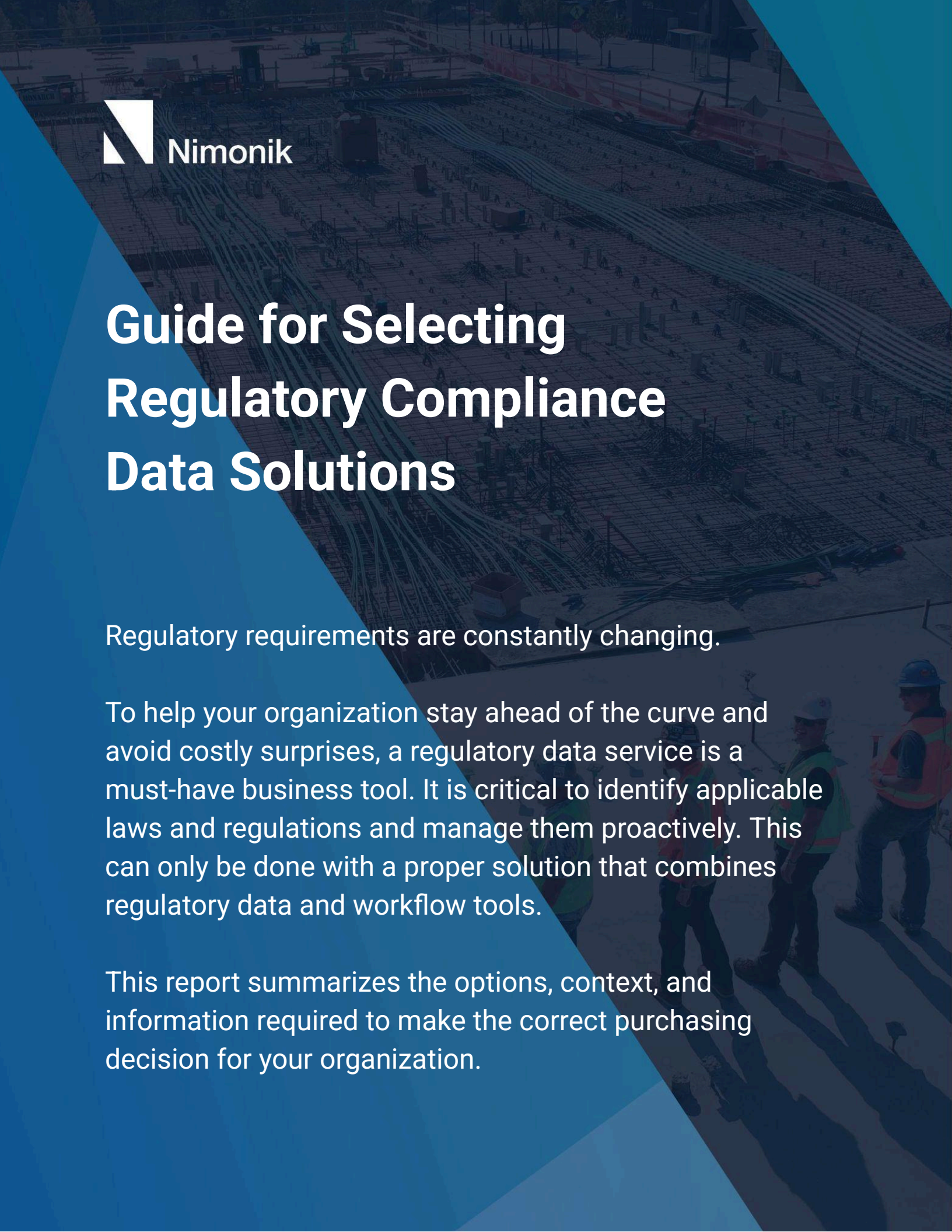


Nimonik

Guide for Selecting Regulatory Compliance Data Solutions

Regulatory requirements are constantly changing.

To help your organization stay ahead of the curve and avoid costly surprises, a regulatory data service is a must-have business tool. It is critical to identify applicable laws and regulations and manage them proactively. This can only be done with a proper solution that combines regulatory data and workflow tools.

This report summarizes the options, context, and information required to make the correct purchasing decision for your organization.

Table of Contents

Guide for Selecting Regulatory Compliance Data Solutions 1
Table of Contents 2
Executive Summary 3
Introduction 4
What is a Regulation? 5
History of Governmental Regulatory Efforts 7
Three Key Regulatory Concepts 8
Emerging and Proposed Laws & Regulations 8
Regulation Development Framework 8
Legal Jurisdiction 9
Consolidated vs. non-Consolidated Regulations 10
The Three Types of Compliance for Organizations 11
Corporate Compliance 11
Operational Compliance 14
Product Compliance 15
Three Sides, One Umbrella 17
Regulatory Change Management Solution Considerations 19
Dedicated Solution or a Module Within a Larger Software Suite 21
Key Features of Regulatory Compliance Solutions 22
Regulatory Compliance Additional Services 23
Conclusion 24
Appendix 1: Case Study 25
Case Study : Carnival Cruise Lines Compliance Overhaul 25
Appendix 2: Sample Evaluation Grid for Compliance Solutions 29
Additional Resources 33

Executive Summary

A Strategic Approach to Regulatory Compliance

Regulatory compliance is a critical, yet increasingly complex, business function. As regulations evolve across global, national, and sub-national jurisdictions, organizations face significant operational risk if they rely on fragmented, manual, or siloed management processes. This guide provides a strategic framework for centralizing compliance management to reduce risk, costs, and operational inefficiencies.

Key Insights for Organizations:

- The Compliance Framework: Effective compliance is defined by three fundamental steps: identifying applicable Requirements, executing necessary Actions, and verifying ongoing Compliance.
- The "Umbrella" Strategy: Organizations frequently struggle by managing Corporate, Operational, and Product compliance in isolation. Adopting an "Umbrella Solution"—a centralized system—prevents conflicting priorities, reduces resource waste, and establishes a single source of truth for regulatory data.
- Best Practices for Implementation: Technical tools alone are insufficient. A sustainable compliance program requires:
    - Leadership Commitment: Secure top-level backing to foster a culture of improvement.
    - Continuous Auditing: Implement regular monitoring to detect and correct gaps in real-time.
    - Staff Training: Educate employees at all levels to ensure they understand their responsibilities.
- The Cultural Imperative: As illustrated by the Carnival Cruise Lines case study (Appendix 1), sustainable compliance is impossible without deep cultural integration. Operational fixes are ineffective if the underlying company culture does not prioritize compliance, leading to recurring failures, reputational damage, and excessive costs.

Successful regulatory management moves beyond reactive checklists. By centralizing data and embedding compliance into the organization's culture, businesses can transform regulatory obligations from a burden into a competitive advantage and a safeguard for long-term operations.

Introduction

Nimonik was originally a product built to identify all the environmental regulations in Canada and explain what companies need to do to stay in compliance. Canada, like other countries, has a decentralized regulatory framework where each province has its own laws and regulations that companies must comply with. Since the start of the Nimonik product in 2004, we have continuously iterated and learned how companies struggle to meet regulatory requirements. We hope this guide will be a helpful tool for any professional looking to improve their compliance with laws and regulations and other requirements you must meet.

