NUCLEUS RESEARCH

GUIDEBOOK

UNDERSTANDING THE FINANCIAL VALUE OF GRC MANAGEMENT

October 2012

Document M121

Nucleus Research is the leading provider of value-focused technology research and advice.

NucleusResearch.com

THE BOTTOM LINE

Governance, Risk Management, and Compliance (GRC) technologies are often seen as sunk costs where the business value can only be defined as "the cost of doing business." Nucleus Research has found that there are both tactical and strategic benefits associated with GRC solutions that can provide a framework for calculating the Return on Investment.

This research was conducted in context of the usage of IBM OpenPages, a software solution used to centralize the management and identification of enterprise GRC initiatives such as operational risk, financial risk, and IT governance throughout a distributed enterprise environment. Since acquiring OpenPages in October 2010, IBM has positioned OpenPages as part of its Business Analytics software portfolio which also includes the Cognos, SPSS, and Algorithmics product lines.

To research the value of GRC, Nucleus studied a number of IBM OpenPages customers in multiple industries, including financial services, IT professional services, utilities, and leisure. This combination allowed Nucleus to study a variety of operational, strategic, and financial control implementations that were both vertical specific and general to a wide variety of large enterprises. By understanding how these firms prioritized GRC issues and deployed OpenPages throughout the organization, Nucleus has created an initial framework for calculating the potential value associated with deploying a GRC solution.

IDENTIFYING THE VALUE OF GRC MANAGEMENT

Nucleus profiled seven organizations currently using IBM OpenPages to support GRC issues ranging from Sarbanes-Oxley to FERC to operational risk management. During this process, Nucleus documented seven key value propositions associated with centralized and efficient GRC management that could be quantified by studying the costs, processes, labor, training, and resources. To understand the value of centralized and coordinated GRC management, Nucleus used interviews from these organizations and added hypothetical examples based on a typical enterprise with five key compliance functions: operational risk, financial controls, IT risk, federal compliance, and state or provincial compliance.

RISK ASSESSMENT AND AUDITING

All of the organizations interviewed had personnel and processes to quantify and identify key risk and compliance issues that were most relevant to their working environments. Some of these issues were studied as high-level issues where a summary top-line or bottom-line audit was sufficient. Other issues required line-of-business input across the company, which then had to be aggregated and standardized. Companies sought to reduce risk auditing by creating more responsibility within the organization:

- *"Previously, audits were like a crutch for compliance."*

- *"We track the percentage of self-identified issues, since we are trying to increase employee participation for risk management."*

By accurately taking human factors into account with a productivity correction factor that acknowledges that the transfer of employee time from a familiar task to a less familiar job will result in an inefficient transfer of effort, your organization can calculate the true savings associated with risk assessment optimization (Nucleus Research *c41 – Quantifying the value of increased productivity*, August 2002).

RISK ASSESSMENT BENEFIT CALCULATION EXAMPLE

Number of risk assessments performed	10
Current days per assessment	30
Number of employees per assessment	2 @ $192,000/year, fully loaded based on a $120,000 salary and 1.6x benefits and resources
Assessment overlap reduced through management	50%
Productivity correction factor	.7
Total Savings	$107,520

In addition to scheduled risk assessments and audits associated with ongoing business compliance needs, mergers and acquisitions require careful scrutiny across multiple entities in a regulated or publicly traded market.

One utilities organization interviewed described two separate M&A situations. The first merger had required the identification and documentation of 309 merger conditions, each with between one and five sub-terms. The master spreadsheet used to track each of these terms was so complex that there was an employee dedicated full-time only for the management and tracking of these conditions. The company had dedicated multiple employees to handle FERC and state regulatory issues and understand which of these areas were compliant or at risk at any given time. This process was cumbersome enough that the company missed several deadlines and had to go to the SEC to request extensions. In total, it took 18 months to document and fulfill all regulatory conditions.

This same organization went live with OpenPages in October 2007. Initially, the organization required a seven month time investment to transfer all of the spreadsheets throughout the organization into IBM OpenPages, but the benefits have quickly demonstrated themselves as the company faced another M&A opportunity. Through IBM OpenPages, this company was able to take the non-standard inputs and documentation associated with its last acquisition and create an organized approach for identifying and tracking risks in the merger process. In addition, with IBM OpenPages, there is no longer a single bottleneck associated with updating a single spreadsheet and there are no problems with tracking historical logs.

Instead, the organization has provided step-by-step instructions for each assessment object within IBM OpenPages so that users can simply log in and enter relevant data. The company has also created an interface between IBM OpenPages and their HR database to track users' information against their current staff records to make sure that the contacts associated with each compliance issue are always up-to-date.

