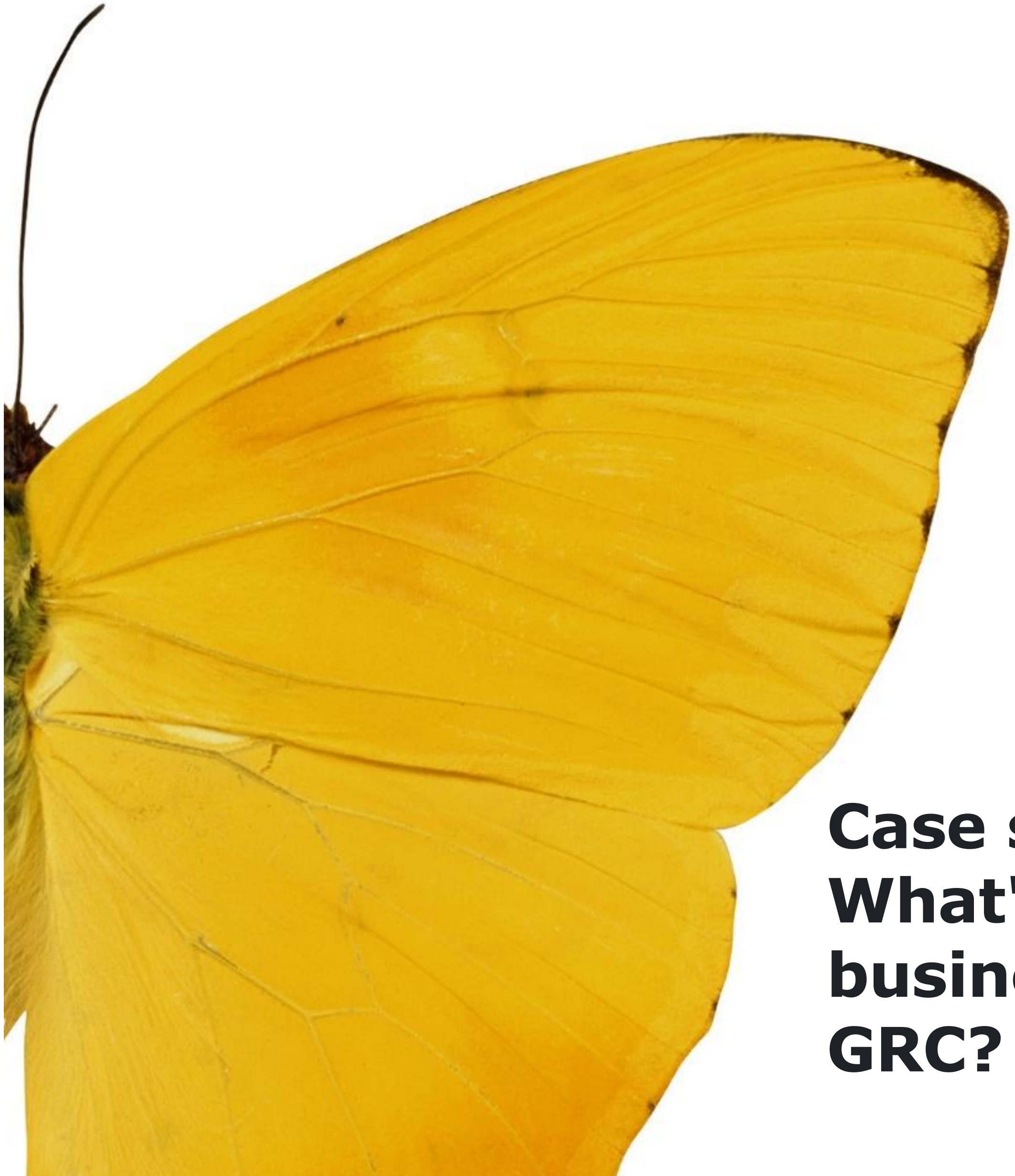

Case study: What's the business case for GRC?

Shanmugavel Sankaran
Chief Nixer | FixNix Inc.,

Governance, risk and compliance (GRC) can be a dauntingly complex undertaking.

But for Cipla, the alternative was even more complicated.

DOES GOVERNANCE, RISK AND COMPLIANCE (GRC) REALLY PAY OFF?

It's a valid question for any organization that's looking to formulate a corporate strategy and implement software for managing GRC.

