



Wanna journey with FixNix to streamline your 1000 page regulations?

FreshGRC™



FixNix.co



RiskDynamiks.com

Invested, Mentored, Steered by good folks of



Business use case for GRC ROI





MAKING THE CASE FOR **GRC SOFTWARE**

Our example organization possesses the following characteristics:

Area of Operation:

GLOBAL

Number of
Employees:

60,000+

Annual Revenue:

\$35 BILLION



Business Units:

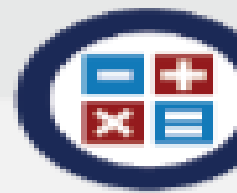
40

Processes
per Unit:

2-5

Controls per
Business Process:

8-10



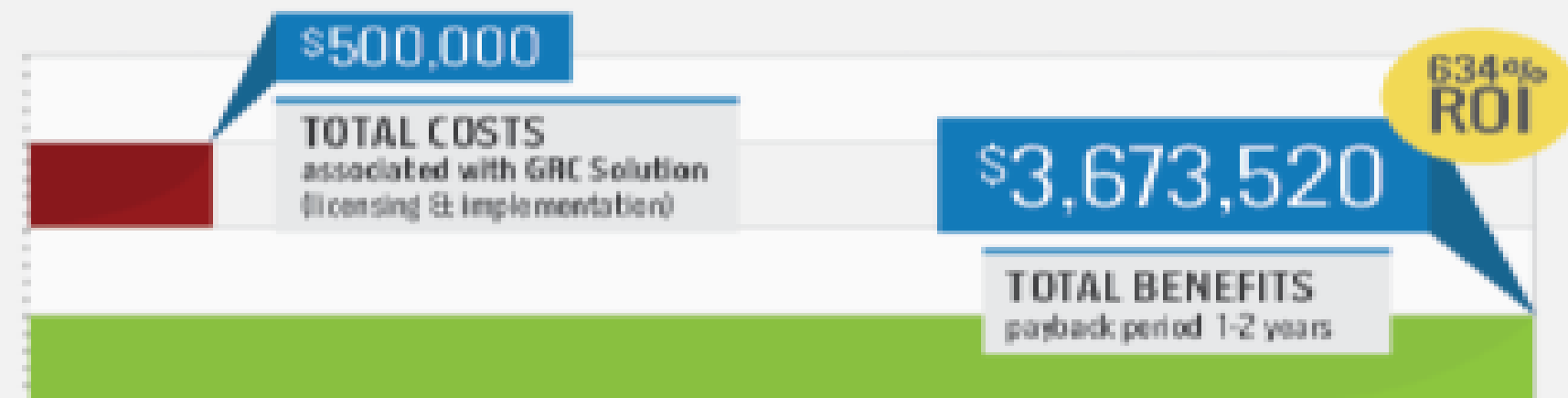
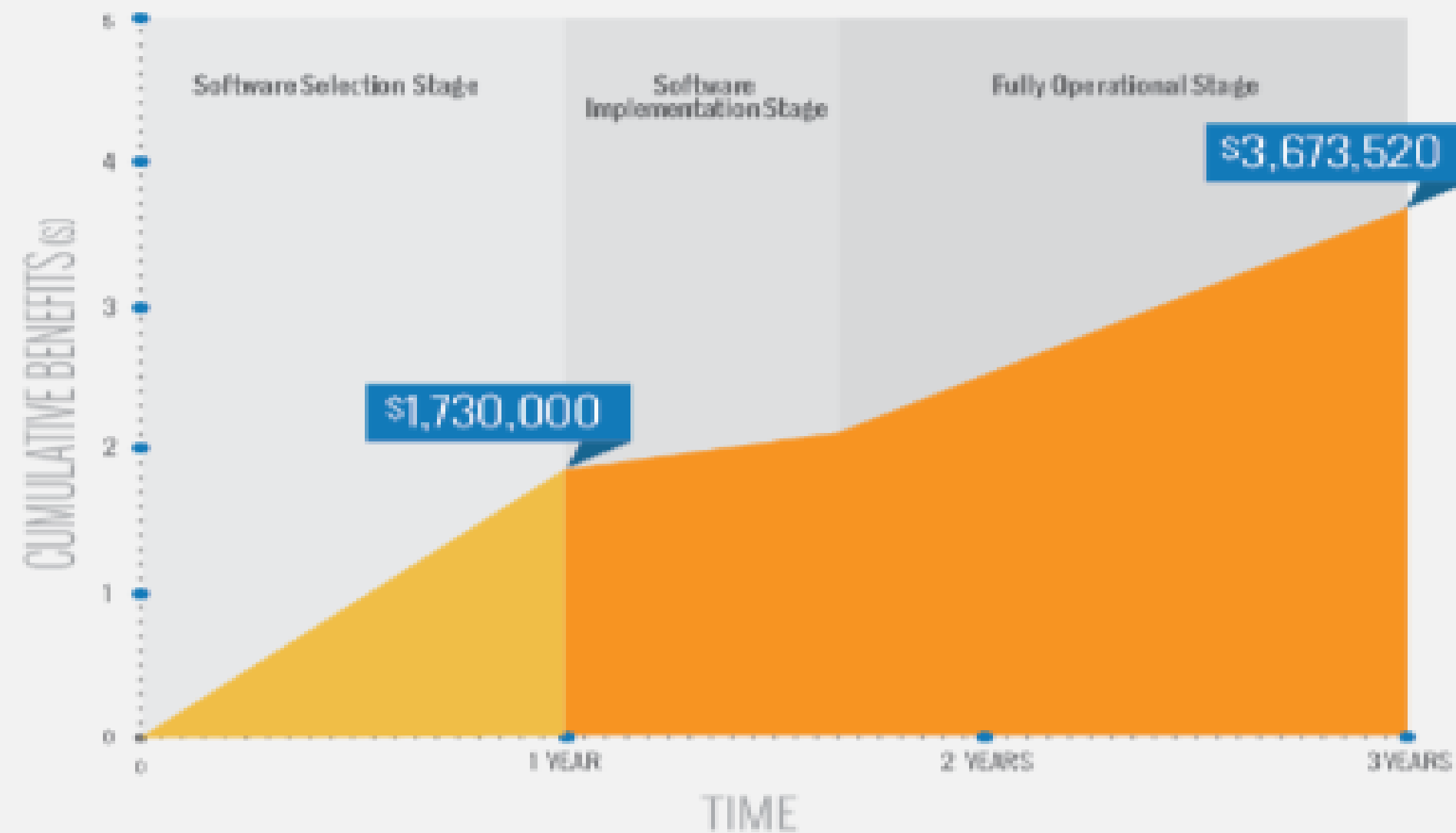
ROI CALCULATION