In 2019, we worked closely with Scott Nadler to define our direction as a company. He explained that **despite all the complexity of laws and regulations, it all boils down to: Requirements, Actions, Compliance**. Said otherwise, you first need to determine what you are required to do, what actions you must take and then ensure you are in compliance. At the end of the day, it is that simple.

Our vision at Nimonik is to centralize all the requirements an organization faces. Requirements can come from a few different places, but in general they come from three sources:

1. Laws and regulations created by government
2. Industry Standards set by industry bodies and standards bodies (ISO, ASTM, IEC, ICC,...)
3. Internal corporate documents (policies, permits, licences, contracts,...)

Together, these three sources determine nearly all of your requirements as a business and these requirements are constantly changing. Implementing a robust tool to handle the thousands or tens or thousands of requirements is becoming increasingly essential. To handle this challenge effectively, we firmly believe that the first step is to centralize the sourcing of your data and then standardize your approach to compliance. This can be done with a commercial tool such as Nimonik or through the purchase of data and the development of an internal tool. Regardless of how you tackle the problem, it is critical that you implement something to effectively manage your requirements.

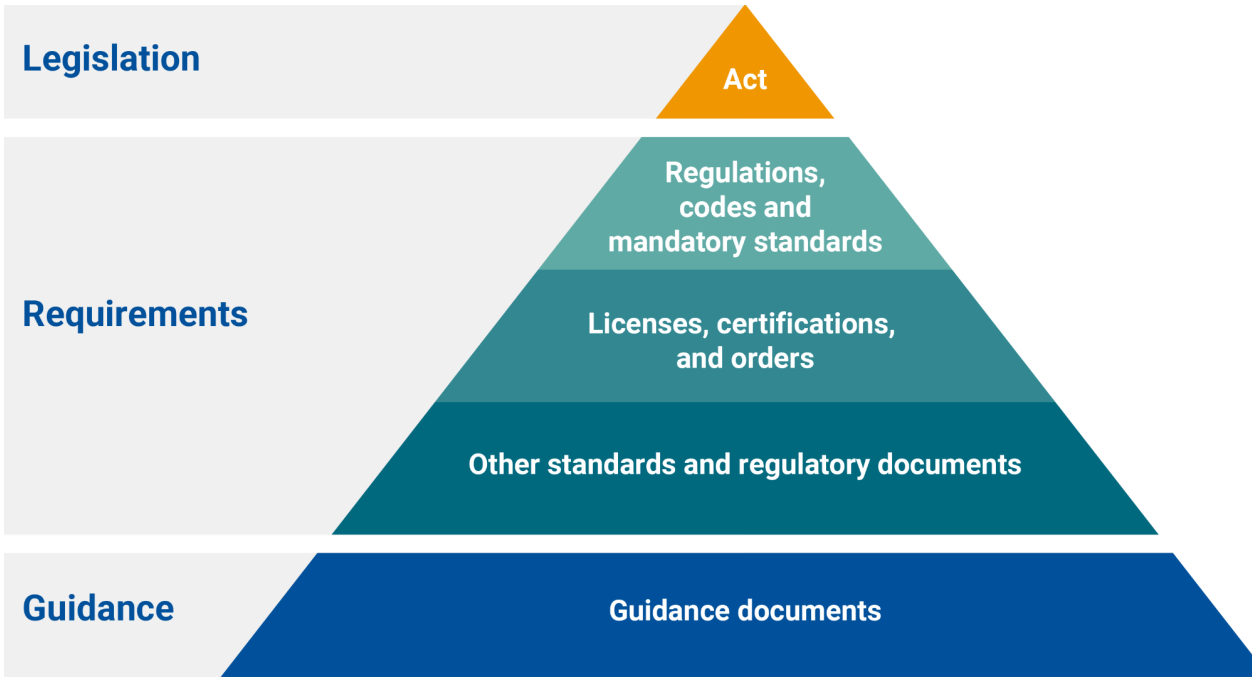
This guide will focus on legal and regulatory compliance information, we hope it is helpful. To learn more about Industry Standards, please see our guide here.

What is a Regulation?

When we think about compliance to governmental requirements, we need to consider a myriad of documents that come under different names depending on the jurisdiction, language and legal structure of the jurisdictions. It should be noted that each country and jurisdiction (state, province, region, city) operate differently and we will make various approximations in this guide for the benefit of the reader.

In general, governments will propose bills that will then turn into laws or acts that form the framework of their policies and may lead to the creation of governmental agencies or ministries. These governmental bodies then create regulations, rules, directives or orders that are more detailed and prescriptive. **The acts are the main direction the government wants to take and the regulations are the details of how people and companies need to act to stay in compliance.** This second tier of documents will provide more specific requirements for organizations, people and agencies. These documents typically fill in the details left out of the broader documents created by the government, be they acts, laws, codes or something with a different name.

Regulations and similar documents will be supported by additional documents issued by agencies in the form of circulars, guidance documents, explanatory notes or other information. Some of this third tier of documents will clearly be labelled as mandatory or optional, but many documents will not be clearly labelled and it will be up to the public to determine their relative importance. For the sake of simplicity, this document will use the term “regulations“ to refer to all the types of documents mentioned above including acts, laws, regulations, rules and guidance documents.


Legislation
Act
Requirements
Regulations, codes and mandatory standards
Licenses, certifications, and orders
Other standards and regulatory documents
Guidance
Guidance documents

History of Governmental Regulatory Efforts

The concept of rules and regulations dates back to ancient times, where rulers tried to apply some set of rules and guidelines to society. Many of the initial rules came from religious texts and doctrines, but over time and with the increasing sophistication of governing structures, laws and regulations started to be created. At the end of the day, the purpose of regulations is to make people and organizations do things they would not otherwise do. This basic principle remains the same.

Today, regulations cover a very broad spectrum of activity. From environmental protection to power transmission and trade, nearly all aspects of human activity fall under some form of law or regulation. To ensure people follow laws and regulations, a variety of strategies and consequences have been put into place. Fines, penalties and sanctions are now a significant driver of compliance along with brand and reputational issues. **In the modern business world, it is critical for organizations to stay abreast of changing regulations and reduce their risks of non-compliance which can have a reputational and material impact on their operations.**

As outlined in Wikipedia,

> Modern industrial regulation can be traced to the Railway Regulation Act 1844 in the United Kingdom, and succeeding Acts. Beginning in the late 19th and 20th centuries, much of regulation in the United States was administered and enforced by regulatory agencies which produced their own administrative law and procedures under the authority of statutes [Laws]. Legislators created these agencies to require experts in the industry to focus their attention on the issue.

Though regulatory agencies vary in their activity, there is a general trend towards more regulation and stricter controls on business activities. Based on the data collected by Nimonik since 2008, the average jurisdiction has over 3,000 active regulations and the regulatory body typically grows by 3% per year. With this burden placed on companies, it is essential to put in place proper systems to manage the change. In short, it seems unlikely that regulatory creation will stop anytime soon.

Three Key Regulatory Concepts

Emerging and Proposed Laws & Regulations

Before a law or regulations exists, it is proposed by the government. For laws, they are typically created by legislative bodies and go through a voting process and committee process before being enacted. Regulations are typically created by government agencies and go through some form of commenting before they become final.

