July 2021

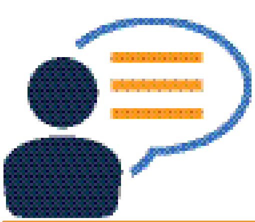
Regulatory Change Management

Efficiency, Effectiveness & Agility in Regulatory Change Processes

STRATEGY PERSPECTIVE

Governance, Risk Management & Compliance Insight

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.

Regulatory Change Management

Efficiency, Effectiveness & Agility in Regulatory Change Processes

Tsunami of Change Overwhelms Organizations

Managing and keeping up with change is one of the greatest challenges for organizations in the context of governance, risk management, and compliance (GRC). Managing the dynamic and interconnected nature of change and how it impacts the organization is driving strategies to mature and improve regulatory change management as a defined process. The goal is to make regulatory change management more efficient, effective, and agile as part of an integrated GRC strategy within the organization.

The challenge is the compounding effect of change. Organizations have change bearing down on them from all directions that is continuous, dynamic, and disruptive. Consider the scope of change organizations have to keep in sync:

- **External risk environments.** External risks – such as market, geopolitical, societal, competitive, industry, and technological forces – are constantly shifting in nature, impact, frequency, scope, and velocity.

- **Internal business environments.** The organization has to stay on top of changing business environments that introduce a range of operational risks, such as change in employees, processes, employees, relationships, mergers & acquisitions, strategy, and technology.

- **Regulatory environments.** Regulatory environments governing organizations are a constant shifting sea of requirements at local, regional, and international levels. The turbulence of thousands of changing laws, regulations, enforcement actions, administrative decisions, rule making, and more has organizations struggling to stay afloat.

Managing change across risk, business, and regulatory environments is challenging. Each of these vortexes of change is hard to monitor and manage individually, let alone how they impact each other. Organizations can devote human and finacial capital resources to keeping up with regulatory change, but that does not make them compliant if that change is not consistent and in sync with business and risk change. Change in economic or market risk bears down on the organization as it impacts regulator oversight and requirements. Internal processes, people, and technology changes continously and regulatory requirements need to be understood in context of business change. As these internal processes, systems, and employees change, this impacts regulatory compliance and risk posture.

Change is an intricate machine of chaotic gears and movements. Keeping current and aligned with change is one of the greatest challenges to compliance management strategies within organizations.

Regulatory Change Overwhelming the Organization

Regulatory change is overwhelming organizations. Many industries, like financial servicers, are past the point of treading water as they actively drown in regulatory change from the turbulent waves of laws, regulations, enforcement actions, administrative decisions, and more around the world. Regulatory compliance and reporting is a moving target as organizations are bombarded with thousands of new regulations, changes to existing regulations, enforcement actions, and more each year. Regulatory change impacts the organization as it reacts to:

- **Frequency of change.** In the past five years the number of regulatory changes has more than doubled while the typical organization has not increased staff or updated processes to manage regulatory change. In financial services, according to the latest Thomson Reuters research, there were an average 257 regulatory change events every business day in 2020, that is just in this one industry.[1] In the past five years the number of regulatory change updates impacting organizations grown extensively across industries.

- **Global context.** Regulatory change is not limited to one jurisdiction but is a turbulent sea of change around the world. Regulations have a global impact on organizations and markets. In Asia, GRC 20/20 finds that there is often more concern over EU and US regulation than over regulation from Asian countries. Inconsistency across regulations from jurisdiction to jurisdiction brings complexity to regulatory compliance.

- **Inconsistency in regulations.** Managing compliance and keeping up with regulatory change, exams, and reporting requirements becomes complicated when faced with international requirements. Regulatory jurisdictions have varying approaches such as principle-based regulation (also called outcome-based regulation) that is popular across Europe and other countries around the world, while the United States and other countries approach a prescriptive approach to regulation that is more akin to a check box list of requirements in specifically telling the firm what has to be done. The principle-based approach gives the organization flexibility with the focus on the achievement of an outcome and not the specific process that got them there.[2] There are conflicting challenges in privacy regulations and other laws impacting organizations across jurisdictions.

- **Expansion into new markets.** It has become complex for organizations to remain in foreign markets as well as enter into new markets. The pressure to expand operations and services is significant as the organization seeks to grow revenue and be competitive, while at the same time being constrained by the turbulent sea of changing regulations and requirements.

1 *Source: Thomson Reuters' Cost of Compliance 2021: Shaping the Future, https://legal.thomsonreuters.com/en/insights/reports/the-cost-of-compliance-2021/*

2 *Note, this can make compliance flexible as well as difficult. In the principle approach to regulation there is a need to interpret the principal as opposed to having the requirement laid out clearly.*

- **Focus on risk assessment.** Regulatory compliance is increasingly pushed to integrate with broader enterprise and operational risk strategies with a focus on delivering specific assessment of compliance risks. For example, regulators in the US seek to ensure that compliance officers do compliance risk assessments. This is also a theme picked up on by law enforcement agencies like the U.S. Department of Justice (DoJ) and the Securities and Excange Commission (SEC). The courts, with the United States Sentencing Commission, alse evaluate the culpability of an organization on compliance based on compliance risk. The discipline of risk management is becoming a pre-requisite for compliance officer skills to ensure that compliance has a seat at the enterprise risk management (ERM) / GRC table.

