COMPLYWORKS

White Paper Series

An Introduction to Compliance and Risk Management

2020

Contents

What is GRC? 3

Third-Party Risk Profile 8

The Cost of an Injury 12

Managing Supply Chain Risks 15

What is GRC?

What is GRC and where did it come from?

At a glance:

Governance *– is how senior leaders and the board of directors, oversee and manage the entire organization. They use risk and compliance information to mitigate, manage or avoid risks.*

Risk Management *– the processes used to identify, review and respond to risks that could impact the organization or prevent it from achieving its business objectives.*

Compliance *– is the consistency in which an organization adheres to defined laws, regulations and standards.*

The acronym "GRC" stands for governance, risk management and compliance. It came into being after several highly publicized, corporate financial, environmental and safety disasters, after which governments and independent regulators imposed stringent GRC requirements on organizations. While this is not a new change, many organizations are still struggling to improve their internal processes to better manage risk and prevent business and compliance failures.

As organizations adopt new business models, deploy new technologies and establish operations in other countries, they must determine the strategic impact of these changes on their organization and modify their governance, risk management and compliance priorities to suit.

Why should I care about GRC?

Organizations are facing increased complexity and unprecedented regulatory change. In Europe, despite many harmonized policies, each country also has its own laws and regulations. In addition, many Asian and North American countries have increased regulations in the last few years. This increase in legislation creates complexity in managing GRC requirements across countries, which can increase demands placed upon organizations.

In reaction to the increase in regulatory demands, many organizations have chosen to outsource their operations and regulatory burdens to third-parties to achieve significant cost savings. However, many employers miss the mark when establishing proper GRC controls between themselves and their third-party contractors which further exposes the organization. Governments have made it clear that while organizations can outsource the work, they cannot outsource the liability.

Increasingly, the board of directors is being held accountable for GRC non-compliance and for issues that it may not be very knowledgeable on. Regulators and governments have made it clear that an organization's operations are not only the responsibility of senior executives but also the board of directors. Misconduct or negligence by board members and the executive can result in fines, lawsuits and even jail time if found guilty.

What is GRC?

What is an integrated GRC program and what are the benefits?

Surveys conducted by Ernst and Young have found that organizations with embedded risk management practices outperform their peers.

Top-performing organizations implement on average twice as many risk management programs as those in the lowest-performing group.

*The top 20 percent of these top performing organizations generated **three times the level** of earnings as those in the bottom 20 percent.*

Despite the risks, many organizations do the bare minimum to meet regulatory requirements and this does not always have the intended effect of addressing its full scope of risk. Organizations can still experience GRC breaches, incidents or reputational impacts even though they have passed the bare minimum regulatory standards. One way to manage these increasing demands is through an integrated GRC program that is embedded in the organizational culture.

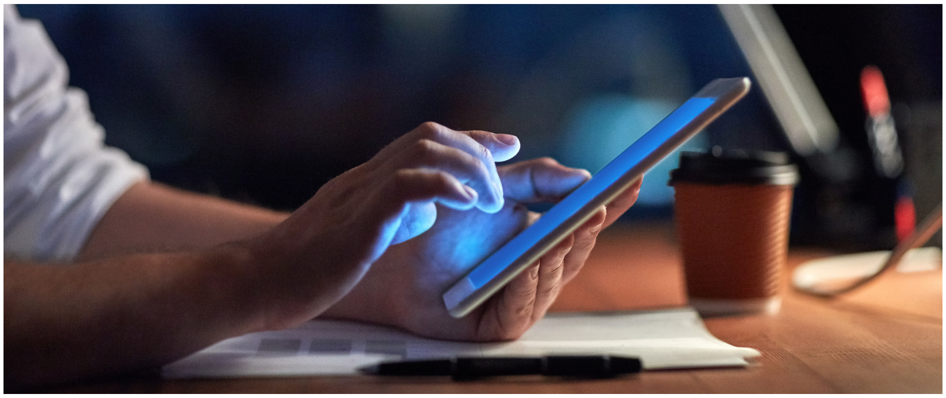
An integrated GRC program is a program that spans all departments of an organization and is ingrained into the organization's operations and culture. The most obvious benefits to an integrated program are streamlined data collection and the ability to quickly generate reports in one centralized platform. An integrated GRC program also helps organizations be flexible in constantly changing environments, mitigate business risk and prevent financial and material loss.