When it comes to tracking emerging and proposed requirements, it is important to understand the complexity and nature of this challenge. **While most organizations claim to want to know and even influence emerging laws and regulations this can be a daunting task for even the largest company.**

Nimonik's product BillTrack50 tracks over 200,000 bills in the United States and tens of thousands of regulations and rules every year as they work their way through government bodies. While the vast majority of bills fail to become law, managing emerging requirements can provide a head start and allow you to influence their direction - given enough resources. In most jurisdictions, most proposed change never makes it into law or regulations, creating a tremendous amount of noise for anyone seeking to understand change. Typically your government affairs department will try to tackle this problem to the best of their ability.

In addition to the sheer volume of proposed change, another major issue is that most jurisdictions do not publish proposed laws and regulations in a clear manner. Due to inconsistent publication formats, it is very challenging to track proposed regulations and it quickly becomes cost prohibitive.

In contrast to operational, product or corporate compliance teams, the people at an organization who are most interested in emerging regulations are government relations and affairs professionals. Only the largest companies have this team and they are often accompanied by consultants who help them track changes. Industry associations also play an active role in tracking new regulations and laws and communicating them to their members. They are often involved in the regulatory process in both an informal and formal manner, through in-person meetings and back-channel discussions.

Regulation Development Framework

Regulations typically go through a multi-step process before they become final. Each jurisdiction and agency can act differently, but it is important to understand the general process a new regulation undergoes. The image below lays out the most typical steps.



Legal Jurisdiction

Legal entities, such as nations, have the authority to create and enforce laws; this authority is considered their "jurisdiction". Jurisdiction can be exercised extraterritorially/supranationally (for example, international laws or treaties, European Union laws), nationally, and sub-nationally.

Nations that are subdivided into states or provinces assign jurisdiction over certain areas to the federal government or to lower-level governments (states, provinces, cities, etc.). These jurisdictions may or may not overlap; in cases of overlap, the laws of one government entity may override the laws of the other entity if the laws conflict.

In practice, this means that most countries have laws and regulations at multiple levels of government. For example,

- In the United States, foreign affairs and currency are regulated exclusively by the federal government, welfare and education are regulated exclusively by state governments (although the federal government has historically also exercised control over matters that were traditionally regulated by states through laws related to federal government grants), and taxation and environment are shared.
- In countries within the European Union (EU), business operations must comply with laws created by the EU (e.g. for motor vehicle emissions) as well as laws in their country of

operation, some of which (e.g. for waste reduction) were created to comply with EU directives.
- Ships flagged under countries that are signatories to The International Convention for the Prevention of Pollution from Ships (MARPOL) are subject to its requirements wherever they sail.

In short, your organization is likely subject to laws from a wide range of sources.

Consolidated vs. non-Consolidated Regulations

Each jurisdiction operates differently, with governments sharing powers based on regulatory areas. In addition to power sharing, certain jurisdictions operate under a civil law system or a common law system, which will affect the way regulations are interpreted and used. Another variable is whether the jurisdiction consolidates their regulations or not. In addition to consolidation of regulatory text, some jurisdictions will also codify their regulations.

In a jurisdiction that codifies its regulations, you will typically find a structured document that organizes the current regulations by topic or by a responsible government department or agency; changes to these regulations are incorporated into the code. This is common in republican legal systems such as those in France and the United States, but you often have exceptions such as the State of Pennsylvania that does not codify all of its documents. In 2020, the United States Code of Federal Regulations (all the US Federal Regulations) contained a staggering 86,356 pages.

A jurisdiction that consolidates its regulations and laws updates the main regulation or law every time an amendment is made and includes the amendments. This makes it easier to know what the current requirements are. Countries that do this include Canada, Germany, Australia, Poland and many others. A country that codifies its regulations typically consolidates them as well - but not always!

Lastly, certain jurisdictions opt to not consolidate their documents or only consolidate certain documents. This means that the jurisdiction will publish amendments to laws and regulations, but may not update the original document. To understand what the current requirements are you need to read both the original texts and the amendments. Some commercial legal services such as LexisNexis, Karnov or others offer non-official consolidations of legal documents. This approach to regulatory change can alleviate government work, but it places a huge burden on the regulated party to understand what the current situation is. Jurisdictions that regulate in this way include Ireland, China, and Belgium.

When working in compliance it is important to understand how the jurisdictions you operate in regulate. Consolidation and codification of texts is one important factor as you want to ensure you are working with the correct and up–to-date information.

The Three Types of Compliance for Organizations

While regulatory monitoring and management is a broad topic that affects all parts of a business, there are generally speaking three types of compliance:

- Corporate (directors, boards, reporting, …)
- Product
- Operational (factories and offices)

Organizations typically purchase separate regulatory solutions tools for the three types of compliance problems they face. The key buyers, budgets and decision makers are distinct for these three elements of compliance and it is important to understand what you are looking for before evaluating potential vendors.

In theory a Company should validate it is in compliance with all regulations. However, due to siloed budgets and decision making, the various parts tend to focus on their main areas of concern. Corporate teams will focus on Corporate Compliance only while operations compliance is often delegated to local plants and operational compliance teams with minimal reporting up to the corporate head office (though that is starting to change). Product compliance is typically relegated to engineering and product design teams and issues are only raised to corporate officers if serious issues are found.

Corporate Compliance

Corporate compliance is primarily concerned with ensuring the corporate entity and its leadership are in compliance with applicable regulations. Compliance by non-management personnel is typically a secondary concern in corporate compliance. To help protect the company and its leadership, companies will design, implement and implement policies along with training and procedures. Corporate compliance programs are centered around corporate policies that help reduce the risk of violations of laws and allow the company to demonstrate their intention to remain in compliance.

When it comes to applicable regulatory information, theoretically, all regulations that apply to a company, its operations and its products are within the scope of Corporate Compliance programs. In reality, most Corporate Compliance programs focus on financial reporting, competition, management and board responsibilities, corporate reporting and other such things.

Primary Internal Compliance Tools

A corporate compliance program is often started with four core items:

1. A company code of conduct,
2. Corporate standards and
3. Policies, and
4. Procedures for various specific processes.

This is often done by legal counsel, though not always. Some sample regulated areas that corporate bodies are concerned with include:

Securities Laws
Any company with publicly or privately traded securities must be sure to comply with securities regulations in the jurisdictions they have corporate entities. These regulations often center around disclosures, accounting practices and financial reporting.

Antitrust Laws
In most jurisdictions, companies are restricted from anti-competitive behavior. Limiting a market, price fixing, collaborating with competitors or certain mergers and acquisitions are restricted by law in most jurisdictions.

Trade and Consumer Protection Regulations
Any company that advertises, sells products to the public, or otherwise interacts with consumers must ensure that they treat the consumer fairly. Some important areas of concern for compliance include advertising practices, refund policies, financing and loan and general transaction practices.

Anti-Bribery, Anti-Slavery, Supply Chain
More and more jurisdictions are regulating responsibilities for organizations with regards to human rights in their supply chain. This includes corruption, bribery, child labour, human trafficking, and other issues within the supply chain. Companies must improve visibility in their supply chain and implement policies to reduce risk of non-compliance to changing corporate regulations.

Software and Data Solutions for Corporate Compliance

Typical tools for corporate compliance programs include Governance, Risk and Compliance (GRC) and Integrated Risk Management (IRM) tools such as LogicGate, Archer, MetricStream or software such as Compliance.AI (now part of Archer). These tools are mostly focused on the financial industry, but can be used by other organizations. However, most of these tools do not include regulatory data and do not include industry standards, making them an important, but incomplete solution to the compliance challenge.