Procurement-Based Benefits

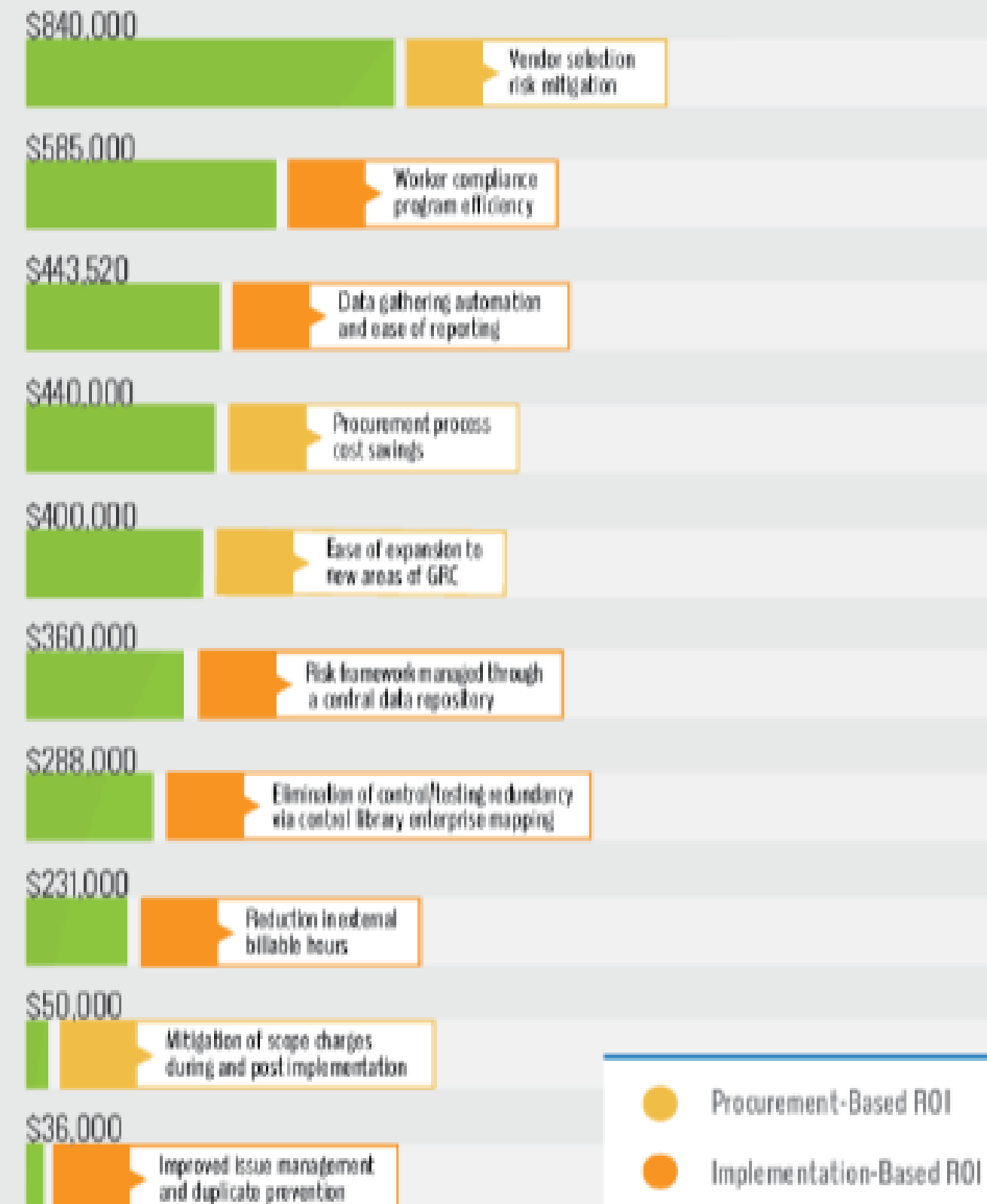


Implementation-Based Benefits



*Benefits fully realized over a period of 3 years

Efficiencies Achieved Within the Organization:



Business use case for GRC ROI

Challenges in GRC



CURRENT STATE OF GRC: THE CHALLENGES

GRC professionals are accustomed to change driven by professional standards or by regulators. Until recently, the vast majority of GRC projects were driven by external regulations or compliance requirements that offered little option over whether, when or how to implement.

For example, the Sarbanes-Oxley Act and related PCAOB audit standards drove significant effort and influenced the methodology used to assess internal control over financial reporting. The business case for Sarbanes-Oxley compliance was simple: comply at any cost or face significant negative market impact or jail time for the CEO or CFO. The same can be said in regards to the mandated adoption of XBRL and many of the provisions of the Dodd-Frank act that are driving business change.

While response to these regulatory changes is necessary, the implementation of process change in isolation has resulted in an environment of working in silos, conflicting information and terminology, disparate technology, and a lack of connection to business strategy

CHALLENGE 1: WORKING IN SILOS

In response to meeting the compliance requirements of a single regulation or driven by internal reporting structures and traditional functional roles; legal, internal audit, risk management, and compliance professionals often are found to work in very rigid silos, focused on a tactical set of departmental objectives. In this environment, too many white spaces exist where information is not exchanged and there is a lack of accountability among GRC groups. The obvious problem with this missing connection and functional overlap is inefficiency. A variety of GRC groups often duplicate efforts, wasting GRC resources and management time.

CHALLENGE 2: CONFLICTING INFORMATION AND TERMINOLOGY

With more than 12,500 regulatory changes made in 2010, keeping up with change and analysis on regulatory information is a challenge for most compliance officers. This challenge is amplified by the fact that most organizations do not dynamically link these changes and information to a standard set of policies, risks and controls. Historically, legal, audit, risk and compliance professionals have all operated using a different “language” of GRC and unique definitions for policies, risks and controls. The end result is the inability to effectively share information and the reporting of complex sets of redundant, overlapping information to the board.