Some of the main goals of implementing an integrated GRC program are to:

1. **Establish long-term best practice protocols**
2. **Improve decision-making agility**
3. **Enable better capital allocation to the right initiatives at the right time**

These goals help to create a consistent corporate management culture, highlight inherent strategic, operational and regulatory risks and drive top to bottom accountability for key GRC objectives.

The benefits are clear. Instead of risk management being a cost burden, the research shows that there is a significant financial incentive for organizations to prioritize risk management and implement it into daily operations.



What is GRC?

What are some of the barriers to success?

A recent global EY survey found that only:

- ***49%** of organizations said they use some type of technology solution for risk management activities*
- ***29%** of organizations said they review risk dashboards/metrics on a monthly basis*

This shows that while our world continues to focus more on technology, organizations can be slow to adopt new solutions, even if the technology can increase visibility into the GRC program.

Some GRC programs are comprehensive and well thought-out in terms of strategy, processes and technology, but they ignore the human dynamic. For an effective GRC program to succeed, it needs an influential executive champion who can lead the program and help drive change. Failure to find a strong leader to drive the program forward can easily derail the initiative, no matter how well planned it may be.

Unifying risk initiatives and programs across an organization is a massive effort. Many organizations develop silos, which often duplicate personnel, processes and technologies, and prevent leaders from obtaining a clear view of the organization's risk landscape. This, in turn, limits organizations from effectively managing risk, while wasting time, money and resources.

Some of the most common pitfalls to implementing a successful GRC program include:

1. **Lack of transparency**
   Implementing a new GRC program in secrecy will limit employee adoption. The GRC team must clearly outline the new expectations and policy measures, the key indicators of success and the overall end goal.

2. **Continued investment in legacy technology**
   Many organizations fail to recognize the deficiencies of their home-grown systems (e.g. lack of integration or the inability to centrally store documents and records). Others manage their GRC program manually across disparate functional groups and geographies. Organizations need to ensure that the technology solution they select will empower the GRC program team, meet the demands of a growing business and is able to support both internal staff and third-party contractors, vendors and suppliers.

3. **Lack of program updates**
   A GRC program needs to be continually updated to stay current with regulations and must adopt regular program reviews, audits and program enhancements. This is where many GRC programs begin to fail.

What is GRC?

What are the best practices?

GRC is not a one-and-done process. Instead, it is an organization-wide program with multiple processes that need to be continuously improved. There are many GRC models that organizations can follow. Some of the more common GRC models from prominent GRC reference organizations include the Committee of Sponsoring Organizations (COSO), the GRC Capability Model (OCEG) and the International Standards Organization (ISO 19600).

Some of the best practices to implement an effective GRC program are to:

Review the organizational risk environment – conduct an analysis of all costs related to GRC activities for their internal and contingent workforce. Next, research and identify where there are existing gaps, overlaps or key areas of risk that need to be addressed. Finally, define the program's objectives and key indicators of success to ensure program transparency.

Empower the GRC program with integration – by supporting an integrated GRC program with representation from across the organization, teams can ensure that the program is consistently deployed organization-wide while allowing for local variances. It enables organizations to break down silos, streamline reporting and provide clear oversight to senior leadership.

Define and implement a risk-based "threshold" approach – define acceptable risk thresholds and implement them consistently across the organization. A key part of this is requiring all employees to undergo risk-related training and formalize acceptance of any policies/the GRC program. It is also important to embed GRC practices into business planning and employee performance reviews to ensure adoption and accountability.

Improve transparency – leading GRC organizations consistently communicate with stakeholders to ensure they are kept up-to-date. This creates accountability, especially if the communication has a sign-off requirement.

Standardize risk monitoring and reporting – it is important for organizations to build their GRC programs with clear objectives, indicators of success and established processes for regular monitoring and reporting.

Even with the use of these best practices, many organizations struggle with the adoption of new GRC programs because it is seen as additional work by employees. Fortunately, technology has created the opportunity for many efficiencies with new GRC programs, reducing duplication, improving risk management and ensuring that the right projects get funded at the right time.

