Business Continuity

How to Make Enterprise-Wide, Compliance Risk Management a Reality Today

Paying the cost of compliance risk management

If compliance risk is on your mind, you're not alone. Business uncertainty and regulatory compliance have both been in the news for some time now. Even before the global pandemic, Brexit and the unexpected 2016 election of Donald Trump, made regulatory overhaul in two of the world's largest economic zones, the EU and the U.S., a near certainty.

Nor had businesses completely recovered from the previous shock to the system: the global financial crisis of the late 2000s. At the height of the Great Recession, subnational, federal, and supranational bodies all issued sweeping financial reforms.

Those regulations majorly upped the ante on compliance risk management. As catalogued by London-based think tank JWG, the years 2009 to 2012 saw the publication of over 50,000 regulations across the G20. That number actually rose to 50,000 regulations in 2015 alone.

The cost of complying with those regulations has, of course, been steep for businesses. In fact, the volume of regulation is the key contributor to rising compliance costs. Compliance with the Dodd Frank Wall Street Reform and Consumer Protection Act, for instance, cost banks USD 36 billion, according to the publication Trade. Cumulatively, regulatory compliance cost banks USD 100 billion in 2016.

Financial regulation, though significant, isn't the only (external) compliance cost driver for firms. Australian enterprises, for instance, spent AUD 94 billion to administer and comply with public sector rules (in general).

Independent of external regulations, companies also develop their own set of rules, regulations, policies, procedures, and laws just to stay competitive in the market and/or limit exposure to unethical conduct.

Compliance with these internal mandates can have significant cost implications, as well. Australian enterprises spent AUD 155 billion to administer and comply with self-imposed rules and regulations, according to Deloitte.

Why doesn't the cost of compliance risk management add up?

So, businesses are paying a steep price for compliance risk management. But the degree of external and internal business volatility is testing the resilience of even the best-resourced programs. The question is, are compliance risk management investments actually holding up?

Well, if you ask the experts, the answer is no. Sure, companies are spending plenty on compliance, especially regulatory compliance. The problem is that firms are allocating resources without having first developed an overarching, enterprise-wide framework for compliance risk management.

Besides being costly and inefficient, this piecemeal approach to compliance risk management ends up limiting the situational awareness of senior leaders. Those same leaders need to make strategic business decisions based on an accurate picture of compliance risk.

Here's how it usually goes. Without a clear mandate from the top, individual teams begin managing specific compliance requirements as they see fit, usually with a different set of roles, activities, and systems.

With little communication between the (resulting) siloes, the risk of work duplication is high. Businesses might also end up paying double for advanced compliance management solutions that perform the same functions but aren't configured to exchange relevant data.

The lack of a centralised compliance risk management strategy and the siloing effects that deficiency creates aren't the only challenges to developing a culture of compliance. The volume of regulation a company must comply with also makes compliance risk management more operationally complex. Often decried in addition to the volume and pace of regulatory changes are:

- The availability and adequacy of resources to implement those changes
- Difficulty in meeting new regulatory expectations
- The potential for increased supervision from regulators

These challenges are all interrelated. More regulatory volatility bumps up compliance risk management costs, creating operational headaches. Those headaches are, then, exacerbated by a lack of an enterprise-wide, centralised approach to managing compliance risk.

The latter is particularly common in companies who tackle compliance risk management in house. After all, those companies are the least likely to have adequate processes, personnel, and tools to achieve basic compliance risk goals.

A lack of integrated compliance risk management and incident management software, in particular, means that teams have to rely more heavily on manual structures, i.e., spreadsheets, word processing, and shared folders. A fledgling company might get by like that. But those home-spun structures won't scale as firms get larger and reporting requirements increase in kind.

Achieving enterprise-wide compliance risk management

Clearly, the challenges are stark. But achieving efficient, cost-effective compliance risk management is possible.

Senior leaders just have to redirect their company's compliance efforts (and resources) away from piecemeal interventions and towards an enterprise-wide, compliance risk management strategy. Such a strategy would entail identifying the areas in the organisation with the highest compliance risk and then recalibrating the compliance risk function to monitor those risks.

So, what are some concrete steps to take to turn enterprise-wide compliance risk management into a reality. Firstly, we propose:

1. Developing a single overarching framework for compliance across the organisation. In turn, that unifying thread would govern processes taken and tools procured. But that strategy needs to be centred on a complete understanding of the company's compliance risk, especially existing levels of regulatory scrutiny, which are predictive of future scrutiny.

2. Running compliance risk assessments regularly, particularly after major business changes (COVID-19 comes to mind). After all, businesses aren't static. That's why these assessments should be done at least annually.

The same logic applies to the dynamic risk and regulatory environment around the business. Teams can't afford only to focus on once-in-a-generation reforms and crises. They also need to be on the lookout for minor tweaks to statutes, standards, regulations, and court rulings that can affect the company's compliance requirements.

Business partners need to be part of this calculus, as well. Vendors and contractors deemed unethical in the past create compliance risk and should be factored into a company's risk-monitoring framework.

After isolating all potential compliance risks, teams will move ahead and analyse those risks. Here is where you should be asking yourself, how likely an individual risk is to occur, and the potential impact of that risk were it to become a compliance incident?

The following step is compliance risk prioritisation. That means triaging risk based on pre-established criteria.