CHALLENGE 3: DISPARATE TECHNOLOGY

GRC technology includes information solutions, documentation and workflow software, business and legal research, screening, and reporting and disclosure solutions. A natural outcome and a potential driver of a siloed approach to managing GRC business processes is using different technology solutions to manage each discrete assurance area. When a company uses disconnected solutions to manage risk management, internal audit, policy management, and compliance, it runs the risk of inconsistencies and inefficiencies that may lead to unnecessary high costs. Multiple systems with multiple deployments cause conflicting versions of the truth. A standardized suite of solutions resolves these problems and establishes a single source of truth for the entire enterprise.

CHALLENGE 4: NO CONNECTION TO BUSINESS STRATEGY

Since most GRC process change has been driven by a reaction to a specific regulatory requirement, most organizations have not mapped their GRC processes to business strategy. This challenge becomes significant when trying to justify an end-to-end GRC project. If the perception of the GRC professionals is that of cost center functions addressing tactical audit or compliance initiatives, a more comprehensive GRC project will be difficult to justify. To overcome this perception and gain the proper funding and support required, a business case that links

BENEFITS OF END-TO-END GRC

Companies who are most successful at deriving the tangible benefits of end-to-end GRC start with a clear plan and set of objectives on how to drive this business value. As with all complex building projects, the building of a GRC initiative requires a detailed blueprint to define the scope, taxonomy, methodology and outcome of the project. In analyzing the benefits of GRC, the project should focus on five major points:

1. Defining the connected GRC lifecycle
2. Establishing a common language for risks and controls
3. Implementing consistent reliable methodology
4. Developing transparency, monitoring, reporting and disclosure
5. Leveraging technology

FixNix Cipla Case Study



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 slashed prices of three life-saving cancer drugs by 50-64%.

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 spreadsheet-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."