COMPLYWORKS

What is GRC?

The power of technology and ComplyWorks

Historically, understanding GRC regulations for each country, state or province would require the help of many teams of full-time employees. This consumed a lot of resources as employees would have to manually collect and organize a significant amount of data, leaving little time left for reporting and analysis. With new technology and an increasingly connected world, technology is now empowering teams in new ways to overcome the challenges of the old manual-based methods.

Web-based solutions like ComplyWorks' Compliance Management System (CMS) can make it much easier to manage a GRC program. Our CMS allows organizations to manage their HSE and GRC programs by addressing the area of highest risk – management of third-party contractors. By working closely with our clients, we can help them gather the information most relevant to them. This allows organizations to have a constant view on their areas of risk to improve operations and provide oversight to senior leaders.

ComplyWorks' compliance management platform covers the entire GRC lifecycle – from basic prequalification to managing your third-party workforce at worksites locally, regionally or globally. We make GRC easy and achievable with our web-based integrated solutions.

ComplyWorks CMS solution can support a robust GRC program with:

- A centralized platform that enables decentralized decision making.
- Multiple department access with client designed user permissions.
- Facilitation of GRC training with knowledge retention.
- Invites and formalization of policy acceptance, procedures and overall program understanding.
- Storage capabilities to house the latest GRC documents, policies and procedures.
- Dynamic reporting and monitoring dashboard that alerts for non-compliance.
- Ongoing GRC communication transparency.
- The improvement of health, safety and environmental (HSE) outcomes.
- Increased end-user adoption, easy to use navigation and action driven dashboards.

Scroll down to keep reading our white paper series, or click here to request a free solution demo.

Sources:

1. A process model for integrated IT governance, risk, and compliance management; Nicolas Racz, Edgar Weippl, Andreas Seufert
2. GRC, 2012 Haymarket Media, Inc.
3. Governance, Risk and Compliance, Deloitte, Sarah Adams, Carlos Ruiz, Elias Rivera
4. Analysing The Governance, Risk And Compliance (GRC) Implementation Process: Primary Insights, Konstantina Spanaki and Anastasia Papazafeiropoulou
5. A Frame of Reference for Research of Integrated Governance, Risk and Compliance (GRC), Nicolas Racz, Edgar Weippl, Andreas Seufert
6. Exploring Strategic Risk, Deloitte
7. GRC Strategy Services, Ernst &Young
8. GRC Lessons Learned: Suggestions for Deployments, ISACA – San Francisco Chapter
9. Governance, Risk, and Compliance (GRC) White Paper, Secure Digital Solutions
10. The Human Side of GRC: The Essence of Governance, Risk and Compliance, Crisis Management International, Bruce T. Blythe and Rick J. Machold
11. Managing Governance, Risk and Compliance with ECM and BPM, The Global Community of Information Professionals, AIIM
12. Centralized operations - The future of operating models for Risk, Control and Compliance functions, Ernst &Young
13. How Mature is Your Risk Management, Michael Herrinton
14. EMR Diplomacy, Lawrence Richter Quinn
15. https://www.ey.com/Publication/vwLUAssets/Ey-global-governance-risk-compliance-survey/$FILE/Ey-global-governance-risk-compliance-survey.pdf

COMPLYWORKS

What does your third-party risk profile look like?

Digitizing compliance and risk management.

*In a survey by Deloitte (2016), **87% of the respondents experienced disruptive third-party incidents.***

Even in leading organizations – it is rare for someone in the organization to have an overarching view of all of its contractors and the risks each of them bring to the enterprise. It is even rarer that they proactively manage risk on a contractor by contractor basis.

The **digital transformation** age is underway and quickly rewriting business and organizational activities, processes, and business models in almost every industry as customers turn to digital touch points in preference of traditional ones. We are now in an age where customers not only expect products and services to make their lives easier, but they expect those services to be delivered instantly – whether provided by the company or third-party contractors.

"Structural changes needed to bring costs down and improve effectiveness in risk can be accomplished much like digital transformations in other parts of the business. Substantial value can be unlocked with a targeted digital agenda for risk – featuring fit-for-purpose modular approaches." (McKinsey, Digital risk: Transforming risk management for the 2020s).