- **Hoards of regulatory information.** Organizations are overwhelmed by information from legal, regulatory updates, newsletters, websites, emails, journals, blogs, tweets, and content aggregators. Compliance and legal roles struggle to monitor a growing array of regulations, legislation, regulator findings/ rulings, and enforcement actions. The volume and redundancy of information adds to the problem. Managing regulatory change requires weeding through an array of redundant change notifications and getting the right information to the right person to determine the business impact of regulatory change and appropriate response. Organizations must search for the marrow of regulatory details and transform it into actionable intelligence, which can be acted upon in a measurable and consistent manner.

> *"Organizations must search for the marrow of regulatory details and transform it into actionable intelligence, which can be acted upon in a measurable and consistent manner."*

- **Defensible compliance.** Regulators across industries are requiring that compliance is not just well documented, but is operationally effective. This can be seen in the latest DoJ Evaluation of Compliance Program guidance.[3] Case in point, Morgan Stanley is praised by regulators as a model compliance program and is the first company in 35 years of the Foreign Corrupt Practices Acts (FCPA) history to not be prosecuted despite bribery and corruption in their Asian real estate business. One of the points the Securities and Exchange Commission (SEC) and Department of Justice (DoJ) referenced was Morgan Stanley's ability to keep compliance current in the midst of regulatory change: "Morgan Stanley's internal policies . . .were updated regularly to reflect regulatory developments and specific risks."[4]

The amount of regulatory change coming at organizations is staggering. Consider an international bank headquartered in South America who embarked on a project to build a database of regulatory requirements impacting the bank globally. The detail went down

3 *https://www.justice.gov/criminal-fraud/page/file/937501/download*

4 *Source of this statement is at: http://www.justice.gov/opa/pr/2012/April/12-crm-534.html*

to the requirement level so an individual regulation may have a few requirements to more than a thousand, depending on the regulation. After eighteen months of cataloging over 81,000 requirements, they abandoned the project. The reason was that the content was already obsolete—so much had changed during the process of documenting that they did not have the resources to maintain the volume of regulatory change. A Tier 1 Canadian bank has expressed a similar regulatory requirement documentation project demise for the same reason. If you print the United Kingdom's Financial Conduct Authority rulebook, it comes to a stack of paper six feet tall. The U.S. Code of Federal Regulations (CFR) is over 174,000 pages. When printed and laid out end-to-end that is a paper trail that is 25 miles long, nearly as long as a marathon.

Broken Process and Insufficient Resources to Manage Regulatory Change

The typical organization does not have adequate processes or resources in place to monitor regulatory change. Organizations struggle to be intelligent about regulatory developments, and fail to prioritize and revise policies and take actionable steps to be proactive. Instead, most financial service organizations end up fire fighting, trying to keep the flames of regulatory change controlled. This handicaps the organization that operates in an environment under siege by an ever-changing regulatory and legal landscape. New regulations, pending legislation, changes to existing rules, and even enforcement actions of other financial services organizations can have a significant impact. Organizations that GRC 20/20 has interviewed in the context of regulatory change management reference the following challenges to processes and resources:

- **Insufficient head count and subject matter expertise.** Regulatory change has tripled in the past five years. The effort to identify all of the applicable changes related to laws and regulation is time consuming, and organizations are understaffed. Most have not added FTEs or changed their processes despite the continued increase in regulatory change.

- **Frequency of change and number of information sources overwhelms.** The frequency of updates is challenging from the regulators themselves but then comes the flood of updates from aggregators, experts, law firms, and more. Organizations often subscribe to and utilize multiple sources of regulatory intelligence [5] that take time to go through and process in order to identify what is relevant.

- **Limited workflow and task management.** Organizations rely on manual processes that lack accountability and follow-through. It's not possible to verify who reviewed a change, what actions need to be taken, or if the task was transferred to someone else. This environment produces a lack of visibility to ongoing compliance — the organization has no idea of who is reviewing what and suffers with an inability to track what actions were taken, let alone which items are "closed." Compliance documentation is scattered in documents, spreadsheets, and emails in different versions.

5 *Such as legal databases, regulator feeds and news, trade associations, enforcement actions, court rulings, administrative decisions*

- **Lack of an audit trail.** The manual and document-centric approach to regulatory change lacks defensible audit/accountability trails that regulators require. This leads to regulator and audit issues who find there is no accountability and integrity in compliance records in who reviewed what change and what action was decided upon. The lack of an audit trail is prone to deception; individuals can fabricate or mislead about their actions to cover a trail, hide their ignorance, or otherwise get themselves out of trouble.

- **Limited reporting.** Manual and ad hoc regulatory change processes do not deliver intelligence. Analyzing and reporting across hundreds to thousands of scattered documents takes time and is prone to error. This approach lacks overall information architecture and thus has no ability to report on the number of changes, who is responsible for reviewing them, the status of business impact analysis, and courses of action. Trying to make sense of data collected in manual processes and thousands of documents and emails is a nightmare.

- **Wasted resources and spending.** Silos of ad hoc regulatory change monitoring leads to wasted resources and hidden costs. Instead of determining how resources can be leveraged to efficiently and effectively manage regulatory change, the different parts of the organization go in different directions with no system of accountability and transparency. The organization ends up with inefficient, ineffective, and unmanageable processes and resources, unable to respond to regulatory change. The added cost and complexity of maintaining multiple processes and systems that are insufficient to produce consistent results wastes time, resources, and creates excessive and unnecessary burdens across the organization.