This approach will reduce legal costs, management labor to support multiple documents, and human error associated with having multiple versions of spreadsheets and reports at any given time. The corporate compliance manager for this utilities firm tracking this new acquisition, which will also require approximately 300 different conditions, notes, "Since using IBM OpenPages, we have been fully compliant. For this merger, we'll do in 30 days everything that took 540 days last time. We won't miss any dates or file any extensions."

POLICY MANAGEMENT

To enforce GRC policies, companies must first have a set process for creating and updating policies on an ongoing basis. It does not matter whether employees are actually following corporate policy or not if the policy itself is outdated and no longer in compliance with relevant legislation. By holding all relevant policies in a centralized system that can remind individuals when policies need to be reviewed and manage the entire internal workflow associated with policy approval and training, companies can make the policy creation process more efficient and potentially reduce the headcount associated with policy management.

In addition, accurate policy management can reduce the chances of non-compliance associated with potentially costly GRC issues. As an example, the cost of non-compliance for PCI/DSS (Payment Card Industry Data Security Standard) can be as high as $500,000 and includes information access standards for every employee within an organization that accepts credit card payments, regardless of their access to payment information. When a single breach of compliance based on outdated or irrelevant policies could result in a six or seven-figure compliance fine, companies should make sure that they automate key reminders or entrust this responsibility to an employee with encyclopedic knowledge of GRC who never makes mistakes.

POLICY ASSESSMENT BENEFIT CALCULATION EXAMPLE

Current FTEs assigned to policy management	4 @ $192,000/year, fully loaded
Policy work reduction through automation	50%
Productivity correction factor	.7
Total Savings	$268,800

Nucleus found that the ability to quickly translate legislation and compliance issues into active policy was a driving factor for multiple companies to implement IBM OpenPages as a consolidated GRC solution.

- *"Our biggest opportunity was to react to new laws or regulations more quickly. Now, I'm documenting risks in IBM OpenPages. With this corporate documentation, I can say what law and regulation enforcement should be developed."*
- *"A rationalized management foundation allowed us to document processes and control information such as procure-to-pay and order-to-cash value chains. People can understand if we have similar processes throughout our departments and everyone has similar and consistent risk assessment capabilities.*

CONTROL OPTIMIZATION

Because GRC has traditionally been a decentralized business function handled by a number of groups with differing views and perspectives, risk control processes tend to be fragmented and inconsistent even if they lead to similar results. By defining and supporting consistent controls throughout an organization, companies can reduce overlapping or inefficient control testing procedures on an annual basis.

Consider the number of departments that are tracking compliance within an organization, such as IT, Finance, Compliance, Legal, Environmental, and other groups. Each of these departments is potentially responsible for managing hundreds of controls within their spheres of responsibility and each control will typically require several hours a year to confirm and test. By understanding which of these areas can be consolidated and optimized, an organization could reduce its control testing time by hundreds of hours per year.

CONTROL OPTIMIZATION BENEFIT CALCULATION EXAMPLE

Number of controls tested in organization	1,200
Time per control (hours)	6
Percentage overlap in control testing	25%
FTE cost per hour	$96 (Based on $192,000 fully loaded /2000 hours)
Productivity correction factor	.7
Total Savings	$120,960

Through control management and testing capabilities, companies were able to consolidate their control environment, gain visibility to existing controls, and prevent the need for creating unnecessary or extraneous controls through the use of IBM OpenPages:

- *"Initially, our need was to document risk controls for all corporate departments. We wanted to remove our dependency on Excel."*
- *"This company asks managers to own their own control environment. This isn't punitive; this is our financial ecosystem. IBM OpenPages serves as a system of record to refresh and rationalize our control environment."*
- *"We can put systematic controls in place and see how they apply to the balance sheet. IBM OpenPages was a conduit for supporting a culture for openness."*

- *"With IBM OpenPages, we moved from having 1,400 SOX controls to 750 by identifying key controls."*
- *"Our organization can identify fraud risk schemes more quickly through our assessment capabilities and identify the appropriate controls that are needed to manage these fraud cases."*
- *"IBM OpenPages was brought in to document and test risk controls for all corporate departments so we could be able to report on issues and deficiencies. We wanted to remove our dependency on Excel to manage our controls so we could assess once and comply many times."*
- *"With a unified compliance framework, we can map our current corporate controls to localized controls to see if corporate-mandated controls are effective or ineffective.*

ISSUE REMEDIATION

On a day to day basis, there will inevitably be challenges and issues that are reported and need to be resolved as companies have compliance lapses. As these issues occur, companies that have centralized ticketing and resolution capabilities will be able to reduce costs in several ways. A central clearinghouse for GRC issues will allow firms to move any problems to the most experienced governance and risk management personnel within the organization. In addition, companies will be able to identify trending or duplicate issues more quickly, which will allow experts to focus on key business threats and concerns. By reducing the effort associated with tracking issues and accelerating the time to resolve compliance problems, companies can achieve regular productivity gains.