Regardless of the macro-economic climate, compliance management is an accepted cost of doing business. While compliance can always be achieved through an army of people and a mass of spreadsheets; a manual approach is often ineffective and/or unsustainable. Going digital can be a key enabler and benefit driver for regulatory compliance.

If you're not using digital solutions to manage your risk and regulatory compliance – think again – because your competitor likely is. (Capgemeni) –In today's competitive landscape, organizations have pushed many of their internal processes out to third parties in an effort to reduce internal costs. They have sought to increase efficiency and productivity in non-core business processes, save on infrastructure and technology, gain access to skilled resources and improve company cash flow.

Third-party contractors are often **key customer touch points** for activities that enterprise customers outsource. Digitizing these manual workflows can significantly streamline processes, reduce risk and ensure that contractors comply with your customer experience and quality standards.

While independent contractors can provide increased cost savings and flexibility to employers – **organizational risk can be very high if contractor compliance is not handled properly**. Third-party incidents in health, safety and the environment, among others, can negatively impact organization's reputation, earnings, shareholder value and can shut down operations for extended periods of time; especially if there is an injury or fatality.

What does your third-party risk profile look like?

Supply chain disruption impacts the bottom line.

*A recent study from Capgemini – **warned that the probability of supply chain disruptions is only going to increase in the future,** with the economic impact of such disruptions increasing as well.*

The survey found that 40% of the disruptions were sourced to problems with second-tier suppliers that supplied products and services to first-tier operators and yet most of the organizations they surveyed indicated that they do not manage suppliers below the first-tier.

Disruptions anywhere along a supply chain – especially for those functions that have been outsourced to third parties – can translate into significant delays or fatalities if health, safety and environmental compliance risk management contingencies have not been put into place.

In 2010, a blowout on the Deepwater Horizon rig killed 11 crewmen and contributed to a disasterous environmental aftermath. BP and Halliburton knew weeks before the explosion that the cement they used to seal the bottom of the well was unstable. Further, lacking safety documentation & emergency procedures as well as differing policies on negative pressure tests all contributed to the disaster. BP and its contractors all paid billions in fines.

Boeing hired numerous contractors to help build it's 787 Dreamliner. Many tier one contractors further subcontracted their work to sub-contractors (tier two) who failed to deliver their components on time, despite having sub-contracted their work to sub-sub-contractors (tier three and four). Many of the parts did not fit together. Not managing the contractors effectively made the program billions over budget and years behind schedule.

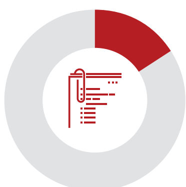
In 2014, Lowe's paid a $500,000 fine for not ensuring that the home renovation contractors it hires through its 1,700 retail stores adequately minimized lead dust, as required by federal rules on renovations, repairs and painting. Using a system to track the thousands of contractors, adequate training and sign-off could have helped mitigate the fine.

While impossible to eliminate risk completely, companies that identify risks in advance and plan for these contingencies are best positioned to survive third-party disruptions. Pro-actively managing risk can also strengthen supply chain sourcing strategies.

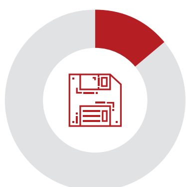
In a recent survey by ComplyWorks – we found that many enterprises still manage their contractors using:

66% spreadsheets

16% paper



14% legacy software



4% do nothing

What does your third-party risk profile look like?

Sustaining HSE programs is as important as implementing them.

Regulators are increasingly focused on how companies are managing their outsourcing and third-party risks.

Some health, safety and environment violations have seen fines reach millions of dollars. As such, many company boards have prioritized risk and compliance management as a top strategic priority.

These traditional approaches often consume considerable time and resources to track contractor relationships and can significantly increase risk to the organization. Further, many who manage contractor relationships lack the background, experience and time to do proper contractor prequalification, onboarding and support.

And while the work can be outsourced to third-party contractors – the liability cannot. Bills such as C-45 in Canada, OSHA in the United States, and strict environmental and industry specific regulations can result in significant fines or incarceration for violations.