Leaders at pharmaceutical company Cipla say the answer for their organization is an emphatic "yes," citing a number of concrete benefits. Let's dig into the details of their GRC business case.

In this Cipla GRC case study:

- Cipla's environment
- Upgrading risk management processes
- Benefits captured
- Overcoming hurdles in GRC implementation
- Lessons learned

CIPLA'S ENVIRONMENT

Cipla was founded in 1935 and currently has about 22,036 employees with 34 manufacturing units in 8 locations across India and has presence in 170 countries.

Cipla Limited is an Indian multinational pharmaceutical and biotechnology company, headquartered in Mumbai, India;Belgium, & Surrey in the European Union; and Miami, Florida, in the United States; with manufacturing facilities in Goa (eight), Bengaluru (one), Baddi (one), Indore (one), Kurkumbh (one), Patalganga (one), and Sikkim (one), along with field stations in Delhi, Pune, and Hyderabad. Cipla primarily develops medicines to treat cardiovascular disease, arthritis, diabetes, weight control and depression; other medical conditions.

As of 17 September 2014, its market capitalisation was ₹517 billion (US$8.1 billion), making it India's 42nd largest publicly traded company by market value.

It was founded by Dr. Khwaja Abdul Hamied as 'The Chemical, Industrial & Pharmaceutical Laboratories' in 1935 in Mumbai. The name of the Company was changed to 'Cipla Limited' on 20 July 1984. In the year 1985, US FDA approved the company's bulk drug manufacturing facilities.

In 1994, Cipla launched Deferiprone, the world’s first oral iron chelator. In 2001, Cipla offered medicines (antiretrovirals) for HIV treatment at a fractional cost (less than $350 per year per patient). In 2012, the company slahed prices of three life-saving cancer drugs by 50-64%.

Cipla sells active pharmaceutical ingredients to other manufacturers as well as pharmaceutical and personal care products, including Escitalopram (anti-depressant), Lamivudine and Fluticasone propionate. They are the world's largest manufacturer of antiretroviral drugs

Cipla has 34 manufacturing units in 8 locations across India and has presence in 170 countries. Exports accounted for 48% ₹49.48 billion (US$770 million) of its revenue for FY 2013-14. Cipla spent INR 517 cr. (5.4% of revenue) in FY 2013-14 on R&D activities. The primary focus areas for R&D were development of new formulations, drug-delivery systems and APIs (active pharmaceutical ingredients). Cipla also cooperates with other enterprises in areas such as consulting, commissioning, engineering, project appraisal, quality control, know-how transfer, support, and plant supply.

As on 31 March 2013, the company had 22,036 employees (out of which 2,455 were women (7.30%) and 23 were employees with disabilities (0.1%)). During the FY 2013-14, the company incurred ₹12.85 billion (US$200 million) on employee benefit expenses.

In 2014, Cipla decided to embrace a formal GRC strategy "because it was the best way to manage through a thicket of simultaneously occurring changes in our business and regulatory environment," says Amit Pradhan, Group Chief Information Security Officer.

The company's business strategy has evolved in recent years from a holding company to an integrated operating model, creating greater complexity in the organization and the solutions it provides to clients, Amit Pradhan says.

"The external environment has also changed, and today we face more government regulation and non-government standards, such as [FDA]," Amit Pradhan says.

"Navigating all these challenges at the same time required a much more structured approach to governance, risk and compliance than our previous spreadheet-driven methods."

Before deploying FixNix's Cloud GRC platform, called FixNix Risk, "I would have characterized our environment as diversity on steroids," Amit Pradhan says. "We had diversity of understanding about what risk assessment and monitoring means. We had diversity of understanding about what was required or expected, and diversity of methods and practices. As a result, we had an absolutely enormous challenge to try to develop a picture of our enterprise risk and enterprise compliance."

There was no common understanding or vocabulary or process related to risk, Amit Pradhan says. "The good news is that, with enough effort, we were able to manage risk, but there was a challenge of being able to document that to our board of directors or regulators, and to look beyond the horizon. All of a sudden, our diversity had become a risk itself."

UPGRADING RISK MANAGEMENT PROCESSES

Today, the company's GRC focus is on risk assessment, compliance monitoring, policy management and remediation tracking. Because Cipla provides technology ¬solutions to the financial services industry, it is regulated by the FDA, as if it were a pharmaceutical company itself.