- **Misaligned business and regulatory agility.** Regulatory change without a common process supported by an information architecture that facilitates collaboration and accountability lacks agility. Change is frequent and coming from all directions. When information is trapped in scattered documents and emails, the organization is crippled. It lacks a full perspective of regulatory change and business intelligence. The organization is spinning so many compliance plates that it struggles with inefficiency. The organization cannot adequately prioritize and tackle the most important and relevant issues to make informed decisions.

- **No accountability and structure.** Ultimately, this means there is no accountability for regulatory change that is strategically coordinated: the process fails to be agile, effective, and efficient in the use of resources. Accountability is critical in a regulatory change process — organizations need to know who the subject-matter experts (SMEs) are, what has changed, who changes are assigned to, what the priorities are, what the risks are, what needs to been done, whether it is overdue, and the results of the change analysis.

The current situation: The typical organization has a myriad of subject matter experts doing ad hoc monitoring of regulatory change and emailing parties of interest with little or no consistent follow-up, accountability, or business impact analysis. The organization is in a resource intensive, confused state of monitoring regulatory risk, enforcement actions, new regulations, and pending legislation resulting in an inability to adequately predict the readiness of the organization to meet new requirements. There is no overall strategy to gather and share regulatory change information and decide what to do about it.

Defining a Regulatory Change Management Process

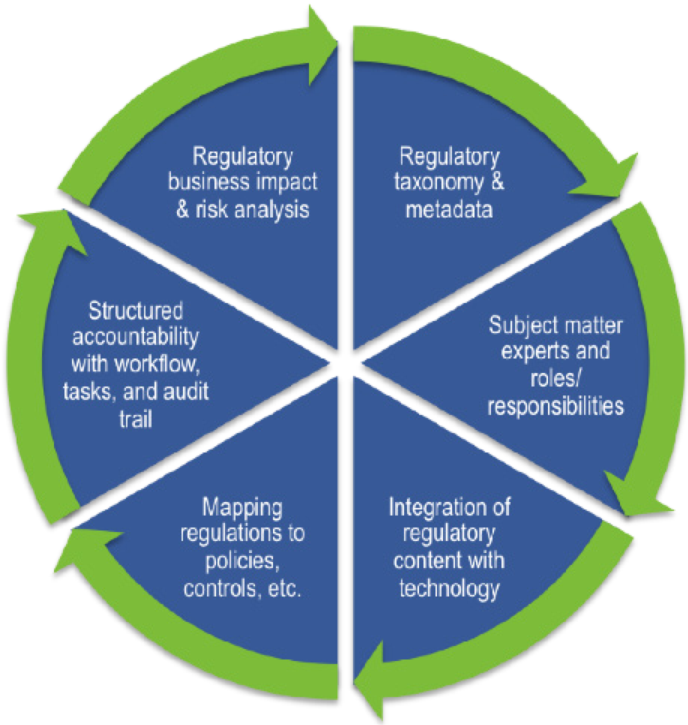
Organizations are struggling with regulatory change and seeking to integrate a regulatory change strategy and process with an integrated information and technology architecture. The goal is to provide actionable and relevant regulatory change content to support consistent regulatory change processes. A dynamic business environment requires a process to actively manage regulatory change and fluctuating risks impacting the organization. The old paradigm of uncoordinated regulatory change management is a disaster given the volume of regulatory information, the pace of change, and the broader operational impact on today's risk environment.

Elements of a Regulatory Change Management Process

Regulatory change management requires a process to gather information, weed out irrelevant information, route critical information to SMEs to analyze, track accountability, and determine potential impact on the organization. The goal should be a regulatory change management strategy that monitors change, alerts the organization to risk conditions, and enables accountability and collaboration around changes impacting the firm. This requires a common process to deliver real-time accountability and transparency across regulatory areas with a common system of record to monitor regulatory change, measure impact, and implements appropriate risk, policy, training, and control updates. To achieve this, organizations must develop a process for collaboration, accountability, and integration between regulatory intelligence content within a GRC information and technology architecture. A well defined regulatory change management processes includes:

- **Regulatory taxonomy and repository.** The foundation of regulatory change management is a regulatory taxonomy and repository. The regulatory taxonomy is a hierarchical catalog/index of regulatory areas that impact the organization. Regulations are broken into categories to logically group related areas (e.g., employment and labor, anticorruption, privacy, anti-money laundering (AML), and fraud). Integrated with this taxonomy is a repository of the regulations indexed into the taxonomy. One regulation may have multiple links into the taxonomy at different areas. The taxonomy and repository maps into the following elements:
    - Regulatory bodies (e.g., lawmakers, central banks, government bodies, regulators, self-regulatory organizations (SROs), exchanges, clearers, industry associations, and trade bodies)
    - Document types (e.g., laws, regulations, rules, guidance, and releases)
    - Sources (e.g., websites, RSS feeds, newsletters, etc.)