How ComplyWorks can help

The benefits of digitizing your third-party contractor risk and compliance management program are often significant - but many struggle with where to start or what to do to transform their company to a digitized compliance management approach.

What if there was a way to accelerate your compliance and risk management digital transformation journey? A way to effectively manage third-party working relationships, maximize business performance, reduce compliance risks, and reduce contractor incident rates? What if there was a way to have contractors share the responsibility of inputting and taking ownership of maintaining their compliance information?

Our pro-active compliance management framework is built upon three core considerations – an easy to use compliance toolset, flexible reporting, unmatched support and ongoing monitoring. ComplyWorks has seen third-party compliance management evolve from contractor prequalification to compliance management at all levels of the organization – from corporate compliance management to operational worksite and workforce solutions.

ComplyWorks is a global leader in compliance management. Our solutions solve GRC needs across multiple departments within companies, in many different industries, all over the world.

What does your third-party risk profile look like?

Digitizing Compliance and Risk Management

We enable organizations to spend more time on their core business activities.

Typically, our customers have seen a payback period in less than 90 days once the solution is active.

ComplyWorks' three solution portfolios can be scaled to your individual company needs. They enable corporate and divisional groups to collaborate with each other in a way that makes sense to each – our key market differentiator.

Corporate Compliance – our contractor management solution often begins with prequalifying basic requirements. It also includes the popular "Communications" bundle. **Benefits:** reduced administration, fines and risk while improving contractor relationships, internal processes and communications throughout the engagement lifecycle.

Workforce Compliance – every individual worker, asset, or piece of machinery that comes to your site must have the right security clearances, medical approvals, proof of maintenance and ticket tracking. **Benefits:** reduced incident liability and downtime for contractors that are not trained for a specific location.

Worksite Compliance – track your contractors by worksite, project, division or country. **Benefits**: monitor contractor workforce, assets and specialized training completions – all at site level.

Make third-party contractor compliance easy! Join thousands of other industry leaders who subscribe to ComplyWorks trusted solutions to manage their governance, risk and compliance (GRC) needs.

Scroll down to keep reading our white paper series, or click here to request a free solution demo.

The cost of not investing in health and safety.

How much does an injury cost?

A natural gas processing facility out of Texas failed to follow National Fire Protection Association (NFPA) standards when installing a heater.

An employee was killed when he tried to light the heater and it exploded due to gas accumulation.

The jury awarded the plaintiff $82.5 million.

Health, Safety and Environment (HSE) initiatives are often misinterpreted as being costly and disruptive to operations. The result is that most companies do not adequately invest in HSE programs and supporting technologies until it is too late, even though many countries have strict HSE regulations requiring complete compliance.

Legislation on HSE violations has become increasingly punitive and tougher penalties for serious infractions can even carry a prison term. But while legislation is usually thorough, without an effective HSE program, merely following legislation isn't enough to ensure that zero accidents occur in your workplace.

While the exact cost of injuries and accidents may vary depending on the source, the reality is that the financial and social costs of accidents have significant impacts on the employees, business and society. A work-related accident or injury can not only put an employee out of work and affect their quality of life, it can also damage an organization's productivity and reputation – all of which can be very difficult to recover from.

Figures above in USD.

The most effective HSE programs are those that include procedures to sustain the program over the long term and ensure constant improvement. Without this vital piece of the plan, HSE programs will dissolve into non-existence.

The US Center for Disease Control and Prevention estimates that a fatal injury accrues an average cost of about $1 million in hospital costs. Adding increased insurance premiums, workplace replacement and loss of productivity costs to a fatality can triple the cost to nearly $3 million.

The cost of not investing in health and safety.

Many HSE violations are rooted in the failures of leadership.

A highway construction company in Florida had no safety system or plan in place for getting heavy construction vehicles safely off its median construction sites.