GRC Software Ecosystem



Operational Compliance

Operational compliance is focused on ensuring the day to day operations and people at your factories, offices and physical locations are in compliance with regulations. This facet of compliance is often related to worker safety, environmental protection, building codes, fire codes, data privacy, human resource regulations and other items that affect normal day to day operations. There are many different types of regulations that affect day to day operations, but some of the most common include:

Environmental
Environmental matters are typically regulated at multiple levels - Federal, State/Provincial and Municipal. These regulations need to be met and very often this can be an ongoing challenge. Many operations receive environmental permits based on the regulations and this creates additional requirements. Environmental compliance can be further driven by certification to management standards such as ISO 14001 which increase the need to demonstrate compliance to maintain your certificate.

Occupational Health and Safety (OHS)
Workers at your locations need to comply with a myriad of safety regulations and companies are subject to a general Duty of Care provision to ensure safe working environments. This Duty of Care provision is widely interpreted by regulatory agencies. OHS compliance can be further driven by certification to management standards such as ISO 45001 which increase the need to demonstrate compliance to maintain your certificate.

Data Privacy and CyberSecurity
More and more requirements are being imposed on organizations with respect to data privacy and protection. Companies need to monitor these requirements and ensure compliance. If you are ISO 27001 certified, there is an additional requirement to demonstrate ongoing monitoring and compliance.

Energy Management
Many jurisdictions are regulating and obliging facilities to improve their energy efficiency. This can include monitoring and reporting as well as retro-fits. If you are certified to ISO 50001, there are requirements to clearly identify and monitor your regulatory requirements related to energy management.

Human Resources Management
All jurisdictions regulate human resources, hiring, firing, and general industrial relations between employers and employees. Keeping track of relevant laws and regulations is critical to ensure you manage your workforce according to the applicable laws. Errors on workforce and human resources compliance can be very costly.

Software and Data Solutions for Operational Compliance

Tools for this type of compliance are divided amongst EHS focused companies such as providers such as ENHESA, Red-on-Line, STP Compliance, CyberRegs or other local providers. Companies like Nimonik offer EHS regulatory data, but also cover other regulatory topics such as Energy Management, Human Resources, Data Privacy and Cyber Security and other regulated areas. Certain companies offer industry specific compliance tools for industries such as motor vehicle compliance or other areas.

	Other EHS Solutions (ENHESA, Regscan, Red-On-Line, STP)	Nimonik Compliance Solution
Regulatory and Standards Coverage	✓	✓
Environment	✗	✓
Occupational Health and Safety (OHS)	✗	✓
Data Privacy and Cyber Security	✗	✓
Energy Management	✗	✓
Industry Standards	✗	✓
Energy Production & Distribution	✗	✓
Financial Services & Insurance	✗	✓
Other Topics Available	✗	✓

Product Compliance

To be able to sell a product within any given market, the producer needs to ensure the product meets applicable regulations and industry standards. This process is, unsurprisingly, called “Product Compliance”.

Product compliance is broader than safety or performance, it also covers import regulations, trade requirements, labeling, and potential disposal of the product. For certain products, data and privacy regulations may impact the product development. There are often regulatory agencies that focus on high risk classes of products such as medical devices, drugs, vehicles and other items. Due to the high level of requirements, commercial compliance solutions for these specific industries and their products are often available and well suited to the needs of a business that produces high risk products in a specific sector. The solutions are rather narrow in scope, but deep in coverage.

Product compliance is often managed by the engineering and design teams. The budget for these tools is often remarkably low and once a product has been designed and put to market, most product compliance work stops. Without a proper monitoring tool in place, products may come out of compliance and create substantial costs to an organization. It is therefore critical that product compliance teams monitor regulations on an ongoing basis for the jurisdictions where their product is sold.

An example of an unexpected cost for a non-compliant product was brought to Nimonik by a customer who sold paint into a variety of markets, notably China.

> A producer of commercial paint had their shipment blocked when entering China because it no longer met the new VOC requirements. The producer made paint similar to the products produced by Benjamin More, Sherwin Willian and PPG. This kind of paint is typically called architectural paint. Though they have been exporting their paint to China for over 4 years, the Chinese government changed some chemical regulations and standards that made their paint non-compliant.
>
> After an investigation, Nimonik and the client found out that the paint regulation had changed in China around December 1st, 2020 and they had no monitoring tools in place for the relevant regulations. The industry standard for testing VOC content in paint was updated to the Chinese Standards GB 18582-2020. Consequently, the paint was out of compliance due to high levels of Alkylphenol ethoxylated. Also, the test method for the Volatile Organic Compounds (VOC) is different in China than in Canada. So the paint

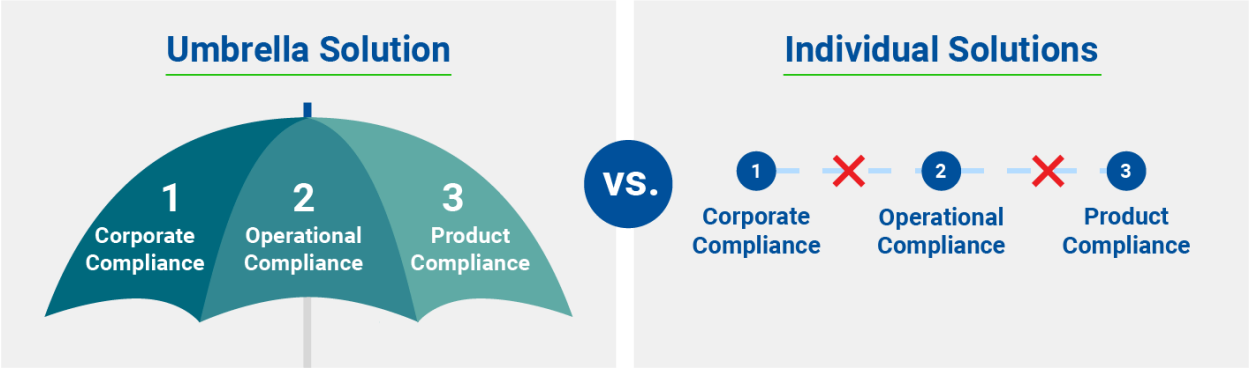
producer had to use the test method outlined in the Chinese standard GB 18582-2020 for APEO (alkylphenol ethoxylated).

Once the test methods and the product composition had been updated, the paint was able to be shipped to China, but a container of paint was returned and substantial costs were incurred by the paint producer. Product compliance requires a robust toolkit to stay on top of ever changing requirements.

Three Sides, One Umbrella

An organization that fails to take proactive steps on compliance will invariably pay the price down the road when a product, operation or corporation comes out of compliance. In contrast, if your organization manages to implement robust compliance programs for corporate compliance, product compliance and operational compliance, you will significantly reduce your risk.

The three sides of the compliance challenge are often handled independently and this can lead to wasted resources and conflicting priorities. Handling them separately will also make reporting and monitoring more challenging as you work across jurisdictions, teams and locations. It is recommended that all three sides of this problem be addressed in one central system, with specific tools being made available to people as needed. No one tool will serve everyone's needs, so it is critical to find a compromise, but implement an umbrella solution that can cover the bulk of the monitoring and compliance needs.



Regulations are created for all sorts of issues, from environmental matters to energy to worker safety and product safety. Each jurisdiction will create laws in their own way and no two countries or jurisdictions are the same.