Research on GRC ROI

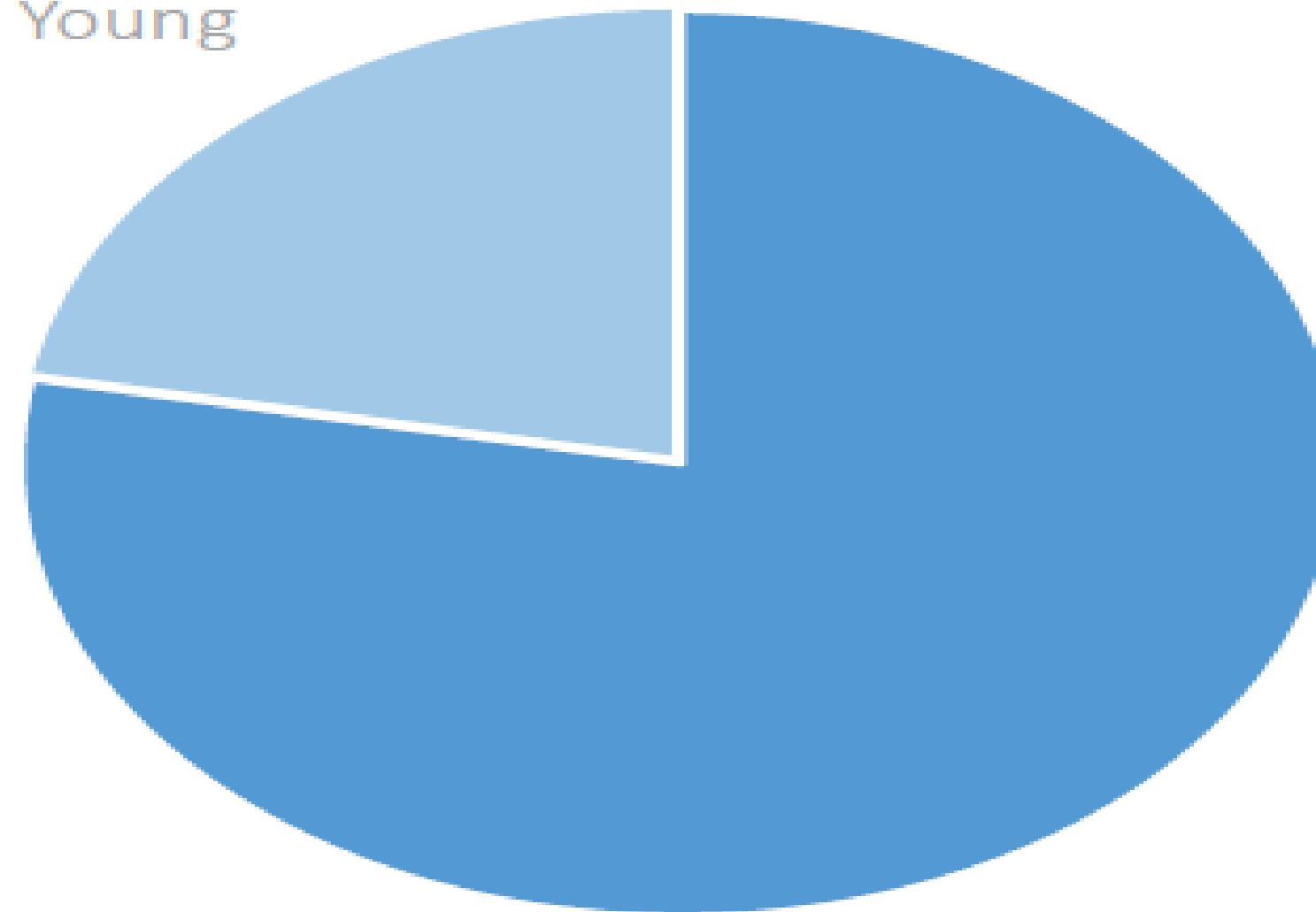


In this case, our sample client's GRC platform supports the following programs: Compliance, Internal Control, Issue Management, Risk Management and Audit.



78%

of companies are concerned with their ability to adapt to changing regulatory requirements and the flexibility of their current system to adapt to these changes. (Ernst & Young 2014)



Most GRC solutions are modular, meaning that expansion into new areas of GRC requires the purchase of additional modules. Choosing a non-modular solution, like GRC Cloud, provides the client with the necessary features to expand into any additional area of GRC without needing to purchase and implement additional software. The only costs of expansion are additional licenses for new users and cost of configuration.