As an example, consider an organization with operational risk, financial risk, IT, federal compliance, and state or provincial compliance functions. Each of these five functions is headed by an individual who is hired at a fully loaded cost of $192,000 and spends two full days per week on managing and tracking issues.

ISSUE REMEDIATION BENEFIT CALCULATION EXAMPLE

Number of functions	5
FTE fully loaded annual cost	$40,000, based on an estimate of 2 days per work week of a $192,000 fully loaded employee
Percentage duplication in issue remediation	25%
Productivity correction factor	.7
Subtotal: Benefit from reduced issue duplication	*$67,200*
Resolution time reduced through GRC solution	2 hours per week
Productivity correction factor	.7
Subtotal: Benefit from improved resolution time	*$33,600*

Total issue remediation benefit	$100,800

For GRC needs that scale to a greater number of functions or a greater number of employees, this benefit would scale proportionately.

Nucleus interviews identified the management and ability to search through past GRC issues as a core role for IBM OpenPages risk management and compliance programs:

- *"Any event or activity with exposure that needs to be documented goes into our global system. We use IBM OpenPages to hold our data and to understand compliance-based activities. Anything that is policy-based goes into our system to identify operational risk management events."*
- *"One of our greatest needs was to make sure that customer complaints were being resolved. We used this data to identify systemic problems."*
- *"The search capability is a core compliance component for us. By searching for specific words or issues, we can make sure that we haven't overlooked any risk and compliance issues."*
- *"The increased visibility associated with our risk environment makes our management practices more practical. We can see the number of past due risk issues and the percentage of risk issues that have been re-opened."*

OPERATIONAL AND EXECUTIVE REPORTING

To maintain full compliance, businesses must track their existing controls and create reports that can be provided to senior management, the company Board, and appropriate compliance bodies. Companies often underestimate the time associated with the manual construction of these reports as an unavoidable business cost. However, both the data collection and the appropriate presentation of data can take up hours of time, especially when the audience is the senior executive team, a state regulatory board, or thousands of public shareholders. The time needed to collect this data could potentially mean that the report itself ends up being obsolete by the time that this report is created (Nucleus Research *m36 – Measuring the half-life of data*, May 2012).

Going back to our model of a five function risk program, assume that each function must provide 52 weekly reports, 12 monthly reports, four quarterly reports, and an annual report each year for a total of 69 reports. Based on this assumption, this company could potentially see the following savings.

EXECUTIVE REPORTING BENEFIT CALCULATION EXAMPLE

Number of reports per year	69 (52 weekly, 12 monthly, 4 quarterly, 1 annual)
Current number of hours to create and produce a complete report	20 hours
Number of functions requiring reports	5
Fully loaded hourly cost per employee	$96

Percentage time saved	50%
Productivity correction factor	.7
Executive reporting benefit	$231,840

When Nucleus spoke to IBM OpenPages customers about their operational and reporting needs, they identified the following issues and solutions associated with their GRC efforts:

- *"Initially, we had hundreds of individualized spreadsheets and databases that we had to integrate into OpenPages. We told our employees that we needed to get their data and processes into OpenPages. By doing this, we got improved robust reporting and security controls associated with our data."*
- *"We don't need to go to as many places to get risk information. Individuals always follow standard practices and risk issues are centralized in one location."*
- *"Our primary reason for implementing OpenPages is to consolidate operational risk data into a single source so that we can create a profile view of existing risks. We can also create reports directly from the system to summarize our risk profile."*
- *"Risk assessment reports previously took multiple days to create as a manual report. We had to submit our risk requests to a single employee who might not be seeing every request. With OpenPages, this has turned into a one-click report."*
- *"To support the eight executive-level reports that get produced, we used to take about half a day to create each report. With OpenPages, each report can now be created in about half an hour."*

INFRASTRUCTURE SAVINGS

Nucleus found that IBM OpenPages often ended up replacing multiple instances of Excel and other databases. These customers gained benefits by replacing the software and hardware with a dedicated product that tracked risk factors and compliance issues and by eliminating the support and maintenance costs associated with these products and software licenses. Customers found that the price of IBM OpenPages was partially or fully offset by the savings associated with database and application consolidation. Companies should consider the software, hardware, support, and maintenance costs associated with their current GRC tracking infrastructure as they consider the savings associated with a dedicated GRC solution.

