Compliance Maps. When an organization's compliance requirements change, this allows you to keep up-to-date and easily propagate changes to relevant projects. Users can also upload and track their own compliance requirements and frameworks.

Technical differentiators that GRC 20/20 finds in ACL Compliance Maps are:

- *Mapping to control activities and aggregating control test results* to derive a compliance coverage or assurance score.
- *Allowing dynamic filtering* (e.g., applicable, not applicable; covered, not covered) for enhanced reporting of the organization's compliance program.
- *Providing a central dashboard view* of which control activities across the organization are related to compliance requirements.
- *Keeping track of related controls*, such as controls that have been mapped to a requirement's parent or child.
- *Easy fulfillment process* whereby an organization issues a request to ACL to be able to access and import premium compliance content.
- *Centralized management of compliance efforts* that integrates within the broader ACL GRC platform.

Benefits Organizations Have Received with ACL Compliance Maps

GRC is an integrated capability to reliably achieve objectives [GOVERNANCE], while addressing uncertainty [RISK MANAGEMENT], and acting with integrity [COMPLIANCE].[1] Successful GRC strategies deliver the ability to effectively mitigate risk, meet requirements, satisfy auditors, achieve human and financial efficiency, and meet the demands of a changing business environment. GRC solutions should achieve stronger processes that utilize accurate and reliable information. This enables a better performing, less costly, and more flexible business environment.

GRC 20/20 measures the value of GRC initiatives around the elements of efficiency, effectiveness, and agility. Organizations looking to achieve GRC value will find that the results are:

- **GRC Efficiency.** GRC provides efficiency and savings in human and financial capital resources by reduction in operational costs through automating processes, particularly those that take a lot of time consolidating and reconciling information in order to manage and mitigate risk and meet compliance requirements. GRC achieves efficiency when there is a measurable reduction in human and financial capital resources needed to address GRC in the context of business operations.

- **GRC Effectiveness.** GRC achieves effectiveness in risk, control, compliance, IT, audit, and other GRC processes. This is delivered through greater assurance of the design and operational effectiveness of GRC processes to mitigate risk, protect integrity of the organization, and meet regulatory requirements. GRC effectiveness is validated when business processes are operating within the controls and policies set by the organization and provide greater reliability of information to auditors and regulators.

- **GRC Agility.** GRC delivers business agility when organizations can rapidly respond to changes in the internal business environment (e.g. employees, business relationships, operational risks, mergers, and acquisitions) as well as the external environment (e.g. external risks, industry developments, market and economic factors, and changing laws and regulations). GRC achieves agility when organizations can identify and react quickly to issues, failures, non-compliance, and adverse events in a timely manner so that action can be taken to contain these and keep them from growing.

Compliance management is not as black and white as it seems. It is often a distributed & disconnected function, involving multiple teams addressing multiple processes such as IT security, HR, health & safety, environmental compliance, CSR, third party management, finance & accounting, etc.

ACL Compliance Maps is designed to place the power back into the hands of the compliance professional (not the regulators) in allowing for the organization to define

[1] *This is the official definition of GRC found in the GRC Capability Model and other work by OCEG at www.OCEG.org.*

where on the compliance spectrum it wants to be. Compliance Maps allows you to decide at what level of granularity the organization wants to map controls to and provide a rationale. This allows the organization to choose how it wants to document compliance. That is, whether or not an organization wants to mark the parent requirement as covered with a rationale, or link child requirements to individual control tests within projects.

Specific benefits organizations receive with ACL Compliance Maps are:

- *Users can create their own Compliance Map.* As an example, a multi-national organization that has internal policies and procedures in place for various geographical office locations. Corporate compliance policies that apply to all locations can be housed using Compliance Maps.
- *Greater visibility into controls* that may be out-of-sync with current regulations. This allows for the user to update regulations in one place and propagate changes to applicable projects.
- *Manage regulator scrutiny* with documentation and rationalization of why certain regulations are not applicable.
- *Reduce assurance efforts by testing a control once* that is part of multiple sets of regulatory standards instead of multiple times in multiple places.
- *Reduce the time burden* on the business with repeated regulatory audits.
- *Measure a compliance assurance score* based on testing of mapped control activities and identify possible gaps in coverage.
- *Cascade compliance related changes* to projects, risks, and controls from one centralized location/view via a frameworks dashboard that detects which projects contain changes, and offers the flexibility in applying these changes to all or select projects.

Considerations in Context of ACL Compliance Maps

Every solution has its strengths and weaknesses, and may not be the ideal fit for all organizations in all situations. While GRC 20/20 has identified many positive attributes of ACL Compliance Maps to enable organizations to achieve greater efficiency and effectiveness in compliance management, readers should not see this as a complete and unquestionable endorsement of ACL.

Managing compliance activities in disconnected silos leads the organization to inevitable failure. Reactive, document-centric, and manual processes for compliance fail to actively manage compliance in the context of business and regulatory change, and leave the organization blind to intricate relationships of compliance across the business. ACL Compliance Maps enables organizations to overcome these challenges and make compliance management efficient, effective, and agile.

About GRC 20/20 Research, LLC

GRC 20/20 Research, LLC (GRC 20/20) provides clarity of insight into governance, risk management, and compliance (GRC) solutions and strategies through objective market research, benchmarking, training, and analysis. We provide objective insight into GRC market dynamics; technology trends; competitive landscape; market sizing; expenditure priorities; and mergers and acquisitions. GRC 20/20 advises the entire ecosystem of GRC solution buyers, professional service firms, and solution providers. Our research clarity is delivered through analysts with real-world expertise, independence, creativity, and objectivity that understand GRC challenges and how to solve them practically and not just theoretically. Our clients include Fortune 1000 companies, major professional service firms, and the breadth of GRC solution providers.

Research Methodology

GRC 20/20 research reports are written by experienced analysts with experience selecting and implementing GRC solutions. GRC 20/20 evaluates all GRC solution providers using consistent and objective criteria, regardless of whether or not they are a GRC 20/20 client. The findings and analysis in GRC 20/20 research reports reflect analyst experience, opinions, research into market trends, participants, expenditure patterns, and best practices. Research facts and representations are verified with client references to validate accuracy. GRC solution providers are given the opportunity to correct factual errors, but cannot influence GRC 20/20 opinion.

GRC 20/20 Research, LLC
4948 Bayfield Drive
Waterford, WI 53185 USA
+1.888.365.4560
info@GRC2020.com
www.GRC2020.com