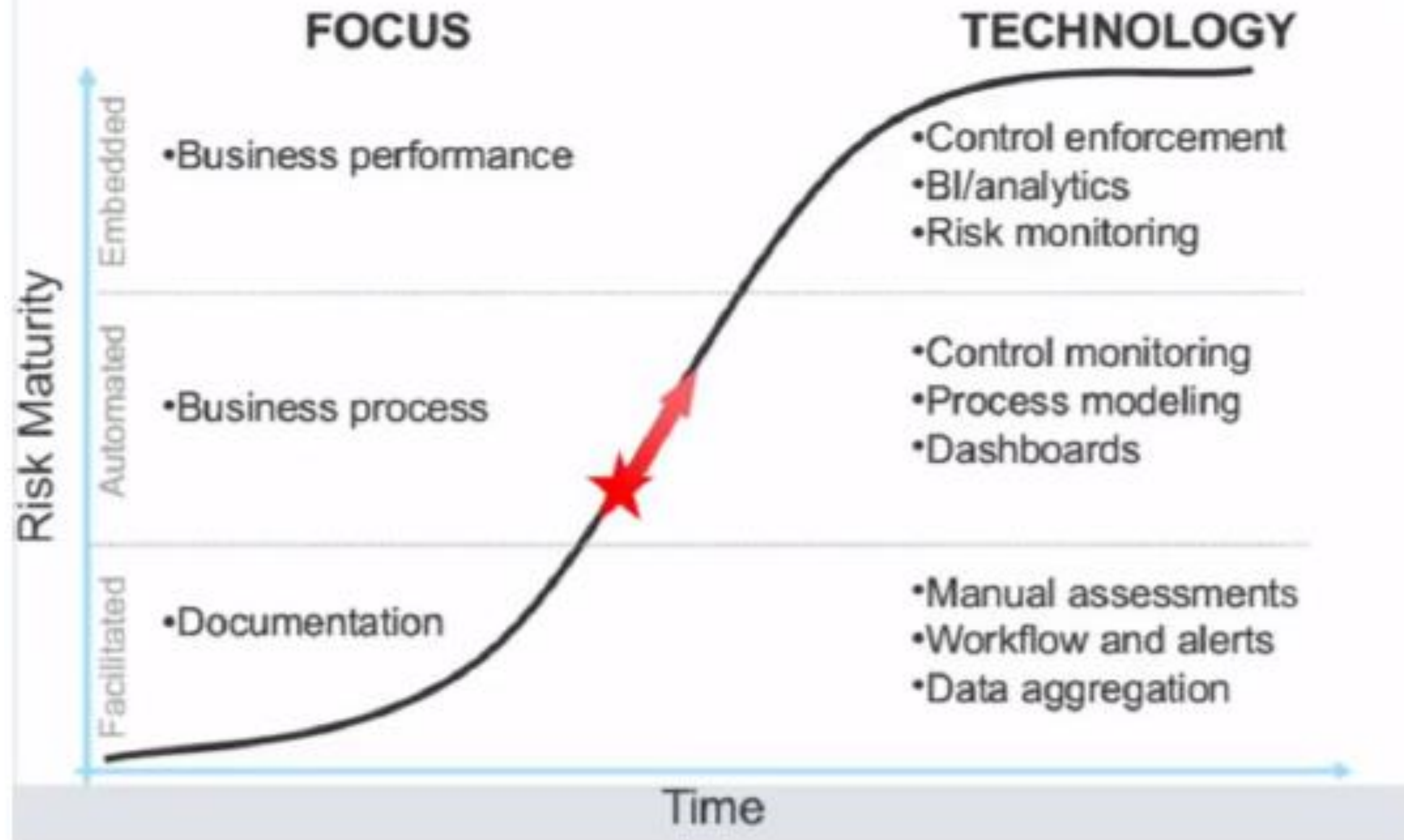
Initial implementation	ICFR/SOX
Strategic decision made to manage a new aspect of GRC	Client would like to configure the system to handle Compliance in addition to SOX
Extra software functionality purchased and implemented through a new vendor	\$100,000 to \$500,000 Size of the enterprise dictates the maximum cost of \$500,000
Cloud configuration cost and extra licenses	\$25,000 to \$100,000 Size of the enterprise, again, dictates the maximum cost of \$100,000
Savings from not purchasing additional modules to handle new GRC area	Savings (\$) = \$500,000-\$100,000 = \$400,000

