BUILDING THE BUSINESS CASE FOR COMPLIANCE

From startups to enterprises—how to convince your board to invest in compliance

INTRODUCTION

Despite the increase in organizational exposure from tighter regulations, many compliance professionals still struggle to convince their board of directors of the vital business justification for a robust compliance program. More often than not, this is because the compliance program isn't directly tied to the organization's broader business objectives and is seen as a cost center, rather than a business enabler.

To fight this uphill battle, chief compliance officers need to understand the company's objectives and be able to explain how a robust program will support the organization in those efforts and ultimately protect all the company's hard work. Beyond the specific needs of your organization, there are a few common themes CCOs should be prepared to tackle when dispelling the myth of the compliance cost center. Before you approach your board, have a good understanding of the following topics:

- Direct Cost - And How to Keep it Down
- The Benefits of Efficiency & Insights
- Risk Mitigation
- Real World Impacts

Considering these core dynamics will help you make a strong business case for the funding for a comprehensive compliance solution that will fit your current and future needs and empower you to do your job.

DIRECT COSTS

If you want a successful, effective program, you'll need more than an off the shelf hotline solution. Understanding your needs (both current and future) and the options available will help give you a clearer understanding of the overall Total Cost of Ownership (TCO), which will in turn dramatically impact the program's ROI. Here are a few things that commonly directly impact program cost.

Solution implementation

Pro-tip:
Carefully weigh the implementation options and look at the total costs to implement and maintain a system over at least three years. For on-premise systems, make sure to add in internal resource costs such as IT resources, hardware maintenance, utility costs, etc.

Before 2010, most organizations opted for on-premise solutions. This costly approach requires the installation of on-site server infrastructure and ongoing maintenance from your IT department. According to Forrester Research[1], average implementation costs for on-premise solutions, including hardware, software and installation, range from **$200,000** to **$600,000**, with implementation timelines of up to **six months**. This doesn't bode well for the compliance professional trying to secure executive buy-in and budget for a comprehensive compliance program, nor is it conducive to a healthy ROI.

Luckily, newer cloud-based compliance solutions provide a more comprehensive, budget-friendly option. The solution is often up running in days or weeks—which is particularly important if you're facing new or heightened risk or trying to shore up your program as part of a deferred prosecution agreement. Additionally, cloud solutions do not require the company to maintain any systems or hardware. This results in a consistently predictable budget line and a more compelling argument.

Pro-tip:
Request security certifications from vendors offering cloud solutions. While a reputable provider will employ extremely rigorous standards, not all companies are created equal and it is important to select the right solution provider for your organization.

When making the argument for budget, noting how affordable modern compliance solutions are compared to past practices might come in handy. Alternately, if your organization still relies on a legacy on-premise solution and you're coming under fire for the cost of the program, switching to a cloud-based service is a way to both cut costs and update your approach.

Predict costs with a program road map

Identify your immediate compliance needs then create a road map of the additional needs you'll likely face in one, three and five years time. When you have a thorough understanding of this timeline you'll be able to better evaluate solutions and understand the long term cost of your program.

Focus on finding a single solution that provides for the majority—if not all—of your current and future needs. Selecting a solution that allows you to operate from a single platform reduces implementation costs, minimizes ongoing operational management costs and negates the need to add or change solutions in the future, resulting in overall major cost benefits.

Pro-tip:
Implementing a cloud solution with modular capabilities allows your organization to think big but start small. Consider traditional compliance functions as a single area of opportunity—not separeate initiatives. This will dramatically improve program ROI potential and protect you from vendor complexity.

Whether your compliance program is just getting off the ground or a decade old, understanding your needs (both current and future) and current shortcomings—and having a solution to those problems ready when you present to the board—will help you paint a more compelling picture and frame the program as an overall cost saver.

Cost of scalability

Scalability can refer to your expanding roster of compliance initiatives, but it also pertains to your company's footprint. Investing in a solution that can't keep up if your company goes on a hiring spree, makes it hard to train and communicate with new employees or simply can't support certain geographic locations will make compliance a burden on a growing or enterprise-level company, instead of the boon it should be. Not being able to keep up makes you look out of step with business objectives. Thinking about this issue ahead of time helps you seem more in tune with company goals and a proactive team player.

