

The 'Goldilocks Zone' of Compliance and How to Face a Regulatory Audit With Confidence

Frequent headlines of compliance breaches — and the likely morass of costly fines and penalties — are common in Australia's regulatory environment. Meanwhile, executives are held personally liable, finding themselves on the monetary chopping block and facing potentially career-ending outcomes and/or criminal sanctions.

Being on the wrong end of an audit by the Australian Securities & Investment Commission and other Australian regulators can result in consequences that are difficult to recover from. To avoid these repercussions, companies must continuously navigate a complex web of Australia's Commonwealth, state and territory laws. And companies in certain sectors — financial, energy and technology in particular, including their directors and shareholders — have heightened compliance obligations such as those adjudicated by the royal commission for the financial services industry.

Ultimately, all businesses want the ideal risk and compliance measures that optimise spend for a desired audit outcome. Lack of optimisation can result in overspending at best and disastrous consequences at worst. But finding that sweet spot of compliance — budgeting just enough on compliance activities to fulfill obligations and avoid fines without spending too much — often proves elusive, leaving companies with either soaring compliance costs or exposure to penalties.

Benchmarking as a way to access the Goldilocks zone of compliance

Finding the right, unique mix and balance of compliance activities for each organisation is key. So, how do organisations determine their Goldilocks zone — the optimal mix of compliance measures — in a way that meets regulatory expectations and simultaneously adds value to the organisation without dedicating finite resources to a compliance porridge that is too hot or too cold?

As a first step, they should gain an understanding of the full extent of their compliance obligations and leverage benchmarking through comparison to other regulated entities in a conglomerate structure of similar size and scale, underlying risk exposures, and regulatory obligations. Benchmarking enables an organisation to ensure that it is not lagging and can anticipate potential red flags raised by regulators.

Benchmarking insights can help bring the company into a Goldilocks zone of compliance so that they are not overspending on compliance activities whose costs outweigh the associated benefits. Obtaining this level of insight is attained through intimate familiarity with the Australian regulatory environment, deep industry expertise, and the ability to compare current maturity levels from a people, process and technology perspective against industry best practice frameworks and peers.

While some internal audit departments may be positioned to deliver this kind of value, the onus of business-as-usual operations, and, often, the lack of capacity and/or capability, create conflicting priorities in allocating the right people at the right time to perform targeted activities in preparation for ongoing regulatory scrutiny.

In these instances, partnering with an external compliance firm is often a feasible solution. In addition to familiarity with the regulatory environment, an external firm often brings breadth of experience across industries gained through exposure to multiple organisations within specific sectors. This enables insights on observed peer best practices through their work with other clients dealing with similar regulatory issues — information not typically available to internal teams.

The intent of engaging with external firms is not to outsource compliance activities, but to develop a partnership to collaboratively tackle problem statements and compliance obligations. This will often involve leveraging the organisation's existing internal audit resources and capabilities in synergy with the tools, frameworks and accelerators presented by the provider to effectively prepare executive management for any audit defence that may be required.

The value of an audit preparedness strategy

Most organisations understand their gaps and potential red flags requiring remediation, as well as what needs to be done to address them. The challenge lies in prioritisation and allocation of funding and resources to determine what can and should be remediated *prior* to an audit. More often than not, the timeline to audit does not afford organisations the liberty of achieving full compliance — this is where a viable, convincing and unified message to the regulator(s) must be developed and put into action via an audit defence strategy.

Whilst it is desirable and the ultimate goal to be compliant with all regulatory obligations, the regulators understand that organisations are at varying stages and levels of maturity in their compliance journeys. With the exception of instances of material noncompliance within the requirements issued by each regulator, there is a level of pragmatism in the application of these obligations. Having a robust audit defence strategy helps organisations manage regulators' expectations through demonstrating that a proactive plan of action is underway to address known gaps.

Audit preparedness and development of an audit defence strategy affords management the time needed to remediate gaps and build out their audit defence approach ahead of an external audit. Specifically, audit preparedness activities will:

- Equip executive management with a deeper understanding of and ability to articulate areas of exposure and prepare plans to address them ahead of an external audit.
- Support management in maintaining an informed dialogue with external auditors and regulators, which offers reassurance that gaps in compliance have associated plans for remediation — whether they are underway or planned activity as part of a broader prioritised remediation program.
- Demonstrate to external parties that the C-suite and executive management understand the remit of their roles and responsibilities, champion accountability, and take proactive steps to remediate known compliance deficiencies.
- Promote a risk and compliance culture across the organisation that strengthens governance and assurance processes, with systems in place to ensure sustained and ongoing compliance readiness for upcoming audits, as well as any audits in the future.

Ultimately, the value in audit preparedness comes from understanding the organisation's compliance status ahead of an internal/external audit and shifting the company's current compliance posture into the sweet spot appropriate for its industry, size, and underlying compliance and risk exposures. Taking the time to understand, benchmark, remediate and prepare can avert massive challenges in the complicated Australian regulatory landscape and keep executives out of the headlines.

Contacts

Leslie Howatt
Managing Director, Technology Consulting
Protiviti Australia
+61.488.301.794
leslie.howatt@protiviti.com.au

Lauren Brown
Managing Director, Internal Audit
Protiviti Australia
+61.437.601.774
lauren.brown@protiviti.com.au

Protiviti (www.protiviti.com.au) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, analytics, governance, risk and internal audit through our network of more than 85 offices in over 25 countries.

Named to the [2021 Fortune 100 Best Companies to Work For®](#) list, Protiviti has served more than 60 percent of *Fortune* 1000 and 35 percent of *Fortune* Global 500 companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.