- Attributes needed for classification, filtering, and reporting (e.g., business process, jurisdiction/geography, related regulations, regulator, status of change, relevant dates,and consequences)
- Rules & regulatory events



- **Regulatory roles and responsibilities.** Success in regulatory change management requires accountability: making sure the right information gets to the right person that has the knowledge of the regulation and its impact on the organization. This requires the identification of SMEs for each regulatory category defined in the taxonomy. This can be subdivided into SMEs with particular expertise in subcategories or specific jurisdictions, or who perform specific actions as part of a series of changes to address change requirements.

- **Regulatory content feeds.** To support the process of regulatory change management, the organization should identify the best sources of intelligence on regulatory developments and changes. Content feeds can come directly from the regulators as well as law firms, consultancies, newsletters, blogs by experts, and content aggregators. Cognitive technologies that deliver artificial intelligence with natual language processing is making regulatory change management more efficient and effective for organizations. The best content includes the regulation itself, summary of the change, impact on typical organization, and recommendations on response with suggested actions for response. The range of regulatory change content should span new regulations, amended regulations, new legislation, regulatory guidance, news and circulars, comment letters, enforcement actions, feedback statements, and regulator speeches.

- **Standard business impact analysis methodology.** To maintain consistency in evaluating regulatory change, organizations should have a standardized impact analysis process that measures impact of the change on the organization to determine if action is needed and prioritize action items and resources. This includes identifying related policies, controls, procedures, training, tests, assessments, and reporting that need to be reviewed and potentially revised in the context of the change. The analysis may indicate a response to simply note that the change has no impact and the organizational controls and policies are sufficient, or it may indicate that a significant policy, training, and compliance-monitoring program must be put in place.

- **Workflow and task management.** The backbone of the regulatory change management process is a system of structured accountability to intake regulatory changes from content feeds and route them to the right subject matter expert for review and analysis. This is extended by getting others involved in review and response, and requires some standardized workflow and task management with escalation capabilities when items are past due. The process needs to track accountability on who is assigned what tasks, establish priorities, and determine appropriate course of action.

- **Metrics, dashboarding, & reporting.** To govern and report on the regulatory change management process, the organization needs an ability to monitor metrics and report on the process to determine process adherence, risk/performance indicators, and issues. This should provide the organization a quick view into what regulations have changed, which individuals in the organization are responsible for triage and/or impact analysis, the state of review of change, who is accountable, and overall risk impact on the organization.

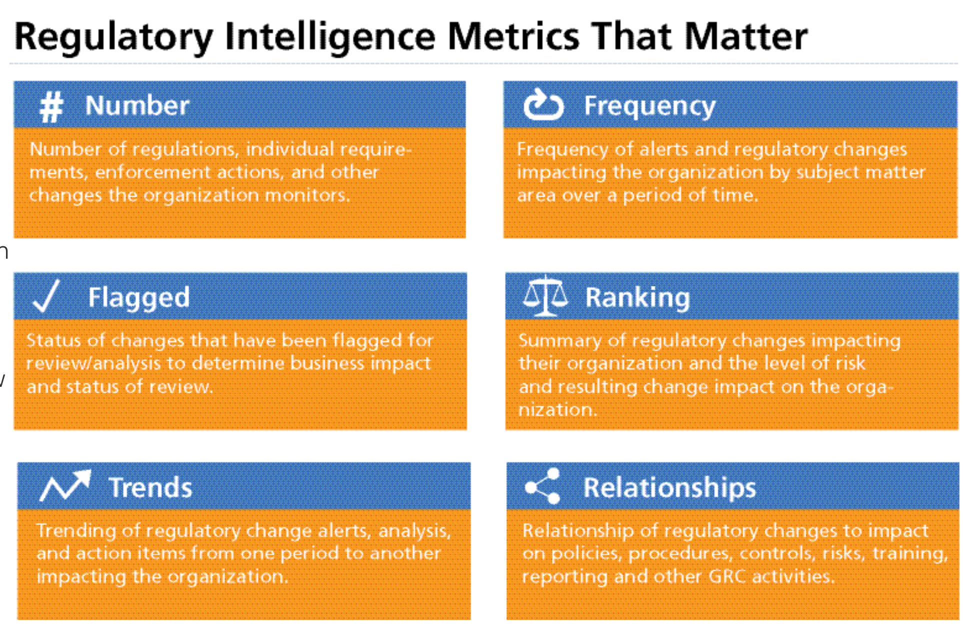
Value and Benefits of a Regulatory Change Process

When organizations develop a regulatory change process, they expect to be:

- **Effective.** They seek to have a greater understanding of changing regulatory requirements and their impact on the organization. To enable the organization to be proactive in gathering, organizing, assessing, prioritizing, communicating, addressing, and monitoring the regulatory change. This allows the organization to demonstrate evidence of good compliance practices.

- **Efficient.** To allow the organization to optimize human and financial capital resources to consistently address regulatory change and enable sustainable management of resources as the business and regulatory landscape grows.

- **Agile.** Competitively enable a dynamic and changing environment as an advantage over competitors that are handicapped by the same change. This requires the organization to understand how the regulatory environment effects the organization and its strategy and how to adapt quickly and be responsive to new developments before competitors are.



GRC Architecture to Manage Regulatory Change

Effectively managing regulatory change is done with a GRC information and technology architecture to improve processes and transform manual document and email-centric processes with automation, integration, and cognitive technologies. Organizations use technology to document, communicate, report, monitor change, and facilitate business impact analysis.