Pro-tip:
Ask about your solution provider's roadmap. If your preferred provider doesn't offer a feature that's important to your program, ask if it's in the works. Plus, knowing what's coming could clue you into a feature you didn't even realize you needed.

While it may be tempting to go with the least expensive option at the moment, not accounting for scalability all but guarantees additional cost for a future system replacement while creating "data islands," limiting the value obtained from your historical compliance data. These concepts should be a major linchpin in your discussions with upper management and the board.

Scalability is increasingly important as the world continues to march toward a global economy and workforce. With employees spread around the state, country or world, communication and consistent compliance enforcement is increasingly important but also increasingly complex. Matters become even more complicated with vendors, suppliers and subsidiaries in the picture—all of whom have a major impact on your company's compliance program and risk profile. If not properly trained and monitored, these entities can result in enforcement action against your company. Your compliance solution needs to seamlessly work for employees in the home office and halfway across the world in a timely manner and a way that they can access and understand. If it doesn't, you open your organization up to greater (unnecessary) risk.

A well thought out and implemented compliance program should naturally and effortlessly grow with your company and result in a positive ROI, not additional future costs.

EFFICIENCY & INSIGHT

While it can be hard to put a dollar sign on employee- and time-based resources, if an organization is using different solutions or relying on man power to perform crucial data-driven tasks, it's guaranteed to run into efficiency issues that will cost you money and headaches.

Silos aren't effective

Companies often start their compliance program by addressing a single solution area, such as a hotline. Over time, a maturing program will expand to include additional vital requirements, such as policy management, communication and training, case management, conflict of interest disclosure management and risk monitoring and management. If not carefully planned, this can result in a variety of services from a range of vendors. This creates several issues:

1. **Vendor complexity.** Piecing a compliance program together with a hotline from Vendor A, case management software from Vendor B, policy distribution via Vendor C and attestation tracking through email and Excel will result in a severely disjointed compliance program, making it much harder to gather and analyze data for overall program health.
2. **Increased costs.** As you introduce more systems you incur more program, implementation and maintenance costs—likely on different payment and contract schedules. Add in the time it takes to run and analyze this collection of programs and suddenly your costs—both real and in resources—are ballooning.
3. **Overall lack of trust.** A patchwork approach to compliance will inevitably leave gaps in your program—some of which you might not notice until they cause a real issue. With the multiple bills and exorbitant amount of man power required to run this ineffective program, the executive team and board are likely to question the validity and monetary worth of your program as a whole.

Recognizing this potential tar-pit can help you properly plan your

compliance program and give you a strong understanding of what to look for when evaluating solutions.

It's also worth revisiting your solutions set if your current approach is patched together. While you're likely locked into contracts, a bit of planning, negotiation and dedication can help you shed the silos and adopt a more effective, integrated approach that will benefit the organization.

Downfalls of inefficiency

There are several major drawbacks compliance professionals face when they rely on a disjointed program:

- Manually creating and analyzing reports that can take days to collate
- Struggling to make meaningful sense of data pulled from several sources
- Inability to make rapid decisions that could reduce business risk by prioritizing the most critical areas and issues
- Risk of human error when complying, documenting and analyzing important information
- Potential for inconsistent data collection, retention and analysis across locations, departments and individual employees

As a result of these drawbacks, it's difficult to prepare reports, properly monitor and manage risks and improve the overall quality of risk-based decision making.

Pro-tip:
Efficient technology adds value to programs by empowering compliance professionals to spend their time looking for important trends, focusing on key risk areas and reviewing and improving the program (a key expectation outlined in the US Federal Sentencing Guidelines).

Inefficiency isn't just wasted time, it's also the potential for catastrophic error—an important developing trend could be missed, attestation documentation could be neglected, risk hot spots could go unaddressed, etc. All these issues open companies up to increased regulatory risk and will inevitably effect the business overall.

When building your business case, don't let efficiency be downplayed. It isn't simply about making your team's job easier, it's about having the ability to effectively protect the company.