Since the 2008 market collapse, "it has been critical to our regulators and clients that we have rigorous processes in place to identify, understand, control, remediate and monitor our risk and compliance posture," says Amit Pradhan, Cipla Group CISO.

To meet that challenge, the company realized it had to upgrade its processes and tools, and it standardized its approach to GRC across an enterprise where decentralization formerly ruled.

Cipla began its program upgrade knowing that it needed a technology solution to support its initiatives. "But we were concerned that the technology solution could drive the program rather than the other way around," Amit Pradhan says.

"There are some solutions in the market that, in my view, appear to be dogma-driven. Someone thinks they know the answers and have a one-size-fits-all approach to how risk and compliance monitoring ought to occur."

The company wanted software that addressed the widest possible range of regulatory and third-party standards. "If we only needed to be compliant with Gramm-Leach-Bliley or with HIPAA or with some other single regulation," then flexibility wouldn't be as much of a concern, Amit Pradhan says. "But all those [regulations], and more, matter to us."

First, Cipla carefully built its GRC program to meet the organization's needs, and then it selected the technology to support that program. Managers opted for FixNix Risk after exploring many alternatives in the market. So far, they have been pleased with the technology, and say it has had a transformative effect on the risk-management program.

"FixNix Risk has empowered our risk-management staff to operate on a higher, more strategic plane," Amit Pradhan says. "In the past, our team spent a disproportionate share of its time manually collecting and manipulating data. Just getting to a baseline understanding of our risk profile consumed most of our available horsepower, leaving far too little time for analysis and problem-solving."

The software has enabled Cipla "to turn our paradigm on its head," says Amit, and to shift her team of former risk tacticians and number crunchers into enhanced roles as risk strategists, allowing them to have a much greater effect on the organization.

"It allows us to get beyond that almost clerical use of people," he says. "The system does that [number crunching] really well. It has taken our people from being focused on minutia to focusing on the big picture."

BENEFITS CAPTURED

The software automates the tasks that were consuming the majority of this team's time, including data collection, aggregation, workflow and reporting. Now, armed with useful, organized output from the system, "they can primarily focus on deeper analysis and engagement that leads to more effective remediation and control of the risk in our organization," says Amit.

Cipla is also benefiting from the workflow and configuration management components of the GRC software.

"In a complex enterprise like ours, inputs and approvals may be needed from multiple units within the company to complete a single assessment," Amit says.

Producing a risk profile via the older method would have required seven to 10 more staff members and would have cost Cipla an additional half-million dollars

"FixNix Risk workflow management expedites our processes and eliminates sneaker-net movement of files. Also, organization and hierarchy changes that formerly required many hours of manual effort to implement are now a simple matter of system configuration that takes only minutes, he says."

Reporting is also simplified by the GRC system's standard reports and its data export feature, which allows the firm to create reports using tools of its own choosing, Amit says.

The software allows Cipla to produce a dashboard for managers, which shows them a color-coded picture of exactly where risk resides in the organization. "It makes it abundantly clear that this is where you ought to be focusing on remediation efforts, investments, policy, people issues," Amit Pradhan says.

"Rather than spending all that time ¬figuring out where the risk is, we now get that intelligence from the system, and can spend more time addressing what we've found."

The company estimates that to produce the type of detailed risk profile it gets from the software over a three-month period now, it would previously have taken about six months using Cipla's old manual process. The older method would also have required seven to 10 more staff members and would have cost Cipla an additional half-million dollars.

Another benefit is the increased credibility the enterprise risk management team has gained in its interactions with management, regulators and members of the board of directors. "We have much broader, deeper and better-presented data than ever before," Amit Pradhan says.

"I can now engage with any of my team's constituencies with greater authority and confidence, and this has strengthened all of these key relationships."

Because it has contacts with other corporate users of the software, Cipla has benefitted by learning about how others have successfully handled GRC processes. Amit is a member of an advisory group for users of the product, and he and Amit Pradhan have taken advantage of formal and informal opportunities to interact with other companies using FixNix.

"Although every company is different, the journey to maturing the risk management function has common elements, whatever your business," Amit says. "We have appreciated the opportunity to interact with others who are at different points on the maturity curve, and who have already figured out how to meet a challenge that is new to us."