Regulatory Change Management Architecture Goals

A GRC information and technology architecture helps the organization to manage regulatory change to:

- **Ensure** that ownership and accountability of regulatory change is clearly established and understood.
- **Manage** ongoing business impact analysis and scoring.
- **Integrate** regulatory intelligence feeds that kick-off workflows and tasks to the right SME when change occurs that impacts the organization.
- **Monitor** the internal organization's environment for business, employee, and process change that could impact the firm's state of compliance.
- **Identify** changes in risk, policy, training, process, and control profiles based on regulatory change assessments.
- **Visualize** the impact of a change on the organization's processes and operations.

The right GRC information and technology architecture allows compliance and regulatory experts to profile regulations, link with external content feeds and content aggregators, and push new developments or alerts into the application and disseminate for review and analysis. It delivers effectiveness and efficiency, using technology for workflow, task management, and accountability documentation—allowing the organization to be agile amidst change. It enables the organization to harness internal and external information and be intelligent about regulatory environments across the organization.

Regulatory Change Management Architecture Considerations

In evaluating regulatory change management solutions that integrate regulatory intelligence feeds and technology, organizations should ask the following key questions:

1. **How adaptable is the regulatory taxonomy?** The regulatory taxonomy provides the backbone of regulatory change management as it maps regulations to other objects such as business processes, assets, subject matter experts, risks, controls, policies, and more. Organizations should specifically understand how adaptable the taxonomy/mapping is to fit the organization's environment, evolve as the business evolves, and how easy it is to adapt the metadata and taxonomy

structure.

2. **How rich is the regulatory content?** A lot of GRC solutions can handle the workflow and task management of regulatory change management. What really differentiates capabilities is the depth and breadth of the regulatory intelligence content feeds that the solution offers and/or integrates with. This includes regulator coverage, geographic coverage, supporting news and analysis, frequency of updates, and actionable content/recommendations.

Benefits of Automating Regulatory Change Management

- Deal more effectively with change
- Quickly understand the implications of regulatory changes
- Assess and mitigate associated regulatory risks consistently across the organization
- Ensure management, at all levels, has a clear understanding of requirements
- Ensure effective governance of risks and the effect of change on the business
- Increase the speed of response to regulatory change
- Reduce the cost of managing and controlling risk

3. **How strong is the technology?** As stated, a lot of solutions can do workflow and tasks management for regulatory change, so the evaluation of the technology itself needs to go deeper in the systems ability to integrate regulatory intelligence feeds, conduct business impact analysis, as well as connect and understand relationships of regulatory impact to policies, processes, and risks. The more advanced solutions will offer cognitive technologies with artificial intelligence to read and map regulations. SMEs across the enterprise may or may not be technical gurus; the overall user experience should be intuitive and natural. Of particular importance is the user experience.

    - **Deficient technology** involves documents and spreadsheets with email used as a workflow and task management tools. The organization struggles with things getting missed and not having a structured system of accountability. Regulatory change is a manual entry system that is time-consuming and taxing on resources.

    - **Moderate technology** provides a system of accountability with basic workflow and task management, and can integrate with regulatory content providers, providing libraries of regulations and alerts on changes.

    - **Strong technology** for regulatory change management has enterprise content, workflow, and task management capabilities with integration to actionable regulatory content. It enables a closed-loop process as it delivers and integrates regulatory content and insight with technology in an integrated architecture. It also allows the indexing and mapping of regulations to other GRC elements. This involves leverageing artificial intelligence, such as natural language processing, to read regulations. Organizations are finding that machines not only read regulations exponentially faster than individuals, but they are also 30% more accurate in cataloging and mapping regulations and changes. A strong architecture for regulatory chanage management will encompass horizon scanning to monitor where change is trending and developing to be prepared for the future.

Delivering a regulatory change management information and technology architecture involves integration of a GRC platform with artificial intelligence technologies to monitor and manage change and conduct horizon scanning.

Regulatory Change Management Architecture Capabilities

All of these elements are critical and are why they come together in a GRC architecture for regulatory change management. Some solutions in the GRC space are delivering across these three areas and are being used to gather regulatory information, weed out irrelevant information, and route critical information to SMEs responsible for making a decision on a particular topic. This, at a minimum, requires workflow and task management capabilities, but in mature systems it provides direct integration with regulatory content providers. These aggregators manage regulatory profiles, and provide data about relevant new developments that can be routed to individuals responsible for evaluating specific regulatory subject areas. Advanced solutions map regulatory changes to the appropriate metadata as part of a fully integrated, dynamic, and agile process supported by artificial intelligence technologies that read and analzye changes and their impact on the organizations processes, policies, and controls.