Identify trends

While an increase in issue intake might seem distressing, it can demonstrate an engaged workforce and give a sharp-eyed compliance professional the insight into risk situations that might not have been uncovered otherwise.

Unfortunately, without an effective solution designed to provide data-driven insights, compliance professionals struggle to quickly and easily understand connections between reported issues and their overall program. For example, with an integrated compliance program can you quickly tell whether a particular employee has completed his/her required training and attested to policies yet is still being named in complaints. Without an integrated solution that connects different pieces of your compliance program, these correlations can be next to impossible to catch without hours of time consuming and frustrating data collection and manual analysis.

Investing in an integrated platform that intuitively flags trends and draws your attention to recurring problem areas helps you identify weak spots in your program, recognize policies that need expansion or clarification and notice the correlation between policy attestation, training completion and incidents. This type of insight is what you should really be reporting to the board. It also can help you address issues before they become problems that might eventually lead to federal investigations and fines. A well implemented compliance program is both risk-based and forward looking. Without the ability to identify and react to trends, your program may not live up to federal standards.

RISK MITIGATION

"The organization shall periodically assess the risk of criminal conduct and shall take appropriate steps to design, implement, or modify each requirement ... to reduce the risk of criminal conduct identified through this process. ... If, because of the nature of an organization's business, there is a substantial risk that certain types of criminal conduct may occur, the organization shall take reasonable steps to prevent and detect that type of criminal conduct." - The Federal Sentencing Guidelines[2]

The Federal Sentencing Guidelines spell it out clearly, your compliance program needs to take into account and effectively address the individual risks of your unique organization. (Not to mention that the guidelines also clearly state that boards are directly responsible for the oversight of corporate compliance.) If your program—or lack thereof—fails to appropriately address compliance risk, you could face not only regulatory prosecution and fines, but the potential loss of reputation, business connections and brand image that could have long-lasting ramifications for your organization.

Identify risks

Part of a comprehensive compliance program—and a strong tool to help you justify investing time, money and resources—is the compliance risk assessment. If your organization has never conducted a risk assessment, the process will identify the biggest risks your company faces and clearly show which are most likely to cause harm and substantial impact. If you have conducted a risk assessment before, refreshing an old assessmen or undertaking a compliance-focused risk assessment can highlight new

or changing priorities and potentially identify weaknesses in your current compliance program.

Building a solid risk-based compliance program will help you focus your efforts and resources on the areas of most importance and with the potential to cause the most harm. This is both a best-practice approach and a good starting point for brining compliance up with the board.

Not all risks are created equal. Creating policies and training to address a less critical risk area before your program has a handle on top risks will not demonstrate a strong, well-implemented program. Harassment policies are important, but if you create policies around harassment before addressing high risk FCPA you are leaving your organization open to significant damages, which can be compounded by the fact that regulators may deem your program insufficient due to this misguided focus.

If your board isn't accustomed to digesting compliance reports and overseeing a program they may be looking for simple (and ultimately less important) stats—like hotline reporting statistics and case resolution numbers. While it's easy to give in and report these empty metrics, emphasize the importance of prioritization and layout a clear timeline for initiative implementation that addresses pressing risks first. Explaining the context of the information you're reporting will also give the board a better idea of the compliance department's focus and its impact.

Monitoring and mitigation

Identifying your risk profile is only useful if you're prepared to properly monitor and mitigate those risks, and a disjointed compliance program can introduce more risk into the equation. Without a complete picture of your program, you can easily miss important factors—such as poor attestation rates, lax training in at-risk locations, failing to update policies, etc. These holes in your knowledge open the door for a compliance misstep.

The most effective risk-mitigation programs have a consistent way to quickly and easily monitor all compliance activities and draw connections between different functions of your program. Integrating analytics and reporting across all compliance areas helps compliance professionals identify and understand risk issues rapidly and react quickly.

Benchmarking your program against itself and external standards is an excellent way to monitor effectiveness. Benchmarking your program also gives your board a good set of standards to review on a regular basis and a better window into program progress and impact. These efforts should also be supported by a regular audit schedule.