Due to the diversity of the regulatory process and publication of regulations, organizations who operate in multiple jurisdictions have a greater burden than sole location operations. Multi-location companies should invest in an all-in-one tool that allows you to obtain the

regulatory data that matters for your organization. If you purchase tools for each topic or domain, such as environmental vs. transportation, and each jurisdiction, USA vs. Europe, you will likely end up with a disconnected series of systems that create more work and risk than they solve.

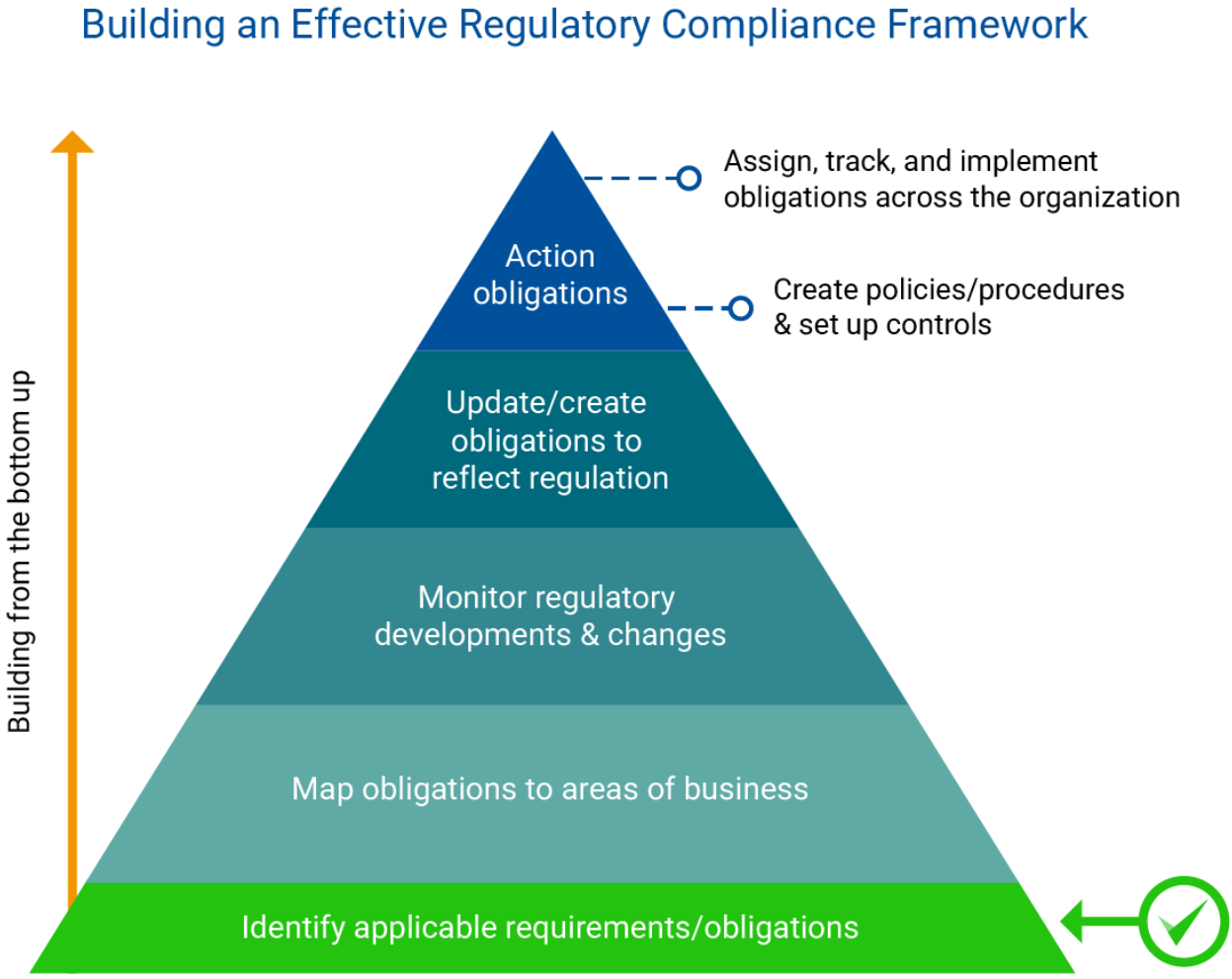
Due to each team having a separate budget and decision making process, companies often buy different solutions that have no way to talk to each other. EHS teams will often buy regulatory compliance tools such as ENHESA, Red-on-Line or STP. HR teams may procure systems such as ComplianceHR, Rippling, or others - but they are often jurisdiction specific. Cybersecurity teams may acquire Vanta, Sprinto, or others - but they typically lack regulatory requirements. And engineering teams may purchase tools from Accuris (IHS), Intertek Inform (SAI Global) or others. While each tool has its pros and cons, the advantage of having the majority of your compliance requirements in one location is significant.

Software and Data Solutions for Emerging and Proposed Regulatory Items

They will tend to use software such as BillTrack50 or StateNet in the US or services from legal publishers such as Thompson Reuters and Walters Kluwers.

Operational compliance tools such as Nimonik will track proposed regulations that have a high likelihood of being adopted and a high potential impact for operational compliance. While select tracking of proposed regulations is not ideal, it is often better than no awareness of upcoming changes. Learn more about our criteria here.

Regulatory Change Management Solution Considerations



Successfully implementing regulatory change management solutions in your organization can be a challenge for any organization. Follow these best practice steps:

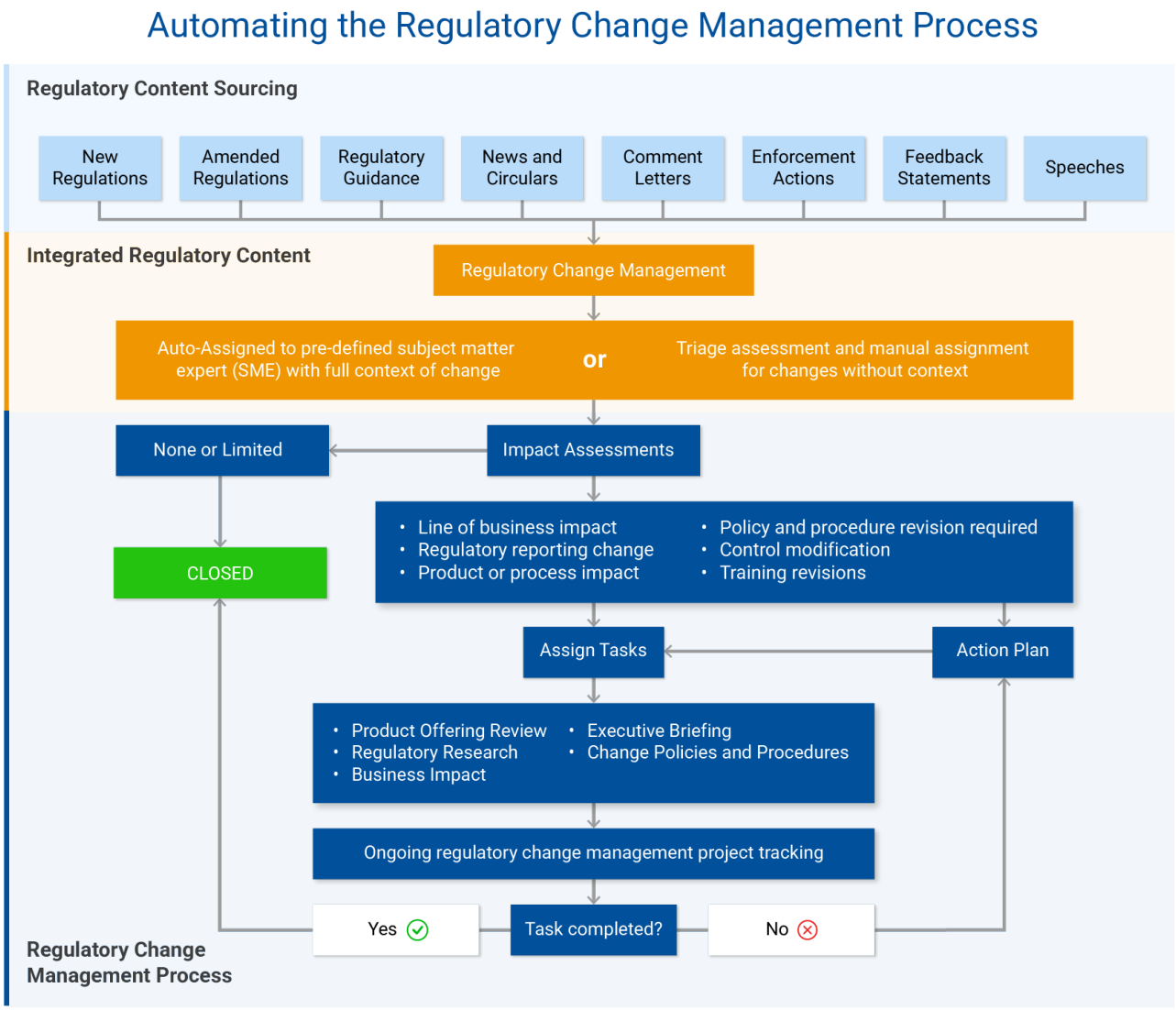
1. **Gain Leadership Commitment**: Secure leadership support to provide the necessary resources and foster a culture of continuous improvement. Management's backing is critical for success.
2. **Form a Team:** In addition to leadership support, you will also require a project manager and a team of colleagues who can review and add information in the system.

Project Implementation

3. **Identify applicable regulations**: Begin by identifying the applicable regulations to your industry and operations.
4. **Conduct a Gap Analysis:** Perform a gap analysis to compare current practices against the chosen regulations. Identify where improvements are needed to meet the requirements.
5. **Develop Implementation Procedures:** Define clear roles and responsibilities. Establish processes that align with the regulatory requirements, ensuring all employees understand their compliance roles and responsibilities.
6. **Provide Employee Training:** Implement regular training programs to educate staff about their roles in maintaining compliance with the standards.
7. **Establish Verification Processes:** Introduce regular audits and reviews to ensure compliance is being managed at your company.
8. **Continuous Improvement:** Maintain and refine your compliance program by collecting feedback and making necessary adjustments to enhance performance.
9. **Seek External Certification (if applicable):** If applicable, pursue certification to validate your compliance with recognized standards such as ISO 37301.

Sample Regulatory Change Management Workflow

The change management process below is a potential workflow for any organization. Due to the volume of regulatory changes, it is imperative that you prioritize changes based on potential impact. Once that is done, a straightforward workflow is often much better than an overly complex one. Keep it as simple as possible and focus on capturing all relevant changes.



Regulatory Data Software Solution Considerations

There are a number of considerations when searching for a solution to access regulatory data. Beyond the obvious cost factor, the primary consideration is the quality of the data you will be receiving from the provider.

Once you have found a data solution, you then need to consider the software you may choose to use or build to manage the data. The next sections dive into this element of the decision making process.

Dedicated Solution or a Module Within a Larger Software Suite

Many organizations implement EHS Management Software (Intelex, Enablon, VelocityEHS,...) or GRC Software to better manage compliance. They may then decide to integrate data from a third party such as ENHESA, Regscan, STP Compliance, or others into a “Regulatory Compliance Module” provided by the software vendor. However, two challenges usually emerge from this approach.

First, the software purchased is rarely accessible to everyone at the company who is affected by regulatory change and costs can be linked to the number of seats. This makes it challenging to provide access to regulatory updates, actions and workflow tools to all relevant stakeholders. You then end up having to communicate items outside the system, creating duplicate work and the risk of miscommunication. In large organizations this is often the case.

The second challenge with the implementation of regulatory data into a separate software solution is functionality and ease of use. As outlined above, each jurisdiction and regulated area functions differently. The nuances and details or regulatory data makes it difficult to implement in a software solution that is not designed with the underlying data in mind. It ends up being a situation of a round peg in a square hole.

Additionally, with the advent of AI and Large Language Models, the processing of regulatory data has become much easier, but for the full benefits of AI to be available to the end user, they must be designed with the underlying data and workflows in mind. This is very difficult to do for a regulatory data provider if they do not control the software layer that the end user interacts with.

Before adding a new software provider or a new module to an existing software to help handle regulatory compliance, verify if a direct solution might be a better fit. A direct access to regulatory data and software can allow you to deliver a better experience to your end users, provide wider access to staff and ensure you obtain the best quality data for your organization.

Key Features of Regulatory Compliance Solutions

When purchasing a **Regulatory Compliance Solution**, consider the following to obtain the best value and functionality for your organization:

Content Location Matrix: Determine the jurisdictions you require based on your needs. In certain cases, sub-national jurisdictions may not regulate on a specific topic (Air Transportation) and if you may therefore not need sub-national content. In other situations, such as worker safety, sub-national jurisdictions may be the most important and you may not need national data.

Tailor Content to Your Needs: Work with your partner such as Nimonik to determine whether your organization benefits most from and what are your needs across your operations.

Annual Contracts: Most licenses are one-year contracts, but longer agreements can be arranged. Plan for annual renewals early to ensure a sustainable long-term program that boosts efficiency and ROI.

Essential Features and Updates: Ensure your subscription includes critical features such as updates, redline, alerts, workflow tools, reporting and more.

Onboarding and Training: Effective onboarding and training are crucial for user adoption. Understand how training will be rolled out and communicated for widespread acceptance and efficient platform use.

User Support through Webinars and Training: Look for platforms offering webinars, self-paced training, and video tutorials to provide users with efficient access to tools and support.

Platform Capacity and Integration: Ensure the platform supports Single Sign-On (SSO) and APIs for seamless integration with your existing systems, maximizing usability and security. Nimonik offers both SSO and API access to data. Nimonik is also certified to the ISO 27001 standard for Information System Security Management.

Administrative Features: Evaluate the platform's administrative features to ensure it meets your needs for managing subscriptions, users, and access rights efficiently.

Regulatory Compliance Additional Services

Knowing, understanding and monitoring regulatory change is not sufficient in and of itself to ensure compliance. An organization must convert its requirements into actions and into institutional knowledge that will create a compliance culture within the organization. Two key initiatives all companies must engage in include:

Compliance Training
Any successful corporate compliance program must have sufficient compliance training programs in order to ensure that all employees are made aware of their responsibilities to follow compliance standards, policies and procedures. The appropriate officers, employees, contractors and third parties must be made to understand all relevant laws, regulations, corporate policies and prohibited conduct. They must also be informed of how to report any potential violations. In the case of a regulatory violation, your company's training program will be heavily scrutinized to determine who will be held responsible, so it is vital that every company have robust training policies and procedures.