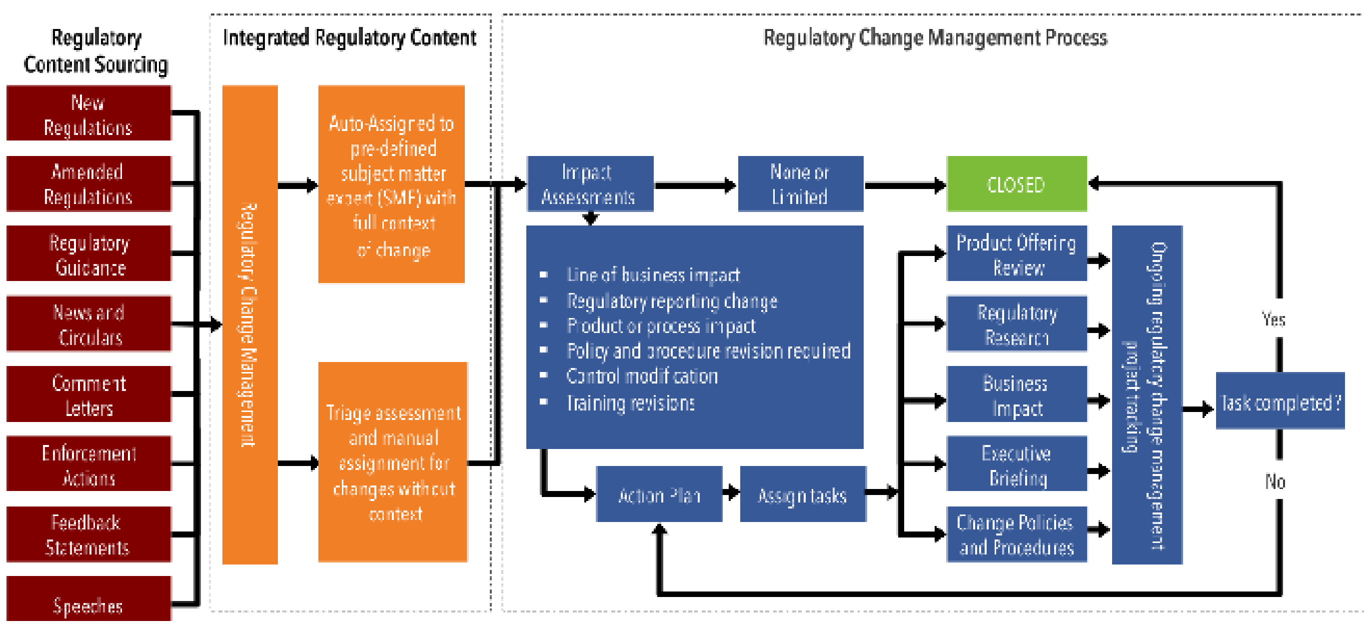
Specific capabilities to be evaluated in a GRC solution for regulatory change management include:

- **Regulatory intelligence content.** At a very basic level, the solution should allow for simple manual entry of new changes and updates so they can be routed to the correct SME for analysis. More advanced solutions provide integration and automation with artificial intelligence platforms built for regulatory change to conduct horizon scanning to search for related laws, statutes, regulations, case rulings, analysis, news, and information that intersect with the change and could indicate regulatory risks that need to be monitored actively. The solution needs to automatically capture and access regulatory related information and events from various external sources that are flagged as relevant to the business. This capability helps ensure that regulatory affairs and compliance teams are up-to-date on new, changing, or evolving regulatory requirements. Regulatory intelligence feeds should be easily configured and categorized in the regulatory taxonomy, providing a powerful and comprehensive inventory of changes in laws and regulations. The regulatory content should identify information such as geographic area/jurisdiction, issuing regulatory body, subject, effective date, modification date, end date, title, text, and guidance for compliance. The guidance should give commentary on how regulatory alerts are effectively transformed from rules into actionable tasks and modifications to internal policies and processes.

- **Cognitive GRC – artificial intelligence.** Keeping up with regulatory content can be a challenge. Many organizations either hire a lot of compliance/legal experts to comb through mountains of regulatory data, or they subscribe to regulatory content subscriptions that do this. This is changing with the role of artificial intelligence applied to a GRC context called Cognitive GRC. Natural language processing, predictive analytics, and robotic process automation make regulatory change management more efficient, effective, and agile for the organization. As stated, the U.K.'s FCA Rulebook stacks to six feet tall; this would take a human a year or more to read. A machine can read it, sort it, categorize it, and link it in under a minute. Not only is a machine faster at reading regulations, but it is also more accurate. One Chief Ethics and Compliance Officer (CECO) told GRC 20/20 that they found natural language processing 30% more accurate in reading, sorting, categorizing, and linking/mapping regulations/requirements than humans. A machine stays focused; there is no mind to wander and get distracted.

- **Content management.** The solution should be able to catalog and version regulations, policies, risks, controls, and other related information. It should maintain a full history of how the organization addressed the area in the past, with the ability to draft new policies, assessments, and other compliance responses for approval before implementation. The solution needs to provide a central repository for storing and organizing all types of regulations and laws based on various templates and classification criteria within a defined taxonomy. The system should be able to maintain a history of actions taken and analysis, including review periods and obsolescence rules that can be set for regulations.