Pro-tip:
Establishing a consistent board presentation or template that tracks the same metrics from meeting to meeting will help your board quickly digest key program takeaways. This frees up time to highlight new issues, initiatives, key points and findings.

A risk assessment is no small undertaking and the best way to ensure a positive return on investment is to act on the assessment and implement an effective program to mitigate those risks.

REAL-WORLD EXAMPLES

The Securities and Exchange Commission (SEC) has not been shy about pursuing regulatory action in recent years and it has cost several companies dearly. From flat-out ignored compliance programs to poorly monitored programs, the following companies paid the penalty for not properly investing in an effective and efficient compliance program. Conversely, we'll look at a story where a well implemented program protected a major company from potentially heavy penalties. Together, these examples can help you put your conceptual arguments for a robust compliance program into easily relatable, real world context that will illustrate compliance's impact on business objectives and organizational health.

Pro-tip:
Visit SEC.gov to see the results of regulatory enforcement actions.

The dangers of a weak compliance program

Improperly addressing compliance and relying on a weak program holds significant consequences.

> *Eli Lilly and Company[3] agreed to a settlement after being charged by the SEC for improper payments that subsidiaries made to foreign government officials in Russia, Brazil, China and Poland. Eli Lilly agreed to pay more than **$29 million** to settle the SEC's charges. The company allegedly learned of the suspicious behavior but did not look into the potential violations. "Eli Lilly and its subsidiaries possessed a 'check the box' mentality when it came to third-party due diligence. Companies can't simply rely on paper-thin assurances by employees, distributors, or customers," said Kara Novaco Brockmeyer, Chief of the SEC Enforcement Division's Foreign Corrupt Practices Unit.*

It's not enough to have a program that covers your main company and employees. In the eyes of the SEC and DOJ, your compliance responsibilities extend to subsidiaries and third party vendors. If they commit a violation while working on your behalf you can—and as evidenced by the Eli Lilly case—will be held liable. This example should particularly touch a nerve with enterprise companies that commonly work with multiple vendors, third parties and subsidiaries around the world.

A bare bones or poorly planned and implemented program, or even a program suffering from restrictive budgeting, can end up costing an organization more than the initial cost of investing in an effective, efficient program that's designed to help professionals manage, monitor and analyze compliance activities and risks.

Examples like this exist for every regulatory issue and nearly every workplace related issue.

The cost of fixing a weak compliance program

Even well known organizations aren't immune to missteps or as attuned to compliance as they should be. When companies like this find themselves on the wrong end of a compliance infraction, the negative publicity and logistical issues can be just as bad as the fines.

> *Despite being a global organization conducting business in several countries, prior to 2009 Ralph Lauren did not have a strong anti-corruption program. It also failed to offer compliance training to or monitor the activities of its subsidiary in Argentina. Because of this gap, a long-standing practice of bribery of customs officials developed and existed for five years in Argentina, unbeknownst to Ralph Lauren. Upon implementing a more robust compliance program, the violation was discovered.*
>
> *Ralph Lauren self-reported the FCPA violation to the SEC and DOJ within two weeks of discovery and fully cooperated with an official investigation. Because of this act of good faith, Ralph Lauren received a non-persecution agreement. However, the company did not walk away scott-free. Ralph Lauren paid* ***$1.6 million*** *in disgorgement, interest and penalties. The company then incurred the additional costs of dismissing all parties involved with the bribery and terminating business contracts, implementing new compliance training and stronger third party due diligence measures, undertaking a full risk assessment of its global organization to identify any additional weaknesses and ultimately making the decision to stop conducting business in Argentina altogether[4].*

This undetected violation cost Ralph Lauren dearly, even with the non-persecution agreement. Not only is it important to implement a strong compliance program, organizations must ensure that it quickly and consistently rolls out to all employees, departments, locations and subsidiaries and third parties—and be studiously monitored. A violation while your program is being implemented is still a violation and can lead to legal action.

A good compliance solution must support multiple languages and be easy to access, use and understand for all your employees. It should also help you identify risk hot spots that require additional attention, training and monitoring. Not cutting corners can save you in the long run.