Compliance Auditing
It is impossible to enforce compliance objectives—or even know if compliance policies are being adhered to at all— without compliance monitoring and auditing. Monitoring programs must be in place to assess compliance in real time, quickly detect problems and correct violations. The goal of a corporate compliance monitoring program must be to identify and address gaps in compliance on a consistent basis. Auditing, on the other hand, is designed to review the overall picture of your company's compliance programs. For many programs, an audit can be conducted every 1-3 years, with select locations and programs being audited.

Conclusion

Regulatory compliance is not a static destination, but an evolving operational discipline. As this guide has outlined, the complexity of global regulations—across corporate, operational, and product domains—makes fragmented, siloed management unsustainable. Organizations that rely on disjointed tools risk not only operational inefficiency but also significant reputational and material damage.

The most resilient organizations move beyond reactive "checklist" compliance. They embrace a centralized, "umbrella" strategy that integrates regulatory data, standardizes workflows, and fosters a proactive compliance culture. As evidenced by the Carnival Cruise Lines case study (Appendix 1), sustainable success requires leadership commitment, cultural integration, and the right technological foundation to link requirements, actions, and ongoing verification.

Your next steps should be to:

1. Perform a Gap Analysis: Objectively assess your current compliance coverage against your actual regulatory (and other) obligations.
2. Evaluate Your "Umbrella" Needs: Seek solutions that offer the depth of coverage required for your specific risks while supporting integration with your broader software ecosystem.
3. Embed Compliance in Culture: Ensure that compliance is not just an IT or Legal task, but a leadership-backed priority integrated into weekly operations.

By centralizing your data and embedding compliance into your organizational DNA, you transform regulatory obligations from a cost-center burden into a safeguard for long-term growth and a significant competitive advantage.

Appendix 1: Case Study

Case Study : Carnival Cruise Lines Compliance Overhaul

Introduction

Carnival Cruise Lines has a history of rough seas when it comes to environmental compliance programs. With over 60 million dollars in fines and after being placed in monitorship by the United States Department of Justice, Carnival decided to embark on a journey to make their compliance management program world-class. This short case study summarizes some of the key points made by the Compliance Weekly case study entitled “Tale of Two Storms”.

Background on Carnival Cruise Lines Compliance Journey

In 2013, a whistleblower documented the cruise line’s compliance issues and submitted them to the UK and US governments. After these environmental compliance issues were raised with regulators, Carnival crews intentionally tried to hide the systematic behavior of discharging waste illegally into open waters. This behaviour was not a new issue, Carnival had already paid an 18 million dollar fine in 2002 for similar actions. The 2002 fine did lead to environmental program overhaul, but did not result in a systematic overhaul of the company’s compliance program. That is to say, specific actions were taken to improve reporting, documentation, training and procedures around environmental issues, but the underlying company culture towards compliance remained unchanged.

Though there were actions taken, they did not go deep enough and ultimately the general company culture determined the behaviour of staff when it came to environmental issues. This is why a siloed compliance program can lead to major shortcomings. The 2013 issues resulted in over 40 million dollars in fines for Carnival, as well as a tarnished reputation, significant internal costs, and being placed in monitorship. When the monitorship began in 2019 following the conviction, Carnival finally started to fundamentally change.

Key Problems at Carnival Cruise Lines

Some of the main points from this fascinating case study:

- Even after the guilty findings in 2019, illegal behaviour continued – from more discharges to briefing the ships prior to inspections from the Department of Justice. This led to judgments that forced Carnival management to accept responsibility for the

compliance issues, pay for more independent audits and a variety of other changes that all incurred substantial costs – not to mention another 20 million dollar fine.

- Carnival was put under monitorship with the second round of fines, this process is very expensive, and it also indicates that the regulator has lost confidence in the company's ability to clean up its systems without very close supervision.
- In 2019, Carnival hired a Chief Ethics and Compliance Officer, Peter Anderson, who was an experienced lawyer. This position was intentionally about compliance AND Ethics They put an emphasis on Ethics as over 50% of carnival's problems and compliance issues were tied to their business ethics.
- Carnival has 105 Vessels and 130,000 employees around the world. Carnival brought together 9 Brands in a relatively short period of time. All of these companies had their own systems in place and many of them were previously competitors. Moreover, prior to 2020, there was no centralized compliance function. Each business unit had its own team, with various standards and systems.
- To tackle these obstacles, Anderson rearranged the offices so that Environment, Safety, Physical Security and General Compliance were all co-located and could better collaborate.
- To add to their environmental compliance challenges, Carnival Cruises also owned Costa Cruises, best known for the 2012 Costa Concordia accident which left 30 passengers and later one salvage diver dead.
- Prior to 2020, crews were given too much leeway in determining actions related to waste. As a result, crews would release dirty bilge water and other hazardous waste at sea to avoid costly fees in port to dispose of the waste properly.
- The company's environmental compliance lead did not have a direct line of sight into each vessel until after the second round of fines and the culture change.
- Carnival, when speaking about the various actions they took to put in place a proper compliance program in 2020, stated that "They wished they had done it the first time around"
- In the second round of fines, Carnival finally came to understand that you cannot really fix operational issues without fixing the underlying cultural issues.

Key Actions Taken to Improve Compliance for Carnival Cruise Lines

The Chief Ethics and Compliance Officer, Peter Anderson, brought a four pillar model of compliance and self governance to Carnival:

- Prevention
- Detection

- Response
- Correction

Like many organizations, Carnival was too focused on response and being reactive. Under Peter Anderson the EHS, Risk and Safety teams came together to better evaluate risk, link to controls and determine actions to take.

The corporate team had to work closely with the ships and the Environmental Compliance Officers. Changing the culture within leadership was a critical step in the journey. An essential change was having Peter Anderson, the Chief Ethics and Compliance Officer, participate in the weekly leadership calls with the CEO, CFO and other top level executives. By bringing compliance to the highest level of discussion, it allowed issues to be raised and also sent a message to the rest of the organization.

The company also added a board member with direct compliance experience, a former VP at Wal-Mart who was responsible for compliance. Too often, boards look for people with financial and strategic experience, but do not look for members with a compliance background.

Another key element in shifting leadership was to engage the Ship Captains in this process. Ship Captains are in charge when at sea and it was critical to get them onboard with a compliance management program that included a more open conversation with crew members and staff about compliance issues.

Carnival's Culture Action Plan

Carnival also developed a culture action plan that leveraged information from staff and created a path to meaningfully change the culture at Carnival when it came to compliance. Since putting these leadership changes in place and implementing the culture plan, the number of reported compliance issues by staff have more than doubled.

To reinforce the programs, plans and changes, Carnival has also put in place a competition and reward system for staff and ships. Carnival provides cash prizes, environmental compliance coins, and they recognize one ship out of the 105 ship fleet as the best environmentally friendly ship each year.

Key Take-Aways

- **Culture Precedes Compliance:** Operational fixes—such as updated training and better documentation—are insufficient if the underlying company culture remains

unchanged. Sustainable compliance is impossible without deep cultural integration, as culture dictates employee behavior in critical, unsupervised moments.