INFRASTRUCTURE SAVINGS BENEFIT CALCULATION EXAMPLE

Initial hardware cost	$1,000,000 (Based on low-end servers for 50 application instances)
Initial software license cost	$750,000 (Based on 50 individual application instances)
Cost of maintenance and software assurance	$217,500/year based on an 29% rate
IT employee cost	$192,000 per year, based on 1 FTE fully loaded

IT productivity correction factor	.9
First year savings	$2,140,300
Subsequent year savings	$390,300

Multiple organizations were able to identify specific technology support benefits associated with moving to a centralized GRC platform:

- *"We were able to shut down between 60 and 100 separate application instances that were previously tracking risk functions, risk management, and information. These applications ranged from Microsoft Access to enterprise applications. We also eliminated over a thousand spreadsheets and incorporated all of that information from desktops to a shared risk environment."*
- *"Previously, we used a number of Access databases each developed in separate departments, such as mortgage or auto insurance, but the data was not consolidated. Now, our risk information is consolidated across the enterprise."*
- *"Our OpenPages deployment doesn't cost more than the previous model because of the cost of the databases and hardware that we previously had."*

SARBANES-OXLEY COMPLIANCE

Most of the IBM OpenPages customers interviewed were initially using the platform to manage Sarbanes-Oxley compliance and acknowledged the importance of a centralized approach for maintaining compliance. In addition to the management of compliance issues, the visibility associated with having an automated and centralized GRC environment can play a key role in avoiding unexpected announcements.

- *"We would not have SOX compliance today without OpenPages, which provided centrally managed financial risk and benchmarked controls. Our flowcharts and controls are now automated, whereas we previously had to create Visio flowcharts manually."*
- *"One of our successes is that we don't have unexpected writeoffs based on prior guidance. This helps us to keep shareholder confidence."*

VALUE FRAMEWORK AND RECOMMENDATIONS

Nucleus has found that there is a combination of direct and indirect benefits associated with the holistic value proposition of a GRC management solution. As an organization begins to develop a business case to either implement a centralized GRC solution or to augment an existing solution, Nucleus recommends taking the following costs and benefits into account based on the experiences of existing IBM OpenPages customers.

CALCULATING DIRECT BENEFITS

The direct benefits of a GRC solution can be measured in terms of tangible and quantifiable savings or improvements. Although GRC can often be difficult to fully quantify, organizations have often made existing investments in personnel, real estate, software, hardware, consulting, and professional services to support this cost center. The

following direct benefits should be considered as part of the potential direct value proposition associated with centralizing and automating risk management capabilities:

- Discontinuing existing support or services contracts
- Eliminating headcount that is no longer needed to manage aspects of risk management or compliance
- Removing extraneous software licenses and maintenance contracts
- Reducing rented data center footprint
- Selling real estate associated with a risk management office

CALCULATING INDIRECT BENEFITS

The majority of benefits identified by end users can be categorized as indirect benefits associated with saving time, increasing productivity, and eliminating potential compliance faults. It is more challenging to measure the value of these benefits, but Nucleus recommends taking a close look at the following risk management, service, and analytics areas typically associated with an enterprise-wide GRC program. In the case of the hypothetical organization referenced in this report, the total potential benefits could be summarized as follows.

GRC BENEFIT CALCULATION EXAMPLE

Risk Assessment Optimization	$107,520
Policy Assessment Optimization	$268,800
Control Optimization	$120,960
Issue Remediation Optimization	$100,800
Executive Reporting Optimization	$231,840
Recurring Infrastructure Savings	$390,300
Total Recurring Direct and Indirect Operational Benefits	$1,220,220
Potential ROI	208% (based on 45% tax rate, 7% cost of capital, 5-year depreciation, and standard costs)

MORE ISN'T ALWAYS BETTER

Many of these benefits were identified by IBM OpenPages customers as they deployed these solutions, which resulted in documented productivity benefits. However, there were two key issues that customers identified as areas that they wished that they could do over.

One was in considering what kind of information would be requested by senior management and governance bodies. IBM OpenPages were most successful when they were designed around the information that senior management was truly focused on. By doing so, GRC and risk management departments were able to gain executive visibility and, potentially, an executive champion.

In addition, organizations also found that, by simplifying their configuration, they were better able to align their GRC management to their core operational compliance demands.

By scoping the initial deployment properly, organizations are able to maximize productivity in key areas and then later achieve greater ROI on a solution by expanding the solution to additional users with more functionality and deeper complexity. Visibility to governance and compliance is not just a software capability; it is an opportunity to create a more open business culture.

CONCLUSION

The organizations interviewed in this document each had different experiences in deploying the same software solution. Some of these companies launched their deployment simply to attain Sarbanes-Oxley compliance while others sought to create a fully centralized operational risk program with automation and cultural change. Nucleus found that the more ambitious that a company was in seeking company-wide change, greater internal visibility to risk management, and the views of senior management, the more likely they were to identify duplication of efforts, extraneous hardware and software, and opportunities for automating tedious data aggregation efforts. GRC can be seen as a pure cost center with limited scope and limited rewards, but organizations that seek to take full advantage of the automation, visibility, and participation associated with a centralized GRC solution will provide themselves with many opportunities to justify their investment with a Return on Investment based on automation, increased productivity, and infrastructure reduction.