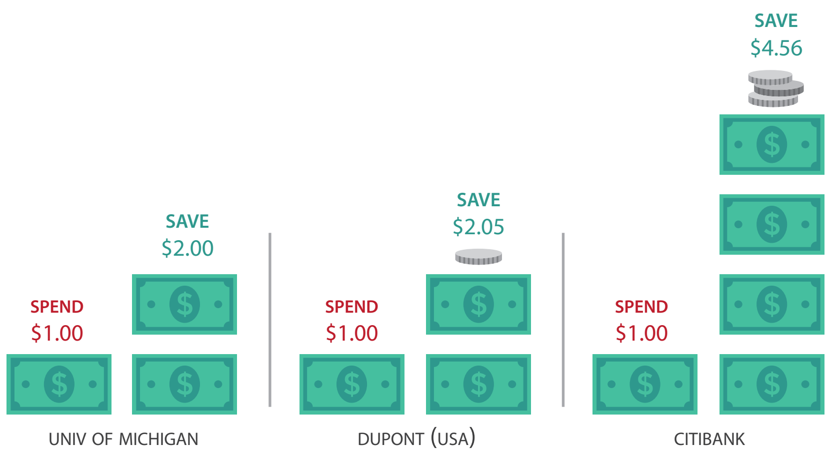
One of its employees moved an 80,000-pound tractor trailer and made a U-turn crossing all four lanes of oncoming traffic causing an accident that resulted in two fatalities.

The jury awarded the plaintiff $45 million

Research has shown that when board members and c-suite executives do not lead the implementation of HSE programs, there can often be a lack of uptake throughout an organization. The consequences of which can be severe. Conversely, when leadership takes a leading role in the implementation of HSE programs, organizations often benefit from improved employee uptake and benefits throughout the entire organization.

Big Benefits from Effective HSE Programs

While cost savings are often a benefit of an effective HSE program, safety's biggest return on investment is human capital. Years of HSE program adoption have shown us that there is a strong correlation between investment in accident prevention and the reduction of work-related accidents.



But the benefits are not limited to financial gains. Other benefits of effective HSE programs can include:

- Decrease in accidents and workplace risks
- Reduced premiums & claims
- Increased employee productivity
- Enhanced community reputation

The cost of not investing in health and safety.

Sustaining HSE programs is as important as implementing them.

In an olefin plant explosion in Louisiana, two employees died and another 167 received serious injuries. A jury found that plant owners and operators "were negligent with respect to the cause of the incident".

The jury awarded four workers $16 million.

Beyond the financial costs to the employer, there are other social, family and employee impacts that come from not having robust HSE programs and solutions. In addition, we know that compensation cannot replace a life, limb or the lifestyle employees had before an incident.

How can ComplyWorks Help?

One of the most effective methods to improve health and safety is software-enabled Governance, Risk Management and Compliance (GRC). GRC is an umbrella term for a comprehensive strategy to manage all initiatives relating to HSE, legislation and risks to an organization.

In a heavily competitive environment, where there is increased attention by regulatory bodies to ensure compliance and where decisions need to be made in a quick and informed manner; those relying on manual processes are at a disadvantage compared to those who use software-enabled solutions.

ComplyWorks' Compliance Management Solution (CMS) enables companies to get work done in a safe and environmentally friendly way to meet all HSE and GRC objectives.

Our web-based CMS has helped thousands of companies foster effective GRC practices, HSE programs and third-party relationships while reducing exposure to liabilities and fines.

ComplyWorks is a global leader in compliance management. Our solutions solve GRC needs across multiple departments within companies, in many different industries, all over the world.

Our solutions cover the entire GRC lifecycle – from basic prequalification to managing your third-party workforce at worksites locally, regionally or globally. We make compliance management easy.

Scroll down to keep reading our white paper series, or click here to request a free solution demo.

Sources:

1. British Safety Council - The Business Benefits – Health – Safety Literature
2. Canadian Center for Occupational Health and Safety - Bill C-45 Canada
3. Deloitte – Workplace safety analytics
4. Safety & Health Magazine - the ROI of Safety
5. Plant – Advancing Canadian Manufacturing
6. European Commission - Socio-economic costs of accidents at work and work-related ill health
7. Health & Safety Executive - Costs to Britain of workplace fatalities and self-reported injuries and ill health
8. EHS Today – Four Workers Awarded $16 Million by Jury in Second Williams Olefins Plant Explosion Case
9. Safety News Alert - Jury awards $82.5M in workplace death lawsuit
10. Cision PR Newswire - Jury Enters $45 Million Verdict in South Florida Crash That Killed 29 Year Old Medical Student
11. Aberdeen Group – Effective GRC Management

Managing risks in your supply chain

Introduction

90%

of firms do not conduct a risk assessment when outsourcing production – Harvard Business Review

85%

of global supply chains experienced at least one disruption in the past 12 months – Deloitte

The supply chain is the foundation of a business. It involves a vast and often complex system of organizations, people and resources that transition products or services through their journey from concept to completion. From the extraction of raw goods through to consumer purchase, hundreds of stakeholders can be involved in sourcing, designing, producing, transporting and delivering a finished product.