- **Centralize and Co-locate:** Siloed compliance teams create gaps and conflicting priorities. To be effective, functions like Environment, Safety, Physical Security, and General Compliance must be co-located and integrated to foster collaboration.
- **Elevate Compliance to the C-Suite and Board:** Compliance must be a strategic priority, not just a back-office function. Success requires embedding compliance experience into the Board of Directors and ensuring the Chief Ethics and Compliance Officer has a seat at the table during weekly executive leadership calls.
- **Empower the Frontline:** A top-down approach is insufficient. Sustainable change requires engaging frontline leaders (e.g., Ship Captains) to move from a culture of avoidance to one of open communication, where issues are reported rather than hidden.
- **Integrate Ethics with Compliance:** Compliance and Ethics are inseparable. Since many compliance failures are rooted in business ethics, the function should be unified under a single officer to ensure both regulatory adherence and ethical alignment.
- **Transition from Punitive to Incentive-Based:** Move beyond reactive measures and punishments. Long-term engagement is better sustained through recognition programs, competitions, and rewards that celebrate proactive compliance and safety.
- **The High Cost of Reactive Management:** Relying on silos or ignoring cultural red flags leads to catastrophic outcomes—including reputation damage, millions in fines, and court-ordered monitorship, which signals a complete loss of regulator confidence.

Appendix 2: Sample Evaluation Grid for Compliance Solutions

Business Requirements

Interface	System will have a minimalistic and user friendly interface requiring few user clicks as possible
Interface	System will allow displaying user interface in multiple languages
Interface	System will allow user to have some level of access on mobile devices
Coverage	Ensure we are tracking and kept updated on legal requirements in the regions we operate in (supranational (EU,...), federal, provincial/state/regions and municipal, regulations, codes, etc.)
Coverage	Meets requirements of formal management system (ISO)
AI	Offers AI to summarize and provide details about documents
AI	Offers AI to summarize and provide details about requirements
AI	AI can identify applicable requirements
AI	AI can propose action items
AI	Offers "human in the loop" functionality
Coverage	Vendor can provide access to copyrighted Industry Standards
Coverage	Vendor covers all applicable environmental regulations and standards
Coverage	Vendor covers all applicable occupational health and safety regulations and standards
Coverage	Vendor covers all applicable cybersecurity and data privacy regulations and standards
Coverage	Vendor covers all applicable HR and industrial relations regulations and standards
Coverage	Vendor covers all applicable design and engineering relations regulations and standards
Coverage	Vendor can add additional regulations and standards as required

Coverage	Management of change for changes to legislation
Coverage	System customizable for tasks, topic area (environmental, safety, hr,...) and jurisdictions operated in
Coverage	Alerts (email) of updates to legislation
Coverage	Alerts (email) of emerging legislation
Coverage	Alerts (email) of changes to industry standards
Coverage	Ability to upload our own documents and identify requirements in permits, licences, and stakeholder engagements
General	Owner of system will provide technical/legislative support for system and documents within system
General	Owner of system will offer compliance training, screening and support
General	Audit function for compliance
General	Native mobile software on iOS and Android
General	Windows software for offline access
General	Ability to issue actions and assign to other users
General	Ability to integrate into existing systems or future systems (API)
General	Risk Matrix allows to prioritize obligations based on risk ranking
Reporting	System will provide a report on new regulations and standards changes within a specific timeframe
Reporting	System will provide a report on new regulation at mutliple levels of government
Reporting	System will have ability to mark new requirements as 'complete' once the new has been updated in appropriate management system documentation
Reporting	System will have ability to mark new documents as not applicable if does not apply to business
Reporting	Dashboard to demonstrate ongoing compliance and continuous improvement

Searching	System will provide easy to use and intuitive search functionality
Searching	System will allow user to search for documents containing specified terms or metadata
Workflow	System will provide ability to set workflow to route legislative updates to assigned employees to update internal documentation
Workflow	Ability to create actions linked to documents, requirements, audits and other items
Workflow	Ability to assign to Teams of users and not just individual users
Workflow	Ability to assign tags or other categorization system to run reports across the business
Workflow	Ability to track actions across business and by various reporting lines
Implementation	Implementation plan is provided and executed by vendor
Support	Supplier offers corporate support packages

IT Requirements for Compliance Solution

1. Which cloud providers currently hosts your service/solution?
1a. If "Other", please specify:
2. In which location(s) is your service/solution hosted?
3. Is your service/solution geo-redundant?
4. From which location(s) do you provide your service/solution as geo-redundant?
5. Has your service/solution ever experienced an unexpected outage which was not planned and communicated to customers? Please include the reason and duration of the outage.
6. How many times in the past 24 months has your service/solution been unavailable due to an unplanned outage?
6a. If "Other", please specify:
7. What methods of authentication are supported with your solution?
7a. If "Other", please specify:
8. Is multi-factor (two factor - 2FA) authentication supported with your solution?
9. What multi-factor (Two Factor Authentication - 2FA) providers does your solution support?
9a. If "Other", please specify:
10. What backup (data protection) capabilities does your service/solution come with?
10a. If "Other", please specify:

11. What is the frequency of these backups? (Daily, Weekly, Monthly)
11a. If "Other", please specify:
12. Are these backups encrypted?
13. What level of encryption is used when storing backup data?
13a. If "Other", please specify:
14. What is the retention period for these backups?
14a. If "Other", please specify:
15. What frequency do you test the recovery of data within these backups?
15a. If "Other", please specify:
16. Are you able to provide proof of recovery testing for audit purposes?
17. Do you perform regular Disaster Recovery Testing of your service/solution?
18. What frequency do you test your Disaster Recovery Plan for this service/solution?
18a. If "Other", please specify:
19. Does this testing impact the service availability? What is the typical duration of this outage?
20. Are you able to provide proof of the success/failure of DR testing for audit purposes?
21. Does your solution have open API's which would facilitate the integration with outside data sources or services?
Salesforce
ServiceNow
SAP / SAP HEC
Infor M3
DBS / DBSi
Rentalman
Splunk
Tableau
21a. If None of the Above, please specify:
22. Please provide a list of all known outside data sources in which existing customers are leveraging these API's.
23. Is the encryption of data or communications with your service/solution supported? (In flight, at rest, other)
23a. In flight, at rest, other?
23b. If "Other", please specify.
24. Does your service/solution adhere to industry certification and standards?
ISO 27001
SSAE16
GDPR
SOC1
SOC2
Other: *Please list*
25. Please provide certificates of compliance with these industry standards.
Please attach copies

26. What data from us, if any, is transmitted or stored within the solution?
27. If our data is transmitted or stored within the solution, what integrations are required to facilitate this?

Additional Resources

ISO 37301, 14001, 45001, 27001, and 50001

Webinars

- Artificial Intelligence and LLM impact on regulatory analysis
- ISO 37301 Compliance Management Systems – Key Elements
- Build your business case for a centralized comprehensive compliance program
- Webinar & Challenge 2021: Internal Obligations Management Best Practices
- ISO 19600 – Compliance Management System Guidelines
- The four key types of EHS regulations and how to comply
- Internal Audit Best Practices for Safety, Environment, and Quality Audits
- Great ISO 14001 Legal Registers, What do they Look Like?
- The Link Between Risk Management, Critical Controls, and Auditing

Global Industry Standards and Regulatory Compliance Software

Organize and control requirements.

Comments and feedback are always welcome. Please reach out to Nimonik with any thoughts concerning the ideas in this document.

Please contact us at **info@nimonik.com** or at **+1-888-608-7511** to discuss how we can help your standards publishing organization improve access to standards, deliver more value and drive more revenue.