- **Process management.** A primary directive of a defined regulatory change management process is to provide accountability. Accountability needs to be tracked as regulatory change information is routed to the right SME to take review and define actions. The SME should be notified that there is something



to evaluate and given a deadline based on an initial criticality ranking. The SME must be able to reroute the task if it was improperly assigned or forward it to others for input. Individuals and/or groups of SMEs must have visibility into their assignments and time frames. The built-in automatic notification and alert functionality with configurable workflows facilitates regulatory change management in the context of the organization's operations

- **Business impact analysis.** The system needs to provide functionality to identify the impact of changes of regulations on the business environment and its operations, and then communicate to relevant areas of the organization how the change impacts them. This is conducted through a detailed business impact analysis in the platform and is facilitated by being able to tag regulatory areas/ domains to respective businesses and products. The overall system needs to be able to keep track of changes by assessing their impact and triggering preventive and corrective actions. Furthermore, the solution should ensure that stakeholders and owners are informed, tasks related to actions are assigned, and due dates for the completion of actions/tasks are defined. Similarly, when regulations are removed, repealed, or deactivated, the solution assesses the impact of the change and sets up the appropriate responsive actions.

- **Mapping regulations to risks, policies, controls and more.** A critical component to evaluate is the solution's ability to link regulations to internal policies, risks, controls, training, reports, assessments, and processes. The ability to map to business lines, products, and geographies allows companies to manage a risk-based approach to regulatory compliance. The workflow, defined above, automatically alerts relevant stakeholders for necessary action and process changes. It also supports electronic sign-offs at departmental and functional levels that roll up for executive certifications. Mapping is another area where artificial intelligence/cognitive technologies are providing greater efficiency and effectiveness value for regulatory change management.

- **Ease of use.** Regulatory experts are not typically technical experts. The platform managing risk and regulatory change has to be easy to use and should support and enforce the business process. Tasks and information presented to the user should be relevant to their specific role and assignments.

- **Audit trail and accountability.** It is absolutely necessary that the regulatory change management solution have a full audit trail to see who was assigned a task, what they did, what was noted, and notes were updated, and be able to track what was changed. This enables

Keys to Success

- Identify content sources to keep current on regulatory change
- Develop a regulatory obligation taxonomy that establishes the categories of change that impact the organization
- Assign subject matter experts (SME) to each category of the taxonomy who are responsible to track changes and their impact on the organization
- Map risks, policies, procedures, reporting, assessments, training, and other GRC items to the taxonomy so that when a change is identified the SME knows what to evaluate
- Use technology to route changes to the SME and track accountability and follow-through
- Implement a standard business impact analysis process to determine the degree a change impacts the organization
- Integrate the change monitoring process and technology with policy management and enterprise GRC process and technology to integrated flow of information and analysis and ensure that nothing slips through the cracks

the organization to provide full accountability and insight into whom, how, and when regulations were reviewed, measure the impact on the organization, and record what actions were recommended or taken.

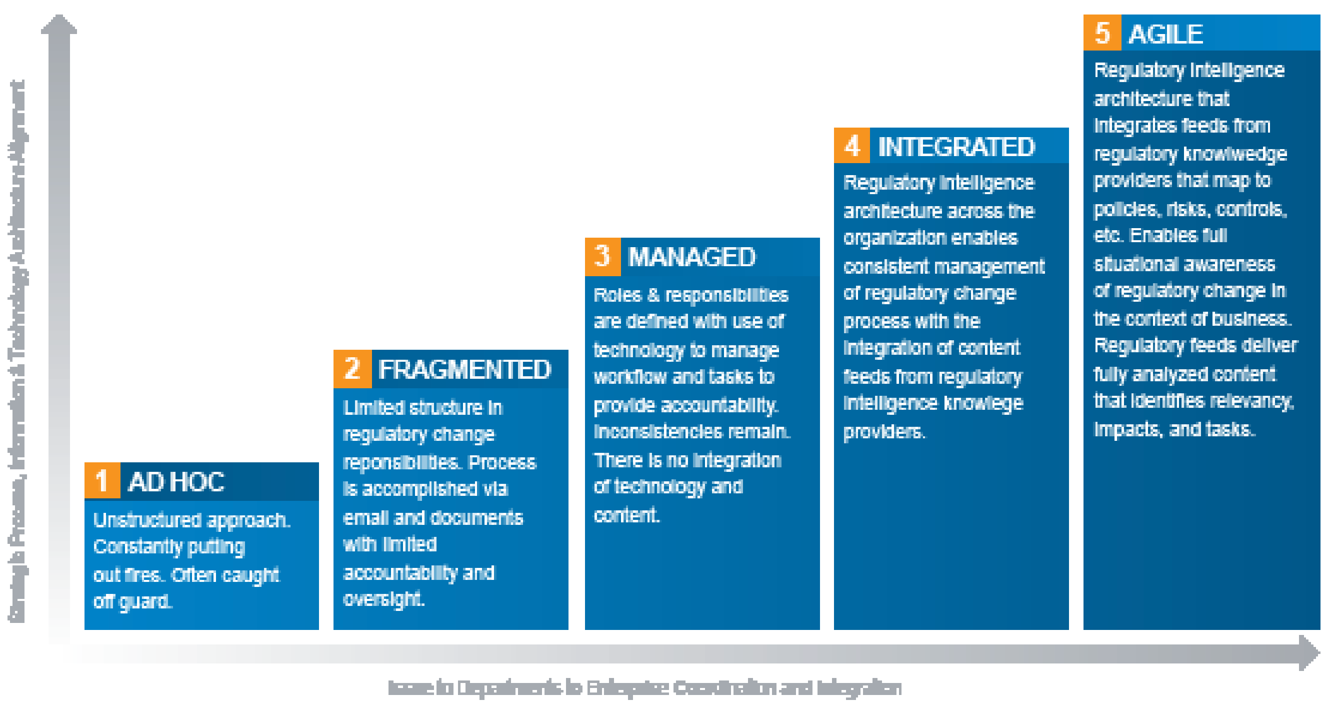
- **Reporting capabilities.** The solution is to provide full reporting and dashboard capabilities to see what changes have been monitored, who is assigned what tasks, which items are overdue, what the most significant risk changes impacting the organization are, and more. Additionally, by linking regulatory requirements to the various other aspects of the platform – including risks, policies, controls, and more – the reporting should provide an aggregate view of a regulatory requirement across multiple organizational units and business processes.