***See Appendix I for a detailed breakdown of the costs

GRC benefits

CATEGORY	BENEFITS	METRICS
Efficiency	<ul style="list-style-type: none">• Reduced costs of risk assessments and aggregation• Speed of policy development, approval, distribution• Improved speed/cost of risk reporting• Improved speed/cost/coverage of audits	<ul style="list-style-type: none">• Staff-hours saved per process• Payroll savings from delay or avoidance of staff increase• Reduction in costs for internal and external audits
Risk reduction	<ul style="list-style-type: none">• Reduction in incidents, near misses, loss events• Reduction in regulatory fines, actions, law suits, etc.• Reduction in time to discover control gaps, violations• Reduction in audit/assessment findings	<ul style="list-style-type: none">• Reduced number and cost of incidents• Reduced number/size of fines• Reduced cost of capital• Reduced insurance premiums
Strategic support/ Enhanced performance	<ul style="list-style-type: none">• Use of risk info in management/exec decisions• Improved decision making when risk is considered• Risk intelligence coverage• Risk management process coverage• Improved reputation among stakeholders (partners, regulators, customers, etc.)	<ul style="list-style-type: none">• Reduction in reactionary costs• Frequency of risk data used in business decisions• Improvement in financial or operational metrics

The maturity of risk programs



GRC spans across many teams

At your organization, who is responsible for the day-to-day coordination of your GRC program?



The Use Of Analytics To Improve Business Decisions Is A Top Initiative

February 2014 "Twelve Recommendations For Your Security Program In 2014"

"Which of the following technology initiatives are you asking IT to prioritize over the next 12 months?"

(Respondents who selected "High priority" or "Critical priority")



Base: 3,616 global business decision-makers

Financial And IT Analytics Are Top Planned Use Cases For Big Data Technologies

Q&A: Forrester's Top Five Questions

"What are your firm's plans to use big data technology for the following analytics use cases?"



Base: 3,005 global data and analytics decision-makers



Strategic risk view & single source of truth

Show leadership that you're aligned on strategic risk. Executives, boards, and oversight committees need intel on what could derail objectives, where, and who is doing what to mitigate. And regulators frown on managing strategic risk in a flimsy spreadsheet. Get a centrally managed holistic view of your risk balance sheet.