Companies don't have infinite resources to deal with identified compliance risks. Instead, they will have to use a standardised risk methodology, usually a risk matrix, to determine which risks they will seek to control. That assessment is often made based on (proportional) levels of risk.

Finally, the compliance decision maker, usually a C-level executive reporting directly into the Board's audit committee, will need to sign off on risk controls. Those are the actual strategies and tools teams will implement to manage high-level risk and promote compliance, either by mitigating the risk or eliminating it altogether.

To make this staged approach work, teams will need to ensure that their processes, policies, and procedures are all standardised. Further, they will need to ensure that the centralisation of the compliance function is reinforced by training and education, as well as clear reporting methods and mechanisms, which keep due diligence and risk assessment efforts current.

The compliance risk management lifecycle

Noticing overlap with the risk management lifecycle? That's no coincidence. The steps you'll take to centralise compliance risk mirror the key tenets of the risk management lifecycle.

- **Risk identification.** The identification stage consists of isolating all potential operational risks, whether recurring risks or potential one-offs. Risk identification involves staff across the business, not just C-suite executives.
- **Risk assessment.** Once identified, risks must be added to a risk register where they are to be assessed based on a number of factors, including how likely the risk is to occur, how frequently the risk will occur, and the potential risk exposure to human and non-human assets if the risk is not managed. The use of a risk matrix, an established risk assessment methodology, is a standard way of prioritising risks by likelihood and consequences. The severity of each risk can then be assessed separately, either as inherent, target, or residual risk, using a common methodology.
- **Analysis.** In analysing risk, teams will consider which risk controls (if any) to put in place. Additionally, teams will provide decision makers with a thorough risk analysis, a clear cost and benefit evaluation as well as outlines of possible alternative measures to take.
- **Decision.** Based on the analysis furnished, decision makers will choose the best control (or combination of controls).
- **Implementation.** Carrying out the decision taken requires having a plan for applying the selected controls. Adequate time and resources must also be allocated for any control measure to be successful. In addition, implementing controls requires clearly communicating your plan to everyone involved.
- **Monitoring.** Implementation, however, isn't the end of the story. Once they're put in place, controls will have to be consistently monitored to ensure they are working as expected.

The benefits of integrated, compliance risk management and incident management software

When it comes down to it, compliance risk management is just another way of monitoring relevant business changes. However, businesses change often, many times in ways that affect their compliance risk profile.

When those changes happen, compliance teams need be able to document them, whether recording observations or conducting investigations. Keeping information current is vital to effective compliance risk management.

Why? Well, data quality is often cited as a key challenge to effective compliance management. That's even for teams who used advanced technology.

It's still too big a task for manual processes. Organisations need automated processes supported by advanced technology to shore up reporting outcomes. Integrated, compliance risk management and incident management software gives those businesses the functionality needed to manage a compliance incident, as well as learn from that incident by investigating its root cause, so as to proactively prevent future incidents.

Don't choose any old solution, though. Compliance-related modules, in particular, should have the following capabilities:

- Capture compliance sources, e.g., mandates, laws, and regulations, or self-enforced, internal programs and policies
- Derive requirements from these sources
- Derive business rules from these requirements, which then dictate specific compliances items, or controls for one or more risks
- And proactively develop activities and capture contacts for compliance actors who must execute those items, as well as assign roles and responsibilities to contacts to determine which activities and business rules are relevant

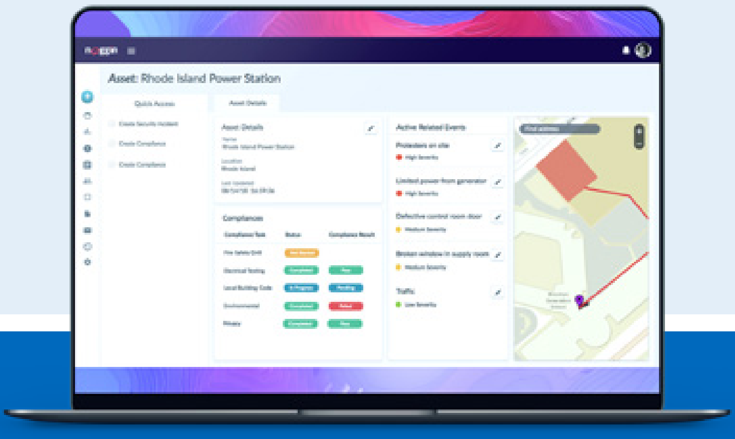
That's not all, though. To find out all the capabilities you need to execute on your enterprise-wide compliance risk management priorities, download our purchaser's guide to integrated risk management and work safety management software.

Like what you read? Follow Noggin on social media

@teamnoggin

facebook.com/teamnoggin

linkedin.com/company/noggin-it



noggin

for Business Continuity

Meet the next-generation tool for corporate crisis and business continuity management teams to collaborate, plan, track their response, and share information. Built on the Noggin Core platform, Noggin Business Continuity gives response teams and decision makers the tools to know what's happening, collaborate quickly and effectively, make better decisions, and enact the right plans to take action when it counts the most.

The Noggin Business Continuity solution pack is backed by the Noggin Library with hundreds of plans and best-practice workflows, out of the box, and installed in minutes.

To learn more,
visit: **www.noggin.io**
or contact: **sales@noggin.io**