OVERCOMING HURDLES IN GRC IMPLEMENTATION

Exchanging best practices and getting advice from more experienced GRC practitioners was especially useful for Cipla because the company faced a number of challenges during its GRC implementation.

For example, when the enterprise set up a new comprehensive information security standards program about a year and a half ago, that created another rule set for GRC.

"So now we were adding another layer to our control policies, and we needed to learn how to build that" into the software, Amit Pradhan says.

"This was a need we didn't anticipate, but we had the ability to talk to others and our advisers at FixNix, who recommended a policy-management module that links directly with existing FixNix Risk content. It saved us many months and at least a couple hundred thousand dollars of exploratory work."

It's important to remember that GRC is a process supported by technology, and companies should avoid focusing only on the software

An even bigger challenge for Cipla was creating a common understanding of the logic, discipline and vocabulary of professional risk management, Amit Pradhan says.

"Cipla was formed through the acquisition of many companies across globe over the past many years, and until a few years ago most of our business units operated with considerable autonomy," Amit Pradhan says. "They managed risk the way they always had, and their practices pre-2007 reflected varying degrees of maturity and sophistication. Lacking common systems and processes across our enterprise, we achieved diverse results."

The value of a packaged solution is that it doesn't skip steps, Amit Pradhan says, "It enforces a rigorous, process-driven approach to risk management that is inherently missing in the kind of homegrown, paper-based processes we used before."

The FixNix Risk implementation has been successful largely due to the comprehensive training of users within the company, and because the tool itself anticipates that users will approach the system with varying levels of understanding.

"Essentially, there's a lot of help built into the tools, and the user interface is solid," Amit says. "In fact, FixNix was willing to take our suggestions and incorporate them as core product functionality."

Because the software was new for everyone, "we chose an implementation path that included a lot of professional services support," Amit says. "This allowed us to stage our roll-out on time, with no surprises, and excellent user support. Usability was one of our most heavily weighted selection criteria, and we feel like we hit a home run with FixNix Risk."

The most challenging aspect of the GRC implementation was security. "Because we have so many business units and a complex hierarchy, the ability to set user permissions at a granular level is very important to us," Amit Pradhan says. "We utilize a 'least privilege' security model, and it has taken time for us and FixNix to fully develop this functionality."

Amit Pradhan thinks two related trends are conspiring to make having a robust GRC strategy and software implementation more of a necessity for many companies.

"First, we seem to be in an era of re-regulation, and every new regulation brings new compliance obligations," he says. "Second, contract and vendor-management processes are being used more frequently to shift the onus of compliance obligations onto vendors."

From a vendor's perspective, sometimes there is a business reason to consider accepting contract provisions from a prospective client that create unusual or incremental risk. "We believe that the better we understand our existing risk profile, the more intelligently we can evaluate nonstandard client terms," Amit Pradhan says.

"When we do agree to unusual requests, we also need the capability to monitor our own compliance. This is a huge advantage of our FixNix Risk implementation. It allows us to accept risks that would be unthinkable if we were flying blind."

Like a number of industry experts, Amit Pradhan thinks it's important to remember that GRC is a process supported by technology, and companies should avoid focusing only on the software.

"An effective risk-management program is part of an organization's quest for self-awareness," Amit Pradhan says. "To begin with technology rather than process is to risk letting the tool define the program rather than support it. Before you can decide which tool meets your needs, you need an overarching process that helps assess your business and its assets, vulnerabilities and risk appetite."

Only when a company understands these baseline concepts can it really know how a GRC software solution will fit into its risk-management program.

LESSONS LEARNED

- The more decentralized the enterprise, the more complex the GRC implementation will be. Do not underestimate basics such as technical project management and behind-the-scenes network readiness.

- Your existing risk-management team might fear that adopting GRC software will eliminate their jobs, or change their job functions in ways that take them outside their comfort zones or skill sets. Work with your GRC software provider and its user community to help your team understand the opportunities for professional growth the new system will provide and other potential benefits of the change.

- Don't try to use every bell and whistle available in your GRC solution on day one. Start small, simple and focused, with a clear idea of the outcome you want. Grow into your system.

- Think of your GRC system as a flashlight, shining into the dark cupboards of your organization. You will be surprised how much better your risk and compliance fact base and reporting capabilities are immediately after you get your new system up and running. You will also be surprised by how hard it is to determine how to most effectively use the increased insight to improve risk management in your organization.