Offline & remote work

No internet? No problem. Use your PC or mobile device. Even rockstar GRC professionals like you need a vacation...or perhaps you're just out in the field for the week. Not a problem: unplug your PC or your iPad®, do your work, capture supporting documentation, and sync later.



Project management to kill silos and spreadsheets

Your (not so secret) love affair with spreadsheets is holding you back. Break up with your project spreadsheets and let technology do your heavy lifting. Plan, manage, execute and report on your assurance projects in one system.



Risk assurance & frameworks

Sleep better knowing your framework is built right into your workflow. Let the system keep you on track by modelling one or many of these common frameworks into your daily workflow: COSO, ISO, SOX, OMB-A123, Green book, COBIT, ITIL, SIEM, NIST, SOC or many others.



360° oversight: triggered workflow remediation for flagged records

Analysis says there's smoke, but is there a fire? Wouldn't it be amazing if a remediation workflow was triggered when data analysis uncovered a potential issue? ACL's outlier record management workflow helps you collaborate, keep tabs on remediation status and track it all in a single system designed to fit your needs.



Investigations & forensic workflow

Manage suspicious incidents discreetly. Security incidents, possible fraud, whistle blower hotlines, special investigations, and forensics may all require escalations and workflow alerts. Manage these in a centralized, permission-based workflow.



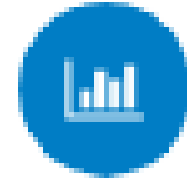
Issue management & tracking

You've identified issues that need remediation...now what? Stop tracking issues in email and instead get a macro view of all your organizational issues and filtered by entity, by project, by owner or severity — and check the remediation status at the click of a button.



Reporting & visualization

GRC is complex. Simplify the noise with tools that easily transform data into pictures. Senior managers just don't have time to read the details. Your value is taking GRC complexity and distilling it into a compelling picture, story, dashboard, KPI/KRI, standard or custom report, which can be quickly consumed and acted on.



Audit Management

Internal Audit

**SUPERCHARGE YOUR AUDIT
COVERAGE WITH COLLABORATIVE
TECHNOLOGY.**

Are you trapped in a time suck between
spreadsheets, manual process and outdated
technology?

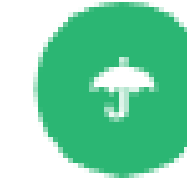


Compliance Management

Internal Audit, Compliance & Legal,
Accounting & Finance, IT

**YOUR REPUTATION SHOULDN'T BE
MANAGED IN A SPREADSHEET.**

Are you tasked with safeguarding IT, finance
or your entire organization?



Operational Risk Management

Risk Management, Accounting & Finance
and Information Technology

**HOW READY ARE YOU TO ROLL THE
DICE?**

Most major global economic meltdowns of
the past few decades were caused by
operational risk failures.

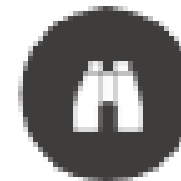


Fraud Management

Compliance & Legal, Accounting & Finance,
IT, Internal Audit

**FRAUD, WASTE AND ABUSE ARE
INVISIBLE.**

Apply technology to X-ray your
organization and illuminate fraud risk.

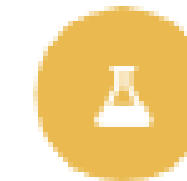


Risk and Control Monitoring

Accounting & Finance, Compliance & Legal,
Business Operations, IT, Internal Audit

**THE NEXT BEST THING TO A
CRYSTAL BALL FOR YOUR
ORGANIZATION.**

Identifying red flags only matters if you do
something about them.



Enterprise Risk Management

Risk Management, Internal Audit

**GET BETTER RISK ROI. VALUE
PROTECTION. VALUE CREATION.**

Infuse your risk management with
performance-enhancing science.



















































Product Comparison



RSA Archer GRC

MetricStream



		RSA Archer GRC	MetricStream	
Internal Audit Management				
Risk Management				
Incident Management				
Policy Management				
Asset Management				
Compliance Management				
Integrated GRC				
GRC Centralized Library				
Software as a Service				
Cloud Delivery, Free Training				
Flexible Pricing				
Predictive Analytics				
Unstructured Data handling	