The power of a strong compliance solution

While seeing the cost of regulatory action a poor compliance program can result in should be enough to convince any board of the dire need for a robust solution, it's also worth noting that proving your organization has a strong program in place can save you from the negative fallout of a violation. In addition to Ralph Lauren's reasonably impressive non-persecution agreement, the DOJ and SEC have declined to fine other organizations entirely when it can be clearly proven that a best effort was made to prevent a violation.

> *Because of a strong compliance program with attentive compliance professionals and a detailed track record of training and reminders, Morgan Stanley[6] avoided regulatory action when one of its employees was found guilty of violating the FCPA by bribing a Chinese government official. Morgan Stanley was able to prove that the employee in question was expressly told that the individuals he was dealing with fall under the FCPA, received and attested to FCPA compliance training and policies and received 35 reminders. Because Morgan Stanley had a strong program in place and made every effort to avoid the violation, the Attorney General chose to bring enforcement on the employee, rather than the company. The employee went to jail for 10 years. Morgan Stanley did not face fines or prosecution.*

The Morgan Stanley case is often discussed as a shining example of a successful program and how a strong compliance program can save an organization money, hassle and reputation. The strength of this program relied not only on policies, training and communication, but a documented, auditable record trail that Morgan Stanley was able to use to prove the efforts of its compliance team. You can be sure a program like this wasn't cobbled together, but had full organizational support and buy-in.

CONCLUSION

While implementing a compliance solution may seem like a large expense, the benefits of a good program—and consequences of a neglected one—make it clear that compliance is worth the initial costs.

By focusing on the big picture, compliance professionals can clearly demonstrate that a robust solution is not only needed, but will ultimately save the organization time, money and resource. Choosing mix-and-match, disjointed solutions pieced together overtime without a clear vision of the program roadmap will only result in increased risk and the need to completely redo your compliance program in the future (maybe after you've already faced regulatory issues).

A program robust enough to handle the size, scope and risk profile of your unique organization (both now and as it changes) is vital. Even with an established solution in place, it's important to regularly revisit your program and conduct annual or bi-annual risk assessments to ensure you've identified and are mitigating key risks and are keeping up with expansion.

Properly investing in compliance today is a worthwhile endeavor for organizations that are concerned with brand, reputation and the bottom line—those are concepts your board of directors certainly understands.

REFERENCES

[1] Forrester, McClean, Build The Business Case For A GRC Platform, 2013 http://www.forrester.com/Build+The+Business+Case+For+A+GRC+Platform/fulltext/-/E-RES56677

[2] USSC.gov, Federal Sentencing Guidelines Manual, 2011 http://www.ussc.gov/guidelines-manual/2011/2011-8b21

[3] SEC.gov, SEC Charges Eli Lilly and Company with FCPA Violations, 2013 http://www.sec.gov/News/PressRelease/Detail/PressRelease/1365171487116#.UlXauWRVBd8

[4] SEC.gov, SEC Announces Non-Prosecution Agreement With Ralph Lauren Corporation Involving FCPA Misconduct , 2013 http://www.sec.gov/News/PressRelease/Detail/PressRelease/1365171514780#.UlXBx2RVBd8

[6] SEC.gov, SEC Charges Former Morgan Stanley Executive with FCPA Violations and Investment Adviser Fraud, 2012 http://www.sec.gov/News/PressRelease/Detail/PressRelease/1365171488702#.UlXFl2RVBd8

convercent™

Convercent's risk-based global compliance solution enables the design, implementation and measurement of an effective compliance program. Delivering an intuitive user experience with actionable executive reporting, Convercent integrates the management of corporate compliance risks, cases, disclosures, training and policies. With hundreds of customers in more than 130 countries—including Philip Morris International, CH2M Hill and Under Armour—Convercent's award-winning GRC solution safeguards the financial and reputational health of your company. Backed by Azure Capital, Sapphire Ventures (formerly SAP Ventures), Mantucket Capital and Rho Capital Partners, and based in Denver, Colorado, Convercent will revolutionize your company's compliance program.

Request a demo today!