- **Flexibility and configuration.** No two organizations are identical in their processes, risk taxonomy, applicable regulations, structure, and responsibilities. The information collected may vary from organization to organization as well as the process, workflow, and tasks. The system must be fully configurable and flexible to model the specific organization's risk and regulatory intelligence process.

GRC 20/20's Regulatory Change Management Maturity Model

Mature regulatory change management requires the organization to align on regulatory risk. It also involves participation across the financial services organization at all levels to identify and monitor uncertainty and the impact of regulatory change.

GRC 20/20 has developed the Regulatory Change Management Maturity Model to determine an organization's maturity in regulatory change management processes, as well as information and technology architecture. The GRC 20/20 Regulatory Change Management Maturity Model is summarized as follows:



Level 1 – Ad Hoc

Organizations at this stage lack a structured approach to regulatory change management and are constantly putting out fires and being caught off guard. Few, if any, resources are allocated to monitor regulatory change. The organization addresses regulatory change in a reactive mode—doing assessments when forced to. There is no ownership or monitoring of regulatory change and certainly no integration of regulatory change information and processes. Characteristics of this stage are:

- Lack of a defined regulatory taxonomy
- Ad hoc and reactive approaches to regulatory and business change
- Document and email-centric approaches
- Lack of accountability

Level 2 – Fragmented

In the Fragmented stage, departments are focused on regulatory change management within respective functions—but information and processes are highly redundant. The organization may have limited processes for regulatory change but largely do not benefit from the efficiencies of an integrated approach. Regulatory change management is very document-centric and lacks an integrated process, information and technology architecture. Positively, there is some structure to regulatory change responsibilities, but the management of regulatory change lacks accountability as it is done largely in documents and email that lack structures of accountability and automation. Characteristics of this stage are:

- Varied approaches to regulatory change
- Lack consistent structure
- Lack integration or formal processes for sharing regulatory information
- Reliance on fragmented technology with a focus on discrete documents

Level 3 – Managed

The Managed stage represents a mature regulatory change management program that is using technology for structured workflow, task management, and accountability. Regulatory change functions have defined processes for regulatory change management, as well as an integrated information architecture supported by technology and ongoing reporting, accountability, and oversight. Though there is no integration of regulatory content feeds into the technology platform. Characteristics of this stage are:

- Visibility into regulatory change across the business

- Established processes for regulatory change
- Good use of technology to manage accountability

Level 4 – Integrated

It is at the integrated stage that the organization begins to integrate regulatory content feeds into the technology platform for automation. The organization has consistent regulatory taxonomy, process, information, and technology to streamline regulatory change management processes. The organization is seeing gains in addressing regulatory change through shared information that achieves greater agility, efficiency, and effectiveness in a common technology architecture that enables consistent management of regulatory change. Standardized workflow is integrated into regulatory and legal content feeds. Characteristics of this stage are:

- Strategic approach to regulatory change across departments
- Common process, technology and information architecture
- Integration of legal/regulatory content feeds
- Reporting across departments

Level 5 – Agile

At the Agile stage, the organization has completely moved to an integrated approach to regulatory change management across the organization and is leveraging artificial intelligence to make it more efficient and effective. Horizon scanning is in place to not only monitor regulatory change in the here and now, but what is coming in the future. This results in a shared-services approach in which core regulatory change technology, content, and processes are shared centrally across the organization. The approach is characterized through a mature regulatory taxonomy with integrated and actionable regulatory content, automated by technology that integrates and leverages artificial intelligence. The organization has enterprise workflow that provides business-process automation for regulatory change with oversight and management of regulatory change. Regulatory content feeds deliver fully analyzed content that identifies relevancy, impacts, and tasks. Characteristics of this stage are:

- Regulatory intelligence achieved through integration of artificial intelligence and cognitive technolgies to read, map, and analyze regulatory content and impact on the organization
- Horizon scanning is in place to monitor trending issues
- Consistent views of regulatory change and impact on operations and policies
- Able to efficiently manage business change in regulatory context

GRC 20/20's Final Perspective

The constant changes in today's regulatory environments translate to a growing burden on organizations in terms of the number of regulations they face and their scope. Many organizations do not possess the necessary regulatory change management infrastructure and processes to address these changes and, consequently, find themselves at a competitive disadvantage and subject to regulatory scrutiny and losses that were preventable. These organizations can greatly benefit from moving away from manual and ad hoc process changes and toward a system specifically designed to manage those changes comprehensively and consistently. Such a system gathers and sorts relevant information, routes critical information to subject matter experts, models and measures potential impact on the organization, and establishes personal accountability for action or inaction.

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