In the complex supply chain environment where many moving components are outsourced, it is critical for businesses to ensure they hire suppliers, vendors and third-party contractors that are compliant with legal and regulatory standards. This can be particularly challenging for businesses with international supply chains. When crossing borders, the business risks present themselves differently. Regulatory standards, legislation, cultural nuances, access to resources – these are just a few of the many elements that can vary drastically when taking your supply chain overseas.

The companies that proactively identify risks and plan for contingencies are those that are better prepared to maneuver disruptions when third-party risk manifests. But before your business can identify risks, it must first understand where to look. The most common risks in a supply chain include:

Economic

Environmental

Political

Technological

Social

Legal

According to the Harvard Business Review, organizations can expect an average share price decline of 40 per cent because of major supply chain disruptions. But the repercussions aren't just financial; businesses also face legal and reputational damage when these risks become reality.

Managing risks in your supply chain

The most common supply chain risks

Case study

In 2018, Hurricane Florence caused major flooding to buildings in North Carolina.

According to Convey, a bulk delivery management technology provider, delivery issues spiked 49 percent in the area as the storm hit.

Delays in the North Carolina ports reopening are estimated to have cost as much as $40 billion according to Oxford Economics.

The risks that most commonly manifest into supply chain issues can be separated into the following categories:

Economic

Currency fluctuations, volatile costs, shifting market share and the changing policy landscape are just a few factors that contribute to economic risk for organizations.

Environmental

Disruptive events such as natural disasters can have a major impact on the free flow of goods and services, including earthquakes, snowstorms, floods, hurricanes and more. Power outages, ceased transportation and damaged goods can quickly bring supply chains to a halt.

Political

Tension amongst geographical jurisdictions has a profound impact on businesses. Governments can issue tariffs, embargoes, or policy changes that put a halt to supply chains. In today's globalized world, the threat of sanctions is commonly used in political war.

Technological

Organizations face risks in the supply chain related to innovation, disruptive technologies and cyber security. Poor adoption strategies or a misunderstanding of the impact of new technology can have a negative effect on supply chains. Alternatively, failing to advance technology can also impede the flow of goods and services.

Social

International supply chains are often exposed to social risks related to human rights such as child labour, poverty level wages and unsafe working conditions. Suppliers also expose companies to bribery, corruption, tax evasion and other socioeconomic risks.

Legal

Complex legal requirements exist in all areas of the supply chain. From claiming patents and licensing, to managing customs and cross-border trade, organizations must be proactive. Legal risks related to product or service quality also extend beyond the supply chain to post-consumer delivery, as commonly seen for vehicle manufacturers or food suppliers.

Managing risks in your supply chain

Effectively managing third-party risks

*Companies that proactively manage supply chain risk spend **50 per cent less** on disruptions – Deloitte*

29%

of organizations have experienced supply chain waste, fraud or abuse in the past year – Deloitte

At the core of the supply chain practice is risk management. Organizations must ensure that their operations and third-party contractors are compliant with legal regulations, are ethically sound and are fiscally responsible. A successful third-party risk management program should take these three steps:

1) Create a risk-aware culture and control team

If dispersed across an organization, risk management can quickly become siloed, disjointed and ineffective. While risk management should be controlled from a central function, assigning champions from each department for cross-functional awareness and buy-in is the first step to risk alignment. Use past experiences to establish realistic goals and objectives while also forecasting for the future and taking into consideration the direction of the company.

2) Evaluate the risks

What is your organization's risk profile? If you are a high-end clothier and fashion brand, your risk profile may be entirely different than that of a commercial construction company. Examine each area of your supply chain, from raw materials through to transportation, for hazards related to each of the above areas. Strategize as to how you can mitigate these risks and develop emergency response plans for when they do escalate.

3) Monitor, audit, report and improve

Many organizations are using outdated tactics like spreadsheets and paper documentation to track their third-party compliance. If this sounds like your business, you could benefit from digitizing your compliance reporting. One, centralized system to automate contractor prequalification will help you to manage third-party risk throughout your entire supply chain. Choose a solution that allows you to:

- Track certificates, licenses and insurance for suppliers
- Assign training courses and requirements to contractors
- Send communications to vendors on policy changes
- Manage risk and incident reporting
- Assess regions, business units, worksites or supply chain functions individually

COMPLYWORKS

Managing risks in your supply chain

Automating supply chain compliance

Agencies that monitor supply chain compliance:

Canada
Canadian Food Inspection Agency (CFIA)

National Energy Board (NEB)

United States
Occupational Health and Safety Administration (OSHA)

Environmental Protection Agency (EPA)

Europe
European Medicines Agency (EMA)

European Agency for Safety and Health at Work (EU-OSHA)

Ensuring your entire supply chain is compliant with legal, ethical and industry regulations is a critical step for organizations who want to avoid financial, legal or reputational damage. If your business is still manually tracking compliance data, or isn't tracking it at all, here are three reasons why you should automate the process:

To produce quality, high-selling goods and services

When supply chain partners don't meet regulatory compliance or corporate standards, the product suffers. Setting standard expectations for supplier selection is only the first step. Auditing and maintaining those standards consistently is the key to sound supply chain compliance, which is where automation can greatly benefit your organization to reduce administration time and costs.

To create a consistent compliance records system

For an organization to have a holistic view, they should maintain one centralized system that allows them to simultaneously view data sets including supplier qualifications, noncompliance history, flagged issues, vendor communication and more.

Once this data is accessible from a single access point, it becomes relatively easy for manufacturers to improve quality assurance and operational efficiency by selecting the most suitable vendors for any given task. But when this process relies on manual workflows, the complex view of vendor compliance leaves more room for human error and opens the door to the consequences of noncompliance.

To use compliance as an agent for improvement

Compliance, at its core, is about maintaining a standard and adhering to best practices in all areas of a business. By automating compliance, businesses not only reduce manual time spent, avoid fines from non-compliance and mitigate risk, but they also commit to product quality and operational excellence. If your business outwardly focuses on maintaining compliant operations, it will naturally attract supply chain partners with that same standard of excellence.

COMPLYWORKS

Managing risks in your supply chain

Getting started with risk reduction

Thriving in today's complex and globalized business environment comes down to a proactive outlook on risk management. Understand that the risks of your supply chain partners are also risks to you, and taking steps to actively control them will only improve the flow and efficiency of your entire supply chain.

To get started with reducing your risk, take active steps to:
- Identify where risks exist in your supply chain
- Make an action plan for mitigating those risks
- Develop contingencies for when risk escalates

A compliance management solution will help you track, analyze and monitor your supply chain partners so you can rest assured that your business has done its due diligence to prevent disruptions and avoid regulatory fines or legal ramifications.

How ComplyWorks can help

ComplyWorks offers a suite of integrated solutions to improve environment, health and safety (EHS) compliance. Our solutions are designed to help you collect, verify, monitor and report on critical data, giving you a clear view into the potential risks of your entire supply chain.

Together with Ariscu, ComplyWorks can help you manage your third parties from the prequalification of supply chain partners through to the implementation and completion of work. We provide one central platform to empower your employees and suppliers to meet their requirements, so you can:

- Ensure different supply chain functions are compliant with local regulations by tracking employees and equipment at a site level
- Receive records with automated expiration reminders to track security clearances, insurance, tickets, certifications and more
- Prove your organization's due diligence by verifying your suppliers are ethical, responsible and fit for work

Sources:

Harvard Business Review – Supply Chain Risk: It's Time to Measure It

Deloitte – Understanding Risk Management in Supply Chain

Supply Chain Dive – How Hurricane Florence is Agitating Supply Chains

Supply Chain Dive – Delivery Issues Jumped 50% as Florence Hit

Supply Chain Dive – North Carolina Ports Delay Reopening